TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Research Activity Fact Sheets

November 2014

UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
TCIPG.ORG | FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

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

Overview of the TCIPG Project

A Stronger, More Resilient Power Grid

Our quality of life depends on the continuous functioning of the nation's electric power infrastructure. That, in turn, depends on the health of an underlying computing and communication network infrastructure that is at serious risk from malicious attacks on grid components and networks, as well as from accidental causes, such as natural disasters, misconfiguration, or operator errors.

The Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project, a unique partnership of four academic institutions, was formed to meet those challenges. We continually collaborate with national laboratories and the utility sector to protect the U.S. power grid by significantly improving the way the power grid infrastructure is designed, making it more secure, resilient, and safe.

In both technology and impact, TCIPG is a **successful partnership of government, academia, and industry.**

Leading the Way

Back in 2005, the electricity sector was largely "security-unaware." Thanks in part to TCIPG, there has since been **widespread adoption of security best practices.** TCIPG led that transition by conducting breakthrough research, by participating on national panels, and in drafting key documents. However, because the threat landscape continuously evolves, resiliency in a dynamic environment is key. **TCIPG will continue to lead the way.**

TCIPG comprises several dozen researchers, students, and staff from four partner universities: the University of Illinois at Urbana-Champaign, Dartmouth College, the University of California, Davis, and Washington State University. TCIPG faculty, students, and research staff have developed interdisciplinary expertise essential to the operation and public adoption of current and future grid systems. TCIPG brings together **recognized leaders** in power engineering; computer science and engineering; advanced communications and networking; smart grid markets and economics; and Science, Technology, Engineering and Math (STEM) education.

TCIPG is funded by the **Department of Energy** Office of Electricity Delivery and Energy Reliability (DOE-OE) and the **Department of Homeland Security** Science and Technology Directorate (DHS S&T) as part of the DOE Cybersecurity for Energy Delivery Systems (CEDS) portfolio. It is the successor of an earlier project established with funding from the National Science Foundation in 2005. In June 2014, TCIPG entered the fifth year of its five-year period of performance.

TCIPG Research in Smart Grid Resiliency

Countering threats to the nation's cyber systems, including both conventional information technology systems and cyber systems in critical infrastructure, has become a major strategic objective. Smart grid technologies promise advances in efficiency, reliability, integration of renewable energy sources, customer involvement, and new markets. To realize those benefits, the grid relies on a cyber measurement and control infrastructure that includes components ranging from smart appliances at customer premises to automated generation control.

TCIPG research has produced important results and innovative technologies in the following areas:

- Detecting and responding to cyber attacks and adverse events, as well as incident management of these events.
- Securing of the wide-area measurement system on which the smart grid relies.
- Maintaining power quality and integrating renewables at multiple scales in a dynamic environment.
- Advanced testbeds for experiments and simulation using actual power system hardware "in the loop."

Education and Outreach

There is a national shortage of professionals who can fill positions in the power sector. The skills required for smart grid engineers have changed dramatically. TCIPG **graduates are well-prepared** to join the cyber-aware grid workforce as architects of the future grid, as practicing professionals, and as educators.

TCIPG has conducted **short courses** for engineers as well as for DOE program managers. The 2013 offering of our biennial TCIPG Summer School hosted more than 170 participants, including university students and researchers, utility and industry representatives, and government and regulatory personnel.

TCIPG organizes a **monthly webinar** series (first Friday of the month, September–May, 1:00 p.m. Central Time) featuring thought leaders in cyber security and resiliency in the electricity sector. Audiences of more than 100 from industry, government, and academia are typical.

In alignment with national STEM educational objectives, TCIPG conducts **extensive STEM outreach to K-12 students and teachers**. TCIPG has developed interactive, open-ended apps (iOS, Android, MincecraftEdu) for middle-school students, along with activity materials and teacher guides to facilitate integration of research, education, and knowledge transfer by linking researchers, educators, and students.

Collaboration

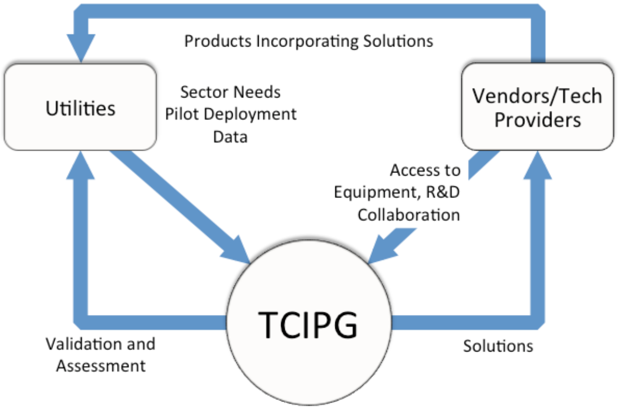
The **electricity industry** in the U.S. is made up of thousands of utilities, equipment and software vendors, consultants, and regulatory bodies. In both its NSF-funded and DOE/DHS-funded phases, TCIPG has actively developed extensive relationships with such entities and with other researchers in the sector, including joint research with several national laboratories.

The involvement of industry and other partners in TCIPG is vital to its success, and is facilitated by an extensive **Industry Interaction Board** (IIB) and a smaller External Advisory Board (EAB). The EAB, with which we interact closely, includes representatives from the utility sector, system vendors, and regulatory bodies, in addition to DOE-OE and DHS S&T.

Partnerships & Impact

While university-led, TCIPG has always stressed **real-world impact and industry partnerships**. That is why TCIPG technologies have been adopted by the private sector.

- Several TCIPG technologies have been or are currently deployed on a **pilot** basis in **real utility environments**.
- A leading equipment vendor **adopted our advanced technologies** for securing embedded systems in grid controls.
- Three **startup companies** in various stages of launch employ TCIPG foundational technologies.


Products Incorporating Solutions
Utilities
Sector Needs
Pilot Deployment
Data
Vendors/Tech Providers
Access to Equipment, R&D Collaboration
TCIPG
Validation and Assessment
Solutions

Leadership

- **Director:** William H. Sanders, whs@illinois.edu
- **Industry Partnerships & Technology Transfer:** Peter W. Sauer, psauer@illinois.edu
- **Testbed Initiatives and Services:** Tim Yardley, yardley@illinois.edu
- **Smart Grid Technologies:** Al Valdes, avaldes@illinois.edu
- **Site Coordinators:** Sean Smith (sws@cs.dartmouth.edu), Anna Scaglione (ascaglione@ucdavis.edu), and Carl Hauser (hauser@eecs.wsu.edu)
- **Research Program Manager:** Cheri Soliday, csoliday@illinois.edu

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 in the Smart Grid

Overview and Problem Statement

In the envisioned smart grid, massive numbers of computational devices will need to authenticate to each other. In the past, such technology would need to rest on a public key infrastructure (PKI) such as X.509. Today, many new cryptographic schemes are being proposed to solve the problem. However, deploying cryptography on such a large entity population—and doing the kinds of things we want the smart grid to do—raises many scalability challenges the community will need to address. Those challenges will only grow with the envisioned "Internet of Things."

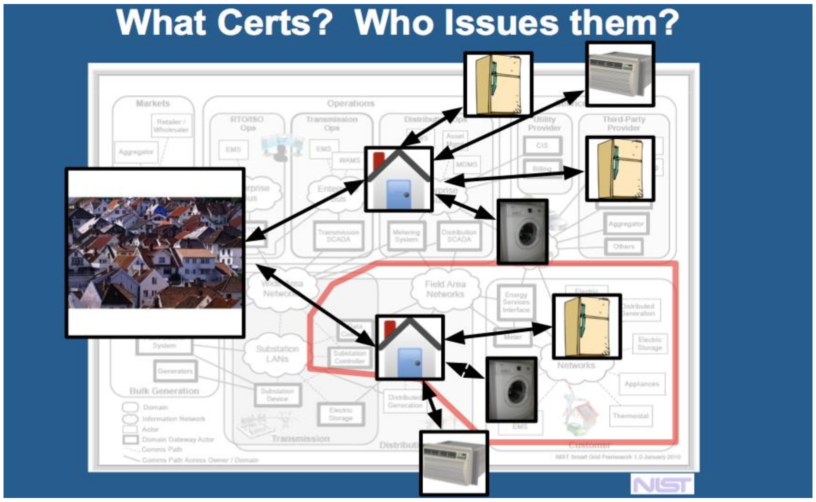
Research Objectives

- Conventional wisdom says to use X.509 PKI in the smart grid. Our goal is to develop high-fidelity multi-scale models and use simulation to look for potential bottlenecks in this trust infrastructure.
- On the transmission side:
    - Real-time is critical.
    - The X.509 PKI standard didn't work on the Border Gateway Protocol (BGP), with only 30k nodes.
    - The transmission side may have 100k nodes in the U.S. alone.
- On the consumer side:
    - Revocation will be necessary.
    - But it didn't work with SSL servers, for which there are only 1 million correctly certified nodes worldwide.
    - There may be 1 billion consumer-side nodes in the U.S. (if we consider large appliances).
    - And there may need to be attribute certificates; that has never been done before at the scale of the smart grid. (What is the identity of an appliance in a household—and what cryptographic infrastructure is necessary to support this?)
- On the modeling and simulation side:
    - Need novel approaches to multi-scale modeling and simulation in order to capture dynamics of extremely large systems with sufficient fidelity.

Technical Description and Solution Approach

- Suppose we're going to solve the problem with the standard building blocks of X.509. At first glance, it would appear that such an implementation would need to go far beyond any current X.509 system in terms of size and functionality. In our initial exploration, we're hoping to validate (or refute) that estimate. By identifying the bottlenecks, we might then suggest ways to keep the problem tractable.
- Previous real-world PKI deployments (deployed on a much smaller scale than the envisioned smart grid PKI) have revealed several practical challenges/costs.
    - Path discovery.
    - Revocation: The number of revoked certificates was orders of magnitude larger than expected in many previous real-world PKI deployments. Will keeping Certificate Revocation Lists (CRLs) be feasible?
- What other hidden costs might there be with a much larger PKI, and with the smart grid's needs and constraints?
    - Nonstatic entities: Certificates are generally issued to a relatively static entity. In the power grid, meters need to be replaced, customers change providers, and ownership of appliances changes. What design and performance trade-offs are needed for the PKI to support that?

  - Grid speed and capacity: Meters pass data through a variety of networks, but will all of the pipes be big and reliable enough for PKI? Are there security vs. capacity trade-offs?
  - Data aggregation: Data may be aggregated at many levels. What design and performance trade-offs are needed for the PKI to support integrity checking across aggregation?



What Certs? Who Issues them?

Results and Benefits

- The envisioned smart grid must connect billions of nodes reporting many times per day.
- Cryptography is crucial for data integrity and intelligent service decisions.
- In 2012, Tucker Ward of the TCIPG Dartmouth team created the GCS, which enables AMI-side smart grid PKI simulation in the NS3 framework.
- Last year, Ivan Antoniv developed GCS2.0, a complete re-work of the earlier version. GCS2.0 allows for more general communication patterns, trust paths, non-dummy revocation lists, CRL fetching, and mobile nodes.
- Using our modeling and simulation techniques, we will be able to quantify the costs of deploying PKI at scale in the smart grid and use the data to mitigate bottlenecks and other problems.
- Our approach will also extend to other large populations—such as the ***Internet of Things***—requiring trust infrastructure.
- Collaborations:
  - Simulation advice: Jason Liu, FIU.
  - Smart grid discussions: Robert Lee of GE; Los Angeles Dept. of Power and Water.
  - Alternative crypto discussions: Scott Rea of DigiCert; ORNL.
- Technology Readiness Level: Development in progress.

Researchers

- Kartik Palani, palani2@illinois.edu
- Mohammad Zohaib Akmal, zohaib@cs.dartmouth.edu
- David Nicol, dmnicol@illinois.edu
- Sean Smith, sws@cs.dartmouth.edu

Industry Collaborators

- DigiCert
- GE
- Los Angeles Department of Power and Water

Functional Security Enhancements for Existing SCADA Systems

Overview and Problem Statement

Although SCADA systems were originally endowed with relatively minimal networking capabilities, over the years they have increasingly migrated to IP networks that allow communication with numerous devices multiplexing the same communication medium. While that migration advances the value proposition of the emerging smart grid, it also clearly provides a vulnerable cyber medium through which potential attackers can access and manipulate critical physical power equipment, and Ethernet protocols are exposed to traffic from a wide variety of sources. Therefore, securing the networked SCADA systems of the emerging smart grid is undoubtedly of great importance in assessing the impact of any potential menace on the stability and security of such systems. A significant number of security countermeasures, such as firewalls, encryption, and network intrusion detection systems (NIDS), have been widely adopted to protect and isolate the network perimeter of the electric power grid from external attacks. Network intrusion detection is a widely used technique to address cyber attacks either inside or at the border of a network.

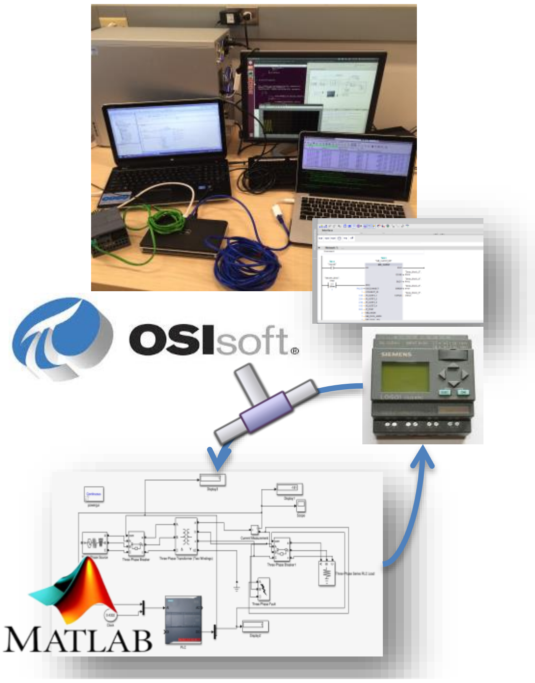


Figure 1. The developed testbed.

In this work, we proposed a novel use of NIDS tailored to detect attacks against networks that support hybrid controllers of power grid protection schemes. In our approach, we implement specification-based intrusion detection signatures based on the execution of the hybrid automata that specify the communication rules and physical limits that the system should obey. To validate our idea, we developed an experimental framework consisting of a simulation of the physical system and an emulation of the master controller, which serves as the digital relay that implements the power grid protection mechanism. Our Hybrid Control NIDS (HC-NIDS) continuously monitors and analyzes the network traffic exchanged within the physical system. It identifies traffic that deviates from the expected communication pattern or physical limitations, which could place the system in an unsafe mode of operation. Our experimental analysis demonstrates that our approach is able to detect a diverse range of attacks that attempt to compromise the physical process by leveraging information about the physical part of the power system.

Most recently, we focused on the expansion of our developed security framework to work under the industry's standard real-time data management systems. In this project, we are collaborating with OSIsoft, one of the industry leaders in data management systems, to implement our security framework on their PI System. The PI System can be queried by our HC-NIDS, which implements a set of security policies and is aware of the physical laws and communication rules that designate the normal behavior of the cyber-physical system. A "network tap" grabs the network traffic exchanged between the Matlab/Simulink simulation of the physical system and a real programmable logic controller (PLC) that implements a protection mechanism, e.g., a power transformer's overcurrent protection mechanism. The captured network traffic is stored in the PI Server in the form of predefined tags, which HC-NIDS retrieves in order to check for possible anomalies or attacks. HC-NIDS executes a set of intrusion detection rules, detects any violations, and reports suspicious events by generating alerts and keeping track of the events that triggered alarms.

Research Objectives

Our goal is to identify and implement intrusion detection rules for protective digital relays in power systems based on the knowledge of the hybrid automata executed by the network of relays. To mitigate an important category of cyber-physical vulnerabilities, our novel use of NIDS integrates traditional NIDS approaches' computer and network security communication rules with information related to the system's physical limits and the expected execution of its hybrid automata models.

Technical Description and Solution Approach

Our Hybrid Control NIDS (HC-NIDS) assumes that the control environment runs protection control algorithms that are codified to allow the system to transition only in specific safe states. Those states are called *hybrid states* because they encompass the state of discrete switches (coils) and the normal dynamics of the analog system variables, under the specific configuration of switches. The allowed transitions between different hybrid states are described in hybrid automata models, which capture the combination of protection schemes and physical properties of a system as well as their safe range of operation. Transitions are triggered by physical changes and commands issued via network packets flowing between field devices and central controllers.

The NIDS method is aware of the hybrid automaton model and continuously monitors and analyzes the network traffic exchanged by the field devices that activate the protection scheme to ensure that the exchanged commands and information are consistent with the appropriate hybrid automaton model.

Each hybrid state corresponds to specific values for the switches and specific ranges for the current, voltage, temperature, and so forth.

Results and Benefits

We developed an experimental framework, shown in figure 1 that allows us to create communication between the simulated physical process and a PLC through an Ethernet interface that sends information via the Modbus TCP industrial control protocol. A "network tap" grabs the network traffic exchanged between the Matlab/Simulink simulation of the physical system, and the real controller (PLC) that implements a protection mechanism, e.g., a power transformer's overcurrent protection mechanism. The captured network traffic is stored in the PI Server in the form of predefined tags, which the HC-NIDS retrieves in order to check for possible anomalies or attacks. Any traffic that deviates from the expected normal operation of the protection scheme, as defined by our intrusion detection rules, is characterized as a possible threat and triggers the HC-NIDS to raise an alert. By utilizing the data stored in the PI Server in order to execute our HC-NIDS rules, which combine both communication and physical rules that the system should obey, we have shown that the HC-NIDS approach can detect sophisticated attacks against an overcurrent protection scheme for a power transformer.

Researchers

- Anna Scaglione, ascaglione@ucdavis.edu
- Georgia Koutsandria, gkoutsandria@ucdavis.edu
- Masood Parvania, mparvania@ucdavis.edu
- Reinhard Gentz, rgentz@ucdavis.edu
- Mahdi Jamei, mjamei@ucdavis.edu

Industry and External Collaborators

- Sean Peisert, UC Davis/Lawrence Berkeley National Lab (LBNL)
- Charles McParland, Lawrence Berkeley National Lab (LBNL)
- OSIsoft, LLC

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 also be utilized for cyber-physical vulnerability analysis.

Research Objectives

- Understand the real-time communication requirements for wide-area power system applications for the emerging smart grid.
- Develop a technical approach to assess those requirements.
- Develop a testbed integrating a power grid, sensors, communication, and applications to create real-life scenarios to validate the GridStat middleware communication and other communication architecture.
- Conduct cyber-physical vulnerability analysis with incomplete data availability.
- **Smart Grid Application Area:** Vulnerability analysis, wide-area applications, and real-time simulation.

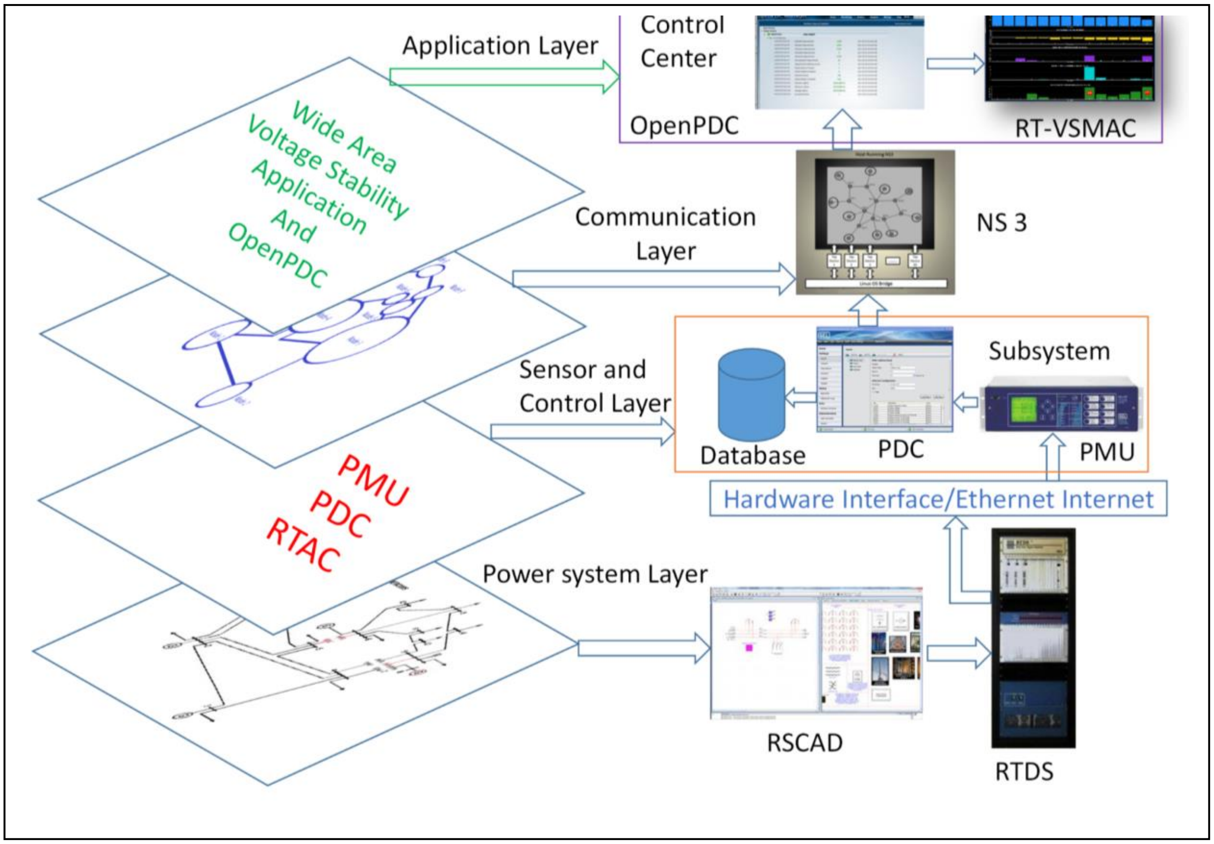


Fig. 1: Integrated Cyber-Power Simulation with Real Time Digital Simulator and Communication Emulator

Technical Description and Solution Approach

- A real-time testbed has been developed using a real-time digital simulator (RTDS) to interface with communication emulator NS-3 and a real-time voltage stability application, as shown in Fig. 1. Interfacing with DeterLab and GridStat is in progress.
- In addition, integrated modeling and simulation in real time using Power Tech software and GridStat have been developed. (This part of the effort is separately funded by DOE.)
- Graph theory-based vulnerability indices for the power grid are being used to analyze multiple contingencies with limited information. Developed vulnerability analysis indices have been integrated with cyber vulnerability indices for integrated cyber-physical vulnerability analysis.
- Cyber vulnerability analysis and attack models for man-in-the-middle attacks, denial of service attacks, and communication line outages have been analyzed using the developed testbed.

Results and Benefits

- RTDS-based testbed development is in progress (partially funded by TCIPG). Communication emulator NS-3 has been interfaced to deliver the data from physical and simulated sensors to wide-area voltage stability applications.
- Cyber vulnerability index has been integrated with graph theory-based physical vulnerability indices given incomplete information. Developed cyber-physical vulnerability indices have been validated for standard IEEE test systems with Aurora-like attacks.
- A real-time man-in-the middle-attack (MITM) has been simulated using the developed testbed. Additional cyber attacks will be modeled and analyzed using the developed testbed.
- DeterLab has already been integrated into the developed testbed to replace NS-3 to emulate the communication network. With the communication features supported by DeterLab, we are able to observe and interact with real malicious software, operating in realistic network environments at scales found in the real world.
- Development of cyber-physical training simulator using the cyber-physical vulnerability index and integrated cyber-physical simulation is in progress.
- Partnerships and External Interactions: Prof. Saman Zonouz, Rutgers University; Prof. Thomas Morris, Mississippi State University; Prof. Thoshitha Gamage, Southern Illinois University.
- **Technology Readiness Level:** Research in progress.

Researchers

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

Industry Collaborators

- SEL
- RTDS

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 overlie the transmission system topology to enable new types of control and protection applications that will make the grid more efficient and 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 two aspects of cyber security in that emerging environment. The first is that of *message origin authentication* when the data delivery model is multicast. That is a challenging technical problem for which various solutions exist, but all exhibit trade-offs among multiple quality-of-service dimensions, so there is no universally best solution. The second aspect concerns how to make control decisions using information from sources whose trustworthiness is unknown a priori. We observe that in any system of the power grid's size, involving thousands of participating entities, security will necessarily 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

- 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 Time-Valid One-Time Signature (TV-OTS) multicast authentication protocol.
- Systematically analyze trade-offs in parameter choices for the TV-OTS multicast authentication protocol.
- Design and implement key-generation and key-distribution services to support use of *k-time* signatures in the GridStat framework.
- Evaluate performance of *k-time* signatures for multicast messages in the DeterLab environment.
- 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 to enable useful instantiation of the models and maintenance of the instantiations over time.
- Incorporate instantiated trust models as part of the security design of wide-area control systems to deal with risks associated with manipulated data.
- Assess, formally and informally, the design trade-offs involved in choosing security protocols for smart grid data dissemination by investigating the vulnerabilities associated with various transport and network-layer security mechanisms.
- **Smart Grid Application Area:** Wide-area monitoring and control.

Technical Description and Solution Approach

- We previously completed work on performance improvements to the key-generation algorithm used in the TV-OTS scheme. TV-OTS exhibits some of the best trade-offs between real-time performance and security but is accompanied by very high off-line key-generation costs. Based on our evaluation of trade-offs among choices in the TV-OTS implementation, such as signature size, number of chains, epoch length, and the resistance of the protocol to brute-force attacks, we are implementing TV-OTS as a fully supported authentication mechanism in the GridStat framework.

- 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 developing a semantically rich and expressive formal trust management model capable of describing the trust relationships between power grid entities. We have a publication in review dealing with trade-offs in design choices for transport layer mechanisms that affect the ability of attackers to mount false data injection attacks on smart grid data streams.

Results and Benefits

- TV-OTS offers tunable security at relatively low computational and latency cost compared to competing methods for multicast message authentication.
- Partnerships and External Interactions: NASPI, SEL, RTE, SCE, ISO New England.
- **Technology Readiness Level:** The full demonstration system of TV-OTS key-generation and deployment in GridStat is nearly complete.

Researchers

- Carl Hauser, hauser@eecs.wsu.edu
- David E. Bakken, bakken@eecs.wsu.edu
- Kelsey Cairns, kcairns@wsu.edu
- Yujue Wang, yujue.wang@email.wsu.edu
- Chin-Wei Chang, chin-wei.chang@email.wsu.edu
- Thoshitha Gamage, tgamage@siue.edu

Industry Collaborators

- Dennis Gammel, SEL
- GridStat, Inc.
- RTE
- SCE

GridStat Middleware Communication Framework: Systematic Adaptation

Overview and Problem Statement

GridStat is a middleware communication framework with ultra-low latencies and high availability that is 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 not addressed, have the potential to make those 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.

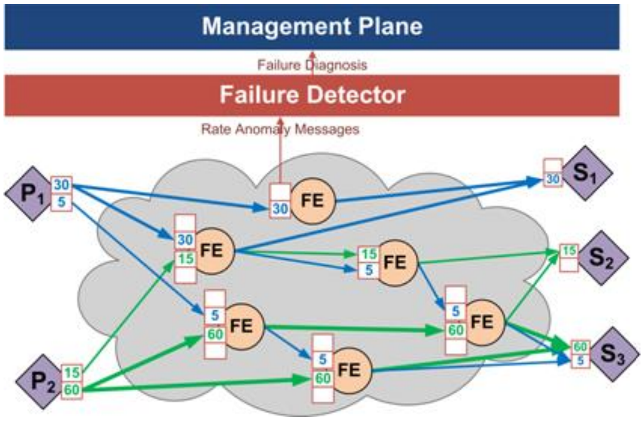
The objective of this research activity is to develop adaptation services and supporting instrumentation services for GridStat in order to systematically adapt to changing conditions and available resources. Those adaptations must be performed such that the strongest possible delivery guarantees (latency, rate, number of paths) are provided to the most critical applications, yet other applications are given guarantees commensurate with their present criticality, rather than being starved of resources. 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 (number of 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 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.
- The ability of GridStat to incorporate a wide range of instrumentation feeds and adaptation strategies that utilize them.
- Partnerships and External Interactions: North American Synchrophasor Initiative (NASPI).
- **Technology Readiness Level:** This research is still at the early stages of development, but the core contribution, once completed and incorporated with the main GridStat software, is expected to be a core GridStat functionality.

Researchers

- David E. Bakken, bakken@wsu.edu

PMU Enhanced Power System Operations

Overview and Problem Statement

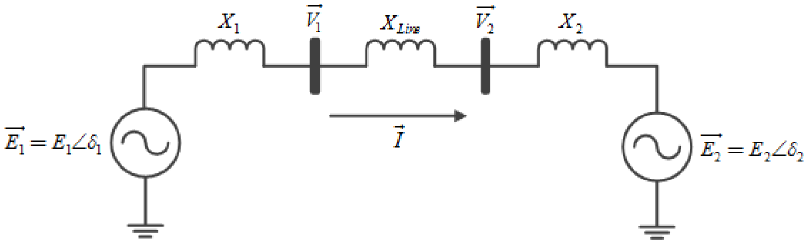
This project is exploring the direct application of Phasor Measurement Unit (PMU) data to improve situational awareness. PMUs are beginning to be widely deployed in electric power systems, and this trend is expected to continue. However, even with that increase in the number of installations, PMUs are still deployed at only a small percentage of system buses. That presents a challenge: how to get useful information from a small number of data points. 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. In addition, this project is developing a new reduced model approach to decrease computational complexity in power system transient simulation. The project is investigating conditions that make fast modes active or inactive.

Research Objectives

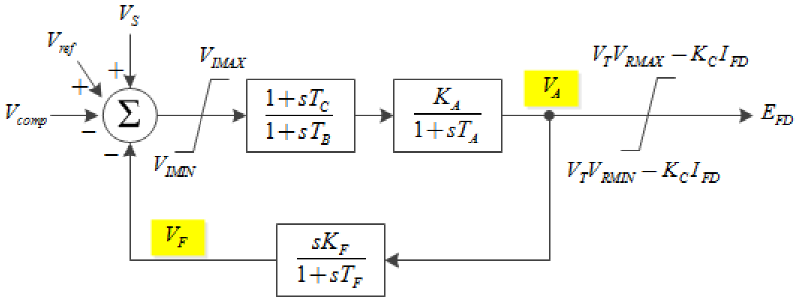
- Develop a framework to allow PMU measurements to create the equivalent system model.
- Develop an algorithm and systematic way to derive system parameters from PMU data.
- Develop online event detection method with PMU data.
- Achieve faster power system analysis.

Technical Description and Solution Approach

- In the first step of this project, we are creating an equivalent system model and deriving the system parameters using PMU data. The Thevenin-equivalent circuit with a classical machine model makes an analysis of a complicated power system simple. A sudden change of the derived system parameters can be interpreted as the system event.


X_1
$\vec{V}_1$
X_{Line}
$\vec{V}_2$
X_2
$\vec{E}_1 = E_1\angle\delta_1$
$\vec{I}$
$\vec{E}_2 = E_2\angle\delta_2$

- Regarding the fast transient simulation work, modes in the original system in which fast dynamics do not appear can be neglected, allowing simulation steps to be increased without numerical stability issues. During a transient simulation, the proposed method switches dynamically between the original system model and the reduced model, depending on the switching criterion. For this work, exciter model reduction has been investigated.



Results and Benefits

- Matlab code to derive the equivalent system using PMU data has been implemented.
- A key benefit will be an algorithm that can accommodate PMU values for improved situational awareness. The use of an equivalent system allows system operators to detect a system event. That will have positive benefits in operations, since the algorithms could be used in real-time without any system model information.
- Exciter model complexity reduction is being completed for faster transient simulation, and case studies are validating the proposed reduction work. This is an advanced dynamic simulation approach that provides a fast solution without sacrificing simulation accuracy. It will enable operators to quickly assess a system's dynamic security.
- **Technology Readiness Level:** The faster simulation method can be directly applied to commercial power system simulation tools.

Researchers

- Soobae Kim, kim848@illinois.edu
- Thomas J. Overbye, overbye@illinois.edu

Real-Time Streaming Data Processing Engine for Embedded Systems

Overview and Problem Statement

The objective of this activity is to develop a low-cost and low-overhead hardware security engine to achieve secure and reliable execution of applications that compute critical data, in spite of potential hardware and software vulnerabilities. To achieve that goal, the barriers to application of the security engine need to be eliminated. Specifically, the security engine needs to achieve low runtime overhead, low hardware resource overhead, high source compatibility, and high binary compatibility.

Research Objectives

- Prevent attacks from different entry points (outsiders, normal users, or insiders).
- Enforce both *spatial memory safety* and *temporal memory safety* at the same time to provide high detection coverage of memory corruption attacks.
- Efficiently transmit monitoring data collected from the main processor to the security engine so that transmission overhead is low.
- *Asynchronously* check the memory safety without interrupting the normal execution of a program.
- Apply the protection technique on existing applications with minimum involvement on the developer's side to convert unprotected programs into protected programs.
- **Smart Grid Application Area:** Apply AHEMS on the data concentrator or security gateway to protect the integrity of critical data, such as password, private key, or power grid data.

Technical Description and Solution Approach

- The AHEMS (Asynchronously Hardware-Enforced Memory Safety) Framework (See Figure 1) is proposed to protect applications from memory corruption attacks by enforcing spatial and temporal memory safety. AHEMS has two major parts:
    - **Source Code Instrumentation:** The source code of a program is instrumented with `alloc` and `dealloc` instructions to establish the interface between the program and the hardware security engine.
    - **Hardware Security Engine:** The security engine receives the memory events from the runtime monitor, checks the memory safety *asynchronously* (i.e., does not stop the main processor) using the metadata stored on the security engine, and raises exceptions if those memory events violate the memory safety according to the metadata.

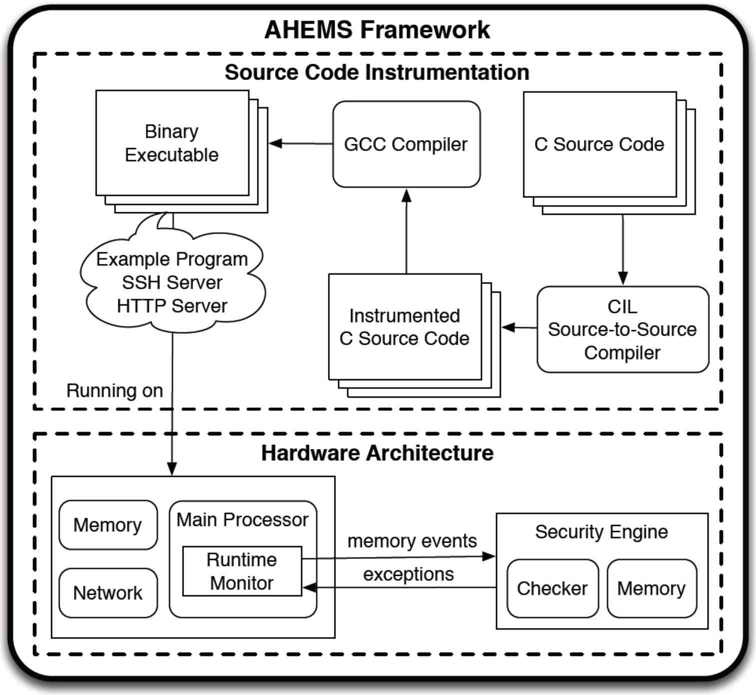


Figure 1: The Architecture of the AHEMS Framework

Results and Benefits

- Our prototype of AHEMS achieves high coverage for memory corruption attacks (detecting 676 out of 677 test cases; see Table 1) with runtime overhead as low as 10.6%. It also outperforms four other state-of-the-art approaches in terms of runtime overhead (See Table 2).

Table 1: Detection Coverage of AHEMS on Juliet Test Suite

Spatial Memory Errors			
CWE No.	**Description**	**Tested**	**Detected**
CWE121	Stack-based Buffer Overflow	209	208
CWE122	Heap-based Buffer Overflow	18	18
CWE124	Buffer Underwrite	102	102
CWE126	Buffer Overread	145	145
CWE127	Buffer Underread	33	33
CWE588	Attempt to Access Child of Non-structure Pointer	34	34
CWE680	Integer Overflow to Buffer Overflow	38	38
CWE761	Free Pointer Not at Start of Buffer	38	38
Subtotal		**617**	**616**
Temporal Memory Errors			
CWE No.	**Description**	**Tested**	**Detected**
CWE415	Double-free	38	38
CWE416	Use-after-free	20	20
CWE562	Return of Stack Variable Address	2	2
Subtotal		**60**	**60**
Total		**677**	**676**

Table 2: Runtime Overhead of AHEMS against Four Other Approaches

Programs	**AHEMS**	**Mudflap**	**Softbound+CETS**	**SAFECode**	**AddressSanitizer**
Bh	0.2%	13655.2%	Compiler error	Runtime error	41.9%
bisort	38.4%	3114%	341.1%	154.3%	74.7%
em3d	10.5%	705.0%	473.0%	192.1%	89.5%
health	17%	13343.9%	737.8%	943.2%	361.5%
Mst	4.3%	1169.2%	395.1%	644.1%	92.2%
perimeter	22.2%	32317.8%	443.1%	212.7%	142.8%
power	0.0%	263.9%	1.2%	1.0%	2.7%
treeadd	8.6%	106008.1%	448.1%	518.8%	398.7%
tsp	0.0%	1404.9%	206.9%	57.5%	76.8%
voronoi	4.6%	2224.2%	False alarm	Runtime error	156.5%
Average	**10.6%**	**17420.6%**	**380.8%**	**340.5%**	**143.7%**

- **Technology Readiness Level:** We have implemented a prototype of AHEMS that can work on medium-size applications such as Olden Benchmarks.

Researchers

- Kuan-Yu Tseng, mycallmax@gmail.com
- Zbigniew Kalbarczyk, kalbarcz@illinois.edu
- Ravishankar Iyer, rkiyer@illinois.edu

Industry Collaboration

- Dennis Gammel, Schweitzer Engineering Laboratories Inc.

State-Aware Decentralized Database Systems for the Smart Grid

Overview and Problem Statement

The modernization of power grid industrial control systems (ICSes) is likely to lead to the adoption of modern cloud services for data historians and to derivation of “big data” analytics. The data destined for that cloud service consist of either PMU measurements cached in several data-concentrators and part of the new wide-area measurement systems, or power injection and flow measurements accrued by SCADA servers. Those data today are processed separately, because current power system state estimation (PSSE) lacks support for heterogeneous sampling and sensing modalities. The data are forwarded from the data concentrators to the PSSE servers, which then compute the state. For nonlinear SCADA measurement, the PSSE is solved iteratively using the Gauss-Newton method. Several authors have proposed methods to perform a hierarchical aggregation as a more efficient and scalable technique to determine the state. More recently, our previous work has improved the PSSE algorithms such that they become adaptive to changing network conditions, e.g., in the worst case with completely randomized cooperation with neighboring sensors.

An implicit assumption made in the previous studies on PSSE is that the time and frequency at which PMU/SCADA measurements are taken are consistent across all the distributed sensing sites. In reality, the times of measurement often lack consistency and integrity, which is an intrinsic vulnerability of wide area sensor systems. Data logs coming from different analog to digital converters are not in phase and may also differ in the frequency of sampling, in some cases because of heterogeneity in the sensors, and in others because the data are simply not refreshed in the data historians with the same frequency. Lack of good synchronization in sensing may be the result of a malfunction or due to intentional delay attacks or spoofing attacks on the GPS signals.

That premise motivated our recent work, in which we advanced the area of decentralized signal processing and explicitly considered timing errors and non-homogenous sampling rates in linear and nonlinear least squares estimation problems with distributed sensing. For linear observation models, we provided a necessary and sufficient condition for identifiability of the sampling offsets. We propose a general algorithm for joint regression on latent vectors and on sampling offsets; in it, we exploit asynchrony and redundancy in the spatial sampling to attain sub-Nyquist sampling resolution of the slow sensor feeds. The efficacy of the proposed decentralized algorithm has been shown by numerical simulations.

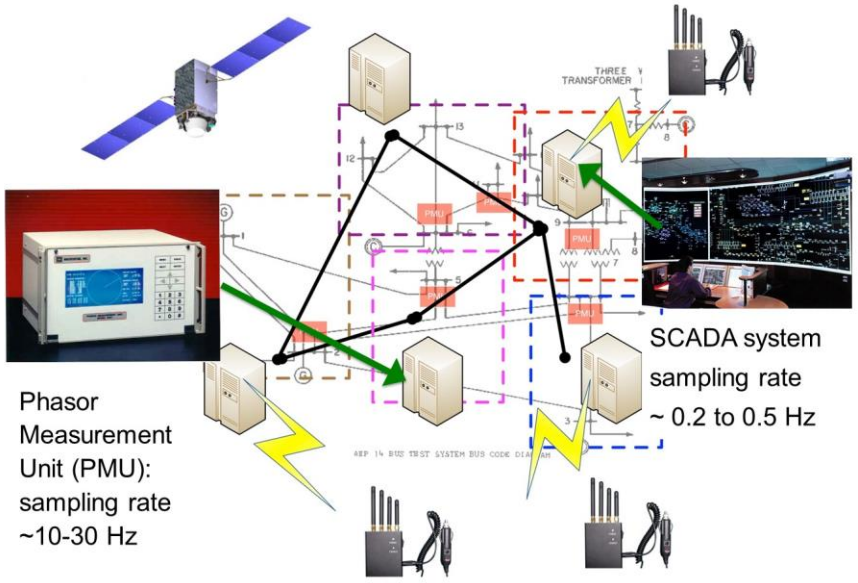


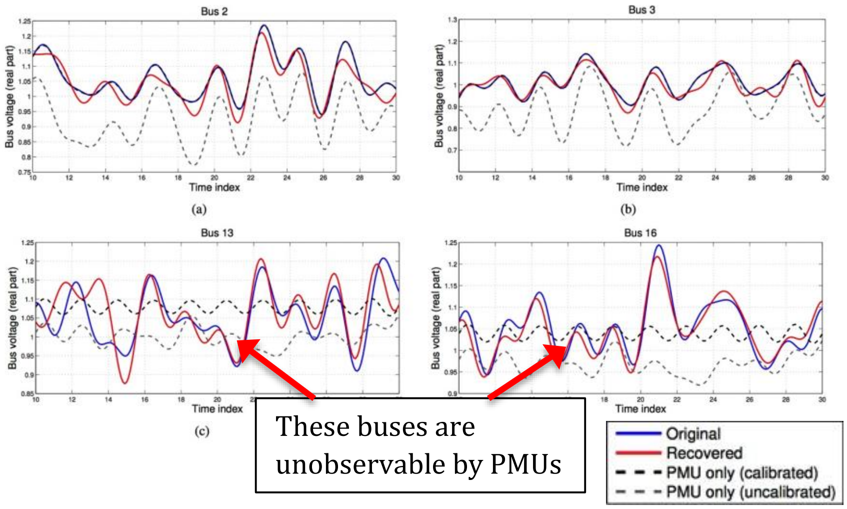
Fig. 1. A hybrid PSSE system in which the sampling rate & measurement mechanisms are allowed to be heterogeneous across sensors.

Research Objectives

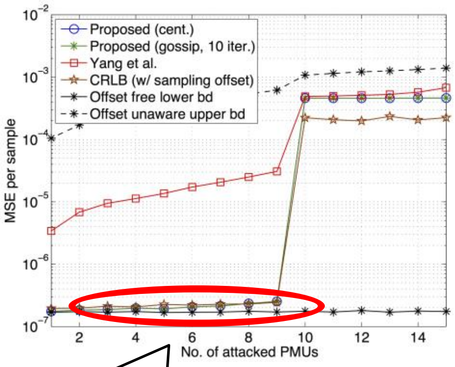
- Study how to infer the power system's state from measurements collected at heterogeneous sensors, i.e., sampled at different rates and with unknown sampling offsets.
- (For the PMU-only case:) Study the conditions under which a GPS spoofing attack can be detected and corrected.
- Study the possibility of "super-resolution" recovery through use of a massive amount of sensors with low sampling rates, e.g., SCADA.
- **Smart Grid Application Area:** The SCADA system for the electrical transmission network and the AMI network in a distribution network.

Technical Description and Solution Approach

- Using a frequency domain representation, we have formulated the joint state and timing error estimation problem as a weighted least squares problem similar to conventional PSSE, with the exception that the timing error now appears as a nonlinear distortion in terms of the phase.
- The joint estimation problem is being tackled using a gossip-based alternating optimization approach, which has been demonstrated to yield good estimation performance.
- We have studied the conditions required for successful detection of timing attacks under the PMU-only model. Roughly speaking, the condition states that we will need to deploy more sensors than are needed in the absence of a timing attack.
- We have performed simulation to demonstrate that the power system state can be recovered even if it was sampled by the slower, sub-Nyquist SCADA sensors.



These buses are unobservable by PMUs



Timing attacks can be detected successfully when enough sensors are present

Results and Benefits

- We have studied the formulation of the PSSE problem with asynchronous sampling.
- We have studied how signal processing techniques can be applied to prevent/correct timing attacks, such as GPS spoofing.
- **Technology Readiness Level:** Basic research.

Researchers

- Anna Scaglione, ascaglione@ucdavis.edu
- Hoi-To Wai, htwai@ucdavis.edu

Trustworthy Time-Synchronous Measurement Systems

Pulse Coupled Oscillators Network Time and Access Protocol

Overview and Problem Statement

Today's power measurement systems operate across multiple interfaces, complex asynchronous communication protocols, and inefficient network topologies that limit their security and prevent their deployment at a wider scale.

Sensors, like Phasor Measurement Units (PMU) or fault line detectors, depend on accurate timing across the network. So far that has been realized using the Global Positioning System (GPS) signal. However, using GPS for timing has several disadvantages, not only in cost but also in security, since GPS signals are easy to spoof or jam.

Power measurement systems often establish point-to-point communications, routing information through Ethernet-based data link layers, often using optical fiber. However, the cost of deploying optical cables and the poor scalability of the aforementioned infrastructure do not make it very suitable for wide area deployment. Other industrial protocols are either centralized solutions (e.g., WirelessHART), which do not scale and have a single point of failure, or are decentralized scheduling algorithms that do not offer common timing (e.g., FLUSH, DRAND).

The solution we propose is to design a synchronization and medium access protocol that can operate as a wake-up radio, which complements existing modems used in the grid, or can be used as the signaling layer for a radio that exploits power-line communications as well as wireless communications to provide accurate and secure network timing for PMU measurements as well as bounded delay in the data delivery.

Research Objectives

We propose an architecture that integrates decentralized synchronization and time division multiplexing together using the same communication link. Our application for the protocol is a cost-effective, resilient, synchronous sensing of the 60Hz power signal, without the need for a GPS receiver.

Our design is based on a model used to explain synchronization and coordination in biological networks, called the *pulse coupled oscillators* model. We call our protocol the **Pulse Coupled Synchronization and Scheduling Protocol (PULSESS)**.

The important objectives of our research are:

- Accuracy: Are the synchronization speed and accuracy sufficient for Power Measurement Systems?
- Scalability: How does the synchronization scale in large facilities, especially under the conditions of hidden and exposed terminals?
- Security: Is the protocol robust to attacks and failures? Is there a way to detect and identify attackers inside the system?
- Location: Can we also provide location services?
- Implementation and cost: What are the costs of the implementation? Is there an easy way to design an architecture that is compatible with commercially available communication systems to work as a wake-up radio, without changing the entire protocol stack of existing solutions?

Technical Description and Solution Approach

Our synchronization method is bio-inspired and exploits previous work on pulse coupled oscillators (PCO) in which connected nodes realign their local network clock by tracking a known pattern within their conversations. After reaching a synchronized state, nodes communicate over the shared channel via time division multiple access (TDMA), whose deterministic timing minimizes collisions, and hence reduces latency.

We are exploring two options. One is to put our protocol in a wake-up radio that provides timing and activates one of the widely employed optical (Ethernet) or wireless (WiFi or ZigBee) interfaces. Another is to implement a powerline communication (PLC) solution that uses the protocol to manage access and has its own physical layer based on multicarrier transmission. The latter solution would be able to use the same electrical wires that deliver power to transmit sensor information, optimizing both the costs and the routing paths between the terminals, given that the information flows along the same lines that deliver the AC power signal.

Our goal is to design and implement a prototype that validates our analysis. We already verified our algorithm in simulations and are now working on a microcontroller implementation as an intermediate step towards the final implementation in a field programmable gate array (FPGA). That has the benefit of using structures that already exist, thus speeding up the development process.

Therefore, we are working on simulating the expected performance of the protocol, introducing improvements in the accuracy of the timing signal; the culmination of this project will be a hardware implementation that uses field programmable gate arrays (FPGA). After verification and testing, in the next step, the design can be included in commercially available communication systems.

Results and Benefits

- We successfully simulated the algorithm and numerically verified its convergence. We are now working on an analytical convergence verification.
- A prototype network layer (layer 3) implementation on MicaZ Motes with Zigbee radios is being realized, and we hope to demonstrate the real-world applicability of this protocol.
- Our experiences with the microcontroller implementation and its limitations will guide the planned FPGA implementation on the MAC layer (layer 2). That will allow greatly improved accuracy in timing and reduced overhead, since customized medium access control (MAC) and signaling can be used, enabling realization of the full potential of the protocol.

Researchers

- Anna Scaglione, ascaglione@ucdavis.edu
- Reinhard Gentz, rgentz@ucdavis.edu
- Lorenzo Ferrari, lferrari@ucdavis.edu

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

Cognitive Bias and Demand Response

Overview and Problem Statement

To improve reliability and efficiency in the "smarter" grid, utilities are looking at *demand-response (D-R)* programs, in which the utilities use higher prices to motivate users to reduce their electric loads during periods of high grid stress. As we move towards smart homes connected by the *Internet of Things (IoT),* it's becoming easier to do that automatically. For example, a user might give his smart thermostat both a desired temperature and a "comfort vs. savings" preference. If the grid is experiencing stress, the utility communicates a higher price to the smart thermostat, which (for the users who chose some amount of "savings") will reduce the local load, and also save the user money—at the expense of a less comfortable temperature.

However, to be effective, that model makes some assumptions:

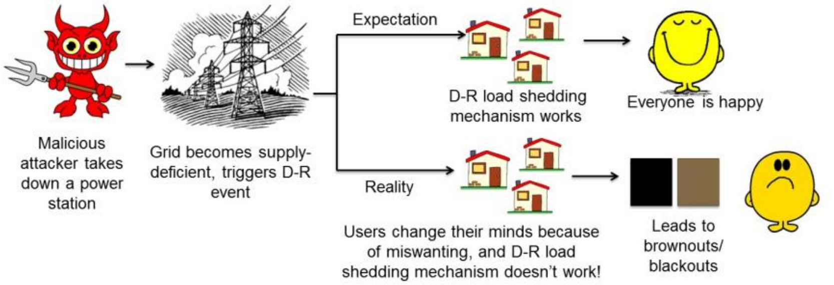
1) Users will construct accurate mental models from what their smart devices tell them.
2) Users will make *rational, logical* decisions based on that information—in this case, an educated decision to minimize their energy costs by enduring some reasonable amount of inconvenience.
3) Users will be able to use the infrastructure provided by the technology to implement their decisions correctly.

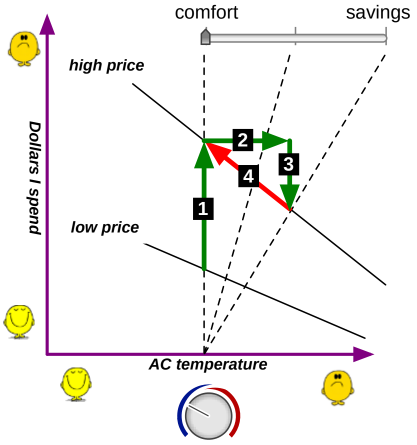
However, a large body of psychology work contradicts these assumptions and provides a catalog of cognitive biases and misperceptions that affect the decision process of the human mind. Those cognitive biases may skew users' perceptions of a scenario, leading them to make decisions that might not be optimal for that scenario, or they may mislead users into selecting choices that do not actually represent their intended decisions.

One of the most common of those biases is the *impact bias*, which is the disparity between what we predict, and what we ultimately experience. Those errors in estimating what would be desirable to us in the future lead to *miswanting*.

In this project, we analyze how the impact bias affects user decisions in a D-R scenario similar to the one employed in the power grid.

<ins>Why Impact Bias is Important:</ins>


Malicious attacker takes down a power station
Grid becomes supply-deficient, triggers D-R event
Expectation
D-R load shedding mechanism works
Everyone is happy
Reality
Users change their minds because of miswanting, and D-R load shedding mechanism doesn't work!
Leads to brownouts/ blackouts

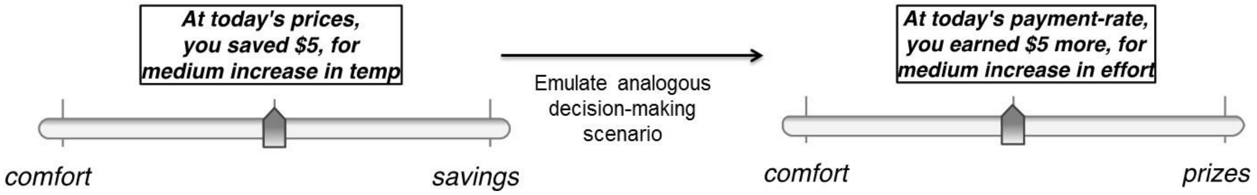


A smart thermostat may let the user specify a comfort/ savings preference in addition to desired temperature, enabling automatic DR: (1) The utility raises the price; (2) the thermostat automatically reduces the AC load; (3) the user saves money. If the impact/miswanting bias occurs, the user, in that moment, will decide he's too uncomfortable, and (4) change the setting back.

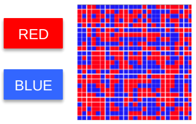
Research Objectives

- To understand how the cognitive biases of users, and, in turn, user decisions, affect the security and reliability of the power grid.
- To understand, in particular, how impact bias and miswanting affect the security and integrity of the demand-response systems in the grid.
- **Smart Grid Application Area:** Demand-response systems.

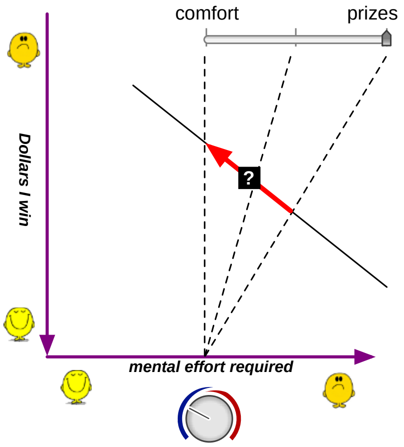
Solution Approach


At today's prices, you saved $5, for medium increase in temp
comfort
savings
Emulate analogous decision-making scenario
At today's payment-rate, you earned $5 more, for medium increase in effort
comfort
prizes

- The goal is to test for impact bias and miswanting in a decision-making scenario similar to that of the D-R system in the power grid.
- Test subjects will be given a perception-based test in which they need to estimate whether a figure is more red or more blue. We control how difficult the task is.



- The more difficult the instance, the less comfortable the test subject will be, analogous to the discomfort experienced with a too-warm AC setting.
- A higher difficulty means higher monetary compensation, but test subjects won't be compensated for giving the wrong answer. Hence, they'll face a comfort/savings trade-off analogous to that of AC settings.
- Each test subject will choose a comfort/savings slider setting. We will calculate the corresponding level of discomfort for a variety of price levels.
- Test subjects will then play the game for a sequence of the discomfort levels, analogous to experiencing what their smart thermostat chooses for them, based on their slider preference, in response to the current price.
- Throughout, we will ask them if they wish to change their slider preference, once they've experienced what it actually means in practice.
- That will give us an idea of how the test subjects would behave in a real-time D-R scenario, showing the impact of cognitive bias, if any.
- (We will use a calibration run to calculate each test subject's psychometric function, so we can normalize perceived difficulty across the subjects.)



In our experiment, we will replace room temperature with difficulty of perception-based tasks, and replace "savings" with prize money for giving the right answers. If we observe miswanting (such that some users overestimate how much "discomfort" they can tolerate and hence want to revert to an easier level), it will prove that impact bias can affect users' predictions of their preferences and, in turn, the effectiveness of security measures that depend on such preferences

Researchers

- Vineetha Paruchuri, Vineetha.Paruchuri.GR@dartmouth.edu (Computer Science)
- Jason Reeves , Jason.O.Reeves.GR@dartmouth.edu (Computer Science)
- Sean W. Smith, sws@cs.dartmouth.edu (Computer Science)
- Alireza Soltani, Alireza.Soltani@dartmouth.edu (Psychology and Brain Science)

Image Sources:
http://www.citizensutilityboard.org/images/20100406_Grid200.jpg
http://www.how-to-draw-cartoons-online.com/image-files/cartoon_devil.gif
http://www.clipartbest.com/cliparts/9ip/bon/9ipbon6iE.png
http://4.bp.blogspot.com/-_IbbM7yB_-Q/Uf5LQZvwCKI/AAAAAAAABuM/06LYvCEHuwc/s1600/MrHappy.jpg
http://tallulahfruitbat.files.wordpress.com/2012/11/sad_mr_happy1.png

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, decreased gasoline tax payments resulting from decreased gasoline sales are becoming a matter of concern, since funds to support transportation infrastructure will need to be collected in some other way. (Currently, the Motor Fuel Tax is a major source of funding for transportation infrastructure.) In the last 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 goal 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

- Design a secure and privacy-preserving tax collection model for BVs that uses mileage and location of the vehicle for tax computation.
- Compute tax amount for each authority (county, state, federal) based on the miles driven in each region. Tax computation must be auditable in case of a challenge by any affected entity.

Technical Description and Solution Approach

- The solution requires the car to calculate the tax based on its location and forward it to the servers of taxing authorities without revealing the location of the car.
- The computed tax is auditable, but in the process, location data will need to be revealed.
- Approach involves documenting and discussing various requirements of the system.
- We are designing the system in conformance with the requirement specification.
- We are implementing the system on an open-source platform, preferably an automotive platform.
- The information flow in our design is presented in Figure 1.

Selecting Android for Implementation

- Car manufacturers are continually introducing embedded functionalities (e.g., Ford Sync®, Mercedes-Benz's mbrace®) similar to those of smartphones, such as navigation, traffic reports, and health status of the car.
- Many ongoing efforts, such as AUTOSAR, OVERSEE, GENIVI, and AutoLinQ™, provide the automotive platform with API support to run third-party applications.
- OVERSEE will be a secure platform for vehicles, with all the intra-vehicle communication regulated through the firewall.
- Software implementing all the above platforms is available only to the project partners or is proprietary.
- The open-source Android platform provides many key functionalities similar to those of automotive platforms, along with excellent documentation.
- Figure 2 presents various Android apps being developed for the system and the interactions between them.

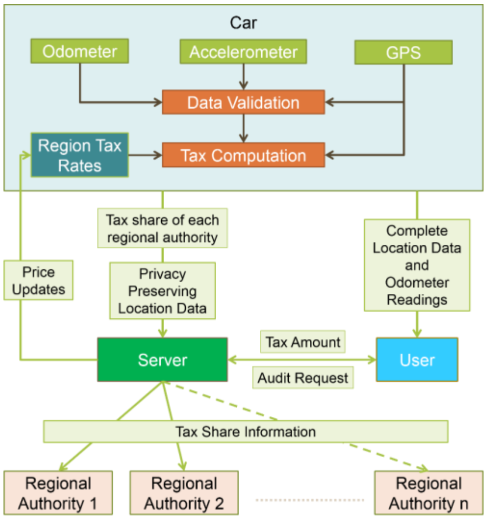


Figure 1. Information Flow

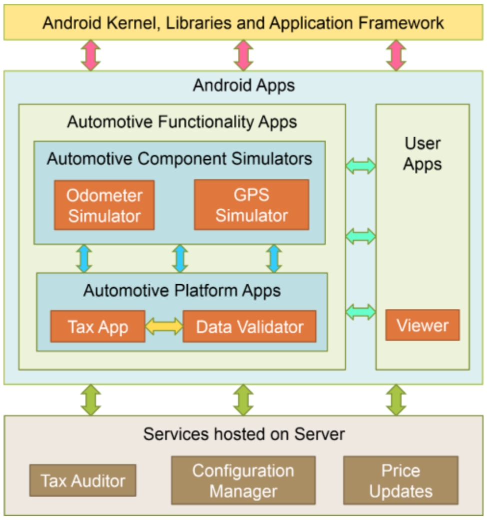


Figure 2. Process Interaction in Android Implementation

Results and Benefits

- The design can also be ported to any automotive platform or smartphone platforms such as iOS, and can be deployed to Pay-As-You-Drive (PAYD) insurance schemes with minor modifications.
- The odometer simulator and GPS simulator can be used to develop other car applications on smartphone platforms.
- **Technology Readiness Level:** In development.

Researchers

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

Password-Changing Protocol

Overview and Problem Statement

In the smart grid, the number of sensors and measurement devices that monitor the health of power lines is immense, and they are becoming even more numerous as the smart grid is upgraded. The devices are easy targets for security attacks, as they are deployed in the field (frequently on top of utility poles), are accessible via wireless networks, and typically are configured with weak passwords for authentication and collection of telemetric data by maintenance personnel.

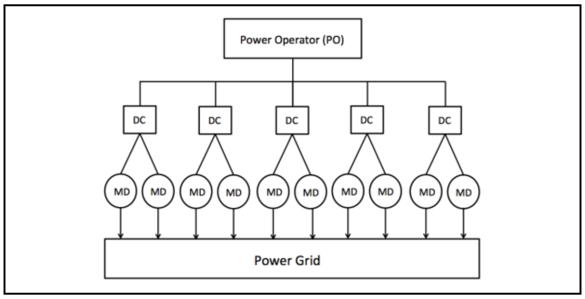
General-purpose security protocols are not suitable for providing data security to devices with limited memory, computational power, and network connectivity. Also, these telemetric devices have lengthy deployment times and limited change management capabilities. Further, the data reported by the telemetric devices to the power operator should remain secret from potential eavesdroppers, active attackers, or compromised data collectors. Our goal is to develop a secure, lightweight, scalable security protocol that ensures (i) unique authentication of power system operators and (ii) delivery of data in a secure, fast, and efficient manner. The framework should allow secure transfer of data from telemetric devices to power operators via mobile or untrustworthy data collectors.

Research Objectives

- Design a secure password-changing and data-collection framework that can defend against malicious attacks.
- Find a cost-effective and fast solution approach.
- Design a protocol suitable for data collection using mobile and untrustworthy data collectors.
- **Smart Grid Application Area:** Local area management, monitoring, and control.

Technical Description and Solution Approach

- First, we designed the framework that generates unique passwords for power system operators and symmetric keys for en/decrypting data every time a telemetric device is accessed. The framework ensures automated generation and verification of short-lived passwords and shared keys based on physical information (such as local time, geographical location of the pole on which the device is mounted, and data collector device ID) and changeable stored secrets. We introduced Physical Unclonable Functions (PUFs) to alleviate the load of telemetric devices in generating and keeping keys without revealing them. Thus, the memory and computational burden from telemetric devices is lessened.
- Second, we designed and analyzed a key establishment and data collection framework that allows a power operator to establish shared keys with multiple telemetric devices (measuring devices) via an untrusted data collector. The data collector behaves like a relay for data communications, although it is not continuously connected to the power operator. Further, the data collector has no access to the keys established between the power operator and the telemetric devices. Thus, the data collector can potentially be mobile and untrusted without compromising confidentiality.



Results and Benefits

- Secure storage and access to data at devices in the field.
- Defense against malicious attacks.
- Attribution: malicious operators can be identified in case of attacks.
- Good situational awareness.
- Partnerships and External Interactions: We are interacting with the project "Trustworthy Framework for Mobile Smart Meters."
- **Technology Readiness Level:** We have implemented the framework in several laptops to check the correctness, scalability, and computational efficiency. We plan to deploy our implementation in existing tools and simulate the protocol to evaluate its scalability.
- Publications in IEEE SmartGridComm 2014.

Researchers

- Prof. Klara Nahrstedt, klara@illinois.edu
- Haiming Jin, hjin8@illinois.edu
- Rehana Tabassum, tabassu2@illinois.edu
- King-Shan Lui, kslui@eee.hku.hk
- Wenyu Ren, wren3@illinois.edu
- Suleyman Uludag, uludag@umich.edu

Industry Collaborators

- Ameren

Smart-Grid-Enabled Distributed Voltage Support Framework

Overview and Problem Statement

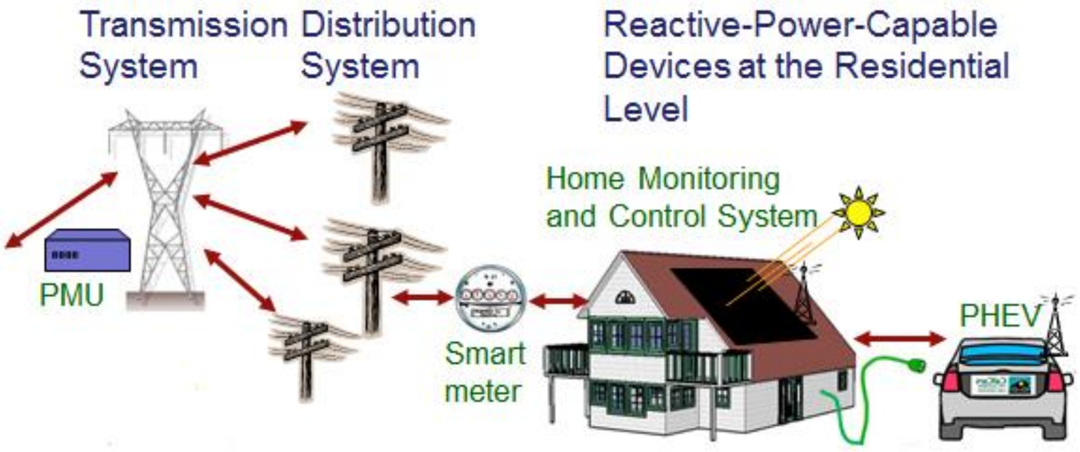
The motivation for this research lies in the use of emerging smart grid technologies, such as smart inverters, to supply reactive power as a means of distributed reactive power support. Power factor compensation closer to the load improves transmission line loading and efficiency. In the distribution networks, reactive power support not only minimizes the system losses, but also improves the feeder voltage profile. The focus of this research is on developing a smart-grid-enabled control algorithm that will determine the amount of reactive power injection or absorption required at each location to minimize the deviation from the control voltage level. Once the voltage level has been achieved, implementing conservation voltage reduction further benefits the system by increasing energy savings and extending equipment lifespan. We examine requirements for a secure communication framework to interact with the large number of devices that would be present. In general, reactive power support occurs at the substation level, whereas the communication advantages and system feedback provided by smart-grid technologies, such as smart meters, facilitate an extensive reactive power support scheme that reaches all the way to the end users.

Research Objectives

- The project seeks the ability to utilize large amounts of distributed resources, so there are major challenges to ensure high security to prevent adverse effects on the system.
- 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 control scheme to be unsuccessful; therefore, the communication between the control center and the end users is important.
- 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 that of investigating the implications for potential contingencies of the system, so that the system can be designed to avoid them. For example, if an adversary were to gain control of the system and command all the distributed reactive power devices to maximize their output, could a sudden voltage rise damage the equipment along the feeder or cause the fuse to burn out? If so, what can we do to prevent that 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.
- Algorithms combining reactive power support, conservation voltage reduction, and on-load tap changer (OLTC) control are being developed in OpenDSS and MATLAB to find the optimal voltage profile for the feeder system in order to minimize system losses and save energy consumption.
- Both centralized and distributed minimization problems have been solved. An adaptive alternating-direction method of multipliers (ADMM) control algorithm has been developed to minimize the communication overhead.


Transmission System
Distribution System
Reactive-Power-Capable Devices at the Residential Level
Home Monitoring and Control System
PMU
Smart meter
PHEV

Results and Benefits

- Reactive power support is most effective when provided locally, and voltage problems tend to start in the distribution system. By addressing the problems at the distribution level, we can also alleviate voltage problems at the transmission system level.
- 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. With a smart-grid-enabled reactive power support scheme, such problems could possibly be prevented.
- Reactive power support tends to lower feeder losses and flatten the voltage profile. By implementing this control algorithm, further load reduction is possible through OLTC coordination.
- **Technology Readiness Level:** The researchers plan to model a distribution feeder in the Real Time Digital Simulator (RTDS) to implement the control algorithm when the devices are ready.

Researchers

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

Trustworthy Framework for Mobile Smart Meters

Overview and Problem Statement

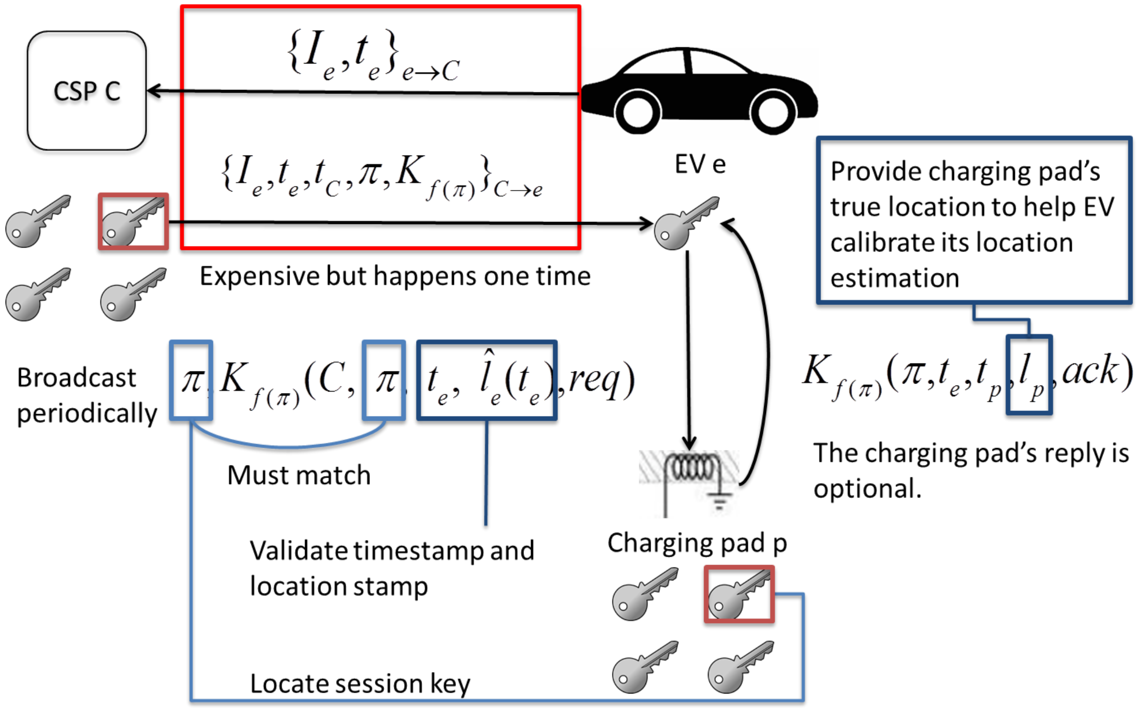
We propose to install on an electric vehicle (EV) a Mobile Smart Meter (MSM) that monitors energy usage by the car and communicates with the utility for periodic reporting, billing information, or route suggestions. The approach enables us to track energy usage more easily. It also brings new energy market models, as people generating surplus energy from their solar panels can directly sell energy to EVs, while the mobile smart meter on the EV records the energy purchase. However, securing communication between mobile smart meters and the utility 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 utility office in a secure and reliable manner. The ultimate goal is to design a trustworthy framework for communication between meters and the utility.

Research Objectives

- Design a system for reliable demand-response communication between the mobile smart meter and the utility.
- 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: proactive key dissemination approach for EV-utility authentication.
- Current approach: key predistribution-based fast authentication for EV-charging pad authentication.
- Current approach: flow-based model for charging pad/charging station location optimization.
- Future work: cyber-physical authentication that binds EV's physical presence with its digital identity.


CSP C
$\{I_e, t_e\}_{e\to C}$
$\{I_e, t_e, t_C, \pi, K_{f(\pi)}\}_{C\to e}$
EV e
Expensive but happens one time
Provide charging pad's true location to help EV calibrate its location estimation
Broadcast periodically
$\pi\ K_{f(\pi)}(C, \pi, t_e, \hat{l}_e(t_e), req)$
$K_{f(\pi)}(\pi, t_e, t_p, l_p, ack)$
Must match
The charging pad's reply is optional.
Validate timestamp and location stamp
Charging pad p
Locate session key

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.
- Recent publications:
  - Hongyang Li, György Dán, and Klara Nahrstedt, "Portunes: Privacy-Preserving Fast Authentication for Dynamic Electric Vehicle Charging," IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014.
  - Siting Chang, Hongyang Li, and Klara Nahrstedt, "Charging Facility Planning for Electric Vehicles," IEEE International Electric Vehicles Conference (IEVC), 2014.

Researchers

- Hongyang Li, hli52@illinois.edu
- Siting Chang, schang13@illinois.edu
- Klara Nahrstedt, klara@illinois.edu

Responding To and Managing Cyber Events

Responding To and Managing Cyber Events Page No.

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

A Game-Theoretic Intrusion Response and Recovery Engine

Overview and Problem Statement

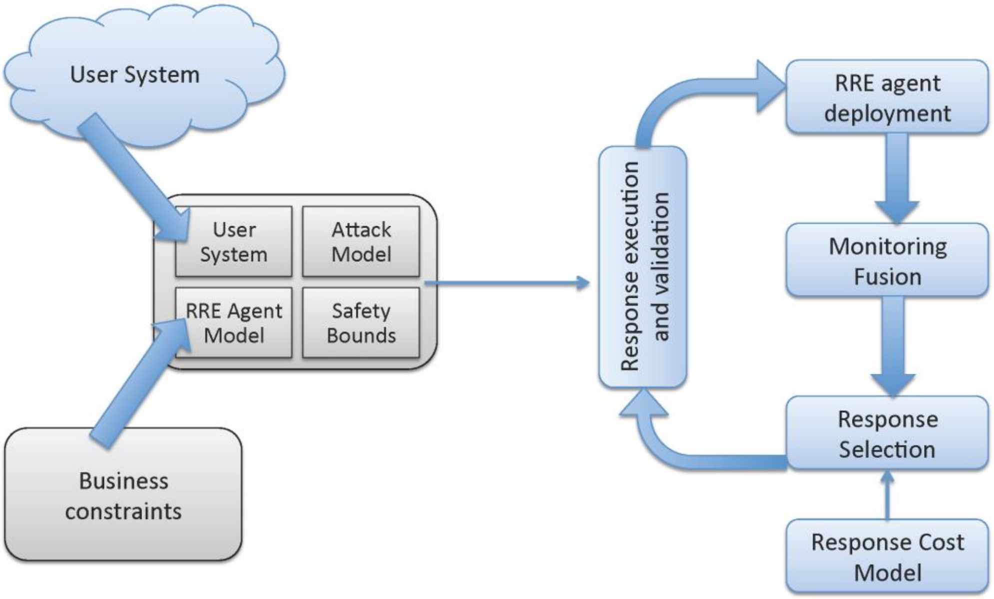
The severity and number of intrusions on computer networks, including networks in electric grids and other critical infrastructures, are rapidly increasing. Preserving the availability and integrity of networked computing systems in the face of those fast-spreading intrusions requires advances not only 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 knowledge about the network's topology (determined offline), and alerts and measurements from system-level sensors (gathered online).

Research Objectives

- Develop reactive response against adversarial attacks that uses knowledge about the power grid's current security state and its security requirements.
- Build a Response and Recovery Engine (RRE) as a distributed system that actively monitors systems and devises reactive and proactive responses.
- Use theoretical methods to find optimal response deployment.
- Adapt RRE to handle the scale of a large Advanced Metering Infrastructure (AMI).
- Model the smart grid as a cyber-physical system to study the cyber-physical interactions in detection and response. Interactions include how to detect a cyber attack physically and how a cyber response can help in a physical situation.
- Implement a response and recovery system that is capable of effectively interfacing with a human operator.
- Verify safety of certain responses with respect to system invariants.
- **Smart Grid Application Area:** Intrusion tolerance.

Technical Description and Solution Approach

- Use the cyber-physical topology language (CPTL) as a description of the system. CPTL will be used by RRE agents when computing optimal responses and fusing sensory data.
- Develop monitoring fusion algorithms that can detect high-level attack steps using diverse data sources. The diverse data sources increase confidence that malicious events will be detected.
- Adapt several languages to express the responses in our response taxonomy. RRE agents use the response language to map high-level actions into low-level actions.
- Design several cost-sensitive response selection algorithms based on distributed control theory, game theory, and graph theory.



Results and Benefits

- Distributed intrusion tolerance architecture suitable for the power grid.
- Implementing a basic OpenFlow (software-defined network) responder in a substation setting.
- Advancing the state of CPS modeling.

Researchers

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

Industry Collaborators

- Schweitzer Engineering Laboratories

Assessment and Forensics for Large-Scale Smart Grid Networks

Overview and Problem Statement

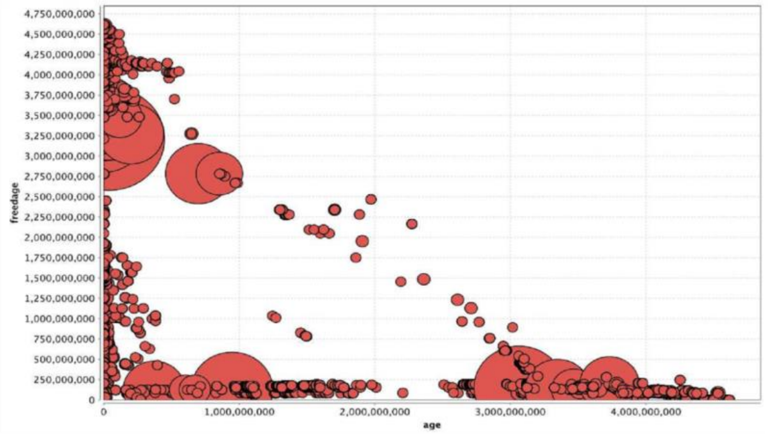
The infrastructure that supports the power grid is vulnerable to attack by intruders who could potentially take control of certain points and cause great damage to systems. The SCADA systems and other components in the smart grid are complex, and many systems rely on information from other sources. An embedded system, such as a breaker, could be compromised and set to report false information. As a result of such a compromise, analyses from monitoring systems and logging would be incorrect, as they would be based on falsified data. Stuxnet and Flame have shown that entities exist that are willing and able to create extremely sophisticated attacks. The Flame malware showed that even an immensely large and complex attack can run undetected for years. The sophisticated rootkits employed by Stuxnet and Flame showed that the current standard of detection software is easily defeated. Sophisticated, targeted attacks such as Stuxnet are inevitable, and both detection of such attacks and development of a deep understanding of what happened are critically important. If machines such as those in SCADA are compromised, we want to know as much about the attacks as possible, and understand what the effects will be on the power grid.

Research Objectives

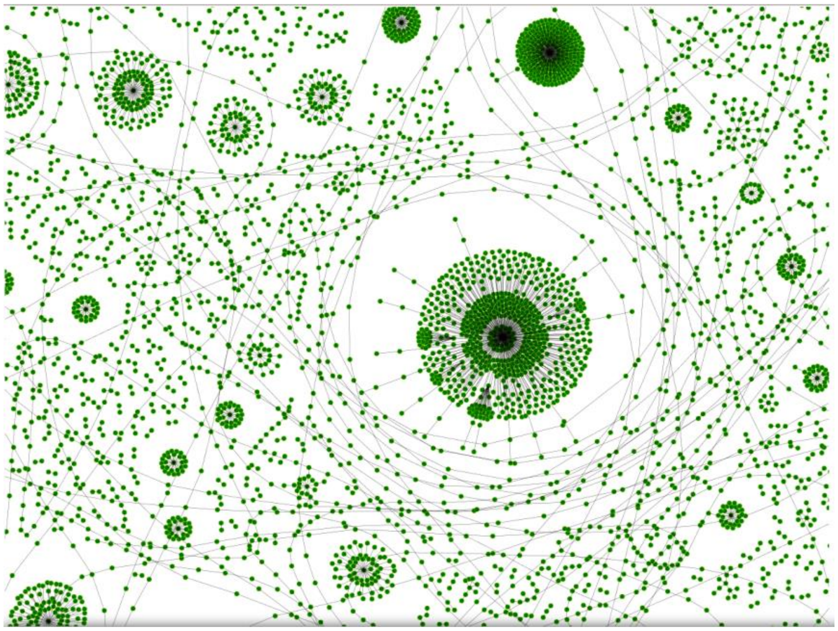
- We will integrate forensics techniques in the monitoring process to ensure the integrity of the applications involved and the information acquired.
- We will communicate with industry to understand what they want to know about compromised hosts and how these compromises will affect the power grid.
- We will leverage new and existing forensics tools for better analysis.
- **Smart Grid Application Area:** Virtual machines, forensics

Technical Description and Solution Approach

- We have continued to develop novel forensic tools and techniques.
- Forenscope collects high-quality information about compromised machines.
- Cafegrind analyzes applications to determine what information is available to forensic investigators.
- Our memory visualization tool provides visual context to assist in creating models to detect attacks from an application's volatile memory.



Cafegrind executed with the Web browser Konqueror. Sizes of circles represent sizes of data structures in Konqueror. The "age" axis represents the number of cycles from when a structure is allocated to when it is freed. The "freedage" axis represents the number of cycles from when a structure is freed until the memory containing the instance of the structure is overwritten.



Memory visualization of the Chromium application. Each green dot represents a pointer, and the lines represent the memory location to which a pointer points.

Results and Benefits

- We have created the Forenscope framework, a memory forensics platform that can perform memory analysis, capture, and sanitization on critical systems outside of the execution context of malware. The platform provided by Forenscope can be extended to perform any number of forensic tasks.
- Additionally, we have created Cafegrind, a memory analysis tool that analyzes applications to determine what information is available in memory for forensic investigation. Cafegrind monitors every instance of every data structure created by an application and monitors all accesses, when the instance is freed, and when the memory in which it was stored was overwritten.
- In order to better understand the structure of an application's memory, we have created visualization tools to provide insight into how we might model memory.
- Partnerships and External Interactions: Information Trust Institute, Assured Cloud Computing Center at UIUC.
- **Technology Readiness Level:** Initial stage.

Researchers

- Kevin Larson, klarson5@illinois.edu
- Karthik Rajashekar Gooli, gooli2@illinois.edu
- Prof. Roy Campbell, rhc@illinois.edu

Detection/Interdiction of Malware Carried by Application-Layer AMI Protocols

Overview and Problem Statement

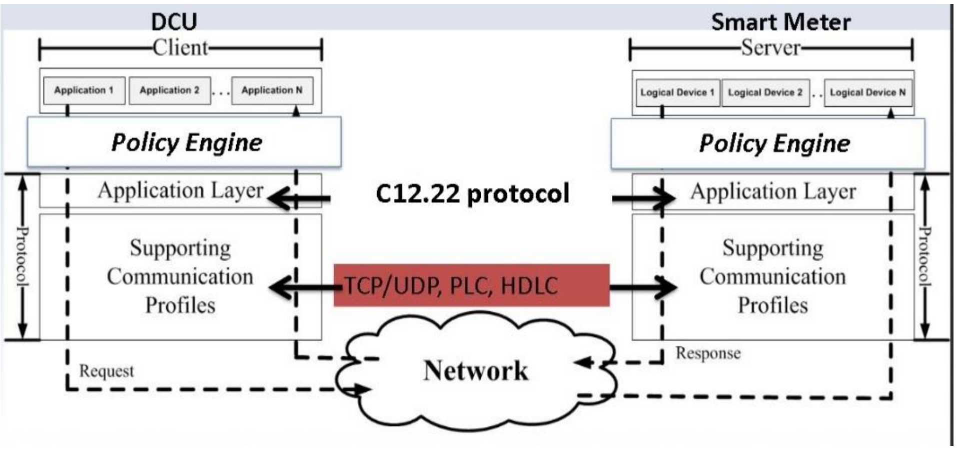
Malware could potentially hide in the payloads of standard application-layer protocols like C12.22 and DLMS/COSEM, which are extensively deployed in the AMI infrastructure. Previous work on this application-level malware detection problem by David M. Nicol and Huaiyu Zhu resulted in the proposal of a policy engine that analyzes both ingress and egress traffic from the application layer using a predefined set of policies or rules that check the packet semantics, analyze entropy levels, and look for ARM executable signatures in DLMS/COSEM protocol payloads. We extend this approach to formulate a set of rules for analyzing C12.22 protocol payloads with an additional requirement of detecting x86 binary executables hiding in packets.

Research Objectives

- Formulate semantic and communication rules to detect anomalies in C12.22 protocol payloads.
- Build a general framework for executing policy rules on C12.22 packets and provide capabilities for extensions.
- Design signature-based policy rules and investigate machine-learning-based approaches to detect x86 binaries that could be in an obfuscated, encrypted, or compressed state inside the packet.
- Evaluate the classification error rate.
- Evaluate the performance overhead.
- Integrate the policy engine with an open-source C12.22 library and demonstrate its functionality.
- **Smart Grid Application Area:** AMI, smart grid meter devices, data concentration unit devices.

Technical Description and Solution Approach

- Analyze the entropy of incoming and outgoing network traffic to detect the existence of encrypted content or packed content that might be part of malware.
- Examine non-encrypted portions of packets for specific signatures that could signify a decryption routine.
- Detect binary executables in the payload. It is harder to detect x86 binaries than ARM binaries, because of the former’s complex structure and variable-length instructions.
- Use x86 instruction opcodes to construct signatures and byte sequence characteristics such as opcode frequencies, order of occurrence, and histograms and feature vectors for training classifiers.



Results and Benefits

- We have integrated the existing policy engine to work with C12.22 protocol libraries, and we have formulated and implemented the semantic rule checks required to successfully parse metering data.
- We are currently investigating and evaluating approaches to detect x86 binaries in packets.
- **Technology Readiness Level:** In progress and currently in the initial stages.

Researchers

- David M. Nicol, dmnicol@illinois.edu
- Vignesh Babu, babu3@illinois.edu

Intrusion Detection for Smart Grid Components by Leveraging of Real-Time Properties

Overview and Problem Statement

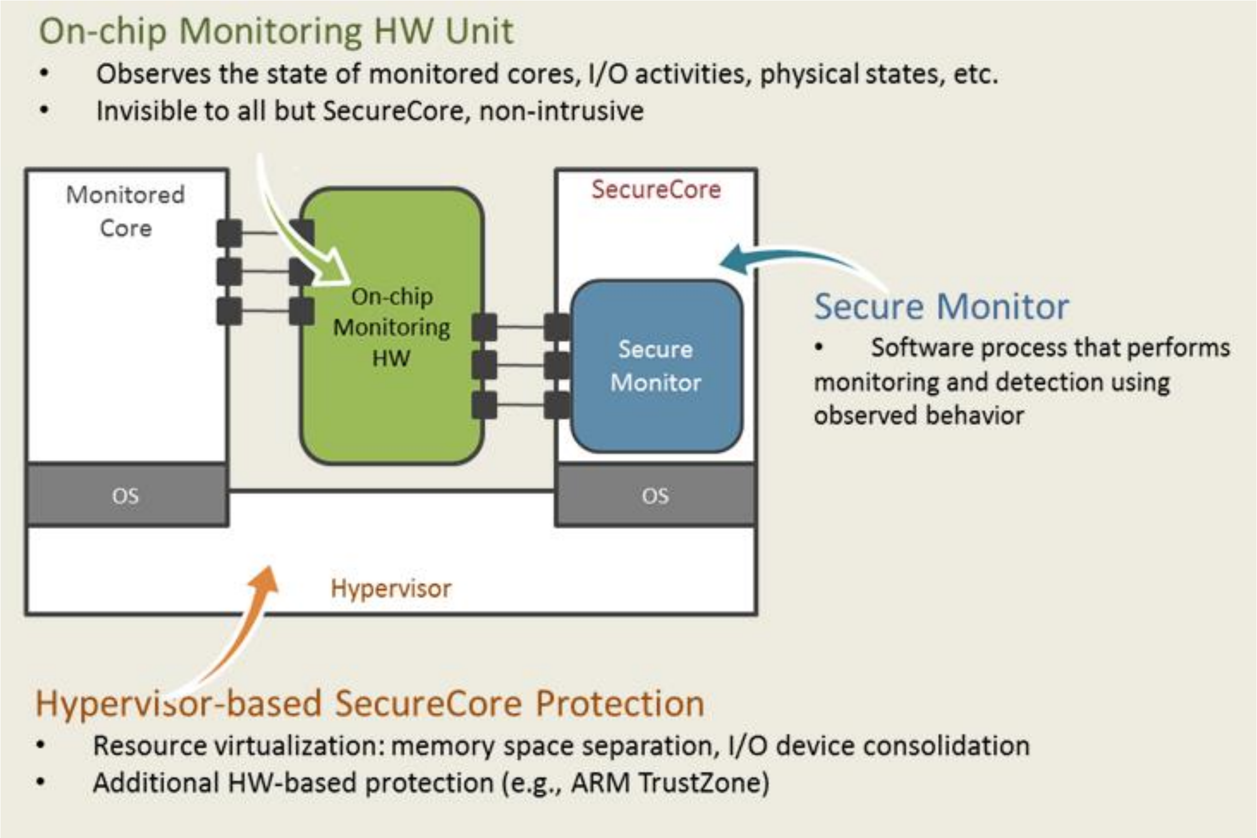
We aim to tackle the problem of detecting intrusions in power grid components with real-time properties. Most components that require a safety-critical model of operation fall under this category. The main technique is to perform behavioral analysis of such systems in order to find anomalies with respect to attributes such as execution time, memory, and I/O. Complementary to traditional cyber security technologies that aim to prevent intrusions, our work focuses on survivability: the ability to continue operating safely even if intruders succeed in penetrating a system. Furthermore, an intruder's act of performing unsafe operations or modifying the existing data acquisition and/or control software will lead to detection and removal using our techniques. The detection approach will be coupled with the development of architectures that will maintain the safety of the overall safety-critical system, even if an attacker is able to intrude successfully into the system.

Research Objectives

- Develop behavioral models of real-time control systems used in the smart grid.
- Use above models along with trusted hardware modules to monitor the components for deviations from expected behavior.
- When intrusions are detected, transfer control away from the main controller to the trusted hardware module; the main controller will be either shut down gracefully or analyzed by engineers. Either way, the physical control system will not be harmed.
- **Smart Grid Application Area:** Security for components with real-time properties in the smart grid and mobile devices used for monitoring components in the grid.

Technical Description and Solution Approach

- The overall solution will be applicable at the *individual node* level, where we monitor cyber properties such as execution time and memory, as well as I/O traffic, using a trusted platform. The technique is likely to be successful because most computational components in cyber-physical systems have deterministic behavior (by design) that can be monitored for anomalies. For this activity, we started with *execution time* and *control* behavior and are now experimenting with other system properties, such as memory and OS behavior and I/O.
- We developed timing-based analysis models for real-time control systems, both for exact timing and for statistical methods. We also implemented methods to follow the control flow of the code in such systems. We are currently analyzing the memory traffic/usage and the distribution of system calls.
- We intend to implement the analysis and detection methods to detect anomalies in smart grid components such as IEDs.
- We are also developing secure hardware-based monitoring platforms; the following image shows the high-level design using a multicore platform (which we call "SecureCore").



On-chip Monitoring HW Unit

- Observes the state of monitored cores, I/O activities, physical states, etc.
- Invisible to all but SecureCore, non-intrusive

Secure Monitor

- Software process that performs monitoring and detection using observed behavior

Hypervisor-based SecureCore Protection

- Resource virtualization: memory space separation, I/O device consolidation
- Additional HW-based protection (e.g., ARM TrustZone)

Results and Benefits

- Increased security for individual computational nodes in the power grid (e.g., IEDs and smart meters).
- Ability of such components to detect and recover from failures due to malicious activity.
- **Technology Readiness Level:** Developed initial analysis based on learning the behavior of execution time profiles; developed initial multicore-based detection architecture; developed initial compile-time analysis to capture control flow of programs; developed initial FPGA-softcore-based prototype to monitor control flow of real-time programs; developed SecureCore architecture and implemented it in the Simics full system simulator; developing memory and system-call-based analyses now.

Researchers

- Sibin Mohan, sibin@illinois.edu
- Rakesh Bobba, rbobba@illinois.edu

Industry Collaborators

- Qualcomm Research.
- In discussions with power system vendors.

Specification-based IDS for Smart Meters

Overview and Problem Statement

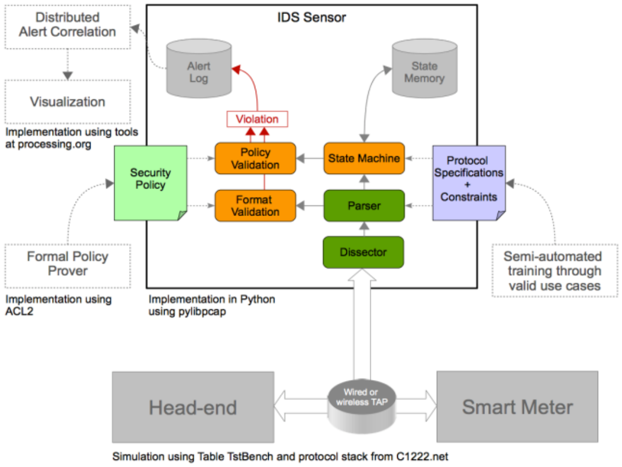
To ensure the security and reliability of a modernized power grid, the current deployment of millions of smart meters requires the development of innovative situational awareness solutions to prevent compromised devices from impacting the stability of the grid and the reliability of the energy distribution infrastructure. To address that issue, we introduce a specification-based intrusion detection sensor called **Amilyzer** that can be deployed in the field to identify security threats in real time. Amilyzer 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 the security policy was defined based on the set of failure scenarios for AMI identified by the NESCOR group. Amilyzer has been successfully deployed by a utility partner since December 2012 and is currently monitoring a 30,000-meter AMI.

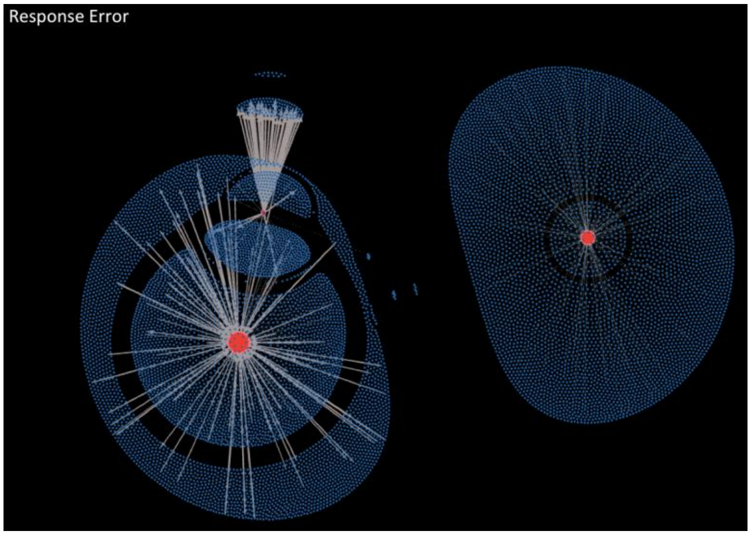
Research Objectives

- Identify potential AMI failure scenarios and translate them into a sound security policy.
- 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.

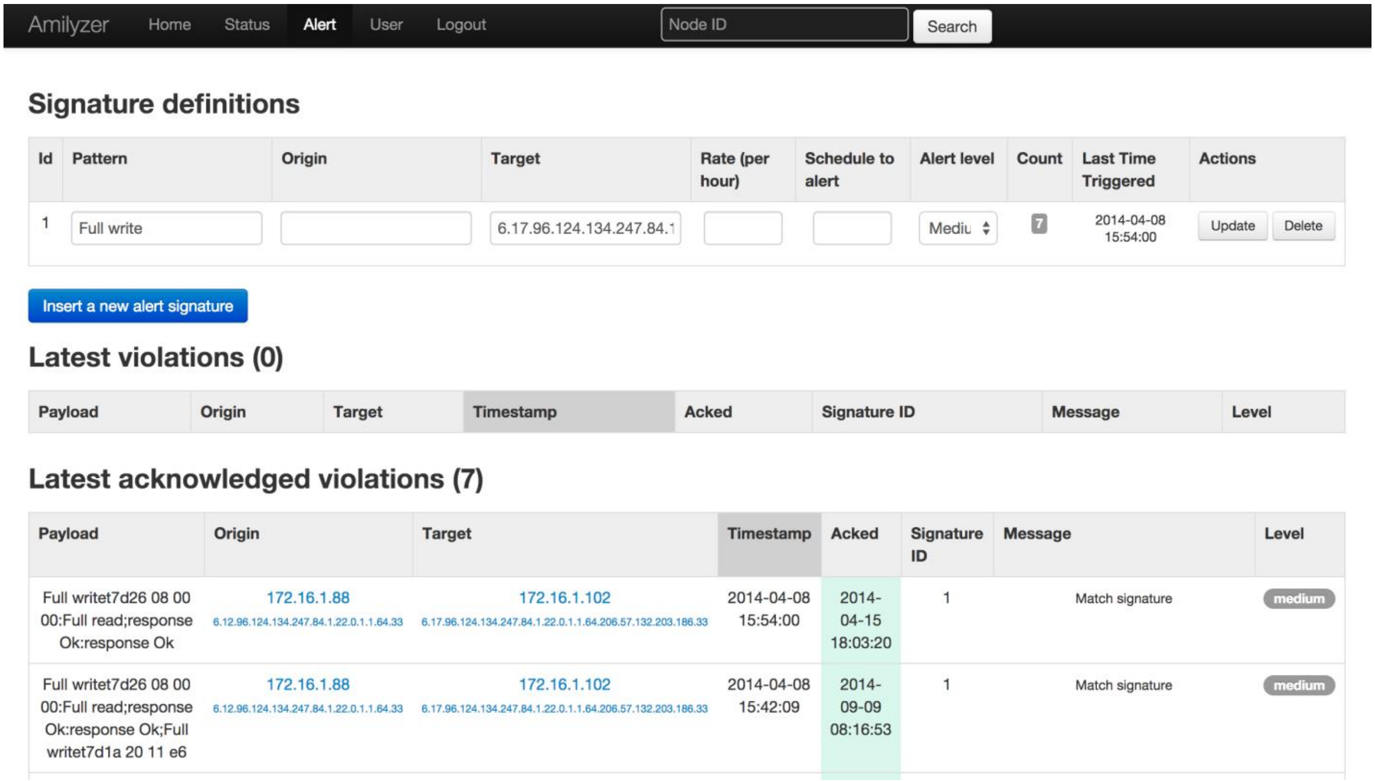

Distributed
Alert Correlation
Visualization
Implementation using tools at processing.org
IDS Sensor
Alert Log
State Memory
Violation
Security Policy
Policy Validation
Format Validation
State Machine
Parser
Dissector
Protocol Specifications + Constraints
Formal Policy Prover
Implementation using ACL2
Implementation in Python using pylibpcap
Semi-automated training through valid use cases
Head-end
Wired or wireless TAP
Smart Meter
Simulation using Table TstBench and protocol stack from C1222.net



Software modules inside Amilyzer (left). Visual representation of 12,000 meters and their communications (right).

Results and Benefits

- Definition of a rigorous process that utilities and vendors can use to develop a comprehensive monitoring architecture.
- Integration of formal methods in a practical framework to offer strong security guarantees.
- Deployment of an Amilyzer sensor in collaboration with FirstEnergy to monitor 30,000+ meters.
- **Partnerships and External Interactions**: In collaboration with EPRI, FirstEnergy, and Itron.
- **Technology Readiness Level**: Prototype.



Signature definitions

Id	Pattern	Origin	Target	Rate (per hour)	Schedule to alert	Alert level	Count	Last Time Triggered	Actions
1	Full write		6.17.96.124.134.247.84.1			Mediu	7	2014-04-08 15:54:00	Update Delete

Latest violations (0)

Payload	Origin	Target	Timestamp	Acked	Signature ID	Message	Level

Latest acknowledged violations (7)

Payload	Origin	Target	Timestamp	Acked	Signature ID	Message	Level
Full writet7d26 08 00 00:Full read;response Ok:response Ok	172.16.1.88 6.12.96.124.134.247.84.1.22.0.1.1.64.33	172.16.1.102 6.17.96.124.134.247.84.1.22.0.1.1.64.206.57.132.203.186.33	2014-04-08 15:54:00	2014-04-15 18:03:20	1	Match signature	medium
Full writet7d26 08 00 00:Full read;response Ok:response Ok;Full writet7d1a 20 11 e6	172.16.1.88 6.12.96.124.134.247.84.1.22.0.1.1.64.33	172.16.1.102 6.17.96.124.134.247.84.1.22.0.1.1.64.206.57.132.203.186.33	2014-04-08 15:42:09	2014-09-09 08:16:53	1	Match signature	medium

User interface to define signatures and review intrusion detection alerts.

Researchers

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

Industry Collaborators

- EPRI: Galen Rasche and Annabelle Lee
- Itron: Ido Dubrawsky
- FirstEnergy: Don Miller, Nathaniel Maier, Marcus Noel, and Nathan Sterrett
- Fujitsu: Jorjeta Jetcheva, Daisuke Mashima, and Ulrich Herberg
- UT Dallas: Alvaro Cardenas, David Urbina, Michael Guerrero
- Honeywell: Jun Ho Huh

Specification-based IDS for the DNP3 Protocol

Overview and Problem Statement

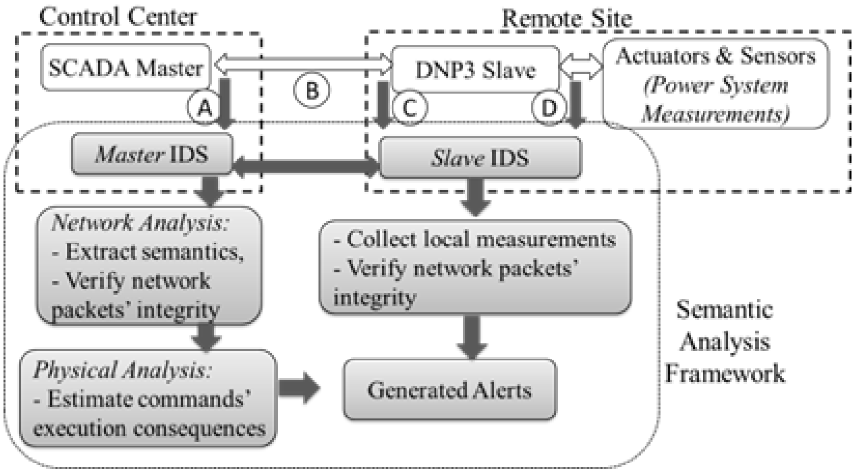
Modern SCADA systems are increasingly adopting Internet technology to control industrial processes. Because of security vulnerabilities and potential exposure (intended or unintended) to public networks, attackers can penetrate control systems to issue malicious control commands that drive remote facilities into an unsafe state, without exhibiting any obvious protocol-level red flags. While a few Intrusion Detection Systems (IDSes) are becoming available to investigate network traffic based on unique proprietary protocols, it is challenging to detect such attacks based solely on network activity. To overcome that challenge, we introduce a semantic analysis framework based on collaborating network IDSes. The framework exploits a power flow analysis algorithm adapted to accurately estimate the execution consequences of control commands with short latency, thus revealing a potential attacker's malicious intentions.

Research Objectives

- Provide theory base to analyze the impact of the attacks that exploit control commands.
- Augment Bro IDS with power flow assessment tools to perform run-time power flow analysis to predict the consequences of executing a (potentially maliciously crafted) control command that is transmitted by run-time network packets.
- Design and implement an adapted power flow analysis algorithm that significantly reduces the detection latency.
- Experiment to evaluate the attack scenario and establish the feasibility of the proposed semantic framework.

Technical Description and Solution Approach

- Master IDS at the control center:
  - Distinguish critical commands from noncritical ones.
  - Collect measurements from multiple substations.
  - Include adapted power flow analysis algorithm to estimate consequences of executing a given command.
- Slave IDS at the remote site:
  - Use local IDS to obtain trusted measurements directly from sensors.
  - Assume that concurrent physical tampering with a large number of distributed sensors is not practical for the attacker.


Control Center
Remote Site
SCADA Master
DNP3 Slave
Actuators & Sensors (Power System Measurements)
A
B
C
D
Master IDS
Slave IDS
Network Analysis:
- Extract semantics,
- Verify network packets' integrity
- Collect local measurements
- Verify network packets' integrity
Physical Analysis:
- Estimate commands' execution consequences
Generated Alerts
Semantic Analysis Framework

Results and Benefits

- Through integration of power flow analysis modules, the deployed Bro IDS is able to detect malicious commands transmitted in network packets that are syntactically correct within the protocol.
- Experiments estimate the physical consequences of malicious control commands for power systems.
  - E.g., increase generation, increase load demands, or open transmission lines.
- Experiments demonstrate the good performance of the adapted power flow analysis algorithm.
  - Significantly reduces the detection latency.
  - Introduces very few false detections.

Researchers

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

Industry Collaborators

- Donald Borries, Ameren TAC

Trust Assessment

Trust Assessment **Page No.**

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

802.15.4/ZigBee Security Tools

Overview and Problem Statement

Mission-critical services and infrastructure, such as the power grid, are increasingly dependent upon communications networks, like IEEE 802.15.4 and ZigBee, to facilitate monitoring, control, and automation. Network administrators must be able to easily observe the footprint of their networks, understand the view they present to would-be attackers of various levels of sophistication, and explore potential responses to crafted and/or malformed traffic. Exposed and brittle networks must be fixed and protected.

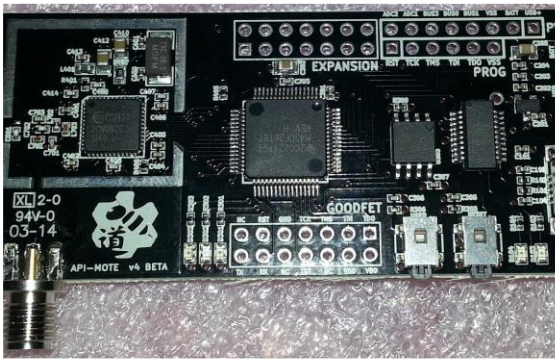
Active fingerprinting is the identification of digital radio devices through exploitation of unique characteristics, introduced by the analog circuitry and firmware implementations, in response to malformed traffic. Fingerprinting allows us to observe network responses to malformed traffic, identify trusted nodes, and explore potential vulnerabilities in both the PHY layer and firmware implementations. In addition to producing a digital radio peripheral and utilities for the passive mapping of 802.15.4/ZigBee digital radio deployments, such as smart meter networks, we have developed techniques for the active fingerprinting of nodes in such networks. Active fingerprinting is both faster and more accurate than traditional passive techniques currently used in self-assessments.

Research Objectives

- Provide IEEE 802.15.4/ZigBee network operators and asset owners with cheap and simple-to-operate tools for self-assessment.
- Enable the exploration of IEEE 802.15.4-based network technologies' attack surface.
- Actively fingerprint IEEE 802.15.4/ZigBee digital radio chips and firmware for self-audits and the detection of rogue nodes.
- **Smart Grid Application Area:** IEEE 802.15.4/ZigBee is the networking technology of choice for SCADA systems, home automation, and smart meter connectivity.

Technical Description and Solution Approach

- The IEEE 802.15.4 standard was used to develop multiple standard-frame mutations that might be effective for fingerprinting.
- Low-cost hardware based on commodity components was designed and developed to inject crafted frames into 802.15.4 networks.



Preamble: 00000000	SFD: 0xA7	Length (<512)	Payload

Standard 802.15.4 physical frame

Variable Preamble	SFD	Length	Payload

Physical frame with variable preamble length

- Vary the number of preamble 0x0 symbols

0x0s ➔ 0xFs	SFD	Length	Payload

Physical frame with Franconian Notch

- Modify the standard 8 preamble symbols from 0x0s to 0xFs

Preamble	0xFs	SFD	Length	Payload

Physical frame with Franconian Bridge

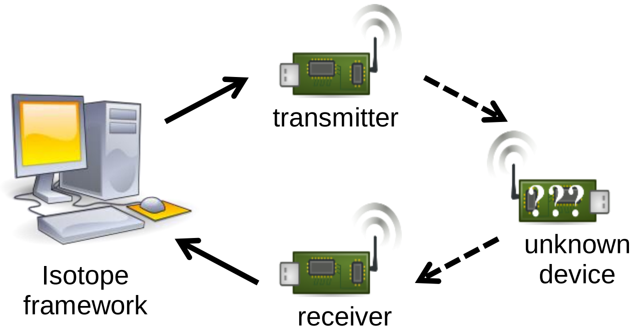
- Insert a variable number of 0xF symbols between the preamble and SFD

Preamble	SFD (bad)	0xFs	Preamble	SFD	Length	Payload

Physical frame with Cumberland Gap

- Transmit a bad SFD followed by a variable number of 0xF symbols and then a valid frame

- A Python framework, codenamed *Isotope*, was developed to facilitate the active fingerprinting of multiple commodity IEEE 802.15.4/ZigBee-compliant network radio devices. Malformed frames are transmitted to an unknown device; potential responses are recorded and later analyzed for a potential fingerprint.



IEEE 802.15.4/ZigBee Fingerprinting Framework

Results and Benefits

- Fingerprinting framework, Isotope, introduced; results published at the ACM WiSec 2014 conference.
- Partnerships and External Interactions: Enabled applied ZigBee research at the Air Force Institute of Technology; made contributions and improvements to Joshua Wright's KillerBee; provided 802.15.4 extensions to Scapy; developed extensions to Api-do with River Loop Security's APImote device.
- Demonstrated new threats for 802.15.4/ZigBee, including feasibility of **targeted attacks** on selected makes of radio chips and **evasion** of Wireless Intrusion Prevention Systems (WIPS).
- **Technology Readiness Level:** Beta; tools in ongoing development; more experimental results to come.

Researchers

- Sergey Bratus, sergey@cs.dartmouth.edu
- Ira Ray Jenkins, jenkins@cs.dartmouth.edu

Industry Collaborators

- Travis Goodspeed, travis@radiantmachines.com
- Ryan M. Speers & Ricky Melgares, River Loop Security, team@riverloopsecurity.com

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

Overview and Problem Statement

Information technology systems are increasingly being incorporated into power systems as a significant part of the smart grid vision. The interaction of cyber components and physical components adds higher levels of uncertainty, vulnerability, and complexity to the power grid. For instance, potential cyber-attacks, device faults, and even noisy measurements and communication networks may raise challenges for system operations. Meanwhile, deep penetration of renewable-based generation introduces an additional source of uncertainty, which may require advanced cyber infrastructure for fast response. Those uncertainties from cyber and physical components are the main factors affecting system monitoring and control performance. This study will quantify the impacts on power systems of those physical and cyber challenges.

Research Objectives

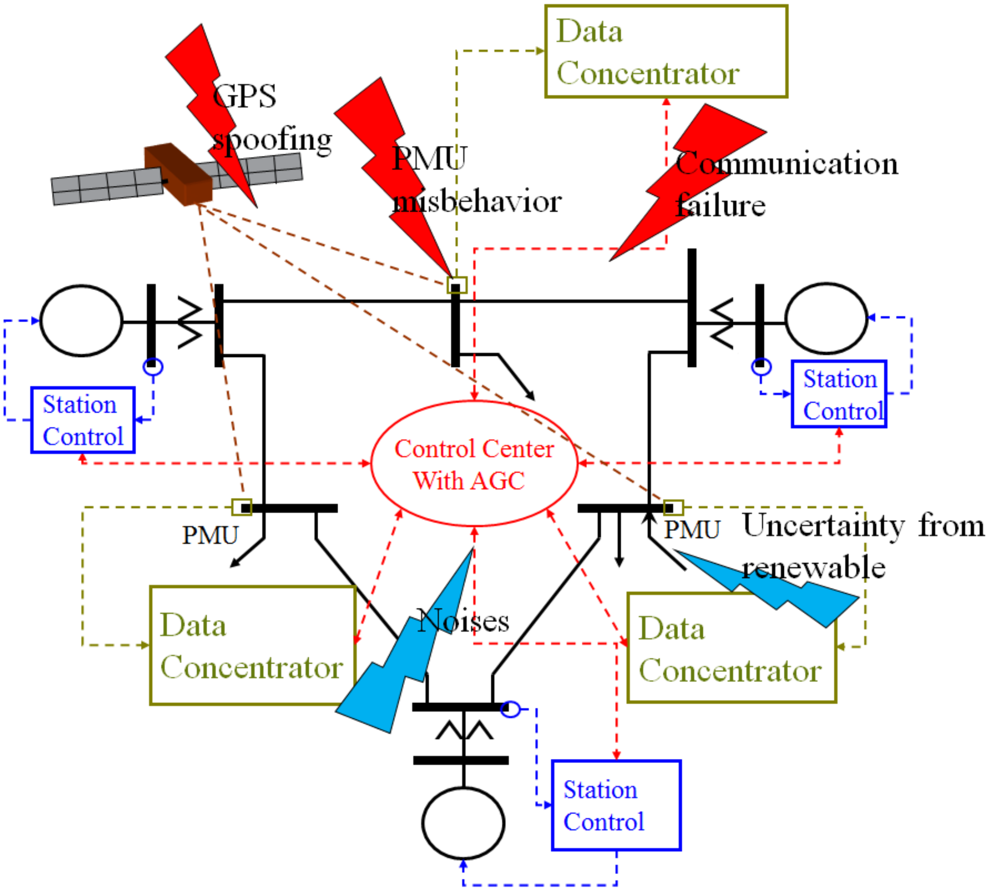
- Develop an exhaustive taxonomy of uncertainty factors in both cyber and physical components in a power grid:
  - Physical-related events: potential faults in physical infrastructure for generation and transmission, and uncertainties from renewable energy sources;
  - Cyber-related events: potential faults, attacks, and noise in cyber infrastructure for measuring, communication, and control.
- Construct appropriate models to quantify the impacts of uncertainties defined in the taxonomy on system dynamic performance and reliability.

Technical Description and Solution Approach

- Identify faults and misbehaviors of cyber components commonly used for communication and control in the power grid. In terms of the impact on the transmitted data quality, the faults/attacks are grouped into two classes: one impacting data integrity (e.g., data are manipulated because of device faults or man-in-the-middle attacks), and the other impacting data availability (e.g., communication delay due to network traffic or malicious DoS attacks).
- Assess the impact of the uncertainties affecting system operations and control on overall system dynamic performance and reliability, through tools from stochastic system analysis.

Results and Benefits

- Uncertainty due to renewable-based generation, measurement and network noise, and potential continuous attacks on communication networks is properly modeled as a set of stochastic processes.
- A framework to evaluate the impact of various uncertainty factors has been set up. First, a comprehensive power system model with automatic generation control has been formulated as a stochastic hybrid system. Based on the model, the statistics of system performance metrics (e.g., system frequency) are being evaluated.



- We have proposed a variety of system communication network attack scenarios that would adversely affect power system performance metrics. Two classes of attack scenarios have been identified that would significantly degrade the system performance. One scenario is to impose properly tuned random noise into the measurements. The other one is to introduce random delay in the communication network.
- **Technology Readiness Level:** Ongoing research. Preliminary results are being obtained as expected on test systems.

Researchers

- Alejandro D. Domínguez-García, aledan@illinois.edu
- Jiangmeng Zhang, jzhang67@illinois.edu

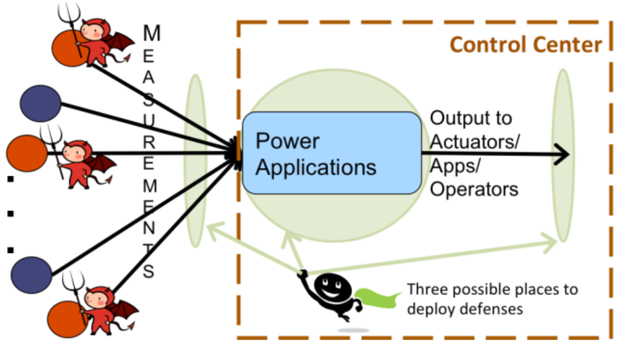
Security and Robustness Evaluation and Enhancement of Power System Applications

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 in order to improve the robustness of power systems against cyber attacks. A new direction is to study ways to secure power system applications in cloud computing environments.

Research Objectives

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


MEASUREMENTS
Control Center
Power Applications
Output to Actuators/ Apps/ Operators
Three possible places to deploy defenses

Technical Description and Solution Approach

- Understand the behavior of power system applications and analyze their robustness in the presence of malicious data modification.
- 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.
- Study ways to protect power system applications for deployment in cloud environments.

Results and Benefits

- Proposed a framework for a security-oriented cyber-physical contingency analysis in power infrastructures. It allows for analyzing the impact of and ranking potential cyber-induced contingencies (*IEEE Transactions on Smart Grid*, 2014).
- Studied security issues surrounding smart distribution grids. Specifically, we looked at data integrity attacks on integrated Volt/VAR control and proposed countermeasures (presented at *American Control Conference*, 2014).
- Developed a scheme to detect malicious data in state estimation that leverages system losses & estimation of (perturbed) parameters (presented at *IEEE SmartGridComm*, 2013).
- Proposed a confidentiality-preserving obfuscation approach for cloud-based power system contingency analysis (presented at *IEEE SmartGridComm*, 2013).
- Studied security issues surrounding the use of cloud computing for the power grid. Specifically, looked at service composition options and assured clouds (presented at *USENIX HotCloud,* 2013).
- Proposed a state estimator that leverages both cyber and power system information and is more robust against false data injection (*IEEE Transactions on Smart Grid*, December 2012).
- Identified ways to inject false data into power flow computations, and investigated defenses (presented at *IEEE SmartGridComm,* 2012).
- Proposed a topology perturbation-based approach for defending against false data injection (*HICSS* 2012).
- 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 (presented at *CPSWeek Workshop on Secure Control Systems,* 2010).
- 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.
- 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: Collaborated with researchers at KTH Royal Institute of Technology in Sweden; collaborated with TCIPG alumni at PowerWorld and the University of Miami.
- **Technology Readiness Level:** This technology is currently in the research and design phase.

Researchers

- Rakesh B. Bobba, rbobba@illinois.edu
- Miao Lu, mlu20@illinois.edu
- Pete Sauer, psauer@illinois.edu

- **External Researchers:** Saman Zonouz (Rutgers), György Dán, Henrik Sandberg, Andre Teixeira, Ognjen Vuković (KTH Royal Institute of Technology), Matt Davis (PowerWorld Corp.)
- **Past Researchers:** Robin Berthier, Roy Campbell, George Gross, Erich Heine, Himanshu Khurana, Kate Morrow, Klara Nahrstedt, Will Niemira, Tom Overbye, William H. Sanders, Al Valdes, Qiyan Wang, and Zheming Zheng

Industry Collaborators

- Matt Davis (PowerWorld), Will Niemira (Sargent & Lundy)

Synchrophasor Data Quality

Overview and Problem Statement

Synchrophasor data are envisioned to be a key enabler for real-time power grid situational awareness and control.

More than 1,000 phasor measurement units (PMUs) have been installed across North America and are generating synchrophasor data. However, the efforts to aggregate and process the synchrophasor data to produce consistently available, reliable, and actionable information have been challenging. Power system operators widely report synchrophasor data availability and trustworthiness issues as significant obstacles to realizing the envisioned capabilities and benefits.

Research Objectives

- Investigate the sources, effects, and implications of absent or erroneous synchrophasor data.
- Seek a fundamental understanding of real-time synchrophasor measurement challenges, as well as synchrophasor data quality measures (error, availability, and reliability).
- Characterize the sources of synchrophasor data quality shortfalls in the utility system from point of measurement to point of use.
- Identify and distinguish data quality issues due to system errors, system events, and maliciously altered data.
- Understand the implications of defective or absent synchrophasor data for system situational awareness.
- Develop methods for detecting and remedying defective synchrophasor data.
- Investigate next-generation phasor measurement device requirements.
- Develop and implement algorithms for next-generation PMUs.
- **Smart Grid Application Area:** Experiment-based trust assessment.

Technical Description and Solution Approach

- Establish collaborative research partnerships with power industry entities that collect synchrophasor data to classify synchrophasor data error sources, characterize the frequency of data errors, and identify strategies for improving synchrophasor data quality. Characterize the errors, availability, and reliability of field measurements and phasor measurement devices.
- Participate in and contribute to North American Synchrophasor Initiative (NASPI) working group meetings and research activities.
- Build and test an “open-box” PMU compliant with industry standards; understand the challenges of measuring, processing, synchronizing, and integrating synchrophasor data.

Results and Benefits

- The activity has established partnerships with the American Transmission Company (ATC) and the Statistics Department of Pacific Northwest National Laboratory (PNNL), laying the groundwork for “discovery” analysis of synchrophasor data being measured on ATC’s system.
- We are working with Jim Kleitsch, System Operations Engineer with the American Transmission Company (ATC), to investigate synchrophasor data quality using ATC synchrophasor data from 90+ PMUs. Kleitsch is the operations lead for the ATC DOE Synchrophasor Project, which involves the addition of 45 PMUs on the ATC system, and helps manage the 40 operational PMUs that ATC already has up and scanning at sites scattered across their footprint.
- In coordination with Brett Amidan, Statistics Department, PNNL, the team has adapted PNNL’s Situational Awareness and Alerting Report (SitAAR) tool to ingest and analyze ATC’s archived synchrophasor data. SitAAR uses the “R” statistical computing environment. The SitAAR tool enabled the identification of several event signatures within a small ATC data set.

- Using a small ATC sample synchrophasor data set, the team has written signal-processing algorithms to investigate methods for screening synchrophasor data in real-time for signatures of transmission system events.
- The activity has demonstrated a PMU developed using National Instruments' LabVIEW software and C-RIO hardware (compact reconfigurable I/O (RIO) architecture). The PMU is being integrated with an uninterruptible power supply to enable transient measurements during power outages on the power distribution system. Synchrophasor data are buffered and transferred hourly to a remote Linux web server via an FTP connection.
- The activity has evolved its PMU design to reduce per-unit cost from ~$1,000 to ~$250.
- The activity has been investigating ways to visualize power system cyber security relationships detailed in NISTIR 7628, Guidelines for Smart Grid Cyber Security. Early development efforts used MATLAB as the visualization platform; the team's poster describing this effort earned 3rd place recognition in the 2014 IEEE Transmission and Distribution Conference student poster session. Recent efforts have pursued creation of a web-based HTML application.
- **Technology Readiness Level:** Technology concept and/or application formulated.

Researchers

- Karl Reinhard, reinhrd2@illinois.edu
- Bogdan Pinte, bpinte2@illinois.edu
- Michael Quinlan, quinlan4@illinois.edu
- Kenta Kirihara, kirihar1@illinois.edu
- Daniel A. Long, dalong2@illinois.edu
- Brianna Drennan, bdrenna2@illinois.edu
- Yang Liu, yliu160@illinois.edu
- Peter Sauer, psauer@illinois.edu

Industry Collaborators

- American Transmission Company, Jim Kleitsch
- Pacific Northwest National Laboratory, Brett Amidan
- National Instruments

Tamper Event Detection Using Distributed SCADA Hardware

Overview and Problem Statement

Utilities collect and monitor data from a number of devices, such as recloser controls, that are distributed across their service areas. The devices are often mounted on utility poles in both remote and densely populated areas, and have little physical security other than the cabinets in which they are placed. However, the devices require a connection to the utility's SCADA network, which means that an attacker could gain access to the network and begin injecting traffic just by defeating the physical security of the cabinet.

While a utility would like to detect tampering with one of its devices, several issues complicate this goal:

- The utility requires its devices—and therefore its tamper detection equipment—to operate in extreme environments without generating false positives.
- The utility must also allow for "legitimate" tamper events, such as servicing by a technician.
- The utility may also want to leave the connection open in the event of a natural disaster, to simplify and expedite recovery effects.

Prior efforts in distributed sensing and tamper detection/physical security do not solve the problem, because:

- They **do not consider the device's physical environment** in their risk assessments, or **cannot operate in all of the environments** that power devices live in.
- They **do not consider user preferences** with respect to certain event types.
- They are focused only on **detecting** events rather than **responding** to them. Those that do respond are **limited to a single course of action.**
- The attack detection models used are **not powerful enough** to look for the event indicators we are concerned about.

Research Objectives

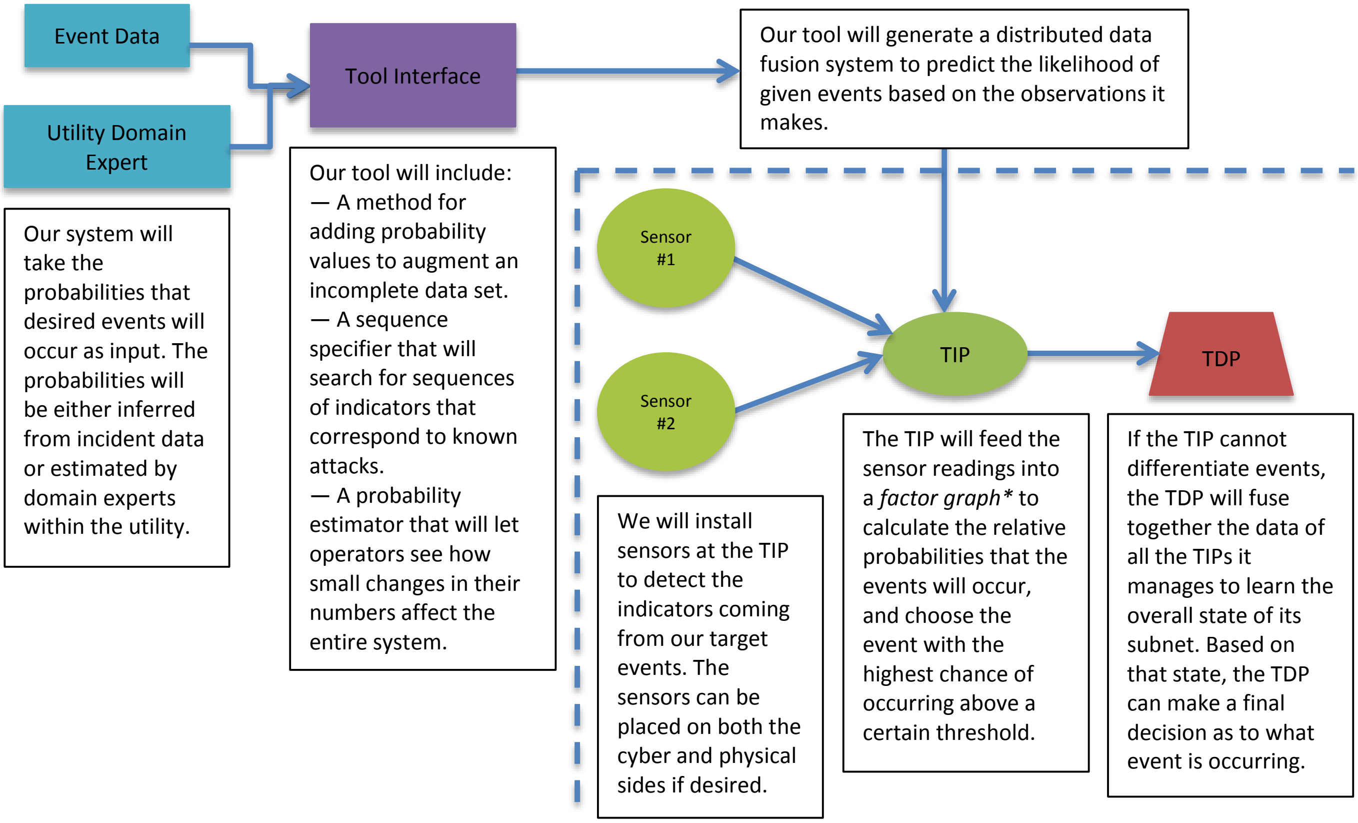
- To prevent attackers from accessing a utility's control network by tampering with its remotely deployed embedded devices.
- To determine whether a tamper signal sent from a device is malicious, is benign (e.g., a technician is servicing the device), or represents an emergency situation, such as a natural disaster.
- To use data from sensors attached to an embedded device, as well as signals from similar devices nearby, to decide whether a tamper signal coming from the device is legitimate or a false positive.
- **Smart Grid Application Area:** Electricity distribution systems, specifically the embedded devices that are spread throughout a utility's service area.

Technical Description and Solution Approach

We propose a *distributed* approach to tamper detection, consisting of three components:

- **Tamper Information Points (TIPs)**, which live inside a utility's cabinets, use their sensors to monitor the cabinet for possible intrusions, and send tamper signals upstream when they see an abnormal reading.
- **Tamper Enforcement Points (TEPs)**, which act on tamper decisions that are made. For example, the TEP could destroy secret data on a device.
- **Tamper Decision Points (TDPs)**, which reside in a higher-security area of the network, collect information from the TIPs within the network, and send tamper event detection decisions to the TEPs in the network.

Our plan is to build a tool that utility operators can use to build customized tamper detection systems for their specific networks.



Our tool will generate a distributed data fusion system to predict the likelihood of given events based on the observations it makes.

Our system will take the probabilities that desired events will occur as input. The probabilities will be either inferred from incident data or estimated by domain experts within the utility.

Our tool will include:
— A method for adding probability values to augment an incomplete data set.
— A sequence specifier that will search for sequences of indicators that correspond to known attacks.
— A probability estimator that will let operators see how small changes in their numbers affect the entire system.

We will install sensors at the TIP to detect the indicators coming from our target events. The sensors can be placed on both the cyber and physical sides if desired.

The TIP will feed the sensor readings into a *factor graph** to calculate the relative probabilities that the events will occur, and choose the event with the highest chance of occurring above a certain threshold.

If the TIP cannot differentiate events, the TDP will fuse together the data of all the TIPs it manages to learn the overall state of its subnet. Based on that state, the TDP can make a final decision as to what event is occurring.

Project Status

- We are currently constructing a prototype TIP/TDP setup for a sample power network. We can evaluate the system for speed and accuracy, and use it to inform our tool design.
- This problem was first proposed to us by Schweitzer Engineering Laboratories, and we are continuing to work with them as we develop our product.

Researchers

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

Industry Collaborators

- Schweitzer Engineering Laboratories
- IBM
- Aruba Networks

* See “Extending Factor Graphs so as to Unify Directed and Undirected Graphical Models” by Brendan Frey (*Proceedings of the Nineteenth Conference on Uncertainty in Artificial Intelligence*, 2003).

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

Overview and Problem Statement

Efforts are underway to switch existing nuclear power plants (NPPs) based on analog control systems to digital control systems. It is expected that digital Instrumentation and Control (I&C) systems will be used in all future NPPs, and they are expected to solve the obsolescence problem of analog components and to improve safety and performance. However, before analog systems can be switched to digital, much work needs to be done to ensure the safety of the new systems to the level required by the nuclear sector. The goal of this research project is to identify and experimentally evaluate possible faults and attacks against the safety-critical digital I&C systems destined for use in NPPs. In pursuit of that goal, the project is developing tools and methods and building a testbed to study and validate the failure/attack behavior of the safety-critical digital I&C systems.

Research Objectives

- Experimentally evaluate the resiliency and security of the digital I&C system.
- Build a testbed with real-time simulation of an NPP in conjunction with physical digital I&C components for realistic NPP operation simulation.
- Identify potential attack vectors, single points of failure, and common mode failures in the future digital I&C systems.
- Develop fault injection and attack simulation tools to simulate various failures and attacks on the testbed to demonstrate their potential impacts.
- Develop logics to analyze and report on the impact of failures and attacks on the safety-critical digital I&C components of an NPP.
- **Smart Grid Application Area:** Develop tools to enable experimental evaluation of the resiliency and security of the safety-critical digital I&C systems to be used in NPPs in the future.

Technical Description and Solution Approach

- A testbed is being developed for the purpose of security and resiliency evaluation of the digital I&C systems for NPPs. It consists of a reactor model, a digital controller, and associated communication links. The digital controller has a Triple-Modular Redundant (TMR) architecture to ensure continuous availability of the controller. (Figure 1 shows the NPP testbed setup.)
- A real-time NPP simulator has been developed in LabVIEW; the point kinetics equation is being used for the core and models of a pressurizer and a pump. The model for the primary loop is fairly complete; the secondary loop is still in progress.
- The NPP simulator and the TMR controller, with its associated application program, have been assembled, and communications between them have been established. The testbed also includes a set of specialized fault/error injectors to inject different types of faults/errors, both transient and permanent.
- A fault injection module is being developed in LabVIEW in order to simulate hardware failures. The module contains a fault list manager (FLM), a fault injection manager (FIM), and a result analyzer (RA). The FLM picks a fault type and fault location at random from the pre-generated list of fault locations and types, and communicates this information to the FIM, which injects faults into the system.
- Since the digital controller has a TMR architecture, common-mode failures, in which a failure or attack would impact all three redundant modules, are of the greatest concern. One potential common mode failure would be corruption of the communication channel during configuration of the digital controller. Since the same configuration is applied to all three modules in the controller, a corruption or attack on the communication channel could result in a common mode failure, as shown in Figure 1.

Results and Benefits

- The testbed provides the ability to simulate the operation of an NPP with real-time control feedback from the digital controller.
- Potential future uses of the testbed include cyber security tests of digital I&C systems for NPPs, stability analysis of the NPP testbed connected to a simulator of the electric grid, and human machine interface and human factor engineering studies of newly developed control rooms for NPPs.
- **Technology Readiness Level:** Ongoing development of the testbed and experimental evaluation tools.

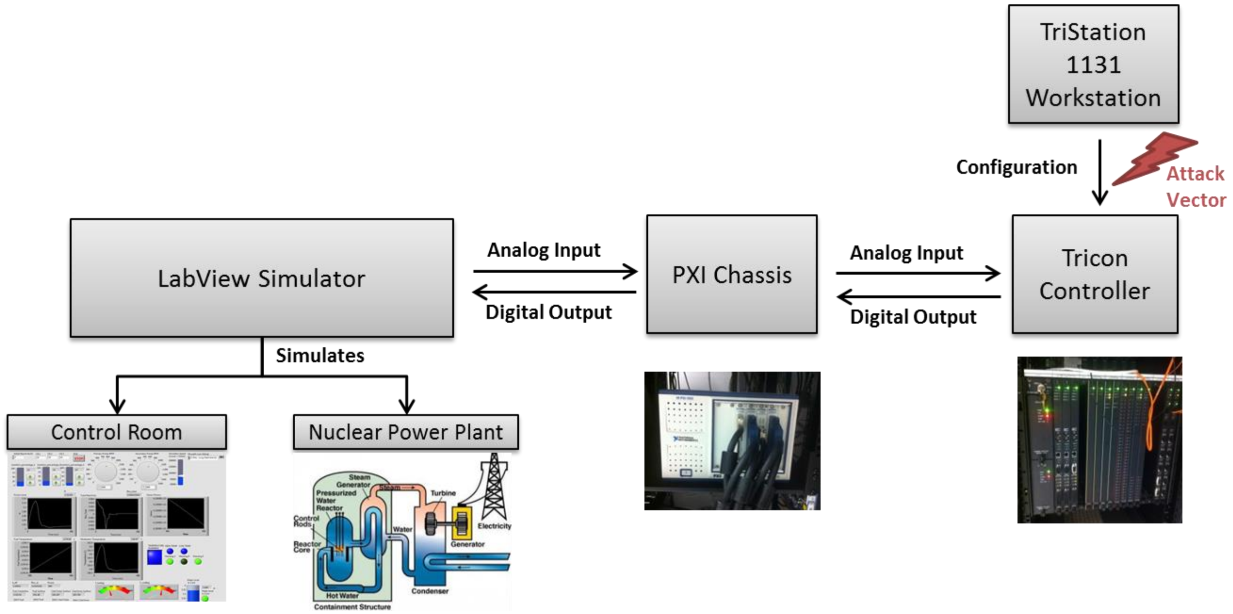


Figure 1. NPP Testbed Setup

Researchers

- Daniel Chen, dchen8@illinois.edu
- Yongkyu An, an24@illinois.edu
- Calogero Sollima, csollima@illinois.edu
- Zbigniew Kalbarczyk, kalbarcz@illinois.edu
- Ravishankar Iyer, rkiyer@illinois.edu

Trustworthiness Enhancement Tools for SCADA Software and Platforms

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: Linux prototype exists; 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 plain-text 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 is 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 basis 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.
- Our ELFbac implementation for Linux x86-64 is in code review; an ARM feasibility study has concluded.
- We developed the concept of Intent-level semantics for application security policies, presented at a variety of industry events, including Intel and Microsoft invited talks.
- We demonstrated a new threat model for embedded systems firmware, which allows an unscrupulous vendor or a supply chain attacker to plant an innocent-looking “bug door” in the interrupt-handling code, which nevertheless allows exfiltration of secrets or sensitive parts of firmware from a “bugdoored” device. To be presented at the ACSAC 2014 conference.
- **Technology Readiness Level:** Varies by product; see table above.

Researchers

- 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., ELFbac)

Understanding and Mitigating the Impacts of GPS/GNSS Vulnerabilities

Overview and Problem Statement

The Global Positioning System (GPS) is the mostly widely used example of what are more broadly known as Global Navigation Satellite Systems (GNSS). GPS provides precise location and time information to any receiver capable of receiving and decoding the timing signals from at least 4 satellites in the GPS constellation. The civilian GPS signal does not come with any authenticators and, given the relatively low signal strength, is vulnerable to intentional or malicious jamming from land-based transmitters. The application of GPS devices in the power sector can potentially have significant impact on the bulk electric system through their integration into synchronization devices such as Phasor Measurement Units (PMUs). Given that PMU technology is expected to transition to control applications in the future and that the primary time synchronization mechanism used by PMUs (today) is GPS, there is growing concern that a dependency on GPS will introduce a built-in vulnerability into the infrastructure.

Research Objectives

- Develop a hardware-based testbed capable of investigating the resiliency of various PMUs to known GPS spoofing attacks.
- Demonstrate the feasibility of an attack using that hardware setup.
- Investigate possible detection and mitigation schemes to harden PMUs to GPS spoofing attacks.
- Understand the timing and synchronization needs in power system applications.
- Develop a trustworthy GNSS-based timing source that is more spoofing-resilient than current GPS-based clocks.
- **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 GPS signals, which are unauthenticated.
- Multi-layer scheme for secure GPS-based timing: Investigate eight countermeasures in three layers: GPS raw signals layer; semi-processed signal layer; and fully processed signal layer.
- Use the fact that the GPS receivers are static to further improve the accuracy and robustness of GPS-based timing.
- Have multiple GPS receivers at different locations cross-check for anti-spoofing.
- Continue development of a GPS simulator using an NI PXI platform to be interfaced to the PMUs in the TCIPG testbed.

Results and Benefits

- Have investigated and implemented Position-Information-Aided Vector Tracking Loop, and have demonstrated:
    - Robustness against jamming with 5dB more noise tolerance compared with scalar tracking;
    - Capability of successfully detecting meaconing attacks;
    - Improvement of the accuracy of the timing solutions when compared with traditional scalar tracking (15 ns vs. 50 ns).
- Have explored cross-checking GPS military P(Y) codes among multiple GPS receivers at different locations, and have shown:
    - Anti-spoofing robustness grows exponentially with the number of cross-check receivers;

  - A modest number of low-cost unreliable receivers can outperform a high-end secure cross-check receiver.
- A hardware-based testbed is being created to investigate effects of spoofing on PMUs.
- **Technology Readiness Level:** Ongoing research.

Researchers

- Grace Gao, gracegao@illinois.edu
- Jonathan J. Makela, jmakela@illinois.edu
- Alejandro Domínguez-García, aledan@illinois.edu
- Daniel Chou, dchou3@illinois.edu

TCIPG

Cross-Cutting Efforts

Education and Engagement

Testbed Initiatives

Incubator Research Activity

Cross-Cutting Efforts Page No.

Education and Engagement Lead: 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

Education and Engagement

Overview and Problem Statement

Members of the TCIPG Education team work with teachers and students, informal educators, industry, and other TCIPG researchers to develop a wide variety of educational opportunities. Our activities are designed to engage learners of all ages. TCIPG Education offers a variety of workshops, seminars, and other learning opportunities for power and cyber professionals. 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 and to provide for an informed citizenry. TCIPG Education curriculum materials are featured in several curriculum projects in various parts of the U.S. and Canada. TCIPG engages in public outreach through participation in the annual Illinois Public Engagement Symposium and in various other conferences, exhibits, and symposiums.

Objectives

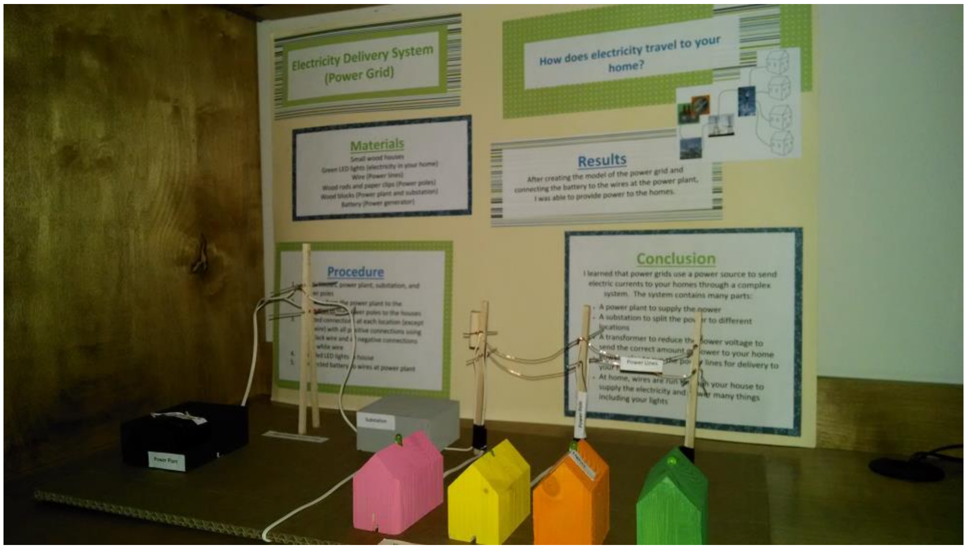
- Link researchers, educators, consumers, and students in efforts to transition to a more modern, secure, and resilient electrical system.
- Illustrate issues necessary for consumer acceptance and use of smart grid technologies.
- Create interest in related STEM careers and provide an engaging interactive curriculum.
- Create interest in further learning.
- Connect with schools, national curriculum endeavors, and informal educators.
- **Smart Grid Applications:**
  - 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.
  - Offer learning opportunities for power and cyber professionals.

Solution Approach

- Create literacy-enhanced, hands-on learning opportunities.
- Correlate hands-on explorations with virtual simulations.
- Create a TCIPG Minecraft Power World that invites users to build a virtual neighborhood, and then explore grid connection and a variety of generation sources to electrify their world.
- Incorporate the science of electricity and the historical and economic development of the electric grid into a "quest" type of video game.
- Develop and disseminate curriculum materials that require learners to communicate their strategies, develop convincing arguments, create models, conduct simulations, and learn in ways not possible prior to the digital revolution.
- Participate in campus and community outreach events.

Results and Benefits

- Curriculum materials, websites, Java applets, apps for tablets, and hands-on activities.
- Partnerships and external interactions:
    - National 4-H SET Initiative.
    - KidWind and WindWise Education.
    - Project Lead the Way pre-engineering curriculum.
    - National Science Teachers Association (NSTA).
    - ASEE.
    - Questar-Bridges project with MESO (Mesoscale Environmental Simulations and Operations, Inc.).
    - Southern Regional Education Board Advanced Career Energy and Power curriculum.
    - Girls' Adventures in Mathematics, Engineering, and Science (GAMES) Camp.
    - Girls Engaged in Math and Science (GEMS) Camp.
    - USA STEM Festival.


Electricity Delivery System (Power Grid)
How does electricity travel to your home?
Materials
Results
After creating the model of the power grid and connecting the battery to the wires at the power plant, I was able to provide power to the homes.
Procedure
Conclusion
Power Plant
Substation

Researchers and Designers

- Jana Sebestik, sebestik@illinois.edu
- George Reese, reese@illinois.edu
- Jason Mormolstein, jmormol2@illinois.edu
- Brandan Pflugmacher, pflugma1@illinois.edu
- Rebecca Byrd, rabyrd2@illinois.edu
- Brendan McDonnell, brendan.r.mcdonnell@gmail.com
- Mark Talbot, mark.talbot12@gmail.com
- Sufei Zhang, szhang37@illinois.edu
- Yingying Cai, ycai23@illinois.edu

Industry Collaborators

- Rod Hilburn, RHilburn@ameren.com
- David Norton, david.norton@ferc.gov
- Brian Huang, brian.huang@sparkfun.com

Smart Grid Cyber Security: Training for the Future

Overview and Problem Statement

The intent of this activity is to develop an open training platform that facilitates the rapid education of a wide variety of participants on important aspects of smart grid cyber security. The training platform will consist of both presentations and hands-on training exercises that will aid in the education of interested parties in research, industry, and government.

In this work, we aim to create a phased and modular learning platform that provides the essential base knowledge for this sector and builds upon that base knowledge with each lesson to advance students' understanding of smart grid cyber security. At each phase in the process, we will provide concrete applications of the topic areas to facilitate participants' learning. By using a combination of diverse educational strategies, we expect to be able to train a variety of people effectively and efficiently.

Research Objectives

- Develop a modular, phased learning platform for cyber security education in the electric power grid.
  - Made up of diverse topic areas spiraling deeper into relevant details of interest (tracks).
  - Consists of lecture material, an electronic exercise environment, and hands-on exercises to support learning.
- Provide a fully open, available, and vetted curriculum.
  - Material needs to be widely usable, and designed such that different experts can easily contribute new content and revise existing content as the landscape changes.
  - Made to be accessible to anyone, ranging from CEOs to engineers to office staff, while taking a project-based, hands-on, active-learning approach to reinforce the subject matter.
- **Smart Grid Application Area:** Education, training, and workforce development.

Technical Description and Solution Approach

- This effort started with an initial gap analysis and mapping of existing cyber security training for the electric power grid, in relation to the DOE Secure Power System Professional (SPSP) and DHS National Initiative for Cybersecurity Education (NICE) competencies and job responsibility designations.
- We are gathering topics of interest and information on sector needs by working with industry and leveraging existing knowledge of the sector.
- Based on the gap analysis, a core curriculum is being developed that is a combination of new material and material from previous TCIPG short courses on cyber security in the electric power grid, and is structured to facilitate easy extension into new areas.
- The material follows a phased approach to learning that includes active, project-based "learning by doing" to anchor the training material.
- We are preparing lectures along with hands-on exercises to reinforce the material under discussion.
- We will release the training in stages, and will revise it in response to feedback from the participants.
- Ongoing analysis will be conducted to determine coverage and needed topics for future releases.

Topics Covered

- Power fundamentals
- Cyber security fundamentals
- Communications and networking

Topics Covered (con't)

- Cyber infrastructure in the electric power grid
- Monitoring and situational awareness
- Advanced metering infrastructure
- Smart grid guidance documents
- Electric sector capability maturity model
- Privacy in the smart grid
- Critical infrastructure security examples and impact
- A perspective on security
- Security challenges in distribution automation
- Embedded assessment
- SCADA fundamentals
- Robust control systems
- And more…

Results and Benefits

- Gap analysis has been conducted along with a mapping to job responsibilities and competencies.
- Preliminary curriculum has been created.
- Several modules have been alpha-tested in the field with industry participants.
- Topical spirals into more detail are being developed.
- The training reflects the broad expertise of the TCIPG research team and acts as a training platform that future researchers, workforce, or government entities can build upon and adapt.
- Offers open, widely available training material on cyber security in the electric power grid that has been vetted by subject matter experts.
- Provides increased accessibility to training in this domain.
- **External Interactions**: CYBATI and SANS
- **Technology Readiness Level:** Alpha (but has already been utilized).

Field Use

- Prior incarnations of the lecture material and short courses have been used to train hundreds of attendees from academia, industry, and government.
- A very early version of the revised lecture material was used at the 3CS conference to provide training for community college educators and other interested parties.
- Modules of the core curriculum have been used to train vendors and utility personnel in this domain.
- Strong continued industry interest in the material.

Future Efforts

- Full open-source release planned for August 2015.
- Explore integration and use with other efforts such as cybatiWorks or the SANS curriculum.

Researcher

- Tim Yardley, yardley@illinois.edu

Testbed Overview

Overview and Problem Statement

To provide a cutting-edge facility that enables foundational research in the smart grid domain.

Research Objectives

- Span transmission, distribution & metering, distributed generation, and home automation & control, providing true end-to-end capabilities.
- Provide foundational support for TCIPG projects.
- Analyze research across varying fidelities and scales.
- Serve as a national resource for experimental work in research and analysis of trustworthy power grid systems.

Technical Description and Solution Approach

- Problem Space:
  - How does one provide a scalable and flexible framework that can operate at varying fidelities to facilitate emerging research?
  - What is the right mix of simulation, emulation, and real equipment to accomplish the research goals?
  - How does one programmatically set up, integrate, control, and interact with this equipment?
- Approach:
  - Develop new modeling and evaluation technologies to enhance evaluation capabilities of the testbed.
  - Continue to expand testbed capabilities, features, and functionality through strategic integration of equipment.
  - Provide integration glue that provides unique capabilities in the testbed environment.
  - Leverage existing & emerging research from other areas when it can advance the testbed effort's goals.
- **Smart Grid Application Area:** End-to-end system and individual components.

Results and Benefits

- Virtual Power System Testbed (VPST and RINSE/S3F): large-scale cyber-physical simulation.
- Network Access Policy Tool (NetAPT/NP-View): policy tool to evaluate network access paths and verify compliance with a global policy.
- Tools and analysis of smart grid protocols (Amilyzer, protocol parsers and test harnesses, and scalable environment).
- Quantum Key Distribution: validation of external quantum computing research through application to smart grid systems.
- Enabling advanced research for smart grid efforts throughout the world via federation and collaboration.
- Flexible framework leverages tailored operating constraints to use resources efficiently.
- Open for collaborative research, facility-driven use, sponsored research, and technical testing.
- **Partnerships and External Interactions**:
  - Enabling smart grid research and transition of technology.
  - Leveraged for other industry interactions and projects.
- **Technology Readiness Level:** Always adding capabilities, but fully functional and in active use.

Researchers

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

Capabilities

- Full end-to-end smart grid capabilities.
- On-grid testing capabilities via Ameren TAC facility (with fiber-optic interconnects to our primary testbed).
- Deployed advanced metering infrastructure (AMI).
- Solar research platforms.
- Real, emulated, and simulated hardware/software for scalability.
- Real data from the grid, industry partners, etc.
- Power simulation, modeling, and optimization of various forms.
- Network simulation, modeling, and visualization of various forms.
- Advanced hardware-in-the-loop cyber-physical simulation.
- WAN/LAN/HAN integration and probes.
- Security and protocol assessment tools (static/dynamic analysis, test harnesses, fuzzing).
- …and more

Assets

- RTDS, PowerWorld, PSSE, PSCAD, PSLF, DSAtools, DynRed.
- RINSE, tstBench, LabView, OSI PI, OSIi Monarch, SEL suites, PGDA.
- Full range of open-source power grid tools (openDNP3, openPDC, openPG, openXDA/openFLE, openHistorian, SIEGate).
- GPSes, substation computers, relays, PMUs, testing equipment, PLCs, security gateways, NI platforms.
- Power analysis tools, PDCs, data analytics.
- Full AMI deployment, TCIPG Smart Meter Research Platform.
- RTUs, F-Nets, inverters, oscilloscopes, firewalls, embedded devices, sensors, spectrum analyzers, SIEMs, IDSes.
- Home EMS, energy and environmental monitoring devices, ZigBee, automation.
- Display wall, visualization platforms (STI, RTDMS), training platforms.
- Mu Dynamics, Fortify, security research tools, IBM Tivoli suite.
- DETER integration and cyber-physical extension via federation.
- … and more.

Use Cases

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

Industry Donations

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

Incubator Project: Privacy-Preserving Vehicle-Miles-Traveled Tax Scheme

Overview and Problem Statement

If, as many expect, vehicular transportation becomes less dependent on liquid fuels and instead comes to rely on electric energy, the historical fuel-based road tax system will become unworkable. Taxes collected on the basis of vehicle-miles-traveled (VMT), adjusted for vehicle weight, are often proposed as an alternative. The U.S. federal government gives states independence in setting taxes, so a system for collecting VMT taxes must calculate and collect taxes at different rates when a vehicle travels in different jurisdictions. At the same time, however, privacy concerns argue that a system that allows vehicle owners to pay correct taxes without identifiably disclosing their personal miles traveled in each jurisdiction is preferable to one that does require such disclosure.

In this work, we have developed a tax reporting and collection system that could be operated cooperatively by federal and state governments and that:

- Allows vehicle owners to pay the total tax owed to the federal government as broker for the states.
- Allows each state to verify what is owed to it based on reports provided by vehicle owners without requiring identifying information in the vehicle mileage reports.
- Provides assured security (confidentiality, integrity, privacy, and non-repudiation) on a per-car, per-state basis, and provides built-in fault tolerance and attack resilience features.

Research Objectives

- Design a system that allows VMT taxes to be reported and collected without requiring identifying information for per-state mileage reports and without disclosing per-state mileage to the federal government, which serves as the broker for the states.
- Explore mechanisms and protocols for conducting transactions with the least possible disclosure of identifying information.
- **Smart Grid Application Area:** Electric vehicle economic systems: taxation.

Technical Description and Solution Approach

- The federal government broker receives identifiable reports from vehicle owners, but because the state-specific information is encrypted, the broker cannot determine state-specific mileage.
- The broker repackages the vehicle report so that it is no longer identifiable and sends it to the various states.
- Each state determines what it is owed for the given vehicle and proves to the broker that it has calculated correctly.
- The broker confirms the transaction with the vehicle owner and collects the total tax owed.
- The broker pays the states the aggregate taxes for each reporting period.

Results and Benefits

- The proposed scheme provides a way to collect jurisdiction-specific taxes without requiring identifiable disclosure of miles traveled to the jurisdictions.
- **Technology Readiness Level:** Exploratory.

Researchers

- Carl Hauser, hauser@eecs.wsu.edu
- Chin-Wei Chang, chin-wei.chang@email.wsu.edu
- Thoshitha Gamage, tgamage@siue.edu