TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

tcipg.org

Research Activity Fact Sheets

October 2012

University of Illinois • Dartmouth College • Cornell University • UC Davis • Washington State University

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

Table of Contents – Activities Listed by Research Cluster Page No.

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Overview of the TCIPG Center

tcipg.org

What TCIPG Does, Why It's Needed

Today's quality of life depends on the continuous functioning of the nation's electric power infrastructure, which in turn depends on the health of an underlying computing and communication network infrastructure that is at serious risk from both malicious cyber attacks and accidental failures. These risks may come from cyber hackers who gain access to control networks or create denial of service attacks on the networks themselves, or from accidental causes, such as natural disasters or operator errors. Researchers from the University of Illinois at Urbana-Champaign, Dartmouth College, Cornell University, the University of California at Davis, and Washington State University are together addressing the challenge of how to protect the nation's power grid by significantly improving the way the power grid infrastructure is built, making it more secure, resilient, and safe. TCIPG is funded by the U.S. Department of Energy and the U.S. Department of Homeland Security.

TCIPG Research Clusters:

- Trustworthy Technologies for Wide-Area Monitoring and Control
- Trustworthy Technologies for Local Area Management, Monitoring, and Control
- Responding To and Managing Cyber Events
- Trust Assessment

TCIPG Cross-Cutting Efforts:

- Education and Engagement
- Testbed Initiatives
- Industry Interaction and Technology Transition

How It Works

In the cluster on Trustworthy Technologies for Wide-Area Monitoring and Control, TCIPG researchers are working on security, key management, quality of service, data management, data compression, application robustness, and network robustness applied to PMU networks, PMU data, state estimation, transmission topology, and power line communications.

The cluster on Trustworthy Technologies for Local Area Management, Monitoring, and Control focuses on improving overall power system performance. As the power grid transitions to a system with larger amounts of less-dispatchable renewable generation, control that previously resided on the generation side will need to be transitioned to the load. The impacts of load control for both real and reactive power are being considered.

The cluster is pursuing research in three main areas. First is the determination of how the real and reactive power load should be modified to accomplish control, including use of nonintrusive methods for determining the load composition (and hence its potential controllability) while also providing the potential for privacy protection. Second is the determination of the best means for enabling the monitoring and bidirectional communication needed to accomplish that control, with a specific focus on electric vehicles. Finally, the cluster is also working on AMI intrusion detection to maintain a secure control system.

The cluster on Responding To and Managing Cyber Events focuses on cyber attacks, particularly tools and technologies for responding to and managing cyber attacks. Most recently, TCIPG research in this area has focused on design of semi-automated intrusion detection and response techniques. More specifically, the researchers are developing a Recovery and Response Engine that makes use of game theory techniques to provide optimal responses to cyber attacks.

The cluster on Trust Assessment has been working on extending TCIPG's current testbed for experimental evaluation of attacks and monitoring strategies; designing and setting up an example substation network using actual substation equipment; and extending and releasing a suite of software solutions that includes tools designed for formal program analysis (SymPLAID), dynamic runtime process patching (Katana), interactive packet manipulation (Scapy), firewall rule validation (NetAPT), intrusion detection on embedded systems (Autoscopy Jr.), and highly scalable network simulation (S3FNet), among others.

TCIPG has also developed interactive and open-ended applets for middle-school students, along with activity materials and teacher guides to facilitate the integration of research, education, and knowledge transfer by linking researchers, educators, and students.

Where It Stands

Impact is being made at all levels in the project. Together, TCIPG innovations provide clear directions toward a next-generation IT infrastructure for the power grid that is resilient, timely, and secure, supporting the continuous functioning of the nation's electric power infrastructure.

Industry Interaction Board

The involvement of industry and other partners in the TCIPG project is vital to its success, and is facilitated by an Industry Interaction Board (IIB). For more information, see the TCIPG website at tcipg.org, or contact the TCIPG leaders listed below.

Leadership

- **Director:** William H. Sanders (whs@illinois.edu)
- **Industry Partnerships & Technology Transfer:** Peter W. Sauer (psauer@illinois.edu)
- **Managing Director:** Al Valdes (avaldes@illinois.edu)
- **Site Coordinators:** Carl Hauser (hauser@eecs.wsu.edu), Anna Scaglione (ascaglione@ucdavis.edu), Sean W. Smith (sws@cs.dartmouth.edu), and Robert J. Thomas (rjt1@cornell.edu)

Research Cluster

Trustworthy Technologies for Wide-Area Monitoring and Control

Trustworthy Technologies for Wide-Area Monitoring and Control Page No.

Cluster Lead: Carl Hauser ..... hauser@eecs.wsu.edu

Cryptographic Scalability for the Smart Grid

Overview and Problem Statement

Efficient and rapid device authentication is essential for effective Smart Grid control. Conventional wisdom holds that standard PKI is the preferred solution, but standard PKI has never been scaled successfully to a network as large as the envisioned multibillion-device grid. Previous research has shown that PKI over BGP is too slow for real-time control in as few as 30,000 nodes; the transmission-side grid is expected to exceed one million nodes. On the consumer side, revocation alone does not work in the current Web SSL with only one million correctly certified nodes, but the consumer-side grid will exceed one billion devices. PKI will be pushed beyond known limits when scaled to the Smart Grid; our research evaluates these cryptographic scalability challenges and identifies solutions for further research.

Research Objectives

- Develop a simulation of the envisioned Smart Grid communications network.
- Deploy our simulation to evaluate the scalability of the X.509 standard in the envisioned Smart Grid in known problem areas such as excessive CRL length.
- Research new states in the network topology, such as a trust root outage, to simulate the effect on the grid.
- Compile a strong dataset of authentication states and outcomes.
- Evaluate the effectiveness of X.509 scalability in the Smart Grid and identify solutions for further research.

Technical Description and Solution Approach

- Our research focuses on the implications of standard PKI for latency and bandwidth in the Smart Grid.
- We utilize the SSFNet network simulation suite courtesy of Professor Jason Liu, Florida International University, to develop our network simulation. SSFNet contains a suite of internet protocols (UDP, TCP, etc.) on which we can build our authentication and application protocol layers.
- Our authentication protocol simulates all aspects of the X.509 authentication standard.
- We are currently developing a network topology with the help of industry experts and other researchers with experience modeling the envisioned Smart Grid. Using this network topology, we will test “normal” grid authentication interactions and intentionally perturb operation with unexpected events.
- Our work builds on PKI simulation work by Nicol, Smith, and Zhao that utilized Nicol’s SSF simulation tools.

Results and Benefits

- Our research will produce a concrete model to evaluate the effectiveness of standard PKI and authentication technology in the Smart Grid. This model will allow further research to develop into scalable authentication solutions for the envisioned Smart Grid and allow prediction of bottlenecks while designs are still flexible.

Researchers

- Professor Sean Smith, sws@cs.dartmouth.edu
- David Rice, david.a.rice.14@dartmouth.edu
- Tucker Ward, tucker.l.ward.12@dartmouth.edu

Industry Collaborators

- We want your topologies, expertise, and visions for the Smart Grid!

Functional Security Enhancements for Existing SCADA Systems

Overview and Problem Statement

The information architecture supporting current commercial Energy Management Systems (EMS) used by utilities to manage their plants includes a complex layered infrastructure that, as expected, closely resembles the hierarchy of SCADA systems. These EMS systems accrue much more than electrical measurements. The networking and computation processes that occur in these infrastructures are mysterious to the utility operators. They include several information silos that are utilized by different personnel with backgrounds in power engineering or mechanical engineering. The desire for convenience has prompted increasing enabling of access to secure network islands via the Internet. The question is, are these systems susceptible to attacks, and how can we detect and prevent attacks?

Research Objectives

The goal is to identify vulnerabilities that exist in the SCADA networks and in the cyber infrastructure connecting machines to Programmable Logic Controllers (PLCs), PLCs to database historians, and historians to SCADA Human Machine Interface (HMI) software.

The technical objective is to complement current EMS commercial software with data analysis tools for discriminating between normal data patterns and abnormal ones, but also for giving an online assessment of *how bad the situation is that has happened* compared to *what should have happened*.

Smart Grid Application Area: Energy Management System security.

Research Plan

Over the summer, we completed the study of the data flows in the SCADA system and the interactions of different components in the CPS for the UC Davis utility. We have selected the management of the central chilling plant assets as the prototypical service to secure, since that plant is the source of the largest electrical load on campus, and its failures can have a number of repercussions for other campus assets, ranging from server facilities to laboratory facilities.

The project plan includes:

- The development of machine-learning models to be applied to the data collected by the system historians (for both the physical system and the communication network).
- The development of outband nonintrusive monitoring that uses the statistical model and a Model Predictive Control (MPC) framework to rank the policies available to the operator in the foreseeable time horizon and that compares predictions with actual actions and events.

Technology Readiness Level: We are in the initial exploratory phase of this project.

Researchers

- Anna Scaglione, ascaglione@ucdavis.edu
- Mahnoosh Alizadeh, malizadeh@ucdavis.edu
- Georgia Koutsandria, gkoutsandria@ucdavis.edu

Industry Collaborators

We are collaborating with LBNL, which is in contact with Wonderware, makers of one of the popular commercial software tools for EMS HMI. They are exploring functional security enhancements for their software.

GridStat Middleware Communication Framework: Application Requirements

Overview and Problem Statement

GridStat is a middleware framework architecture tailored for power system data delivery. Power system applications set specialized requirements in terms of delay, rate, availability, etc., and GridStat needs to be tested and validated to meet the specific application requirements. Communication requirements also need to be investigated for conventional SCADA and PMU-based wide-area network systems. Cyber-physical test cases need to be developed for such validation and testing. Developed test cases can be utilized for cyber-physical vulnerability analysis.

Research Objectives

- Understand the real-time communication requirements for power system applications for the emerging smart grid.
- Develop a technical approach to assess these requirements.
- Develop a testbed that integrates the power grid, sensors, communication, and applications to create real-life scenarios to validate the GridStat middleware communication and other communication architecture.
- Vulnerability analysis with incomplete data availability.

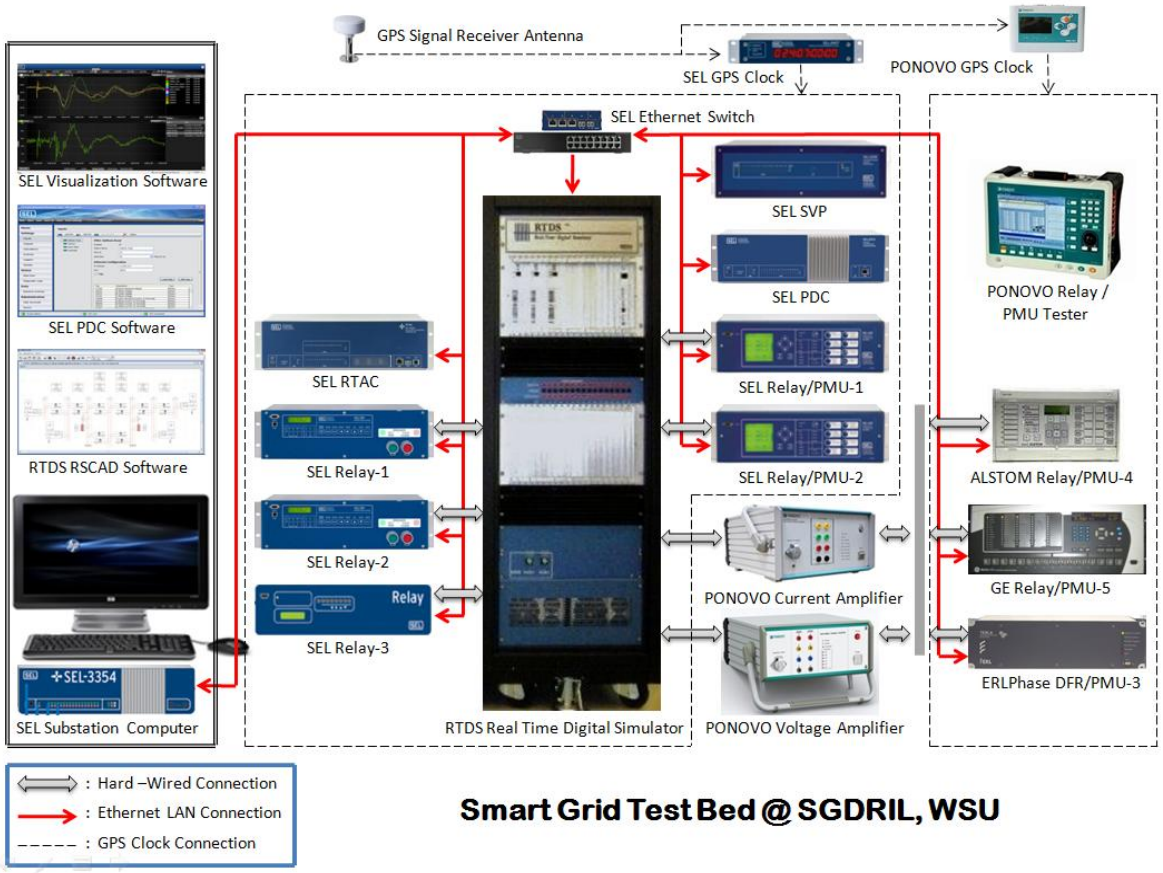


Fig. 1: RTDS-based integrated modeling and simulation

Technical Description and Solution Approach

- Approach is to model and do integrated simulation in real-time using Power Tech software and GridStat. (Part of the effort is separately funded by DOE.)
- A real-time testbed is also being developed that uses a real-time digital simulator to interface with a communication emulator, as shown in Fig. 1.
- Graph theory-based vulnerability indices for the power grid are being used to analyze multiple contingencies with limited information and validate them with DC- and AC-power flow indices.

Results and Benefits

- Integrated simulation for 179 bus system has been completed in the GridSim project (separately funded by DOE), which uses GridStat to integrate the TSAT power system simulator with the Hierarchical State Estimator application and a separately developed oscillation monitor.
- RTDS-based testbed development is in progress (partially funded by TCIPG).
- Vulnerability analysis with incomplete information has been analyzed using graph centrality-based algorithms. Validation has been done against DC sensitivity-based algorithms and with full AC power-flow-based algorithms.
- **Partnerships and External Interactions:** SEL, NASPI, GE, RTDS, PowerTech, Schneider.
- **Technology Readiness Level:** Research in progress.

Researchers

- Carl H. Hauser, hauser@eecs.wsu.edu
- David E. Bakken, bakken@eecs.wsu.edu
- Anjan Bose, bose@eecs.wsu.edu
- Anurag Srivastava, asrivast@eecs.wsu.edu

Industry Collaboration

- SEL, NASPI

GridStat Middleware Communication Framework: Management Security and Trust

Overview and Problem Statement

It is generally recognized that a high-bandwidth and highly available networked communication system should overlay the transmission system topology to enable new types of control and protection applications that will make the grid more efficient and more reliable. Those applications will make use of data originating at many locations in the grid, which may be under the control of operators with various levels of competency and motivation, or even under the control of attackers. The research in this activity addresses three aspects of cyber security in this emerging environment. The first is that of *message origin authentication* when the data delivery model is multicast. This is a challenging technical problem for which various solutions exist, but all exhibit trade-offs between multiple quality of service dimensions, so there is no universally best solution. The second aspect is concerned with storage and dissemination of secret keys, whether they are private keys for PKI systems or keys for symmetric encryption systems, to smart grid participants. Such a storage service is a potential weak point in the overall security of smart grid systems, both because compromise of those nodes could disclose highly sensitive information (the keys that protect data in transit) and because unavailability of the service could render certain communication impossible. The third aspect addresses how to make control decisions using information from sources whose trustworthiness is unknown a priori. We observe that in any system the size of the power grid, involving thousands of participating entities, security will inherently be imperfect and uncertain. The approach being pursued here attempts to use trustworthiness assessment in combination with decision theory to make good control decisions, even in the face of uncertainty about the trustworthiness of some inputs.

Research Objectives

- Assess the ability of a variety of multicast data origin authentication protocols to meet quality-of-service requirements for smart grid applications.
- Make several multicast authentication protocols available in the GridStat framework, allowing application designers to choose a protocol that best meets the application's needs.
- Improve the performance of the TV-OTS multicast authentication protocol.
- Build a key storage service that protects against key disclosure when nodes making up the service are compromised and that offers high service availability using distributed systems techniques.
- Develop a mathematical model or models for trust assessment and decision-making that are appropriate for use in power grid control settings.
- Design approaches to trust data collection for power grid devices and participants so as to be able to usefully instantiate the models and maintain the instantiations over time.
- Incorporate instantiated trust models as part of the security design of wide-area control systems.
- **Smart Grid Application Area:** Wide area monitoring and control.

Technical Description and Solution Approach

- Having previously investigated the security and performance characteristics of several multicast authentication protocols from the literature using analysis and experimentation, we are now working on performance improvements to the key generation algorithm used in the TV-OTS scheme. In our previous research, TV-OTS exhibited some of the best tradeoffs between real-time performance and security but was accompanied by very high off-line key generation cost.

- The key storage service implementation is based on threshold cryptography, which both ensures that the system can tolerate a pre-specified number of *disclosure failures* and enables the service to remain available during a pre-specified number of *Byzantine failures.* The service is designed to ensure that none of the nodes it comprises ever learn the stored secrets.
- Trust models investigated thus far include a Bayesian probabilistic estimation model for incorporating trust information and its uncertainty and a new ranking-based approach that provides useful, if less complete, trust input to decision-making while requiring less input information. Our ongoing research efforts focus on development of a semantically rich and expressive formal trust management model capable of describing the trust relationships between power grid entities.

Results and Benefits

- A prototype implementation of the improved TV-OTS key generation algorithms has been completed, and a write-up of proofs-of-correctness is in progress.
- A prototype implementation of the key store service demonstrating the essential threshold cryptographic elements has been completed. Additional work is needed on an access control mechanism.
- **Partnerships and External Interactions:** NASPI
- **Technology Readiness Level:** The prototypes of the TV-OTS key generation and key storage service could be moved fairly rapidly to product status; trust is ongoing fundamental research.

Researchers

- Carl Hauser, hauser@eecs.wsu.edu
- David E. Bakken, bakken@eecs.wsu.edu
- Thoshitha Gamage, tgamage@eecs.wsu.edu

Industry Collaboration

- SEL

GridStat Middleware Communication Framework: Systematic Adaptation

Overview and Problem Statement

GridStat is a middleware communication framework with ultra-low latencies and high availability aimed at providing wide-area data delivery capabilities for the power grid. GridStat's *data plane* is a tightly managed mesh overlay network that provides stringent, rate-based delivery guarantees. However, the data plane components are susceptible to arbitrary (byzantine) failures and cyber-attacks that, if unattended, have the potential to make these guarantees unachievable. Furthermore, even non-malicious changes within the operating environment—for example, a sudden burst of large subscription requests triggered by a power contingency or benign component failures—may also force reconfiguration in order to meet the guarantees, particularly for the most important applications, given the present power and cyber conditions.

The objective of this research activity is to develop *adaptation services* and supporting *instrumentation services* for GridStat in order to systematically adapt to changing conditions and available resources. These adaptations must be performed such that the strongest possible delivery guarantees (latency, rate, #paths) are provided to the most critical applications, yet other applications are given guarantees commensurate with their present criticality, rather than being starved. The adaptations also must strike a principled balance between *over-adapting*, which could be exploited by adversaries, and *under-adapting*, which, for example, would allow highly critical sensor inputs to a closed-loop control or regional protection scheme to have less resiliency (#paths) than is acceptable.

Research Objectives

- Design and develop a minimally intrusive yet pervasive instrumentation service to monitor the data plane.
- Design and develop a failure detection service appropriate for mission-critical, rate-based sensor traffic.
- Identify the most important perturbations that can affect GridStat's delivery guarantees.
- Develop an adaptation framework for GridStat that reconfigures all affected sensor delivery flows in a systematic fashion, providing delivery guarantee strength commensurate with the criticality of the applications subscribing to those sensor flows.
- **Smart Grid Application Area**: Wide-area monitoring and control.

Technical Description and Solution Approach

- Model and assess the performance characteristics of GridStat under various constraints that affect normal functionality. Activities will broadly fall under simulation-based assessments and use-case-based assessments.
- Determine the required level of instrumentation that maximizes adaptation-related evidence gathering with minimum effects on data delivery performance.
- Survey and research existing Security Information Event Management (SIEM) and Complex Event Processing (CEP) techniques to discover analogous compound adaptation triggers based on multiple kinds of instrumentation inputs.
- Implement an adaptation service for GridStat that is highly tailorable both in the steady state and under changing conditions.
- Explore the use of utility functions in order to optimize the benefit of the data delivery service over an entire grid, given the present power and IT conditions.
- Explore the use of pre-computed information on failures (links, forwarding engines, etc.) and their effects. Such pre-computations exploit the (quantitative and qualitative) knowledge GridStat must maintain at every location in the delivery network to provide mission-critical delivery guarantees and respond to failures rapidly.

Results and Benefits

- The ability of GridStat to incorporate a wide range of instrumentation feeds and adaptation strategies that utilize them.
- The ability of GridStat to rapidly and accurately detect a wide range of anomalies and adapt in a way that makes the power grid and other critical infrastructures as resilient as possible.
- **Partnerships and External Interactions:** North American Synchrophasor Initiative (NASPI).

Researchers

- Thoshitha T. Gamage, tgamage@eecs.wsu.edu
- David E. Bakken, bakken@eecs.wsu.edu

PMU Enhanced Power System Operations

Overview and Problem Statement

This project explores the direct application of Phasor Measurement Unit (PMU) data to improve situational awareness. PMUs are beginning to be widely deployed in electric power systems, and this trend is expected to continue. However, even with this increase in the number of installations, PMUs are still deployed at only a small percentage of system buses. This presents a challenge: how to get useful information from a small number of data points. The key driver for PMU technology is the application of the precise time sources provided by GPS (Global Positioning System) satellites to accurately measure the relative voltage and current phase angles at buses across an interconnect. This characteristic of being able to measure the phase angles directly across an interconnected power grid is a key advantage that PMUs have over SCADA (with the other advantage being the much faster PMU sampling rate). The motivation for this application arises from the fact that the time-synchronized PMU data allow the creation of dynamic snapshots of the system, and those can be used to update system models and provide online decision support to the system operator. In other words, the transmission line and simple machine parameters can be estimated from the PMU data with high time resolution, and system event identification can then be presented from the estimated parameters. This project presents a new method to demonstrate how PMU measurements can be utilized to get unique insights into the global operation of the grid.

Research Objectives

- Develop a framework to allow PMU measurements to create the equivalent system model.
- Develop an algorithm and systematic way to derive system parameters from PMU data.
- Develop an algorithm to validate simulation model.
- Develop a way to reduce system size for dynamic simulation with measured PMU values.
- Develop an online event detection method with PMU data.

Technical Description and Solution Approach

- In the first step of this project, we are creating an equivalent system model and then deriving the system parameters. The Thevenin-equivalent circuit with the classical machine model is being used to make a complicated power system simple and to estimate the system parameters.
- Several possible approaches, such as numerical integration and Kalman filters, can be used for parameter estimation.
- Model validation can be done with the estimated dynamic model parameters.
- A sudden change of the derived system parameters can be interpreted as a system event.

Results and Benefits

- A key benefit will be algorithms that can accommodate PMU values for improved situational awareness. This will have positive benefits in operations, since these algorithms could be used in real time even when the system models are unknown.
- A system event can be identified without any system information and validate a simulation model.
- **Technology Readiness Level:** The algorithm for creating the equivalent circuit has been implemented with Matlab; it is necessary to improve the accuracy of system parameter values.

Researchers

- Tom Overbye, overbye@illinois.edu
- Soobae Kim, kim848@illinois.edu

Industry Collaboration

- PowerWorld

Real-Time Streaming Data Processing Engine for Embedded Systems

Overview and Problem Statement

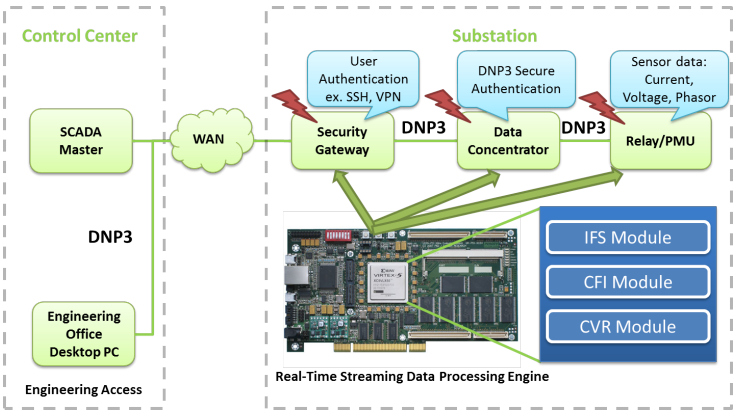
The objective of this activity is to develop high-coverage and low-overhead detection techniques to achieve secure and reliable execution of applications that compute critical data, in spite of potential hardware and software vulnerabilities. We propose a flexible, low-cost, and low-interference data processing engine for ensuring reliable and secure computing without incurring much resource and performance overhead. In particular, the engine can be inserted as a PCI Express card into substation devices, such as the Substation Security Gateway, the Data Concentrator, or the Relay/PMU to protect the data stream against corruption due to accidental errors or malicious attacks.

Research Objectives

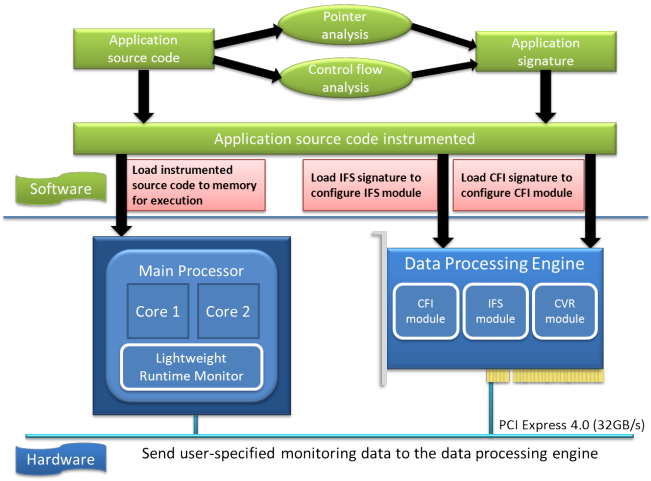
- Protect critical power grid data from malicious tampering or transient errors.
- Prevent attackers from using different entry paths (outsiders, normal users, insiders).
- Design the Data Processing Engine so that it can efficiently collect monitoring data coming from the main processor of the substation devices with low interference and low overhead.
- Achieve low-cost, low-overhead, high-performance, and scalable security and reliability checking.
- **Smart Grid Application Area:** We will apply our Real-Time Streaming Data Processing Engine on the Data Concentrator or Security Gateway to protect the integrity of critical data, such as passwords, private keys, or power grid data.

Technical Description and Solution Approach

- Developing the Real-Time Streaming Data Processing Engine, which provides a standard interface between a processor and hardware modules that implement reliability and security services.
- Using IFS (Information Flow Signature) and CFI (Control Flow Integrity) modules to provide security service, and CVR (Critical Value Re-computation) module to provide reliability service.
    - **Information Flow Signature (IFS)**: Analysis of the high-level source code of a program to derive the IFS (the set of data objects that one instruction is allowed to access) to ensure that runtime modifications of the data object follow the language-level semantics of the application.
    - **Control Flow Integrity (CFI)**: The runtime check to ensure that the execution of the program follows the Control-Flow Graph (CFG) extracted from the high-level source code. In particular, only indirect transitions, such as an indirect jump or function return, need to be checked.
    - **Critical Value Re-computation (CVR):** The application source code is statically analyzed to extract the backward slices for each piece of the critical data, which will be recomputed in runtime by a different computation path from the original one to prevent soft errors such as transient errors.
- **Real-Time Streaming Data Processing Engine in the Context of the Power Grid:**



- **Design and Integration of Real-Time Streaming Data Processing Engine:**



Results and Benefits

- A simplified version of the IFS module has been synthesized on Altera Startix II FPGA running SSH, WuFTP, and NullHTTP on top of Linux to demonstrate the effectiveness of IFS with low overhead (3–4%) and high coverage.

Attack	Target	Difficulty of launching attacks	Detectability
Control-data attacks	Return address	Low	Yes
	Function pointer	Low	Yes
	Old base pointer	Low	Yes
	Longjmp buffer	Low	Yes
Non-control-data attacks	Information signature	High	No
	Configuration data	Low	Yes
	User input	Low	Yes
	User identity data	Low	Yes
	Decision-making data	Low	Yes
Code injection attacks	Code segment	Moderate	Yes (for certain class)
Register corruption attacks	Register	High	No
Malicious 3rd-party library	Shared library	Moderate	Detectable by CFI
SETUID attacks	SETUID programs	Moderate	No

- **Technology Readiness Level:** We have implemented the simplified version of the Real-Time Streaming Data Processing Engine with the IFS module on our Stratix II Altera Board as a working prototype to evaluate our techniques.

Researchers

- Kuan-Yu Tseng, ktseng2@illinois.edu
- Zbigniew T. Kalbarczyk, kalbarcz@illinois.edu
- Ravi K. Iyer, rkiyer@illinois.edu

Industry Collaboration

- Altera, Xilinx, SEL

State-Aware Decentralized Database Systems for the Smart Grid

Overview and Problem Statement

What database models would ensure high data integrity and availability in the face of network failures? Considering the problem of secure management of large amounts of sensor information, we proposed a scalable decentralized (peer-to-peer) architecture to store, process, and deliver the data reliably and rapidly. The main security metric targeted is data availability, and resilience to network attacks that deny access to part of the database. The key idea is to exploit the structure of the data, namely how measurements are tied to state equations, to find an efficient model to replicate and reconstruct the data. That is achieved by estimating the global state vector in a distributed fashion (so that each server is "state-aware"), and then coding the measurements with the distributed state estimates used as the side information that efficiently glues together the various parts of the database.

Research Objectives

We developed a peer-to-peer (P2P) database model that deals with the key problems of ensuring critical data availability and accessibility, while storing information in an efficient and robust manner. P2P architectures are generally more scalable and resilient than the centralized client-server architectures. The new architecture we propose for streaming P2P Database Systems (DBS), which will be useful in general for Cyber-Physical Systems (CPS), is called "State-Aware" Distributed DBS (SA-DDBS). The SA-DDBS comprises a stored routine for decentralized state estimation, and a data representation and an archival model that utilize the stored routine to obtain 1) a reliable and flexible data replication mechanism, and 2) a faster method for querying measurement data across the SA-DDBS, making it possible to find critical state data in alternative servers in the presence of network attacks. In particular, the state information will always be one "hop" away from any application client. Furthermore, using consistent state information across the DBS as well as storage codes that encode measurement residuals, the SA-DDBS will provide reliable access to the archived records in an efficient way. The aspects we have left to investigate are:

- Improving the state estimation procedures by including more specific dynamic models of voltage revolutions using polynomial phase signal representations.
- Incorporating bad-data detection strategies in our protocols and testing their resilience to data injection attacks in the presence of limited PMU measurements.
- Introducing trust metrics and strategic network formation models that allow the P2P algorithms to mitigate the effect and cost of communicating with untrustworthy data sources.

Smart Grid Application Area: Energy Management System security.

Technical Description and Solution Approach

A considerable number of controls in power networks rely on frequency estimation. Signal processing techniques used in RADAR imaging can be extended to provide frequency estimates in power grids, approaching the fundamental estimation limits attainable with noisy observations. The idea is to use a parametric polynomial model for the Phasor evolution over time, instead of the dynamical models that are typically used in control systems, and to generate a maximum likelihood estimate of the frequency and the frequency drift of the Phasor data. The idea is to combine this model with the power flow equations and obtain a simple and novel Dynamic State Estimation model, tailored for the accurate estimation of the bus frequency.

SCADA power measurements and Static State Estimators are known to be vulnerable to data injection attacks that are not detectable by the state estimator. We intend to include bad-data detection rules in our P2P protocols and to examine the optimal placement of PMUs to provide the best security protection against these attacks.

One of the aspects left to investigate is that of *strategic network formation*. Specifically, in the P2P architecture, how should the nodes choose other peers with which to interact? The objective of this study is to examine how to develop *trust models* that would make it possible to revise the list of peers dynamically, based on an updated trust metric. The question is whether the emergent pattern of communications can adapt to mitigate the effect of bad data coming from potential attacks to some of the participating peers, or simply coming from peers whose data, relative to the cost of communications, contribute little to the accuracy of the state estimates.

Researchers

- Anna Scaglione, ascaglione@ucdavis.edu
- Xiao Li, eceli@ucdavis.edu
- Georgia Koutsandria, gkoutsandria@ucdavis.edu

Industry Collaborators

- We are currently seeking industry collaborators.

Research Cluster

Trustworthy Technologies for Local Area Management, Monitoring, and Control

Trustworthy Technologies for Local Area Management, Monitoring, and Control Page No.

Cluster Lead: Tom Overbye ..... overbye@illinois.edu

Development of the Information Layer for the V2G Framework Implementation

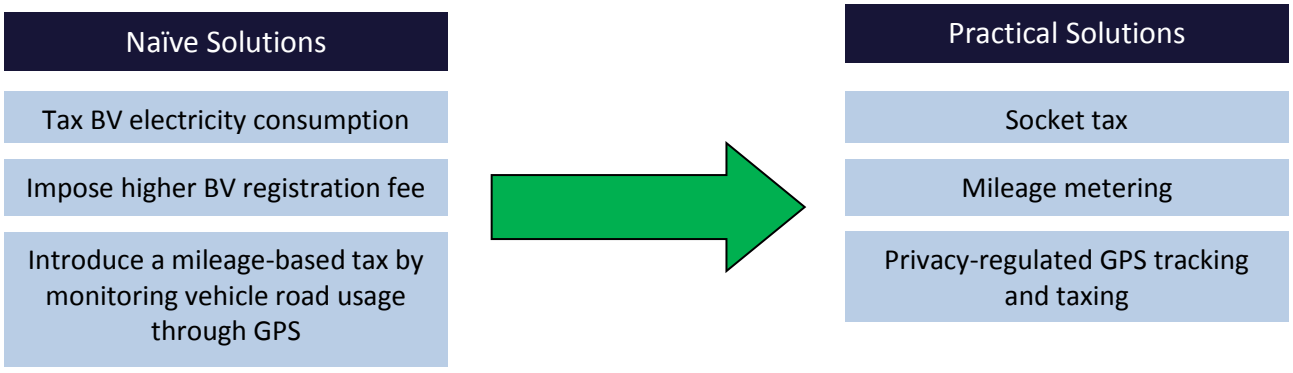
Overview and Problem Statement

The Vehicle-to-grid (*V2G*) concept integrates Battery Vehicles (*BVs*) into the grid as controllable loads and generation/storage devices. As the penetration of BVs deepens, gasoline tax payments are becoming a matter of concern, since those funds will need to be collected in some other way in light of the decreased gasoline sales. Currently, the Motor Fuel Tax is a major source of funding for transportation infrastructure. In the past 5–6 years, a concept of mileage-based tax has been developed in an attempt to address that concern. This approach calculates tax by monitoring vehicle road usage through the deployment of GPS data. The security and privacy aspects of the monitored fine-grained location data raise major concerns, particularly for the vehicle owners. Our scope is to effectively address those concerns while providing the ability to collect the data needed to allow the collection of funds for the road transportation infrastructure.

Research Objectives

- To develop an effective and efficient methodology to replace the motor fuel tax collection.
- To ensure that the security of the approach and associated data collection/processing/storage is maintained without compromising data integrity and confidentiality and with acceptable availability.
- To effectively address the privacy concerns and make the system publicly acceptable.
- To ensure that the system is pragmatic with respect to cost, scale, and usability.

Technical Description and Solution Approach



- The proposed methodology must represent usage accurately and have adequate security against hackers or attempts to distort data; moreover, the implementation and the associated data collection/processing/storage must preserve privacy without impacting the practicality of the approach.
- The focus is on mileage-based data usage because of its broad versatility and flexibility.
- A mileage-based system requires the use of a GPS device in the BV and appropriate computing/communications to collect, process, and store data.

Results and Benefits

- The generality and nature of collected data allow the approach to be useful for any taxing authority, be it local, state, or federal, and also across international borders.
- Accurate data to ensure that each user pays the appropriate amount based on actual mileage.
- Quantification of the energy savings and associated emissions.
- Modularity and the flexible implementation provide the ability to introduce new legislative and regulatory rules.
- The comprehensiveness and generality of the approach allow application for all types of BVs, from all-electric vehicles to pluggable hybrid vehicles, with the ability to take into account partial fuel charge utilization.
- The methodology can include any vehicle characteristic, such as weight, to allow the imposition of charges to be a function of the specific characteristic.
- The approach's generality provides the ability to collect tolls and to differentiate usage of differently priced roads.
- The system may be used to reflect time of day or road condition pricing and can be particularly useful in allowing congestion pricing based on commute hours or location.

Researchers

- Gaurav Lahoti, lahoti2@illinois.edu
- George Gross, gross@illinois.edu
- Carl A. Gunter, cgunter@illinois.edu

Password-Changing Protocol

Overview and Problem Statement

The current power grid system and its power lines in the field are monitored by telemetric devices, and maintenance personnel from utility companies regularly collect data readings from these telemetric devices on handheld devices to ensure that the health of power lines is sound and stable. The scale on which poletop devices that monitor power line health are used is already large, and with the continuing upgrade of the smart grid, the number of these resource-constrained devices is further increasing. Currently, security of data on the telemetric and handheld devices is one important concern. The telemetric and handheld devices and their data are easy targets of security attacks due to the wireless communication over which data are read from/to the telemetric device to/from the handheld device, and due to the weak passwords and vulnerable authentication protocol that utilities use to access the handheld and telemetric devices. As these small resource-constrained devices are increasingly used because of the ongoing upgrade of the smart grid, the security threats are further increasing as well.

In this project, our goal is to investigate a robust, scalable, and automated password-changing protocol framework to ensure unique authentication of human personnel in the presence of widespread use of poletop devices, and to ensure secure access to data inside the handheld and telemetric resource-constrained devices along with secure delivery of data over the wireless network in the field in real-time under varying maintenance scenarios.

Research Objectives

- Study the security and robustness of the existing system in the face of malicious attacks.
- Design a secure password-changing protocol that can defend against malicious attacks.
- Find a cost-effective and fast solution approach.
- **Smart Grid Application Area**: Security, networking.

Technical Description and Solution Approach

- Automated generation and verification of passwords using a strong authentication protocol.
- Creation of passwords and keys based on physical characteristics such as per-pole-device locality, per-pole temporal, and per-maintenance-personnel identifications.
- Cryptographic mechanisms and authentication protocols are being studied.

Results and Benefits

- Secure storage and access of data at devices in the field level.
- Defense against malicious attacks.
- Responsible operators can be identified in case of malicious attacks.
- Good situational awareness.
- **Partnerships and External Interactions**: We are interacting with the project “Trustworthy Framework for Mobile Smart Meters.”
- **Technology Readiness Level:** Research and design phase.

Researchers

- Prof. Klara Nahrstedt, klara@illinois.edu
- Rehana Tabassum, tabassu2@illinois.edu

Smart-Grid-Enabled Distributed Voltage Support Framework

Overview and Problem Statement

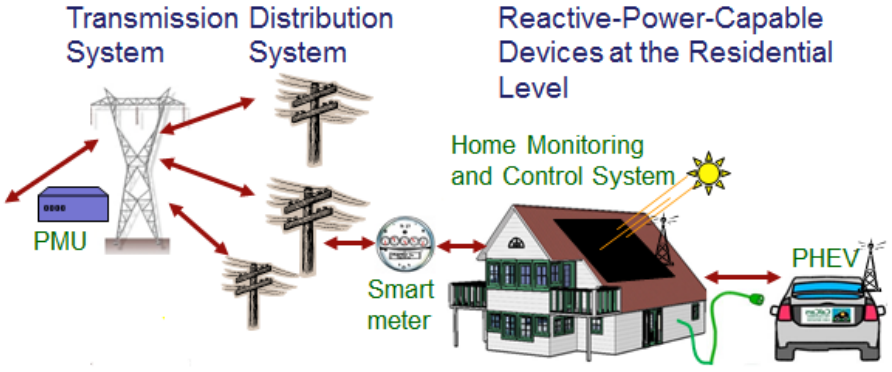
The motivation for this research lies in the use of emerging smart grid devices, such as PHEV/EVs, solar panels, and other power electronics devices, to supply reactive power as a means of distributed reactive power support. Power factor compensation closer to the load improves transmission line loading and efficiency; furthermore, it may inject reactive power to the system to maintain preferable bus voltage. We examine requirements for a secure communication framework to interact with the large number of devices that would be present. The focus of this project is on determining the cyber infrastructure needed to obtain this reactive power control.

Research Objectives

- The project seeks the ability to utilize large amounts of distributed resources, so there are major challenges to ensure that the devices cannot be used to harm the system instead of improve it.
- Information received by the devices must be trustworthy, so they will respond only in an intended way.
- Availability of the resources is important, and the capabilities of the system at any time should be known, since having wrong or out-of-date information about resource availability may cause the scheme to be unsuccessful.
- There are also questions about the best way to utilize the support from a power system perspective; for example, should the system operate so that it receives the distributed support all the time to match the voltage profile, or just operate so that it minimizes the loss in the system?
- Another challenge is to investigate what the implications would be for potential contingencies of this system so that the system can be designed to avoid them. For example, if an adversary were to gain control of a neighborhood's distributed reactive power control system and tell all the devices to maximize their output, could all the fuses trip at the same time? If so, what can we do to prevent this situation?
- **Smart Grid Application Area:** This project is developing a framework to allow secure control of distributed resources in an intelligent manner.

Technical Description and Solution Approach

- Example power systems, such as distribution feeders, are being modeled to show the benefits of local injections of reactive power. Varying load and supply voltage conditions are being modeled.
- Algorithms are being developed to determine the validity of using distributed reactive power control with different assumptions about the cyber infrastructure, such as local control versus global control.
- Impacts of cyber disruptions are being studied.



Results and Benefits

- Reactive power is most effective locally, and voltage problems tend to start in the distribution system. By addressing the problem at the distribution level, we can alleviate voltage problems at the transmission system level as well.
- A framework utilizing distributed reactive resources is important, because an increasing number of inverter devices that can potentially provide this support are being placed in the power grid, and this additional reactive power capability is useful from a power systems perspective.
- As noted in the 2003 blackout report, a commonality among most previous major North American blackouts was that the system was experiencing inadequate reactive power support.
- **Partnerships and External Interactions:** Energy Dashboard project, Load Control and Monitoring project, and Agent Applications project.
- **Technology Readiness Level:** The researchers plan to work with the campus distribution system facilities personnel to implement a test system on the University of Illinois campus when the devices are ready.

Researchers

- Hao (Max) Liu, haoliu6@illinois.edu
- Thomas J. Overbye, overbye@illinois.edu

Trustworthy Framework for Mobile Smart Meters

Overview and Problem Statement

We propose to install on an electric vehicle (EV) a mobile smart meter that monitors energy usage by the car and communicates with a central utility office for periodic reporting, billing information, or route suggestions. The approach will enable us to track energy usage more easily. It will also bring new energy market models, as people generating extra energy from their solar panels can directly sell energy to electric cars, while the mobile smart meters on the cars record the energy purchase. However, securing communication between mobile smart meters and the utility office might be challenging; the data may be routed through a combination of wired networks, open WiFi, and cellular networks. We are focusing on the question of how a mobile smart meter communicates with other meters and with the central utility office in a secure way. The ultimate goal is to design a trustworthy framework for communication between meters and a central utility, together with the corresponding secure communication protocol.

Research Objectives

- Design a reliable demand-response communication system between the mobile smart meter and utility office.
- Design a fast authentication scheme that mobile smart meters can use to prove their identity to other smart meters or to roadside units.
- Design a periodic reporting scheme for mobile smart meters that preserves users' location privacy.

Technical Description and Solution Approach

- Current Approach: the routing protocol takes various hints from digital maps, such as locations of signal-blocking obstacles, network congestion status, etc., to make better forwarding decisions.
- Future Work: the routing protocol uses a combination of networks in different scenarios, e.g., using cellular when the EV is moving at high speed, using WiFi for high-bandwidth communication when the EV is parked, and using ZigBee to communicate with other smart meters nearby.
- Future Work: mix-zone and pseudonym approach for location privacy.
- Future Work: fast authentication for vehicular ad hoc networks.

Results and Benefits

- Easy monitoring and accurate tracking of energy usage: meter is directly associated with the car that consumes energy.
- Flexible pricing model: a mobile smart meter receives pricing information specifically targeted at the associated car.
- Flexible energy exchange: meter-to-meter communication makes it possible for a car to sell energy directly to another and record the exchange correctly.

Researchers

- Hongyang Li, hli52@illinois.edu
- Klara Nahrstedt, klara@illinois.edu

Research Cluster

Responding To and Managing Cyber Events

Responding To and Managing Cyber Events Page No.

Cluster Lead: William H. Sanders ..... whs@illinois.edu

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

A Game-Theoretic Intrusion Response and Recovery Engine

tcipg.org

Overview and Problem Statement

The severity and number of intrusions on computer networks are rapidly increasing. Preservation of the availability and integrity of networked computing systems in the face of those fast-spreading intrusions requires advances not only in detection algorithms, but also in intrusion tolerance and automated response techniques. In this project, we study an intrusion-tolerant system design that can adaptively react against malicious attacks in real-time, given offline knowledge about the network's topology, and online alerts and measurements from system-level sensors.

Research Objectives

- Reactive response against adversarial attacks that uses knowledge about the power grid's current security state and its security requirements.
- Adapt the Response and Recovery Engine (RRE) to handle the scale of a large Automated Metering Infrastructure (AMI) and to integrate AMI-specific responses.
- Model the cost of a response in an AMI to include the cost due to the underlying distribution grid and the cost incurred by customers.
- Verify safety properties of possible responses.

Technical Description and Solution Approach

- Generate a custom response action taxonomy for AMI to guide the design of response actions that are suitable for AMI.
- Model accurately the cost of responses and attacks based on the cyber and physical states of the power grid, using dependency graphs and the state of the distribution grid. (The cost model uses a dependency graph of the AMI services to compute the effect on confidentiality, integrity, and availability (CIA) criteria.)
- Implement the cost model using an AMI topology provided by real GSI data to generate the dependency graph and simulate a realistic distribution grid using Gridlab-d to understand the effect of a response on the grid.
- Use hybrid automata to model the power grid and prove that responses fall within the safety boundaries of the system.
- Design and develop a scalable game-theoretic decision-making solution that can provide optimal response and recovery actions in real-time for large-scale power grid networks.

Results and Benefits

- Proposed a taxonomy of response actions for AMI that aided in the generation of a set of response actions.
- Proposed a cost model for responses and actions in AMI that uses the dependency graph to compute the effects on CIA and convert those to a financial cost based on the electricity market, empirical data, and simulation of the distribution grid.
- Our developed tools can now automatically generate and learn system-wide dependency graphs and adversary-driven attack graphs for large-scale power grid networks. We evaluated our

implementations using a simulated and realistic power grid control network topology inspired by real-world control room configurations.

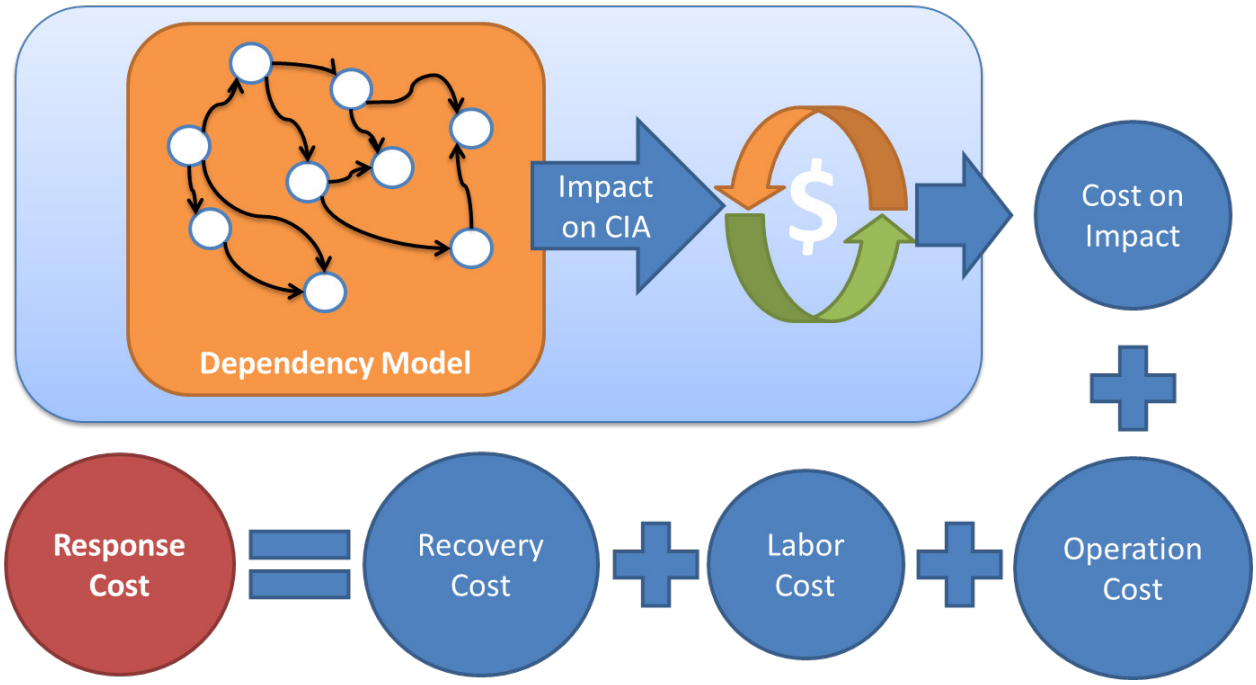


Figure 1: High-level Conceptual plan for the Proposed Response Cost Model

Researchers

- Ahmed Mohamad Fawaz, afawaz2@illinois.edu
- Robin Berthier, rgb@illinois.edu
- William H. Sanders, whs@illinois.edu

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Assessment and Forensics for Large-Scale Smart Grid Networks

tcipg.org

Overview and Problem Statement

The infrastructure that supports the power grid is vulnerable to attack by intruders, who could potentially take control of certain points and cause great damage to systems. It is therefore important that organizations develop infrastructure security policies to handle unwanted configuration changes and failures within the grid. Often, large systems concentrate their security by creating central monitors that can act as single points of failure if compromised. These centralized systems are also difficult to scale up and may not adequately ensure the validity of information passed in the network.

Sophisticated, targeted attacks such as Stuxnet are inevitable, and it is critical that we detect them and develop a deep understanding of what happened. If machines, such as those in SCADA, are compromised, we want to know as much about them as possible, and understand what the effects will be on the power grid.

Research Objectives

- We aim to improve the security and efficiency of automated systems for monitoring compliance of power systems to policies.
- We introduce and analyze a secure architecture for monitoring compliance based on security event monitoring at the network level, software level, and hardware level.
- Our approach is based on removing central points for monitoring to increase scalability and security.
- We will configure an architecture that protects integrity and confidentiality of the nodes within the system.
- We will integrate forensic techniques in the monitoring process to ensure the integrity of the information acquired.
- We will communicate with industry to understand what they want to know about compromised hosts and how these compromises affect the power grid.
- We will leverage new and existing forensics tools for better analysis.
- **Smart Grid Application Area:** Distributed Systems, Forensics.

Technical Description and Solution Approach

- Create a framework to input and interpret infrastructure policies in the architecture.
- Develop a compilation algorithm to transform policies into multiple redundant aggregation trees. These aggregation trees ensure a distribution of policy verification load among multiple systems for scalability. Redundancy makes the architecture resilient against a limited number of compromised nodes within the system.
- Create simulator to test scalability and effectiveness of architecture.

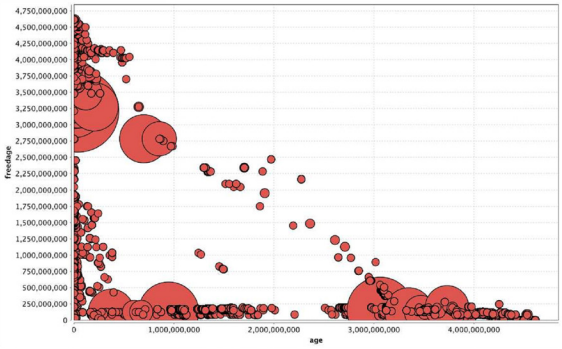


Figure 1: Distribution of the lifetime of objects in memory for a given process

- The integrity of the nodes can be checked using a live forensic tool called *Forenscope* to ensure that the information provided to the monitoring system has not been compromised.

Results and Benefits

- Found that the architecture is successful in distributing policy statements across nodes in an effective manner.
- Communication in this architecture only grows linearly with the size of the infrastructure, which indicates scalability of this solution.
- System is robust in protecting itself against a limited number of attacks.
- This architecture could be useful in protecting distributed systems against attacks.
- We have developed a tool, called *Forenscope*, that collects high-quality information about compromised machines.
- We have developed a system, called *Cafegrind*, capable of analyzing what information is available in memory to forensic investigators.
- **Partnerships and External Interactions:** Information Trust Institute, Assured Cloud Computing Center at UIUC, Boeing
- **Technology Readiness Level:** Initial stage

Researchers

- Kevin Larson, klarson5@illinois.edu
- Mirko Montanari, mmontan2@illinois.edu
- Prof. Roy Campbell, rhc@illinois.edu

Industry Collaboration

- Boeing

Hardware-based IDS for AMI Devices

Overview and Problem Statement

A major challenge is that many embedded system devices used in critical infrastructure applications are easily accessible in the supply chain and can be tampered with or altered such that the authentication of the devices cannot be assured. The installation of a hardware-based backdoor gives a cyber-attacker unlimited eavesdropping access to logic-level communication within a Smart Grid device and is virtually undetectable by state-of-the art intrusion detection systems. In addition, a hardware-based backdoor can be inserted during the manufacturing processes or deployment lifecycle. A one-time verification is insufficient. This research activity looks at ways to identify that kind of attack at the embedded system board level, while keeping in mind the constraints of manufacturing cost and normal system performance. This research also looks at the supply chain as a cybersecurity system-level problem, looking for ways to bridge manufacturing practices and lifecycle information assurance.

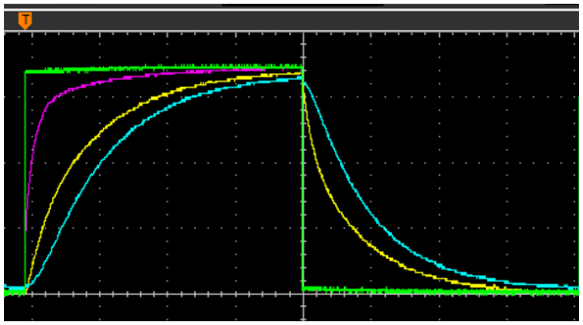
Research Objectives

- Identify the electrical characteristics of a hardware-based, logic-level attack.
- Derive a hardware detection algorithm that can be scaled to different communication bus speeds.
- Determine design considerations with regard to IDS sensitivity and accuracy.
- Identify nonlinear circuits that provide a differential comparison between normal inter-chip communication and unauthorized use during a hardware-based attack, without the use of stored “secret” values.
- Study the analog characteristics of low-cost circuit components to determine if normal manufacturing process variance is enough to create unique hardware signatures that are very difficult to replicate.
- **Smart Grid Application Area:** AMI, SCADA, any embedded system Smart Grid device.

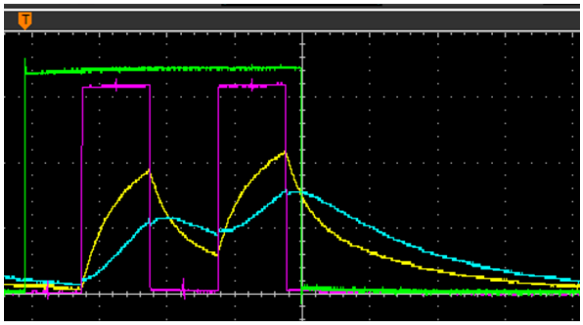
Technical Description and Solution Approach

- Use low-cost, resistive-capacitive circuits connected to an inter-chip communication bus that causes a temporary transfer in system energy; presents a physics-based challenge to the system.
- Synchronously measure the dynamic analog responses to the challenge and derive several IDS metrics: discrete values, voltage, time, interval slopes, and area under curves.
- An intruder attached to the communication bus causes a perturbation of waveform and response characteristics.
- Use statistical analysis to build effective IDS models to distinguish between intruder types.

Normal IDS Circuit Response

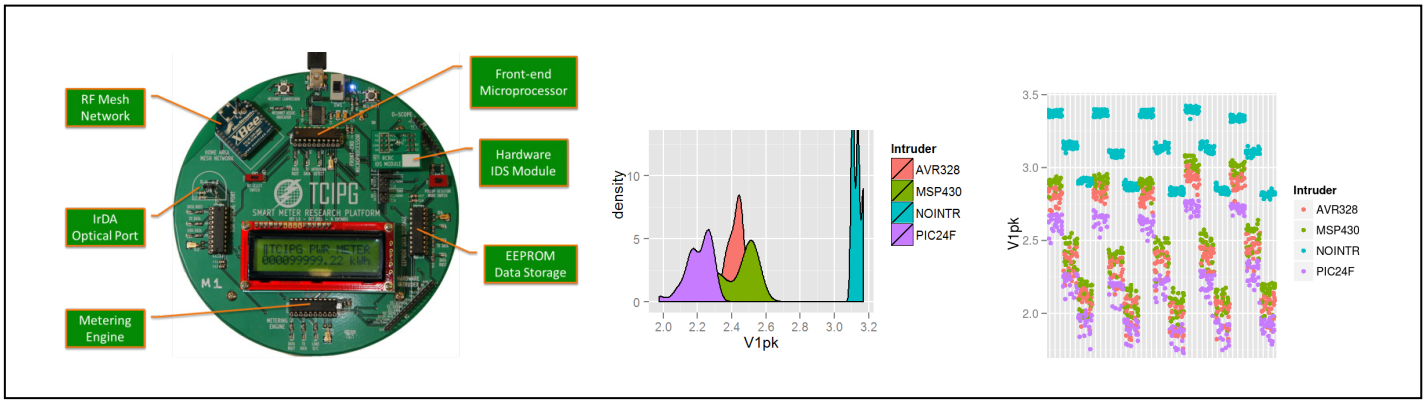


IDS Circuit Response with Intruder



Results and Benefits

- Created the Smart Meter Research Platform to enable embedded system security research.
- Completed empirical model of hardware-intruder electrical characteristics from 80 million measured data points.
- Signatures of various intruders are distinct.
- Intrusion Detection System can accurately distinguish among several varieties of hardware intruders at 89% accuracy with non-optimized algorithm (i.e., the accuracy can easily be improved).
- Provides a high-resolution view of the security status of AMI devices and systems.
- Low impact on system performance.
- Low-cost and easily integrated into new Smart Grid devices.
- **Partnerships and External Interactions:** Sandia National Laboratories (DOE).
- **Technology Readiness Level:** Proof-of-concept complete, 3 provisional patent applications from this activity.



Researchers

- Nathan J. Edwards, njedwar@sandia.gov (recent TCIPG graduate)

Industry Collaboration

- Jason Hamlet, Sandia National Laboratories (DOE)
- Ryan Helinski, Sandia National Laboratories (DOE)
- David Robinson, Sandia National Laboratories (DOE)

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2012-8083P

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Specification-based Intrusion Detection System for Smart Meters

tcipg.org

Overview and Problem Statement

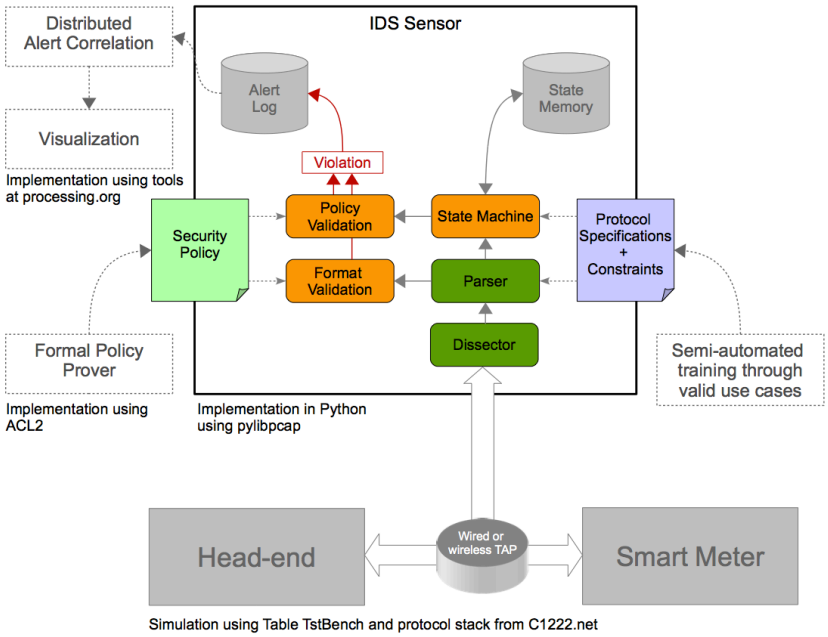
To ensure the security and reliability of a modernized power grid, the current deployment of millions of smart meters requires the development of innovative situational awareness solutions to prevent compromised devices from impacting the stability of the grid and the reliability of the energy distribution infrastructure. To address that issue, we introduce a specification-based intrusion detection sensor that can be deployed in the field to identify malicious activity in real time. The sensor monitors the traffic among meters and access points at the network, transport, and application layers to ensure that devices are running in a secure state and that their operations respect a specified security policy. It does so by implementing a set of constraints on transmissions made using the C12.22 AMI protocol that ensure that all violations of the specified security policy will be detected. The soundness of those constraints was verified using a formal framework, and a prototype implementation of the sensor was evaluated with realistic AMI network traffic.

Research Objectives

- Define a security policy for AMI.
- Develop detection technologies to run on low-computation hardware with limited memory.
- Design a comprehensive but cost-efficient monitoring architecture.
- Provide large-scale situational awareness.
- **Smart Grid Application Area:** AMI security.

Technical Description and Solution Approach

- Identification of the characteristics of common smart meter communication use cases.
- Design of a distributed monitoring framework and a security policy to ensure the detection of violations.
- Development of a C12.22 dissector and a C12.22 state machine to monitor meter traffic in real time.
- Implementation of a prototype in an embedded computer.
- Evaluation in a real AMI environment with hardware meters.



Results and Benefits

- Definition of a rigorous process utilities and vendors can use to develop a comprehensive monitoring architecture.
- Integration of formal methods in a practical framework to offer strong security guarantees.
- **Partnerships and External Interactions**: in collaboration with Fujitsu, EPRI, FirstEnergy, and Itron.
- **Technology Readiness Level**: prototype.

Researchers

- Dr. Robin Berthier, rgb@illinois.edu
- Ahmed Fawaz, afawaz2@illinois.edu
- David Grochocki, dgrocho2@illinois.edu
- Edmond Rogers, ejrogers@illinois.edu
- Prof. William H. Sanders, whs@illinois.edu

Industry Collaboration

- Fujitsu: Alvaro Cardenas and Jorjeta Jetcheva
- EPRI: Galen Rasche and Annabelle Lee
- Itron: Ido Dubrawsky
- FirstEnergy: Don Miller, Marcus Noel, and Ronald Ross

Specification-based IDS for the DNP3 Protocol

Overview and Problem Statement

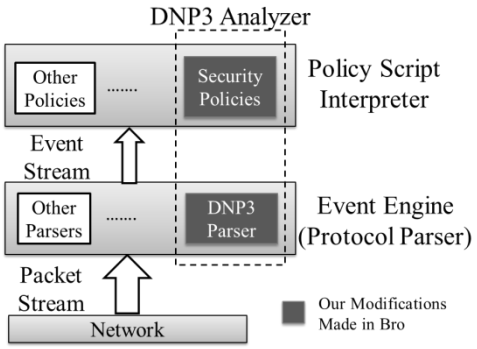
Modern SCADA systems are increasingly adopting Internet technology to control industrial processes. Attackers can penetrate into control systems to put remote facilities in danger. While protection of SCADA systems is of critical value, few Intrusion Detection Systems (IDSes) have sufficient capabilities to investigate network traffic based on unique proprietary protocols. To overcome that challenge, we introduce a specification-based intrusion detection framework that provides high visibility of semantics carried by proprietary network protocols. With a built-in parser of proprietary protocols, our IDS collects network events in SCADA systems. SCADA-specific semantics related to each event are thus analyzed based on policy configured by system operators.

Research Objectives

- Integrate application layer parsers supporting DNP3 and Modbus into Bro, a runtime network traffic analyzer.
- Exploit Bro's intrusion-detection features, such as runtime event handling and state management, to analyze SCADA network events.
- Develop attack scenarios, i.e., man-in-the-middle attacks.
- Design applicable and reconfigurable security policy via Bro domain-specific scripts.
- Experiment on feasibility of the proposed Bro-based IDS in SCADA systems.

Technical Description and Solution Approach

- Build parsers supporting DNP3 and Modbus and integrate them into Bro.
    - A compiler-assisted method, called *Binpac*, is exploited to reduce development periods and possible logic errors.
- Build event handlers to collect all semantics carried by DNP3 network packets.
- Develop policies based on DNP3 protocol definition to validate packet syntax.
- Propose sample security policies performing semantic analysis.
    - Compare payloads in the ingress and egress DNP3 packets related to the same device to locate the compromised device.



Results and Benefits

- With the support of protocol parsers, the proposed Bro-based IDS is able to detect stealth attacks constructed by normal SCADA system operations.
- Experiments have been done in an emulated SCADA network environment in which proprietary software and hardware are configured.
    - Simulated man-in-the-middle attacks for which mediating data aggregator was compromised.
    - Exploited the proposed DNP3 analyzer with security policies implemented to monitor networks.
    - Analyzed feasibility of the proposed DNP3 analyzer in terms of performance.

Researchers

- Hui Lin, hlin33@illinois.edu
- Adam Slagell, slagell@illinois.edu
- Zbigniew Kalbarczyk, kalbarcz@illinois.edu
- Ravishankar K. Iyer, rkiyer@illinois.edu

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Usable Management Tools for the Smarter Grid's Data Avalanche

tcipg.org

Overview and Problem Statement

The present and future smart grid has a vast population of diverse devices that generate lots of data. The variety, large volume, and spontaneous generation of data result in what one of our industry partners has called a "data avalanche." Data avalanches of the future will likely be quite large if the number of devices on the smarter grid is larger than the number of devices on the Internet.

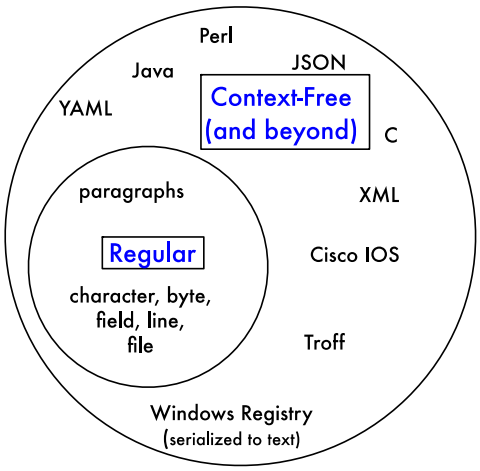
Our research focuses on the following question: How can humans deal with the smart grid "data avalanche" and thereby gain an increased situational awareness for the smarter grid?

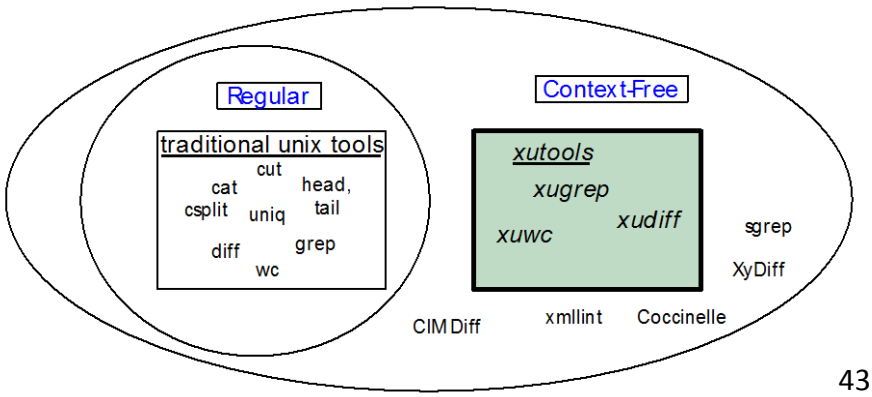
Research Objectives

- **Goal:** We want to enable a more reliable, consistent, affordable audit driven by the flood of data used to configure devices on power control networks.
- **Motivation:** Power control networks must comply with NERC CIP
  - Failure to comply costs up to $1.5 million per day of violation
  - **Audit is expensive**: 30 man days per day; hundreds of thousands to millions of dollars.
  - **Can we** automatically generate change logs and reports of change and thereby **reduce the cost of audit**?
- We research new approaches to **efficient management and auditing of devices on control networks.**
- **Smart Grid Application Area:** Cyber-security situational awareness, NERC CIP compliance audit.

Technical Description and Solution Approach

- Security policies are in **many different languages**.
- Most **policies** and associated security artifacts are **structured text**.
- Many language-specific structures are not recognized by traditional tools.
- Our eXtended Unix text-processing tools (XUTools) process high-level language constructs.
  - xugrep: extract
  - xuwc: count
  - xudiff: compare
- **Our approach** appeared in a **Slashdotted** and widely covered poster **at USENIX LISA 2011** and will appear as a full paper at USENIX LISA 2012.





Results and Benefits

- In IEEE PECI 2012, we identified specific NERC-CIP provisions that our tools address.

	CIP Provisions	Revision	Summary Description	Device Dataset
Software	CIP 003-4	R6	Change Control and Configuration Management	Windows Registry
Software	CIP 010-1	R1.1, R1.2, R1.5, R2.1	Baseline configuration development and comparison	Windows Registry
Network	CIP 005-4a	R5.2	Update network documentation within 90 days of the change	Cisco IOS

- Fall 2012, we demonstrated the ability to **inventory, measure similarity, and see the usage of high-level language constructs in a router configuration file**.
- Since the constructs have names that persist across multiple versions of a configuration file, **we can use these construct types as units of analysis to directly quantify network evolution**.
- **Technology Readiness Level:** Seeking real-world practitioners to evaluate our results.

Object Groups in the Dartmouth Core: 2005-2009		
year	number	size (min/avg/max)
2005	0	0/0/0
2006	0	0/0/0
2007	0	0/0/0
2008	6	2/4.0/6
2009	117	2/4.0/21

ACLs in the Dartmouth Core: 2005-2009		
year	number	size (min/avg/max)
2005	18	2/6.0/39
2006	34	2/8.0/80
2007	39	2/7.0/39
2008	62	2/6.0/39
2009	64	2/7.0/39

Object Groups in the Dartmouth Core: 2005-2009					
year	number	clusters	3-clusters	2-clusters	unclustered
2005	0	0	0	0	0
2006	0	0	0	0	0
2007	0	0	0	0	0
2008	6	0	0	0	0
2009	117	100	4	9	87

ACLs in the Dartmouth Core: 2005-2009					
year	number	clusters	3-clusters	2-clusters	unclustered
2005	18	17	0	1	16
2006	34	31	0	3	28
2007	39	36	0	3	33
2008	52	49	0	3	43
2009	64	58	2	2	54

Researchers

- Gabriel A. Weaver, Gabriel.A.Weaver@Dartmouth.edu
- Sean W. Smith, sws@cs.dartmouth.edu

Research Cluster

Trust

Assessment

Trust Assessment Page No.

Cluster Lead: Zbigniew Kalbarczyk ..... kalbarcz@illinois.edu

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Automatic Verification of Network Access Control Policy Implementations

tcipg.org

Overview and Problem Statement

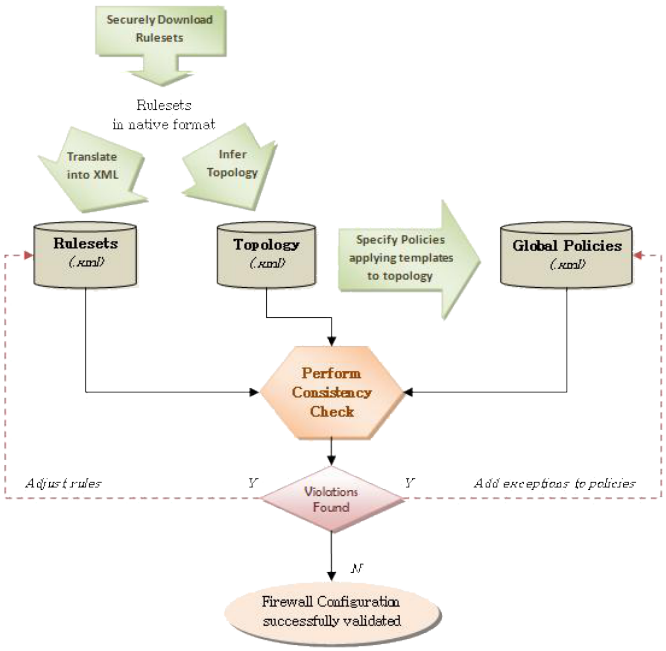
This project aims to develop a highly usable, scalable, and effective tool for analyzing security policy implementation for conformance with global security policy specification for industrial control networks. The tool provides comprehensive analysis of compliance to ensure that all access control mechanisms work collectively in harmony. The tool, called *NetAPT (Network Access Policy Tool)*, has been fully implemented and has been used successfully to aid in vulnerability assessments and compliance audits at our industry partners. NetAPT is available to potential users and has entered a final beta testing phase.

Research Objectives

- Process control networks are connected to other networks in enterprise systems; access is controlled through a large number of devices, such as firewalls.
- Best practices recommendations and compliance requirements are difficult to meet rigorously without significant man-hour investment. Pressing questions include:
    - How can we express English-language recommendations for global policy in a machine-checkable form that network administrators can easily formulate and understand?
    - How can we determine whether the access control that firewalls provide precisely meets the requirements of the machine-checkable global policy?
- Any analysis method or tool must
    - Incorporate policy rules from myriad sources.
    - Ensure scalability with size and complexity of networks.
    - Provide analytic and/or empirical demonstrations of efficacy.
- **Smart Grid Application Area:** NetAPT can be used to make sure that the access controls for the communications infrastructure of the Smart Grid are configured correctly. It can help prove compliance of the existing mechanisms with the various recommendations and standards (e.g., NERC CIP 005) and can help ensure that compliance is maintained despite any new changes to configuration of layer 3 devices (firewalls, routers).

Technical Description and Solution Approach

- NetAPT takes as input firewall configurations, and discovers the topology.
- It uses advanced data structures and modular design to incorporate a variety of policy rules and maintain extensibility.
- It has a sophisticated graphical front-end for increased usability, along with an analysis engine optimized for performance.
- The GUI and analysis engine can be decoupled and run on separate machines (GUI on an admin workstation, the engine on a powerful server). SSL is used to communicate between the two components.
- Specific optimizations for process control networks are included.
- NetAPT includes parameterized global policy templates, encoding various best practices recommendations and compliance standards that can be quickly customized to the network being analyzed.



Results and Benefits

- NetAPT has been implemented and released to select industry partners for evaluation.
- NetAPT was used for an internal audit and vulnerability assessment at a major utility, for a network with nearly 100 firewalls and several thousand hosts.
  - Helped produce comprehensive, highly visual reports to prove compliance with NERC CIP standards.
  - Identified exceptions in firewall configurations that required policy review or changes.
- NetAPT can greatly reduce the burden of managing complex security setups in large networks, allowing for creation and administration of more secure networks.
- **Partnerships and External Interactions:** Close interaction with utility partners and NERC CIP auditors.
- **Technology Readiness Level:** Development and support for NetAPT have transitioned (through a contract with DHS S&T) to commercial licensing and support; see Nicol or Sanders for details.

Researchers

- David M. Nicol, dmnicol@illinois.edu
- William H. Sanders, whs@illinois.edu
- Mouna Bamba, mbamba@illinois.edu
- Sankalp Singh, sankalp@illinois.edu
- Edmond J. Rogers, ejrogers@illinois.edu

Industry Collaborators

- Steve Coppenbarger, Cornbelt Energy
- Chris Johnson, Eastern Illini Electric Cooperative
- Kevin Perry, Southwest Power Pool (SPP)

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Modeling Methodologies for Power Grid Control System Evaluation

tcipg.org

Overview and Problem Statement

Research on various smart grid technologies requires high-fidelity experiments in realistic, large-scale settings. In this project, we are creating a high-fidelity, highly scalable simulation and emulation platform for security evaluation in power grid control networks. The testbed deploys virtual machine-based network emulation and parallel network simulation technologies to achieve that goal, and is designed to efficiently connect various virtual and real systems in the TCIPG lab as a testing and evaluation platform for other smart grid projects.

Research Objectives

- To create a backbone at the core of the Smart Grid testbed at Illinois that connects various components.
- To create models that support security assessment in a realistic large-scale setting.
- To create experimental designs and output analysis.
- **Smart Grid Application Area:** Testbed of power grid control systems.

Technical Description and Solution Approach

- Our testbed uses virtual-machine-based emulation and parallel network simulation technologies.

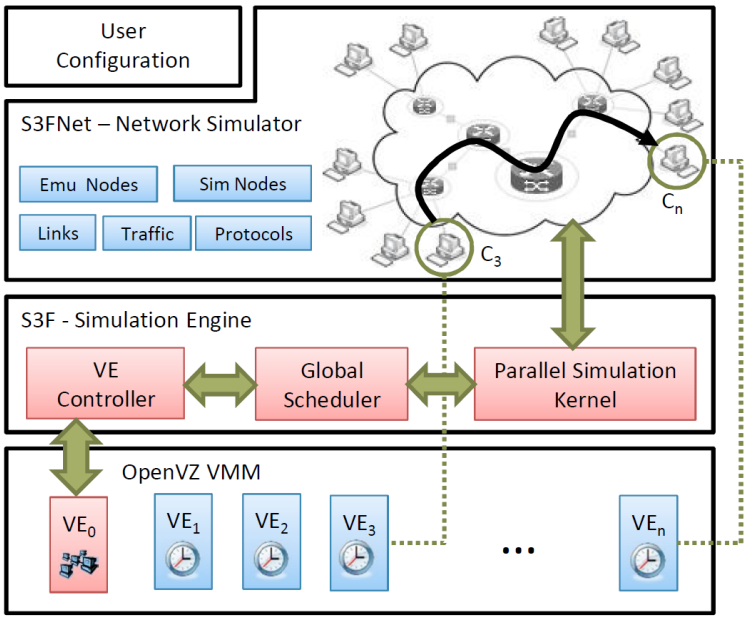


Figure 1: System Design Architecture

- Virtual-machine-based implementation of network emulation.
  - Because of the use of virtual machines, we allow unmodified application code to run in our testbed directly. This yields high functional fidelity.
  - Each virtual machine has its own virtual clock, and it perceives time as if it were running independently and concurrently with other machines in the physical world.
  - We currently have a virtual time system based on OpenVZ virtualization technologies, whose light weight provides good scalability. We are able to run 320 VEs on a single commodity server.
  - The achievable temporal accuracy of our system is subject to scheduler granularities, which are tunable in our system. We can explore the trade-off between execution speed and temporal accuracy (up to 30 µs).

- Parallel network simulation: S3F/S3FNet.
  - S3F simulation engine supports modular construction of simulation models that easily exploits parallelism.
  - The new engine design enables interactive communication with emulation.
  - It is flexible enough to create/explore various testing scenarios in a large-scale setting.
  - S3FNet provides sophisticated, low-level network layers and background traffic simulation.
- Integration of virtualization platforms to S3F/S3FNet.
  - Simulation is for modeling an extensive ensemble of background computation and communication.
  - Emulation is for representing execution of critical software.
  - Design of a global synchronization algorithm that integrates simulation and emulation.

Results and Benefits

- Developed our large-scale, high-fidelity network testbed.
  - S3F/S3FNet parallel network simulation.
  - OpenVZ emulation with virtual time system.
- Validated our testbed (S3F/S3FNet + OpenVZ).
  - System temporal error is bounded by one timeslice (100us).
  - Evaluation of application behavior:
    - Network-intensive (e.g., FTP, web browser) and CPU-intensive applications.
    - The error introduced by a virtual time system is often smaller than that introduced by the OpenVZ platform.
- Publications
  - Zheng and Nicol. “A Virtual Time System for OpenVZ-Based Network Emulations,” PADS’11.
  - Nicol, Jin, and Zheng. “S3F: The Scalable Simulation Framework Revisited,” WSC’11.
  - Zheng, Nicol, Jin, and Tanaka. “A Virtual Time System for Virtualization-Based Network Emulations and Simulations,” JOS’11.
  - Jin, Zheng, Zhu, Nicol, and Winterrowd. “Virtual Time Integration of Emulation and Parallel Simulation,” PADS’12. (Best paper award)
  - Zheng, Jin, and Nicol. “Validation of Application Behavior on a Virtual Time Integrated Network Emulation Testbed,” WSC’12, to appear.
- **Technology Readiness Level:** ongoing

Researchers

- David Nicol, dmnicol@illinois.edu
- Dong (Kevin) Jin, dongjin2@illinois.edu
- Yuhao Zheng, zheng7@illinois.edu
- Huaiyu Zhu, hzhu10@illinois.edu
- Lenhard Winterrowd, winterr2@illinois.edu

Industry Collaboration

- Boeing Corporation
- IBM Research

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components

tcipg.org

Overview and Problem Statement

As the power system updates itself to new Smart Grid standards, its dependence on a cyber infrastructure of sensing, communication, and control is ever-increasing. Novel methods to address the coupling of this infrastructure to the physical components responsible for generation, transmission, and utilization of electrical energy need to be developed. Conventional analysis techniques mainly focus on the effects of faults in the physical components, e.g., power sources and transmission lines. Therefore, faults in the physical components are reasonably well-understood. However, the effects of faults in cyber components and their coupling with the physical infrastructure are not clear and require additional research.

Research Objectives

- Develop a taxonomy of possible faults in the cyber components pertaining to power systems.
- Investigate the effects of GPS spoofing on PMU time synchronization.
- Demonstrate the feasibility of an attack through hardware setup.
- Characterize potential PMU misbehavior due to faults in the cyber structure.
- **Smart Grid Application Area:** This research will allow for a more secure and reliable power grid.

Technical Description and Solution Approach

- The synchronization of PMUs depends on satellite GPS signals. Therefore, spoofing of these signals constitutes an attack on data of the PMUs.
- The feasibility of such an attack is being demonstrated through MatLab simulation. The problem is cast as an optimization problem in which the objective is maximum phase error in the PMU data.
- The effects of losing time synchronization of PMU data on fault detection algorithms are being investigated.
- Based on the applications of PMU data, the impact of corrupted PMU data on power system dynamic performance and reliability is being characterized.

Results and Benefits

- Different methods of attack on PMU synchronization are being developed and simulated.
- Demonstration of the feasibility of these attacks is allowing for better preparedness against security threats.
- Simulation of GPS spoofing has been carried out in MatLab.
- Potential PMU misbehaviors are being identified and characterized. The possible causes of misbehavior include hardware faults, filtering algorithm implementation errors, data communication failures, and/or GPS signal spoofing.
- Effects of spoofing on applications in which PMU data are used are being investigated. A Thevenin-equivalent model to qualify the impact of PMU misbehaviors is being developed and simulated.
- Simulations show that spoofing can cause erroneous results in voltage-stability algorithms utilizing PMU data.
- **Technology Readiness Level:** Ongoing research.

Researchers

- Alejandro D. Domínguez-García, aledan@illinois.edu
- Xichen Jiang, xjiang4@illinois.edu
- Brian Harding, bhardin2@illinois.edu
- Jiangmeng Zhang, jzhang67@illinois.edu

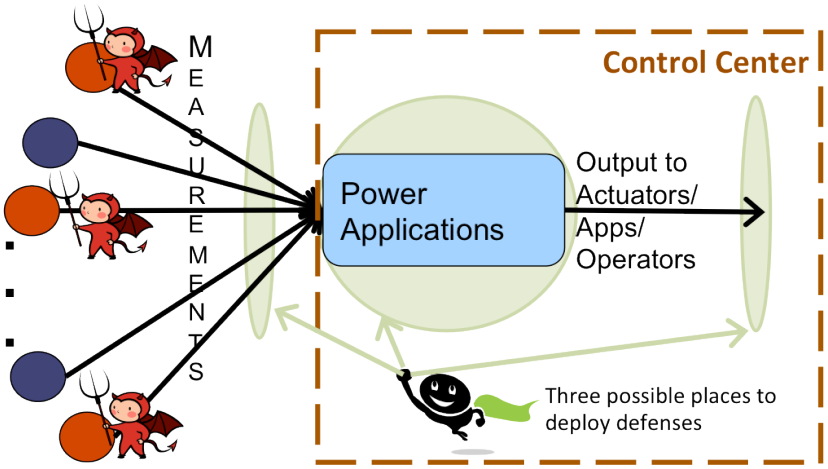
Security and Robustness Evaluation and Enhancement of Power System Applications

Overview and Problem Statement

Power system operations rely on a multitude of sensor data from remote measurement devices at substations and in the field. Sensor data are communicated back to the control center using a variety of protocols (e.g., DNP3, Modbus) and communication media. The remote sensors and the communication channels over which their readings are communicated present an attack surface for adversaries wanting to disrupt power system operations. While power system applications are typically robust against erroneous sensor data and data loss due to accidents and failures, they are typically not robust against coordinated malicious sensor data modification. In this work, we study impacts of malicious sensor data manipulation in power systems, and research mitigation and defense strategies. In general, the integrity of power system operations depends on the underlying cyber infrastructure, and we research ways to explicitly take the state of the cyber system into account for power system operations in order to improve the robustness of power systems to cyber attacks.

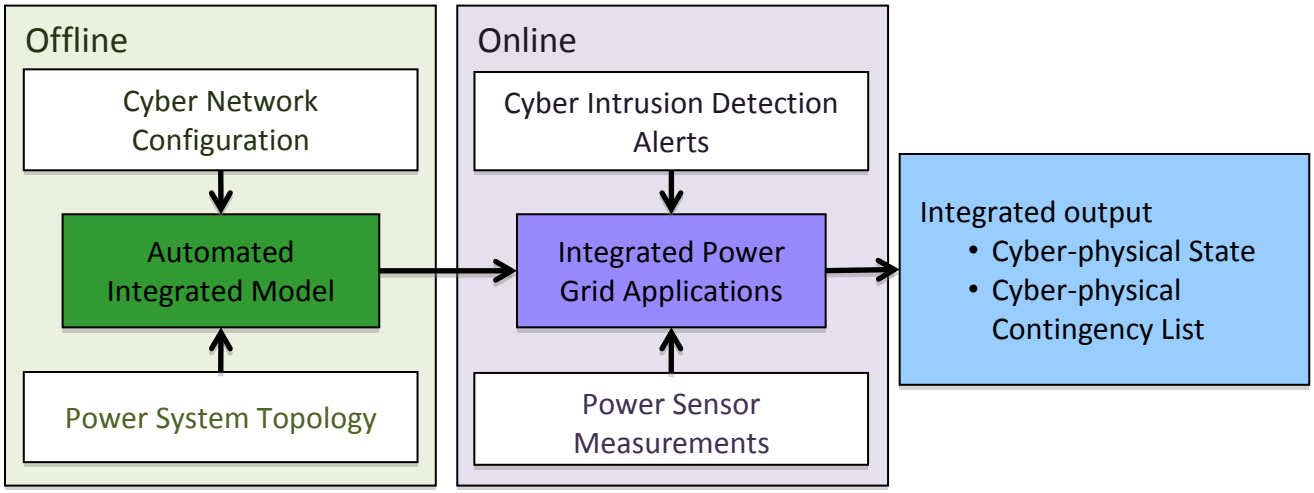
Research Objectives

- Study the security and robustness of power applications in the face of malicious sensor data manipulation attacks.
- Develop effective and cost-efficient defenses against malicious sensor data manipulation attacks.
- Develop effective ways to consider security state of the cyber infrastructure in power system operations to improve their robustness to cyber attacks.
- Evolve a process to include security and robustness considerations during the power system application design phase.
- **Smart Grid Application Area:** Risk and security assessment.



Technical Description and Solution Approach

- Understand the behavior of power system applications and analyze their robustness in the presence of malicious data modification.
- Leverage the physical properties (e.g., topology) of the underlying electrical network along with cryptographic and other cyber security mechanisms to design effective and cost-efficient security schemes.
- Understand the dependency of power system operations on the security state of the underlying cyber infrastructure.
- Design effective ways to combine and use knowledge about both cyber infrastructure security state and power system electrical state during power system operations for increased robustness against cyber attacks.



Results and Benefits

- For DC state estimation, we showed that protecting a set of *basic measurements*, that is, those necessary for observability, is necessary and sufficient for detecting a class of false data injection attacks.
- Proposed a topology perturbation-based approach for defending against false data injection.
- Identified ways to inject false data into power flow computations; are investigating defenses.
- Proposed a state estimator that leverages both cyber and power system information and is more robust against false data injection.
- Proposed an approach to analyze the impact of and rank cyber contingencies.
- The outcomes of this project will provide:
  - Robustness characterization of specific power applications with respect to malicious data modification attacks and mechanisms to improve the robustness of those applications.
  - Guidance on where to focus an organization's security budget to secure power grid infrastructure.
  - Input to operators and incident response engines as to when an application should be considered compromised.
- A longer-term benefit of this project would be the evolution of a process that includes security and robustness considerations during application design for future power applications.
- **Partnerships and External Interactions:** Collaborating with researchers at KTH Royal Institute of Technology in Sweden; collaborating with TCIPG alumni at PowerWorld and the University of Miami.
- **Technology Readiness Level:** This technology is currently in its infancy (research and design phase).

Researchers

- Rakesh B. Bobba, rbobba@illinois.edu
- Robin Berthier, rgb@illinois.edu
- Erich Heine, eheine@illinois.edu
- Kate Morrow, morrow4@illinois.edu
- Will Niemira, niemira2@illinois.edu
- William H. Sanders, whs@illinois.edu
- Pete Sauer, psauer@illinois.edu
- Tom Overbye, overbye@illinois.edu
- External Researchers: Kate Davis & Matt Davis (PowerWorld), Saman Zonouz (Univ. of Miami)
- Past Researchers: Miao Lu, Zheming Zheng, Qiyan Wang, Himanshu Khurana, and Klara Nahrstedt

Overview and Problem Statement

Renewable generation, energy storage, and demand response are key components of the Smart Grid vision. Effective use of these resources in future grids will require appropriate control architecture. This research focuses on investigations of control strategies for power grids with significant penetration of renewable generation, energy storage, and demand response resources. The goal is to understand how energy storage and demand response can provide ancillary services such as operational reserves and frequency regulation, thereby facilitating the use of volatile renewable generation in highly complex and constrained power networks. This understanding can lead to robust control schemes for future power grids.

Research Objectives

- Evaluate impacts of renewable generation, energy storage, and demand response on markets and operations.
- Investigate dispatch of energy storage and demand response resources to facilitate deployment of renewable generation.
- Explore the potential for storage and demand response resources to provide ancillary services in constrained power networks with high-penetration renewable generation.
- **Smart Grid Application Area:** Results can guide new policies, planning, and operations, thereby smoothing the transition towards the Smart Grid.

Technical Description and Solution Approach

- Questions of interest: How can energy storage and demand response be used in conjunction with renewable generation to provide services such as operational reserves, load following, and frequency regulation?
- Stochastic models for generation, demand, and storage that allow explicit consideration of impacts of volatility, dynamics, and uncertainty in both operations and markets are being used. Modeling abstractions for energy storage and flexible loads (e.g., HVACs and refrigerators), which explore similarities between both resources, have been developed.
- Operational tools for dispatch of power grids with renewable generators, flexible loads, and energy storage resources are being developed. Analytical techniques from approximate dynamic programming, reinforcement learning, and model predictive control are being used.
- Simplified models of flexible loads, such as HVAC loads of commercial buildings, are being developed for control synthesis in the context of extracting ancillary services from these loads.

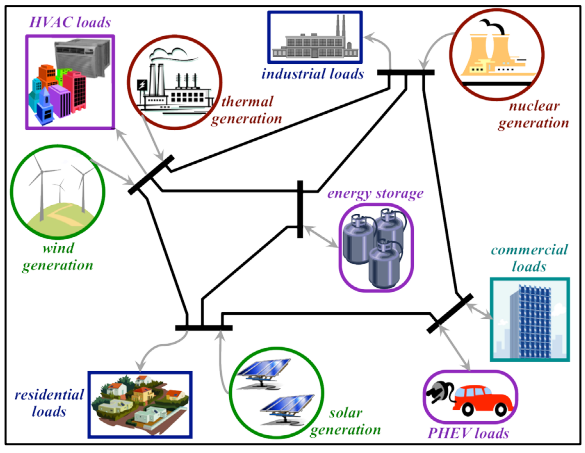


Figure 1: Conceptual illustration of the key Smart Grid resources considered in the analysis

Results and Benefits

- A conference paper detailing the control synthesis for energy storage and demand response resources with reinforcement learning techniques tuned with real world data has been presented at the IEEE PES General Meeting, July 2012.
- Computationally efficient control algorithms have been developed for operating power grids with renewable generators, flexible loads, and energy storage units. The proposed control algorithms are derived by combining reinforcement learning (RL) techniques with model predictive control (MPC). The application of the proposed algorithms to the dynamic economic dispatch problem has been extensively studied; simulation studies indicate that combining MPC with RL can significantly reduce the computational complexity of the dynamic dispatch problem.

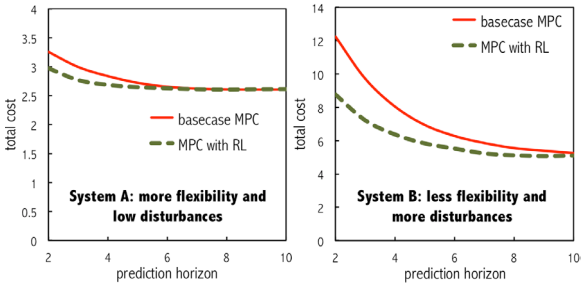


Fig. 2: Numerical studies demonstrate the effectiveness of the proposed algorithm in reducing computational requirements.

- The potential flexibility in the power consumption of heating, ventilation, and air conditioning (HVAC) loads of commercial buildings has been investigated to enable extraction of ancillary services from these loads. Simple control strategies, such as manipulation of the fan speed, have been studied in the context of regulation services. Simulation studies indicate that HVAC loads can be manipulated without discomfort to building occupants if the bandwidth of regulation is suitably constrained. Also, control of fan speeds of "suitable" HVAC loads alone can provide up to 6 GW of regulation reserves, which constitutes about 70% of the total requirements in the United States.

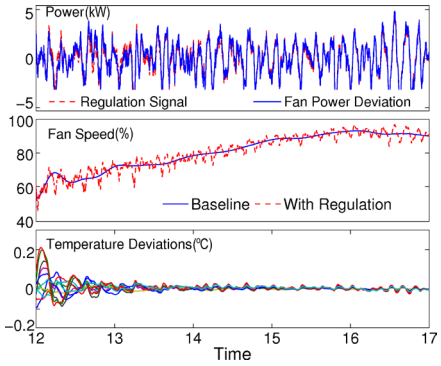


Fig. 3: Simulations on a high-fidelity model of a building and its HVAC demonstrate the impacts of fan speed control; the fan power consumption can be suitably modified to track the regulation signal sent by the grid operator.

- **Partnerships and External Interactions:** Anupama Kowli was a summer intern at PNNL.

Researchers

- Anupama Kowli, akowli2@illinois.edu
- Sean Meyn, meyn@ufl.edu

Industry Collaboration

- PNNL

Synchrophasor Data Quality

Overview and Problem Statement

It is envisioned that synchrophasor data will enable real-time power grid state measurement, assessment, and control. The nascent integration of synchrophasor data has yet to gain widespread trust among power system operators, because of reliability, availability, and quality issues.

The "Synchrophasor Data Quality (SDQ)" research activity is investigating the sources, effects, and implications of absent or erroneous synchrophasor data. The research is pursuing a fundamental understanding of real-time synchrophasor measurement challenges, synchrophasor data characteristics (reliability[1], availability[2], and quality[3]), methods for detecting defective synchrophasor data, and the implications of and remedies for defective synchrophasor data.

Research Objectives

- Gain a fundamental understanding of synchrophasor measurement challenges.
- Characterize synchrophasor data (reliability, availability, and quality).
- Investigate synchrophasor data utility for "Smart Grid" applications.
- Investigate the relationships between synchrophasor and state estimator data.
- Identify methods for detecting faulty synchrophasor data.
- Investigate implications and remedies for faulty synchrophasor data.

Technical Description and Solution Approach

The Synchrophasor Data Quality initiative has developed a research partnership with the Midwest Independent Transmission System Operator (MISO) to pursue the research objectives. MISO has been studying the synchrophasor data received from its stakeholders to identify error sources.

Figure 1 depicts nominal synchrophasor data flow from the point of measurement to the control room and data archive with four levels and connecting transmission paths. Each level has an identifiable role in generating, processing, and forwarding data to meet power system requirements, and as such becomes a possible point of failure. Attribution of defective synchrophasor data sources and corresponding error rates is key to prioritizing efforts to improve data quality. Table 1 (see other side) shows a sampling of MISO's identified error sources; it also classifies the errors by type and identifies levels within the synchrophasor data flow in which the error can occur.

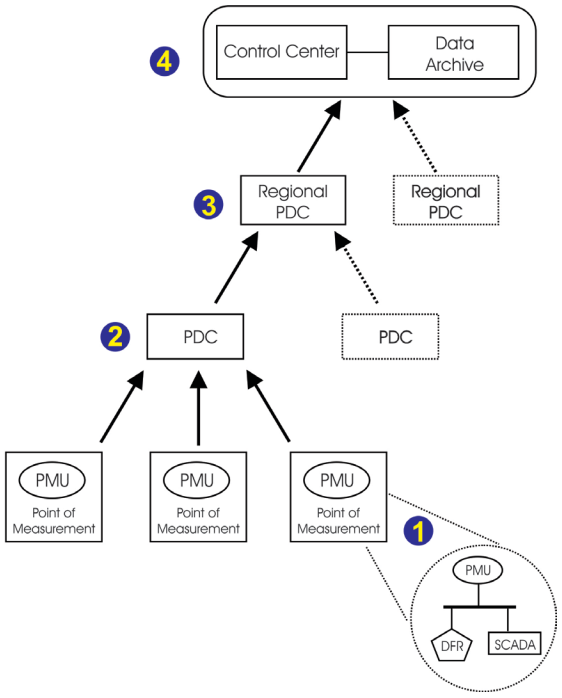


Figure 1. Nominal synchrophasor data flow from the point of measurement to the control center and data archive

[1] *Reliability:* the probability that an item (allowing for calculation of the reliability of components or the system as a whole) will function without failure under stated conditions for a specified amount of time. *IEEE Standard Dictionary of Electrical and Electronics Terms, 1996.*

[2] *Availability*: the fraction of a time period that an item is in a condition to perform its intended function upon demand. *IEEE Standard Dictionary of Electrical and Electronics Terms, 1996.*

[3] *Quality*: the degree to which an item, function, or process satisfies the user's needs. *Reliability, Quality, and Safety for Engineers,* CRC Press.

The SDQ Activity and MISO have developed a 3-phase research concept:

- Phase 1: Synchrophasor Data Quality Assessment.
- Phase 2: Development of Error Mode Study Plans.
- Phase 3: Completion of Error Mode Studies.

Other SDQ Activity efforts:

- Building and testing an "open-box" synchrophasor measurement device (also known as a *phasor measurement unit*, or *PMU*); understanding the challenges of measuring, processing, synchronizing, and integrating synchrophasor data. (In collaboration with National Instruments.)
- Researching the application of synchrophasor data to power system Thevenin-equivalent circuit representations.

TABLE I. Identified Error Sources and Proposed Error Type Classifications

Error Source	Level(s)	Error Type
Status code errors	1, 2, 3	Data Processing
Data streams disordered/shifted in processing	1, 2, 3	Data Processing
Loss of PDC configuration	2, 3, 4	Data Processing
Improperly configured PMUs (window length/windowing method)	1	Digital Signal Processing
Frequency calculation discrepancies (C37.118.2005)	1	Digital Signal Processing
Quality of metering	1	Equipment Specification
Accuracy issues (CT/PTs not properly rated for application)	1	Equipment Specification
Calculation uncertainty; vendor equipment operating differences	1	Equipment Specification
Metering locations separated by breakers	1	Installation
Meters not installed at recorded locations	1	Installation
PMU data streams not named according to system policies	1	Installation
Asynchronous local behaviors (e.g., DC bias injections during solar storm)	1	Measurement
Malformed network packets	2, 3, 4	Network Failure
Network data loss	2, 3, 4	Network Failure
Mislabeled phasor data streams	1, 2, 3	PMU Configuration
Differences between PMU manufacturer calculation approaches	1	PMU Standards

Results and Benefits

- Preliminary synchrophasor data error list identified.
- Research partnership with MISO established; research concept developed and agreed to.
- Built prototype "open-box" PMU; additional refinements required.
- Identified and characterized fundamental challenges to computing power system Thevenin equivalents from synchrophasor data measurements.

Researchers

- Karl Reinhard, reinhrd2@illinois.edu
- Prof. Pete Sauer, psauer@illinois.edu

Industry Collaboration

- Jim Kleitsch, American Transmission Company (ATC)
- Kevin Frankeny, Midwest Independent Transmission System Operator (MISO)
- Andrew Watchorn, National Instruments
- Rick Smith, Ameren Corporation
- North American Synchrophasor Initiative (NASPI) Working Group
- Paul Myrda, Electric Power Research Institute (EPRI)

Testbed-Driven Assessment: Experimental Validation of System Security and Reliability

Overview and Problem Statement

The objective of this project is to develop methods and tools for evaluating security and reliability protection mechanisms for the next-generation power grid. Specifically, this research will focus on development of a framework for error diagnosis and experimental validation of system/application resiliency to errors and attacks. In particular, we want 1) to experimentally evaluate the impact of accidental errors on microprocessor-based power grid equipment, and 2) to develop and experimentally validate error/attack detection and recovery mechanisms.

Research Objectives

- Experimentally study the impact of errors on next-generation microprocessor-based power grid equipment.
  - Characterize error behavior and failure severity due to transient errors in the power grid equipment.
  - Understand error propagation and its impact from one piece of equipment to other connected equipment.
  - Develop and test error detection and recovery techniques to address the weaknesses discovered.
- Develop and experimentally validate error/attack detection and recovery mechanisms.
  - Develop practical and effective detection and recovery mechanisms.
  - Experimentally assess the coverage and overhead of the developed mechanisms.
  - Provide experimental result feedback to industry partners as potential solutions to vulnerabilities discovered.
- **Smart Grid Application Area:** To uncover possible security vulnerabilities in current power grid applications and investigate reliability and security protection mechanisms/strategies.

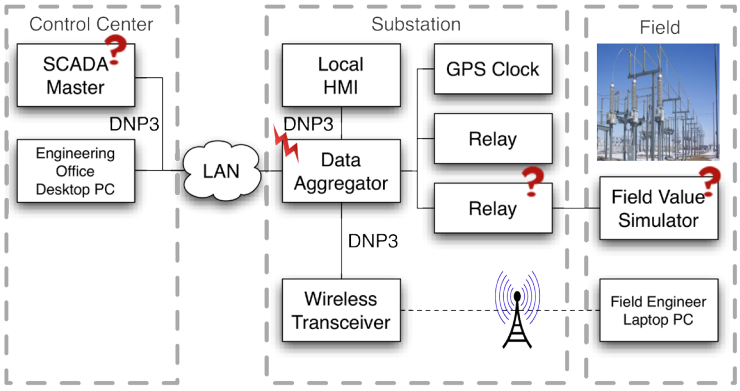


Figure 1: Testbed Setup

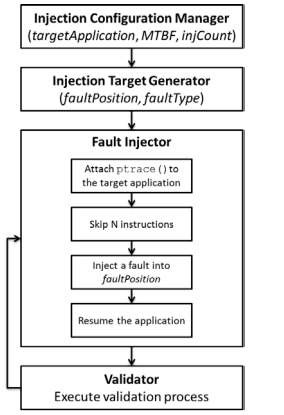


Figure 2: Fault Injection Process

Technical Description and Solution Approach

- **Software-implemented Fault Injection (SWIFI)** is used to evaluate and characterize the behavior of power grid equipment in the presence of transient errors and malicious attacks.
- Different devices in the TCIPG testbed are coordinated to mimic the working scenario of a power grid (Figure 1).
  - The *Field Value Simulator* simulates field transmission line voltage and current value and the line breaker.
  - The *Relay* reads the voltage and current value from the *Field Value Simulator*.
  - The *Data Aggregator* collects all the sensor data within the substation.
  - The SCADA master pulls the substation data from the *Data Aggregator*.
  - The SCADA master can send control signals to control *Relay* (e.g., open/close breaker).
- A fault injection framework based on `ptrace()` is being developed to automate the fault injections to the critical applications (see Figure 2).

- Three critical applications running on the *Data Aggregator* (*DNP3 Client*, *DNP3 Server*, *Monitor App*) have been chosen as targets for fault injections.

Results and Benefits

- Experimentally showed that silent data corruption (SDC) could cause an operator in the *Control Center* to lose control over the equipment in the substation. Our fault injection study on the Data Aggregator showed that if a fault occurs in the DNP3 client/server software, there is a 7 to 13% chance that the fault will result in silent data corruption (see Figure 3), i.e., the DNP3 client/server applications apparently stay alive (e.g., can still accept commands from the *Control Center*) but do not operate correctly.
- Error propagation (from an application to the operating system) can lead to deadlocks of system resources. For instance, misbehaving DNP3 client/server software (e.g., cannot pass commands to or acquire data from the relay) may lock system services, such as the *kill* command. As a result, a forced reboot of the device is required to restart the offending application.
- **Partnerships and External Interactions:** Real Time Power System Simulation, Schweitzer Engineering Lab.
- **Technology Readiness Level:**
  - Testbed infrastructures simulating communication from the Control Center to Substation are in place.
  - Fault/error injector to create transient errors/memory corruption attacks has been developed.
  - Fault/error injector to spoof the GPS clock has been developed.
  - Prototype of bad-data detection algorithms has been developed for evaluation.
  - In the process of implementing a detector for silent data corruption for DNP3 client/server software on SEL-RTAC.

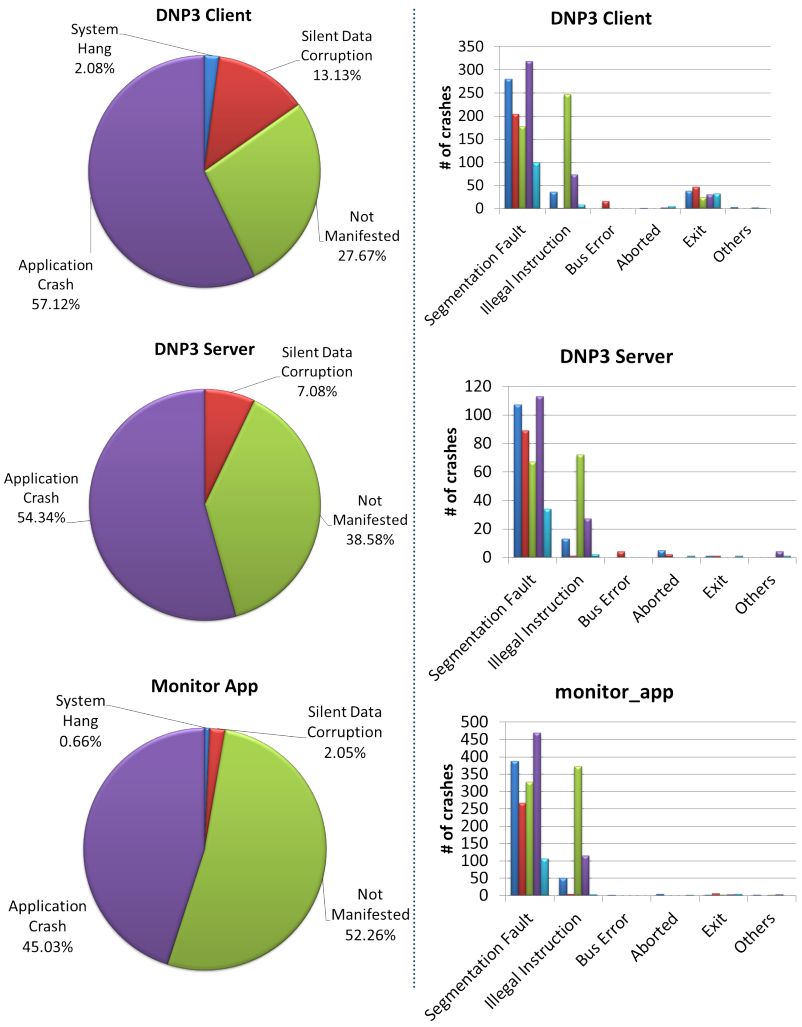


Figure 3: Outcome & Crash Causes of Injected

Researchers

- Daniel Chen, dchen8@illinois.edu
- Kuan-Yu Tseng, ktseng2@illinois.edu
- Zbigniew Kalbarczyk, kalbarcz@illinois.edu
- Ravishankar Iyer, rkiyer@illinois.edu

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Tools for Assessment and Self-Assessment of 802.15.4/ZigBee Networks

tcipg.org

Overview and Problem Statement

Operators of wireless networks must have cheap, commodity tools for assessing security of their networks. Lack of such tools leads to unnecessary exposure and false assumptions regarding stability of the networks, as the experience of 802.11/Wi-Fi has amply shown. At the very least, a network operator must know how much of his or her RF is showing and what it looks like to an attacker with a sufficiently powerful antenna and the ability to emit and inject wireless frames of the protocols used by the network. Our ***Api-do*** tools give the operators this functionality with commodity USB peripherals and software that runs on a regular Linux laptop.

Research Objectives

- Make 802.15.4/ZigBee wireless network assessment tools as easy and efficient as those for 802.11/Wi-Fi.
- Enable asset owners to survey their network footprint ("wardrive" their networks).
- Enable asset owners to test the effects of crafted frame injection and reflexive/selective jamming.
- Facilitate the exploration of the 802.15.4/ZigBee attack surface.
- **Smart Grid Application Area:** 802.15.4/ZigBee is the networking technology of choice for SCADA systems, home automation, and smart meter connectivity.

Technical Description and Solution Approach

- Api-do tools use commodity digital radio platforms built on chips such as Chipcon CC2420 and similar ones, with custom firmware (based on Travis Goodspeed's GoodFET). Frames received by digital radio chips are processed by a microcontroller on the peripheral (such as the MSP430 or Atmel AVR). This allows fast interaction with the target network, which is difficult to achieve with more expensive software-defined radios.
- "**Security does not improve until tools for practical exploration of the attack surface become available**" – Joshua Wright.

Results and Benefits

- First generation of tools released, presented at security practitioner conferences, and used in assessments.
- Important signaling vulnerability exposed in 802.15.4 digital radios, presented at USENIX WOOT 2011.
- **Partnerships and External Interactions:** Contributions and improvements to KillerBee tools (Joshua Wright), Scapy suite, enabled applied ZigBee research at Air Force Institute of Technology.
- **Technology Readiness Level:** Beta, hardware prototype test run completed, tools in ongoing development.

Researchers

- Sergey Bratus, sergey@cs.dartmouth.edu
- Ryan M. Speers, Ricky Melgares, team@riverloopsecurity.com

Industry Collaboration

- Travis Goodspeed, Joshua Wright, other contributors

TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Trustworthiness Enhancement Tools for SCADA Software and Platforms

tcipg.org

Overview and Problem Statement

Our ultimate goal is to preserve the trustworthiness of the various control systems being rolled out as part of the smart grid. These systems present a unique challenge from an IT perspective, since they a) are fairly static devices, b) are expected to remain in service for up to several decades, and c) must perform their prescribed tasks in the face of both accidents and malicious intrusions. On top of all that, any security solutions installed on such systems must be lightweight enough not to get in the way of the system's primary function.

To address those issues, we have built a number of flexible, lightweight security systems that can live at many different levels inside a device, ranging from process-level protection to low-level network message encryption. The complete list of solutions can be found below.

The Stack of Trust: A Multi-Layered Protection Strategy

Trust Stack Level	Our Solution
Process-Level Mediation	ELFBac: An instrumentation system for programs that allows users to isolate and secure pieces of a binary without needing to rewrite the original program. *Status: In development - looking for collaborators!*
System Call Mediation	Behavior-Based Policy: Policy languages that clearly identify trustworthy behaviors, and use techniques such as context-dependent goals and isolation primitives to enforce the policy. *Status: In development - looking for collaborators!*
Kernel Host Intrusion Detection System	Autoscopy Jr.: An intrusion detection system that lives within the OS kernel itself, monitoring for control-flow anomalies while imposing minimal overhead. *Status: Complete*
Hardened Kernel	grsecurity/PaX*: A set of kernel hardening patches that include additional OS protection mechanisms. *Status: See * note below table*
Custom Trapping Scheme	FlexTrap: A system that allows for variable-sized caching in the Translation Lookaside Buffer (TLB) of a system, letting users define their memory accesses to be as coarse or granular as needed. *Status: In development - looking for collaborators!*
Kernel Drivers	CrossingGuard: An application of traditional IP network defenses to the USB interface. *Status: In development - looking for collaborators!*
Network Hardware	Predictive YASIR: A low-latency message authentication system that tries to predict the plaintext content of messages and pre-send the ciphertext before receiving the entire message. *Status: Complete*

*Note that grsecurity/PaX is © Open Source Security, Inc., and NOT a Dartmouth product, but rather a set of patches that are freely available at http://grsecurity.net.

Results and Benefits

- We have developed an ELFBac prototype and demonstrated its potential by using it to protect sensitive data within a parsing library, even after a bug in the library had been exploited.
- We evaluated the performance impact of Autoscopy Jr. on a non-embedded kernel configuration, and found that after our profiler was applied, it imposed less than a 5% overhead on our benchmark tests. We have since provided the program to Schweitzer Laboratories, which used it as the inspiration for their own protection system for their product line.
- In testing using the Modbus protocol, Predictive YASIR offered a significant latency improvement over both its non-predictive YASIR predecessor and the AGA SCM bump-in-the-wire device.
- **Technology Readiness Level:** Varies by product; see table above.

Researchers

- Julian Bangert, julian@cs.dartmouth.edu
- Sergey Bratus, sergey@cs.dartmouth.edu
- Peter C. Johnson, pete@cs.dartmouth.edu
- Jason Reeves, reeves@cs.dartmouth.edu
- Rebecca “bx” Shapiro, bx@cs.dartmouth.edu
- Anna Shubina, ashubina@cs.dartmouth.edu
- Sean W. Smith, sws@cs.dartmouth.edu
- And many others! (ask one of the above for contact info)

Industry Collaborators

- Schweitzer Engineering Laboratories (Autoscopy Jr.)

Cross-Cutting Efforts

and

Incubator Research Activity

Cross-Cutting Efforts

Education and Engagement Lead: Jana Sebestik ..... sebestik@illinois.edu

Testbed Initiatives Leads: David Nicol, Tim Yardley ..... dmnicol@illinois.edu
yardley@illinois.edu

Industry Interaction and Technology Transition Lead: Pete Sauer ..... psauer@illinois.edu

Incubator Research Activity

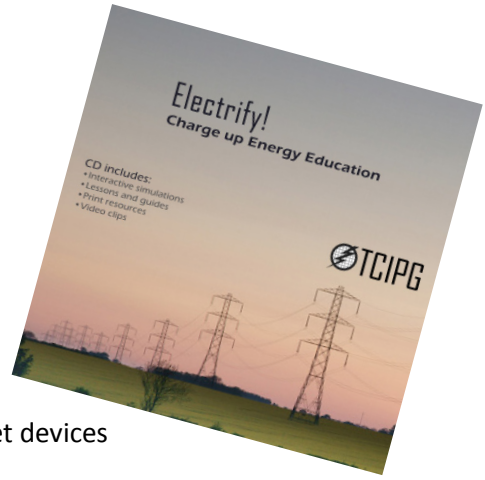
TCIPG Education and Engagement

Overview

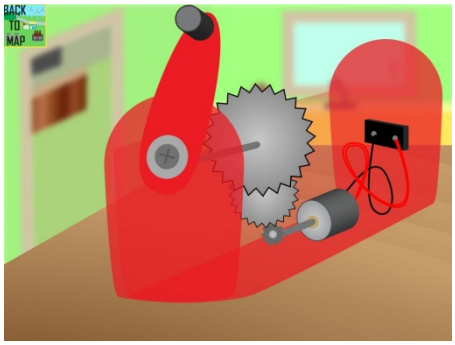
Members of the TCIPG Education team work with teachers, informal educators, and other TCIPG researchers to develop a variety of educational opportunities. Our activities are designed to engage learners of all ages. We develop curriculum materials that involve young people in virtual power system simulations. We have produced an interactive app for younger children using the iPad and other touch tablet devices. Our materials and hands-on activities provide information about the science of electricity and the importance and workings of current and future electricity generation and delivery systems. They are also designed to engage students who may pursue careers in related industries. TCIPG Education curriculum materials are featured in Project Lead the Way's pre-engineering curriculum. TCIPG engages in public outreach through participation in the annual Engineering Open House at the University of Illinois at Urbana-Champaign, various conferences, exhibits, and symposiums, and through the ongoing interactive "Mission Smart Grid" exhibit at the Orpheum Children's Science Museum in Champaign, Illinois.

Objectives

- Link researchers, educators, students, and consumers in efforts to transition to a more modern, secure, and resilient electrical system.
- Create interest in related STEM careers and provide an engaging, interactive curriculum, appropriate for middle-school-level and older students, featuring:
  - time-sensitive pricing
  - demand-side management
  - impacts of plug-in hybrid vehicles
  - distributed generation
  - technologies that increase energy efficiency and reliability
  - concepts related to communication networks



- Create an interactive app, Tesla Town, for the iPad and other touch tablet devices that is appropriate for young learners.
- Disseminate hands-on activities and smart grid curriculum.
  - IEEE Science Kits for Libraries partnership grant
  - Champaign School District Math Science Partnership



- Create smart grid picture resource cards.
- Define best and worst workplace practices and make these available to the appropriate audiences.
- Illustrate issues necessary for consumer acceptance and use of smart grid technologies.
- Create consumer information modules and consumer guidelines for distributed generation and energy management systems.
- **Smart Grid Application Area:**
  - Reach the wider audience of educated citizenry necessary for the successful implementation of smart grid technologies.
  - Educate consumers to use new technologies that allow them to actively manage their energy use and costs.
  - Engage pre-university students who may pursue a related career.

Results and Benefits

- Java applets and curriculum materials.
  - Updates to print materials.
  - Applets converted to html5.
- Interactive app, Tesla Town, for the iPad and other touch tablet devices.
- Partnerships and External Interactions:
  - Exhibit at the Orpheum Children's Science Museum (OCSM)
  - Partnership with Energy Education Council
  - Curriculum connections with National 4-H SET (Science, Engineering and Technology) Initiative
  - Curriculum connections with KidWind and WindWise Education
  - Inclusion in Project Lead the Way pre-engineering curriculum materials

Events

- University of Illinois Engineering Open House, March 9–10, Champaign, IL
- Project Lead the Way Core Training Preparation, March 23–24, Indianapolis, IN
- University of Illinois Public Engagement Symposium, April 18, Champaign, IL
- Toronto Science Rendezvous, May 7, Toronto
- Smart Grid Customer Education Symposium, May 16, San Diego, CA
- Mahomet Library Science Open House, May 20, Mahomet, IL
- 2012 ASEE Annual Conference and Exhibition, June 13, San Antonio, TX
- Project Lead the Way Summer Training, June 17–29, University of Illinois at Urbana-Champaign
- International Society for Technology Educators Conference (ISTE 2012), June 25, San Diego, CA
- Partnership for Enhancing Mathematical Modeling, July 23–August 4, Champaign, IL
- Illinois State Fair, August 9–19, Springfield, IL

Education Team

- Jana Sebestik, sebestik@illinois.edu
- George Reese, reese@illinois.edu
- Zeb Tate, zeb.tate@utoronto.ca
- Quinn Baetz, qbaetz2@illinois.edu
- Jason Mormolstein, jmormol2@illinois.edu
- Andrew Gazdziak, gazdzia1@illinois.edu

Testbed Overview

Overview and Problem Statement

- How does one provide a large-scale, realistic, end-to-end power grid experimentation platform that is both repeatable and flexible to cover both legacy and emerging research?
- How does one leverage real equipment, simulation, and emulation to provide the necessary capabilities?
- How does one programmatically integrate, control, and interact with power grid equipment that was not designed with that in mind?

Research Objectives

- Provide for experimental support/integration of TCIPG projects.
- Provide a simulation and emulation environment with real hardware and software used in the power grid.
- Serve as a national resource for experimental work in research and analysis of trustworthy power grid systems.
- Span transmission, distribution & metering, distributed generation, and home automation and control, providing true end-to-end capabilities.
- **Smart Grid Application Area:** End-to-End.

Technical Description and Solution Approach

- Develop new modeling and evaluation technologies to enhance evaluation capabilities of the testbed.
- Continue to expand the equipment capabilities, features, and functionality through strategic integration of both software and hardware.
- Develop integration glue to seamlessly integrate power grid equipment and software into the testbed by combining simulation, emulation, and real equipment.
- Leverage existing and emerging research from other areas when the testbed effort can benefit from it.

Results and Benefits

- Real-time Immersive Network Simulation Environment (RINSE): large-scale network simulation.
- Virtual Power System Testbed: cyber-physical combination of simulation, emulation, and real equipment.
- Network Access Policy Tool (NetAPT): policy tool to evaluate network access paths and verify compliance with a global policy.
- **Partnerships and External Interactions:**
  - Enabling smart grid research and transition of technology.
  - Leveraged for other industry interactions and projects.
- **Technology Readiness Level:** Extending capabilities, but fully functional and in-use.

Capabilities

- Full end-to-end “Smart Grid” capabilities.
- Real, emulated, and simulated hardware/software.
- Real data from the grid, industry partners, etc.
- Power simulation, modeling, and optimization.
- Network simulation and modeling.
- Visualization.
- WAN/LAN/HAN integration and probes.
- Security assessment tools (e.g., static analysis).
- Protocol assessment tools (e.g., harnesses, fuzzing).

Hardware and Software

- RTDS, PowerWorld, PSSE, PSCAD, DSAtools Suite, DynRed.
- RINSE, tstBench, LabView, OSI PI, OSIi Monarch, SEL suites.
- GPSs, substation comps, relays, testing equipment, PLCs, security.
- RTUs, F-Net, ICS firewalls, inverters, DAQs, oscilloscopes, multimeters, gigabit firewalls and switches, embedded devices.
- Home EMS, monitoring devices, Zigbee, automation.
- Display wall, visualization platforms, training.
- Mu Dynamics, Fortify, security research tools.
- DETER/Emulab integration and extension.

Use Cases

- Provide a multifaceted approach to security through testbeds, education and training, field testing, and tool creation.
- Facilitate collaboration among researchers and industry towards creation of more resilient critical infrastructure.
- Facilitate rapid transition and adoption of research by industry.
- Provide positive real-world impact through engagement.

Researchers

- Tim Yardley, yardley@illinois.edu
- David Nicol, dmnicol@illinois.edu
- William H. Sanders, whs@illinois.edu
- Jeremy Jones, jmjone@illinois.edu
- Erich Heine, eheine@illinois.edu

Industry Donations

Byres Security, Endace, GE, InStep Software, Mu Dynamics, Open Systems International (OSI), OSIsoft, PowerWorld, Schweitzer Engineering Lab, Siemens AG, Trilliant, Bayshore Networks, Nuclear Regulatory Commission, Space Time Insight, Electric Power Group, Itron, Sisco, National Instruments

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

New Idea: Cognitive Bias and Demand Response

Overview and Problem Statement

Today's power grid faces a number of challenges that threaten its reliability, both on the demand side (large additional loads, such as electric vehicles) and on the supply side (renewable energy sources with variable availability). Up to this point, utilities have responded with demand response programs, which use lower prices as a motivator for consumers to reduce their electric loads and shift them to off-peak periods.

In a price-based demand response program, a utility will often provide consumers with time-based electricity prices, to allow the consumer to make educated usage decisions. However, the utility makes several assumptions that are vital to the success of the program, namely:

- Consumers will draw accurate conclusions from the data and how our technology shows the data to them.
- Consumers will make rational decisions based on that information; in this case, a decision to minimize costs.
- Consumers will be able to use the infrastructure provided by the technology to implement their decisions correctly.

However, those assumptions are contradicted by a large body of psychology work, which offers a list of cognitive biases and misperceptions that affect the decision process of the human mind. For example, biases may skew consumers' view of a scenario, leading them to make decisions that might be optimal, but only for a scenario other than the one that is actually happening; or they may mislead consumers into selecting choices that do not actually represent their decisions.

Since demand response programs aim to maintain the reliability of the power grid during peak-load periods, an attacker could take advantage of these biases to reduce the grid's reliability. For example:

- By changing the way information is displayed to the consumer, an attacker could cause a consumer to draw incorrect conclusions from his or her data.
- By manipulating consumers' price tolerance, or altering their view of their electricity usage, an attacker could reduce the load-cutting capacity of a demand response program.
- By convincing consumers to participate in load-reduction programs despite not being able to reduce their load enough in reality, an attacker could induce an overestimate of a program's effectiveness. When such a program is then called upon during a peak-load period, it would not be as effective as grid operators hope, and could lead to overloaded lines and, potentially, blackouts.

This activity aims to identify some of the cognitive biases that arise in a demand response scenario, determine how they influence consumers' choices, and find ways to mitigate them and ensure that demand response programs achieve their desired results.

Research Objectives

- Identify the cognitive biases that may affect consumers in a demand response scenario.
- For every bias identified, determine the appropriate response:
    - Can we counteract its effects?
    - Can we use the bias to influence consumers in the desired direction even more?
- **Smart Grid Application Area:** The consumer side of demand response programs.

Research Plan

- Conduct user studies using an example demand response scenario, and identify the following:
  - How do consumers "use" current demand response programs? Do they interpret the information given to them in the way the utility expects, and can they implement their preferences properly?
  - What biases come into play in a typical demand response scenario? How do they affect a consumer's decision-making?
  - How do different displays of the same information affect a consumer's decision?
- Determine how the cognitive biases that appear in the user studies can be incorporated into current demand response programs and/or models.
- Try to identify the best way to give information to consumers such that they behave in the way the utility expects/desires.
- **Technology Readiness Level:** We are in the initial exploratory phase of this activity.

Researchers

- Jason Reeves, reeves@cs.dartmouth.edu
- Sean Smith, sws@cs.dartmouth.edu

Industry Collaborators

- Your name here! (Contact us if you would be interested in collaborating on this work.)

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security