TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Research Activity Fact Sheets

November 2013

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 both malicious cyber attacks and accidental failures. Risks may come from adversaries who gain access to control networks or launch denial-of-service attacks on the networks. They can also come from accidental causes, such as natural disasters 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 built, 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 through 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 more than 20 faculty, 20 technical staff, and approximately 45 students at 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 National SCADA Testbed (NSTB) portfolio. In June 2013, TCIPG entered the fourth year of its five-year period of performance. TCIPG is the successor of an earlier project established with funding from the National Science Foundation in 2005.

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 to automated generation control.

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

- Detection of, response to, and management of attacks.
- Securing of the wide-area measurement system on which the smart grid relies.
- Approaches to maintaining power quality and integrating renewables.
- 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 meet the demands of 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. We recently presented the 2013 offering of our biennial TCIPG Summer School. More than 170 participants attended, 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 and Android) 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

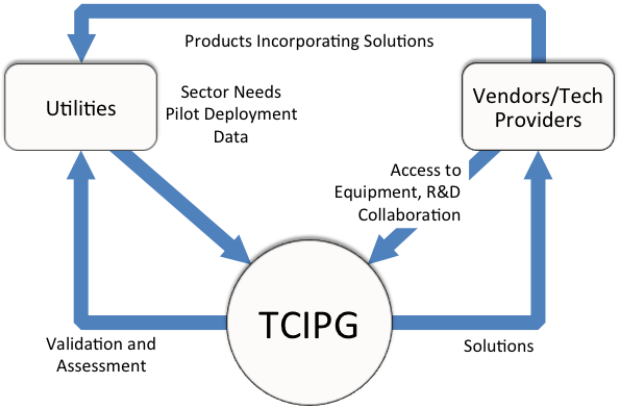
The **electricity industry** in the U.S. is made up of thousands of utilities, equipment and software vendors, consultants, and regulatory bodies. In both its NSF-funded and DOE/DHS-funded phases, TCIPG has actively developed extensive relationships with such entities and with other researchers in the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



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
- **Managing Director, 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@ecs.wsu.edu)

TCIPG

Research Cluster

Trustworthy Technologies for Wide-Area Monitoring and Control

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

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

Cryptographic Scalability in the Smart Grid

Overview and Problem Statement

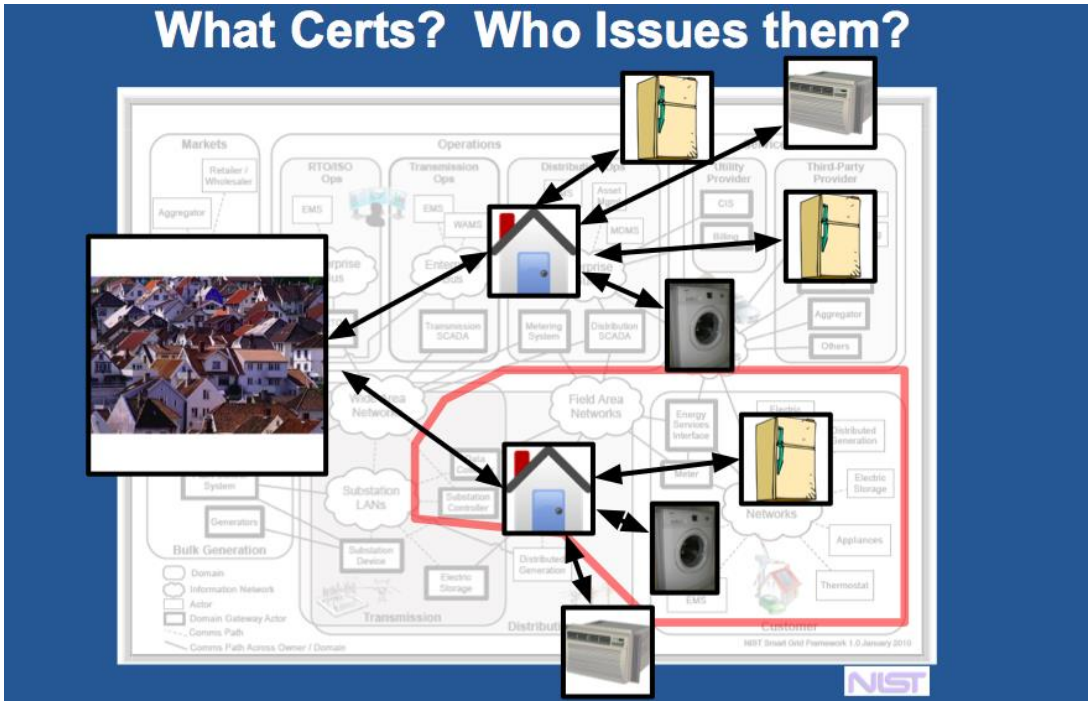
In the envisioned smart grid, massive numbers of computational devices will need to authenticate to each other. In the past, such technology would need to rest on a public key infrastructure (PKI) such as X.509. Today, there are many new cryptographic schemes being proposed to solve this problem. However,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

Research Objectives

- Conventional wisdom says use X.509 PKI in the smart grid. Our goal is to use simulation to look for potential bottlenecks in this trust infrastructure.
- On the transmission side:
    - Real-time is critical.
    - X.509 PKI standard didn't work on BGP with only 30k nodes.
    - Transmission side may have 100k 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.

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 this?
    - 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 tradeoffs?
    - 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?



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.
- Last year, Tucker Ward created the GCS: AMI-side smart grid PKI simulation in the NS3 framework.
- Using that simulation, we can quantify the costs of deploying PKI in the smart grid and use the data to mitigate bottlenecks and other problems.
- Our tool can also extend to other large systems requiring trust infrastructure.
- Collaborations:
    - Simulation advice: David Nicol, UIUC, and Jason Liu, FIU.
    - Smart grid discussions: Robert Lee of GE; Los Angeles Dept. of Power and Water.
    - Alternative crypto discussions: ORNL.
- Technology Readiness Level: development in progress.

Researchers

- Ivan Antoniv, ivan.antoniv.14@dartmouth.edu
- Tucker Ward, tucker.lee.ward@gmail.com
- Sean Smith, sws@cs.dartmouth.edu

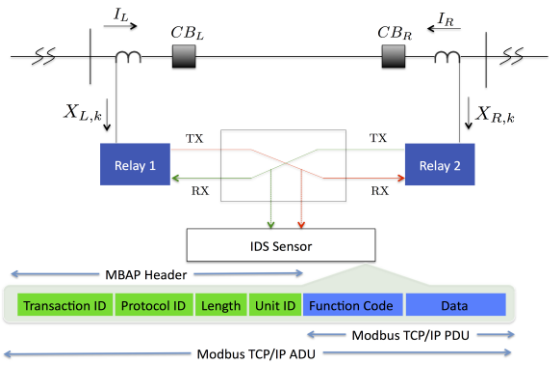
Industry Collaborators

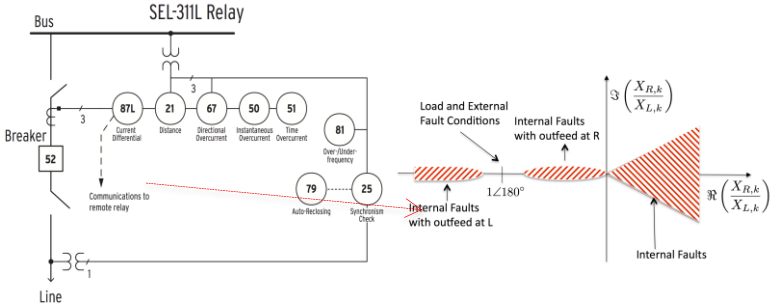
- GE
- Los Angeles Department of Power and Water

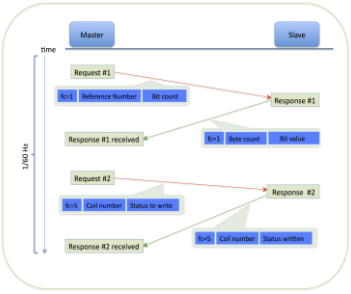
Functional Security Enhancements for Existing SCADA Systems

Overview and Problem Statement

Today the various embodiments of SCADA in Networked Industrial Control Systems (NICS), aimed at protecting critical assets in electrical power transmission and distribution, are incorporating advanced methodologies to shield the communication perimeter of the control area from intruders through firewalls and encryption. However, no methodology is completely attack-proof, and the identification of attacks through an intrusion detection system (IDS) inside the control perimeter is another important potential improvement to ensure security of the cyber infrastructure. The digital relays communicating in order to perform their protection mission send messages conforming to application-layer protocols that are open (e.g., DNP3, Modbus) or vendor-specific. In normal operations, the format and sequence of messages, as well as their timing, are highly predictable in light of the control mechanism with which they are associated. The question we want to address in this activity is how and to what degree it is possible to combine awareness of the control mechanisms executed by the NICS as a possible avenue to further verification that the network is not under attack. After all, most protection schemes available from vendors combine functions that are specified in the comprehensive standard ANSI/IEEE C37.2, as in the example shown in the figure that shows the SEL 311L below and the expected traffic between the two relays in a Modbus implementation of the same function.







While they differ in implementation details, these functions exchange binary (coils) values or analog values in a predictable sequence, which typically lasts half a cycle and repeats with a 60Hz or 120Hz periodicity until faults are detected. These repetitive patterns are important clues to normal monitoring behavior, and out-of-band network IDS systems should leverage the repetitive patterns of functions called in the headers of NICS application layers to detect anomalies.

In the case of an anomaly, mitigating strategies require the ability to make a prediction of the state of the system and its possible evolution. Previously, we also examined if it is possible to use historical data and model predictive control to assess vulnerabilities and best action profiles when the system is experiencing communication failures and attacks.

Research Objectives

The goal of this research is to define a novel framework for network IDS that is tied to knowledge of the underlying control system. The network IDS should be capable of:

1) Verifying whether the communications are consistent with those naturally associated with the automata that the NICS is intended to implement, without interference from exogenous communications;
2) Predicting what the physical vulnerabilities of the system would be once the anomaly has been detected, engaging sensor data historians and using model predictive control strategy to assess the risk.

Technical Description and Solution Approach

To address the first of the two objectives of our project, we are considering network IDS sensors deployed to monitor the links among digital relays and passively analyze packets that are flowing through the network. In order to design a library to identify intrusions, we are leveraging the list of protective devices/functions for power grid assets that are codified in standards (ANSI/IEEE C37.2). Digital relay algorithms are typically described in terms of a concatenation of such functions. Our solution approach is to check the integrity of the information that is used in digital relay algorithms by casting these functions in a library that network IDS software can recognize and understand and use to detect violations.

Our approach includes:

- The study of models for the communication pattern associated with specific application layers used in NICS for specific protection schemes. We are now considering the Modbus protocol exchange corresponding to the hybrid automatons of common protection controllers and their validation using Siemens PLC to verify our research hypotheses on their behavior.
- The development of intelligent anomaly detection techniques that leverage knowledge of the automata information flow and integrate these rules in out-of-band, non-intrusive monitoring sensors, checking consistency between the communications and the digital relay algorithm information exchange.
- Design and implement effective mitigation techniques and controls that could ensure the stability of the system.

Results and Benefits

- We have implemented examples on Ladder logic using a couple of Siemens PLCs.
- We defined the physical models and the hybrid automaton of each case.
- We developed rules of permissible device actions and applied the rules to the observed network traffic using the BRO Network Security Monitor software.
- We monitored in real time the network traffic and raised an alarm whenever an intrusion or malicious action occurred that led the system to operate on an undesired state.
- Partnerships and External Interactions:
    - We are collaborating with Lawrence Berkeley National Laboratory.
    - PG&E has visited UC Davis and proposed to collaborate on developing security studies that pertain to their cyber-infrastructures.
- **Technology Readiness Level:** Theoretical and experimental development.

Researchers

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

Industry Collaborators

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

GridStat Middleware Communication Framework: Application Requirements

Overview and Problem Statement

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

Research Objectives

- Understand the real-time communication requirements for power system applications for the emerging smart grid.
- Develop a technical approach to assess those requirements.
- Develop a testbed integrating 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.

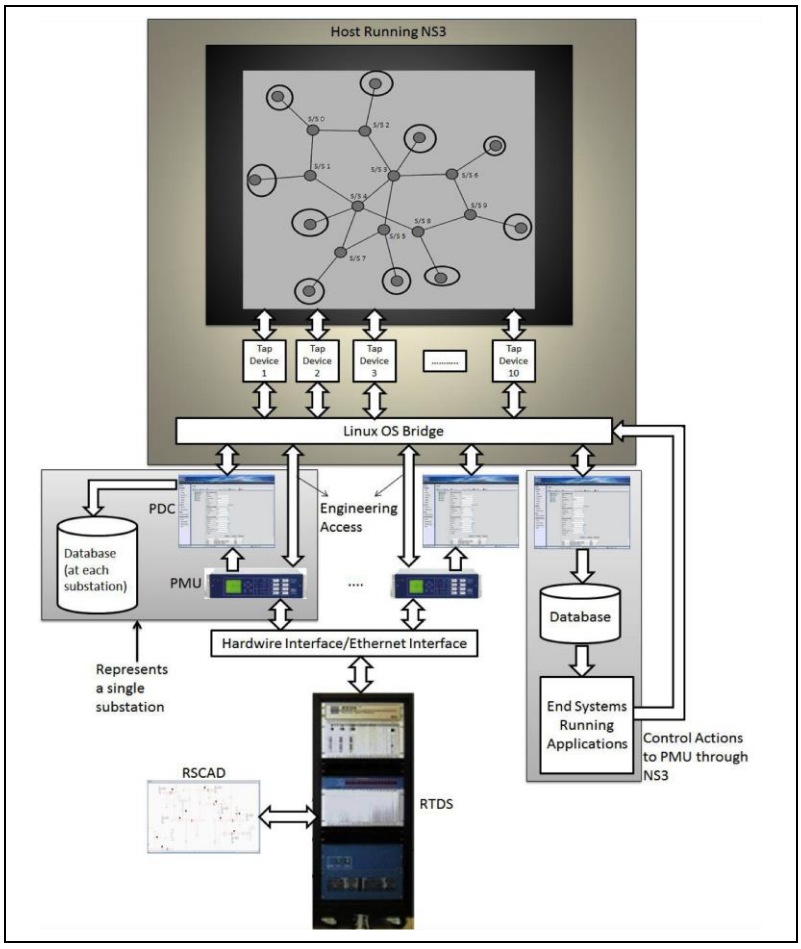


Fig. 1: Integrated Cyber-Power Simulation with RTDS and NS-3

Technical Description and Solution Approach

- A real-time testbed is being developed using a real-time digital simulator to interface with communication emulator NS-3, as shown in fig. 1.
- Additionally, integrated modeling and simulation in real time using Power Tech software and GridStat has 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.

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 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 attack.
- Development of cyber-physical training simulator is in progress.
- Partnerships and External Interactions: Prof. Saman Zonouz, University of Miami; Prof. Thomas Morris, Mississippi State 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 overlay 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 this 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 the size of the power grid 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 TV-OTS multi-cast authentication protocol.
- Systematically analyze trade-offs in parameter choices for the TV-OTS multi-cast authentication protocol.
- Develop a mathematical model or models for trust assessment and decision-making that are appropriate for use in power grid control settings.
- Design approaches to trust data collection for power grid devices and participants so as to be able to usefully instantiate the models and maintain the instantiations over time.
- Incorporate instantiated trust models as part of the security design of wide-area control systems to deal with risks associated with manipulated data.
- **Smart Grid Application Area:** Wide-area monitoring and control.

Technical Description and Solution Approach

- We are now completing work on performance improvements to the key-generation algorithm used in the TV-OTS scheme. In our previous research, TV-OTS exhibited some of the best trade-offs between real-time performance and security but was accompanied by very high off-line key-generation costs. We are also evaluating trade-offs among choices in the TV-OTS implementation, such as signature size, number of chains, and epoch length, and the resistance of the protocol to brute-force attacks.
- 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 are beginning to investigate how multiple power applications that consume sensor data streams can cooperatively leverage their analysis of the data to enhance existing bad-data detectors. For example, if the bad-data detector in one consumer of a data stream is rejecting the data, other consumers of the same stream should consider that as evidence in their own use of the stream.

Results and Benefits

- A prototype implementation of the improved TV-OTS key-generation algorithms has been completed, and a paper is being published.
- A paper evaluating the security trade-offs in parameter choices for TV-OTS has been published.
- Papers are in preparation regarding the trust management model.
- A previous line of research in this activity has resulted in a patent application for a distributed key storage service to enhance key availability and reduce vulnerability to compromise of individual nodes in the system.
- Partnerships and External Interactions: NASPI, RTE, SCE, ISO New England.
- **Technology Readiness Level:** The prototypes of the TV-OTS key-generation and key-storage service could be moved fairly rapidly to product status; trust is ongoing fundamental research, which within the next year will move towards creation of demonstrable applications in the power area.

Researchers

- Carl Hauser, hauser@eecs.wsu.edu
- David E. Bakken, bakken@eecs.wsu.edu
- Thoshitha Gamage, tgamage@eecs.wsu.edu
- Kelsey Cairns, kcairns@wsu.edu
- Yujue Wang, yujue.wang@email.wsu.edu

Industry Collaborators

- Greg Zweigle, 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.

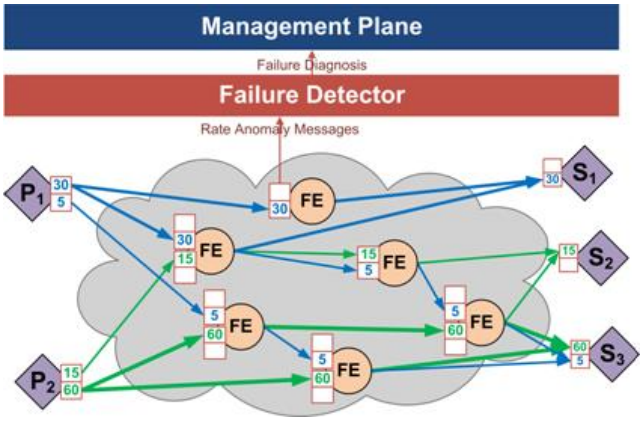
The objective of this research activity is to develop adaptation services and supporting instrumentation services for GridStat in order to systematically adapt to changing conditions and available resources. Those adaptations must be performed such that the strongest possible delivery guarantees (latency,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

Research Objectives

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

Technical Description and Solution Approach

- Model and assess the performance characteristics of GridStat under various constraints that affect normal functionality. Activities will broadly fall under simulation-based assessments and use-case-based assessments.
- Determine the required level of instrumentation that maximizes adaptation-related evidence-gathering with minimum effects on data delivery performance.
- Survey and research existing Security Information Event Management (SIEM) and Complex Event Processing (CEP) techniques to discover analogous compound adaptation triggers based on multiple kinds of instrumentation inputs.
- Implement an adaptation service for GridStat that is highly tailorable both in the steady state and under changing conditions.



- Explore the use of utility functions in order to optimize the benefit of the data delivery service over an entire grid, given the present power and IT conditions.

- Explore the use of pre-computed information on failures (links, forwarding engines, etc.) and their effects. Such pre-computations exploit the (quantitative and qualitative) knowledge GridStat must maintain at every location in the delivery network to provide mission-critical delivery guarantees and respond to failures rapidly.

Results and Benefits

- The ability of GridStat to 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:** Primitive. This research is still at the early stages of development, but the core contributions, once completed and incorporated with the main GridStat software, are expected to be a core GridStat functionality.

Researchers

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

PMU-Enhanced Power System Operations

Overview and Problem Statement

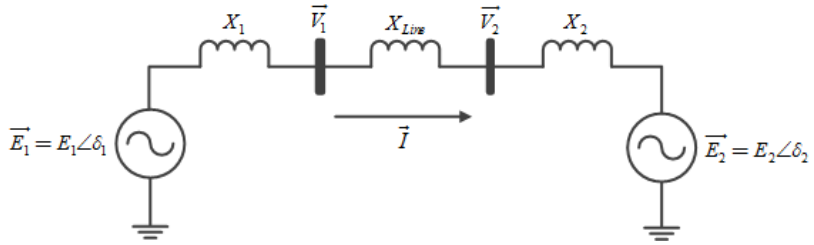
This project explores the direct application of Phasor Measurement Unit (PMU) data to improve situational awareness. PMUs are beginning to be widely deployed in electric power systems, and this trend is expected to continue. However, even with this increase in the number of installations, PMUs are still deployed at only a small percentage of system buses. This presents a challenge: how to get useful information from a small number of data points. The 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 investigates conditions that make fast modes active or inactive.

Research Objectives

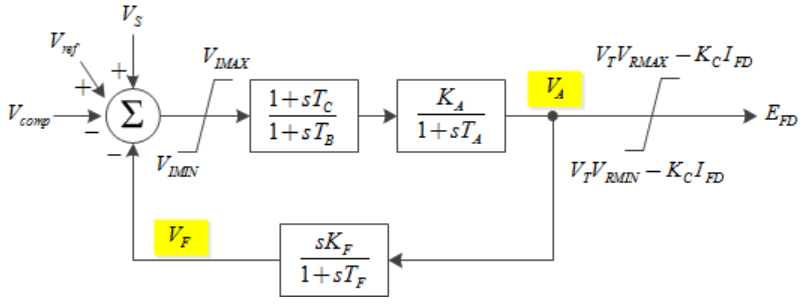
- Develop a framework to allow PMU measurements to create the equivalent system model.
- Develop an algorithm and systematic way to derive system parameters from PMU data.
- Develop online event detection method with PMU data.
- Achieve faster power system analysis.

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.



- 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 site 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.

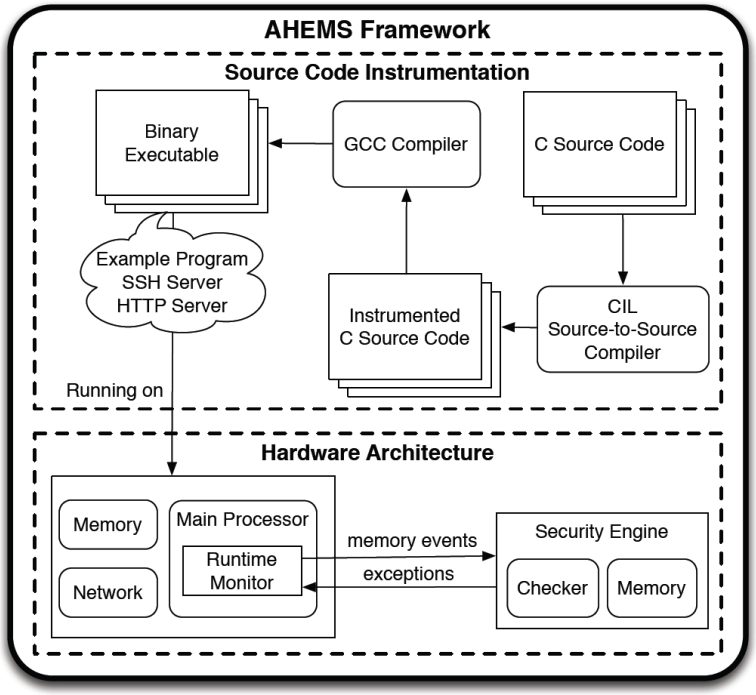


Figure 1: The Architecture of AHEMS Framework

Results and Benefits

- Our prototype of AHEMS achieves high coverage for memory corruption attacks (passing 676 out of 677 test cases; see Table 1) with as low as 10.6% runtime overhead. 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.

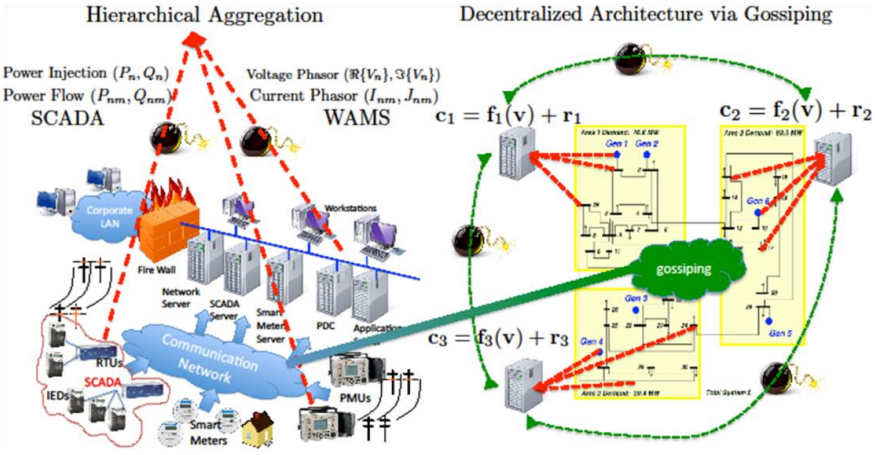
State-Aware Decentralized Database Systems for the Smart Grid

Overview and Problem Statement

The modernization of power grid Industrial Control Systems (ICS) is likely to lead to the adoption of modern cloud services for data historians and to derivation of "big data" data analytics. The data destined for this cloud service are 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 Static State Estimators (PSSE) lack 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. However, their methods lack the ability to adapt to changing network conditions.

This activity moved a step further and did the fundamental groundwork to determine if one could design database systems for the smart grid that can, without a central controller, merge hybrid measurements and harness the local computation of data concentrators and the network that connects them to compute the state in a decentralized fashion. The mechanism can also be used to replicate measurement data more efficiently for reliable storage in the cloud. Because the algorithm is built on the assumption that servers can communicate in a randomized pattern of activity and with random peers, the resulting PSSE system is naturally adaptive to changing network conditions and sampling rates.

The computation/networking model we adopt is borrowed from state-of-the-art research in decentralized optimization and learning in multi-agent networks, which in the PSSE case is the least-square regression problem of fitting the local measurements with the corresponding function of the state in the mean square sense. This function is linear for PMU measurements and nonlinear for power injections and power flow measurements. In addition, optimizing the weights in a weighted version of the least-square problem allows us to adaptively reduce the influence of outliers/bad measurements. Because the computation protocol (called the "gossip protocol" or "gossiping") is based on random message-passing, and because there is no central control involved, it is resilient and adaptive to changing network conditions, and can support information gathering even in the face of failures and congestion.



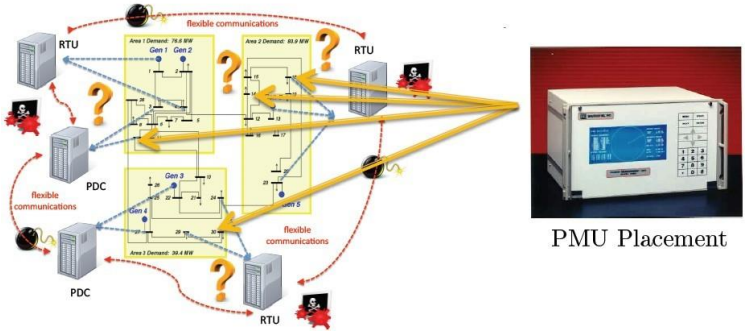
Research Objectives

- Investigate how to perform parallel computations of the Gauss-Newton-based PSSE in a set of servers in a manner that is robust to network and sensing failures, where each server is a repository for a portion of the measurements, either from SCADA or from PDC aggregating PMU data.

- Study the benefits of exploiting PMUs in a hybrid state estimator that gives fast convergence, robust observability, and stable performance.
- Study the interplay between the communication network graph and algorithm convergence speed.
- **Smart Grid Application Area:** The SCADA system for the electrical transmission network and the AMI network in a distribution network.

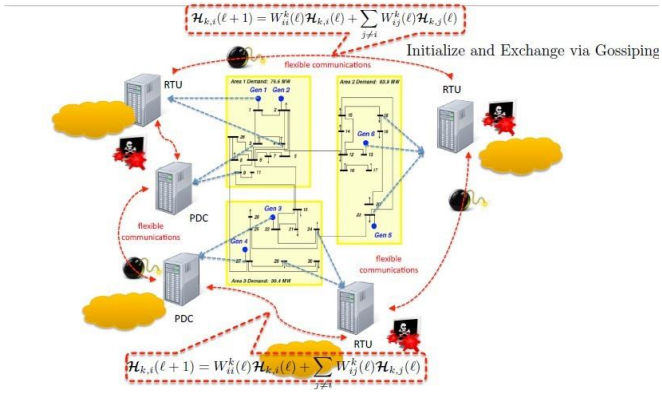
Technical Description and Solution Approach

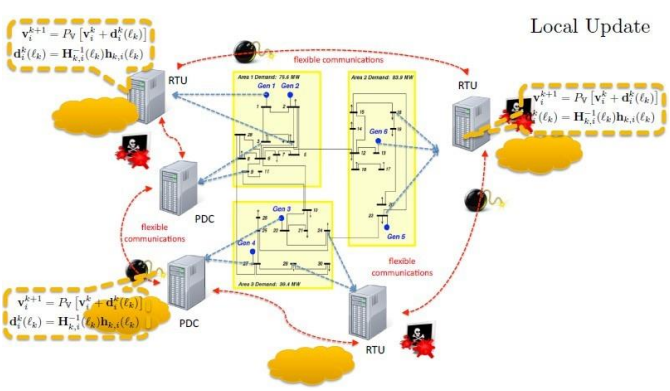
- We have established how to place the PMU sensors judiciously to ensure that the parallel version of the Gauss-Newton regression that is typically performed in centralized state estimators converges to the optimum estimate.



PMU Placement

- It would be possible to query the database cloud directly for the state and rapidly replicate and reconstruct the data, using the state as the side information that glues together the various parts of the database efficiently.





Results and Benefits

- We have analyzed the convergence of the decentralized state estimation algorithm under different communication topologies.
- We have completed a study on topology identification from power injection data.
- **Technology Readiness Level:** Basic research.

Researchers

- Anna Scaglione, ascaglione@ucdavis.edu
- Xiao Li, eceli@ucdavis.edu
- Hoi To Wai, s360pf@gmail.com

Trustworthy Time-Synchronous Measurement Systems

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 on 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 through the use of Global Positioning System (GPS) signals. However, use of 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 wires. However, the cost of deploying optical cables and the poor scalability of the mentioned infrastructure make that approach unsuitable for wide-area deployment. Other industrial protocols that instead promote a shared channel to reduce costs are limited by poor accuracy in performance due to the asynchronous nature of the carrier sensing multiple access (CSMA).

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, for the backhaul communication and the sensing of the 60Hz power signal into a single power line interface. Our design is based on a model called the *Pulse Coupled Oscillators model* that is used to explain synchronization and coordination in biological networks. We call our protocol the *Pulse Coupled Oscillators Network Time and Access Protocol (PCO-NTAP)*. 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 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?
- 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), for 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, hence reducing 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. That solution would be able to use the same electrical wires that deliver power to send 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 develop and implement a prototype that validates our analysis. 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 using field programmable gate arrays (FPGA). After verification and testing, this design can be included in commercially available communication systems.

Results and Benefits

- We successfully simulated the algorithm and verified its convergence analytically and numerically. The simulations are now being extended to estimate the achievable accuracy for a given network topology.
- A prototype network layer (layer 3) implementation was realized on MicaZ Motes with Zigbee radios, and we demonstrated the real-world applicability of the protocols. That experience is guiding the planned FPGA implementation of the MAC layer (layer 2), which will enable greatly improved accuracy in timing and reduced overhead, since a customized medium access control (MAC) and signaling can be used.

Researchers

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

Industry Collaborators

- We are pursuing funding to support development efforts with TCIPG researchers, and help from the Engineering Translational Technology Center at UC Davis.

TCIPG

Research Cluster

Trustworthy Technologies for Local Area Management, Monitoring, and Control

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

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

Development of the Information Layer for the V2G Framework Implementation

Overview and Problem Statement

The Vehicle-to-grid (*V2G*) concept integrates Battery Vehicles (*BVs*) into the grid as controllable loads and generation/storage devices. As the penetration of BVs deepens, 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 scope is to effectively address those concerns while providing the ability to collect the data needed to allow the collection of funds for the road transportation infrastructure.

Research Objectives

- 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 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 continuously 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 car.
- Many ongoing efforts, such as AUTOSAR, OVERSEE, GENIVI, and AutoLinQ™, provide the automotive platform with API support to run third-party applications.
- OVERSEE aims for 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.

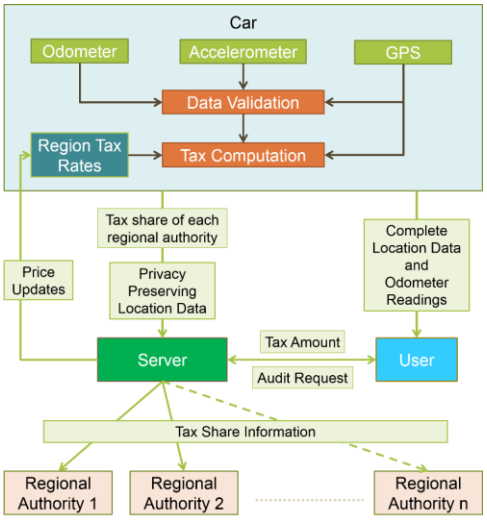


Figure 1. Information Flow

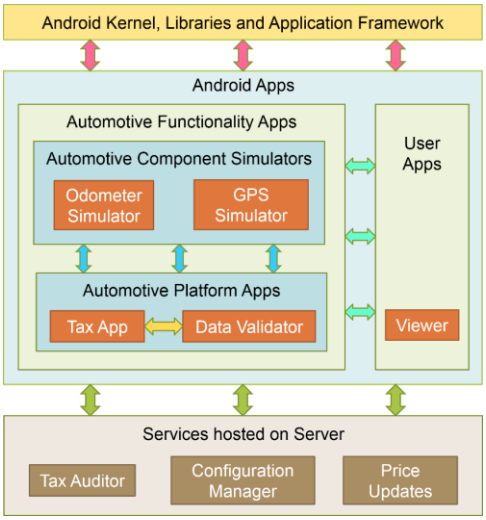


Figure 2. Process Interaction in Android Implementation

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 scale of sensors and measurement devices that monitor the health of power lines is large. With the upgrade of the smart grid, the number of these resource-constrained devices is further increasing. The devices are easy targets for security attacks, as they are accessible via wireless networks and use weak passwords for authentication and collection of telemetric data by the pole maintenance personnel.

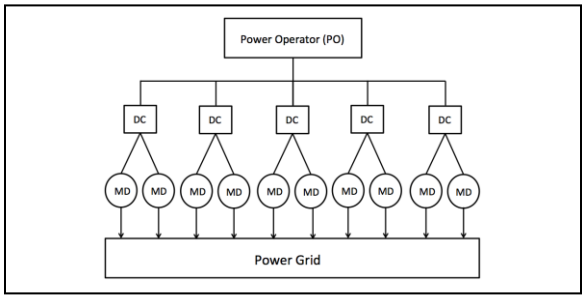
General-purpose security protocols are not suitable for providing data security to devices with limited memory, computational power, and network connectivity. Also, these telemetric devices have lengthy deployment times and limited change management capabilities. Further, the data reported by the telemetric devices to the power operator should remain secret to a potential eavesdropper, an active attacker, or a compromised data collector. 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 data to be securely transferred 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, pole geographical location, 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.



Results and Benefits

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

Researchers

- Prof. Klara Nahrstedt, klara@illinois.edu
- Haiming Jin, hjin8@illinois.edu
- Rehana Tabassum, tabassu2@illinois.edu
- King-Shan Lui, kslui@eee.hku.hk

Industry Collaborators

- Ameren

Smart-Grid-Enabled Distributed Voltage Support Framework

Overview and Problem Statement

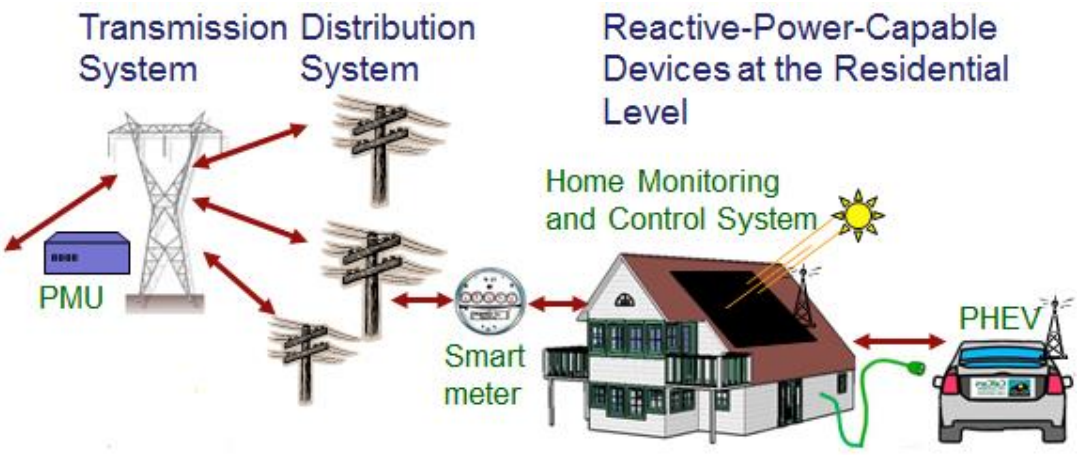
The motivation for this research lies in the use of emerging smart grid devices, such as PHEV/EVs, solar panels, and other power electronics devices, to supply reactive power as a means of distributed reactive power support. Power factor compensation closer to the load improves transmission line loading and efficiency. In the distribution networks, reactive power support not only minimizes the system losses, but also improves the feeder voltage profile. We examine requirements for a secure communication framework to interact with the large number of devices that would be present. The focus of this project is on determining the cyber infrastructure needed to obtain that reactive power control.

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? Those two objective functions cannot be achieved at the same time.
- Another challenge is to investigate what the implications would be for potential contingencies of this system so that the system can be designed to avoid them. For example, if a hacker 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 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. Ultimately, an optimal solution should maximize social welfare.
- Impacts of cyber disruptions are being studied.



Results and Benefits

- Reactive power support is most effective 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 work with campus distribution system facilities personnel to implement a test system on the University of Illinois campus when the devices are ready.

Researchers

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

Trustworthy Framework for Mobile Smart Meters

Overview and Problem Statement

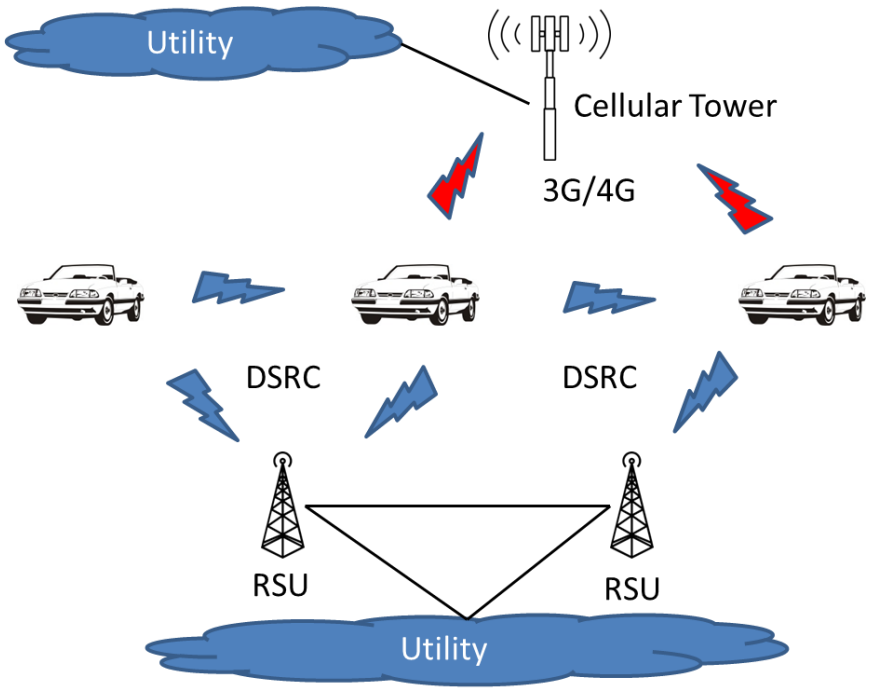
We propose to install on an electric vehicle (EV) a Mobile Smart Meter (MSM) that monitors energy usage by the car and communicates with the utility for periodic reporting, billing information, or route suggestions. The approach enables us to track energy usage more easily. It also brings new energy market models, as people generating excessive energy from their solar panels can directly sell energy to EVs, where 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 reliable demand-response communication system between the mobile smart meter and the utility.
- Design a fast authentication scheme for mobile smart meters 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: fast authentication for communication between electric vehicles and the utility.
- Future Work: communication over multiple network interfaces for better availability.
- Future Work: mix-zone and pseudonym approach for location privacy of electric vehicles.



Results and Benefits

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

Researchers

- Hongyang Li, hli52@illinois.edu
- Wenyu Ren, wren3@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

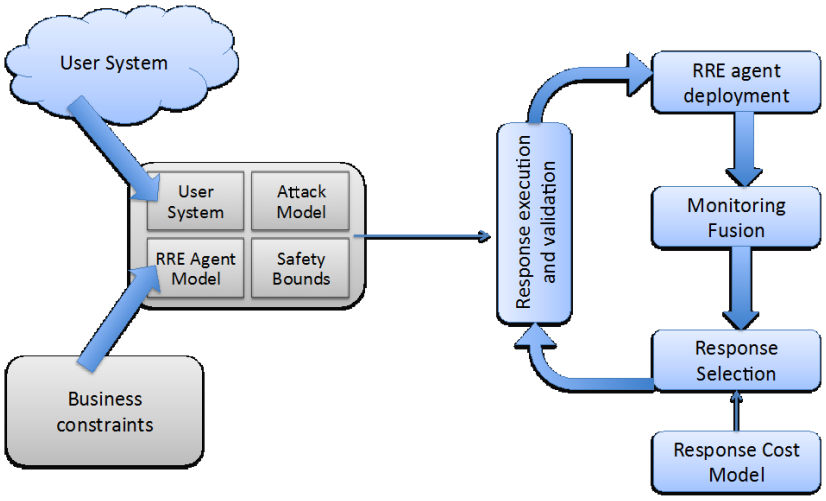
The severity and number of intrusions on computer networks are rapidly increasing. Preserving the availability and integrity of networked computing systems in the face of those fast-spreading intrusions requires advances not only in detection algorithms, but also in intrusion tolerance and automated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

Research Objectives

- Reactive response against adversarial attacks that uses knowledge about the power grid's current security state and its security requirement.
- Build a Response and Recovery Engine (RRE) as a distributed system that actively monitors systems and devises responses.
- Adapt the RRE to handle the scale of a large Automated 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.
- Verify safety properties of possible responses.
- **Smart Grid Application Area:** Intrusion Tolerance.

Technical Description and Solution Approach

- Devise a new modeling method for cyber-physical systems that takes into account detection and response interactions. The goal is to avoid the current layered approaches for CPS models that use a simulation or linearization of the power flow equations to model the grid while ignoring the real cyber interactions.
- Develop monitoring fusion algorithms that can detect high-level attack steps based on low-level information, such as IDS alerts, firewall logs, syslog, dtrace, and other sources.
- Adopt several languages to express the responses in our response taxonomy. Those languages include SDN (OpenFlow) and Mandatory Access Control (SELinux).
- Design several cost-sensitive response selection algorithms based on distributed control theory.



Results and Benefits

- Distributed intrusion tolerance architecture suitable for the power grid.
- Implement a basic OpenFlow responder in a substation setting.
- Advance 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

- SEL

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.

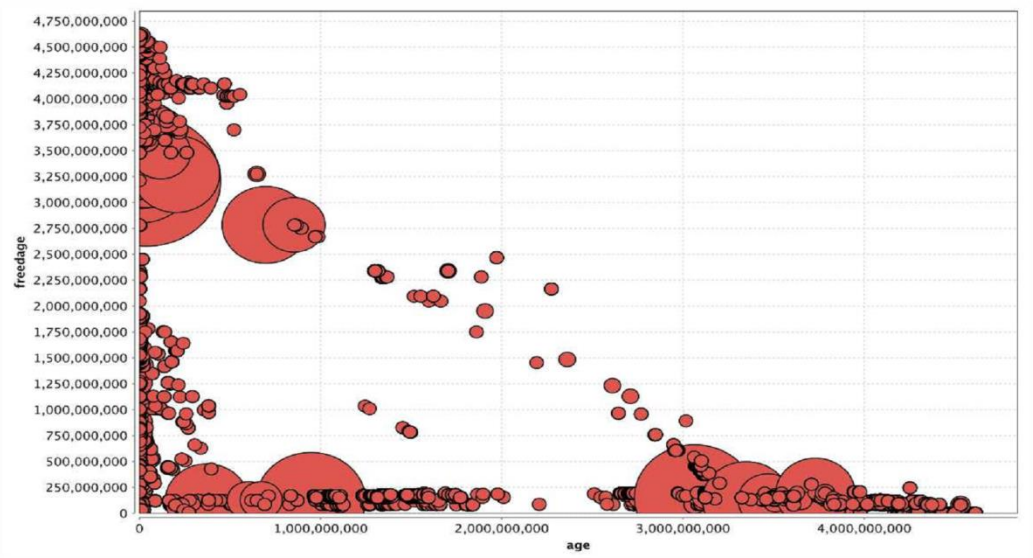
Sophisticated, targeted attacks such as Stuxnet are inevitable, and both detection of such attacks and development of a deep understanding of what happened are paramount. If machines such as those in SCADA are compromised, we want to know as much about the attacks as possible, and understand what the effects will be on the power grid.

Research Objectives

- We will integrate forensic techniques in the monitoring process to ensure the integrity of the information acquired.
- We will communicate with industry to understand what they want to know about compromised hosts and how these compromises affect the power grid.
- We will leverage new and existing forensics tools for better analysis.
- **Smart Grid Application Area:** 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.
- We are working to extend Forenscope to further support SCADA systems and allow for more robust analysis.



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

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 it was stored in was overwritten.
- In collaboration with UIUC's Assured Cloud Computing Center, we developed a system to reduce the memory overhead in virtualized cloud environments. It is built off the idea that many virtual machine images have large quantities of common data stored in memory. Read-only pages containing kernel code, kernel data, application binaries, and application libraries can all be shared across virtual machines, reducing the memory costs of the systems.
- Partnerships and External Interactions: Information Trust Institute, Assured Cloud Computing Center at UIUC.
- **Technology Readiness Level:** Initial stage.

Researchers

- Kevin Larson, klarson5@illinois.edu
- Fangzhou Yao, yao6@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

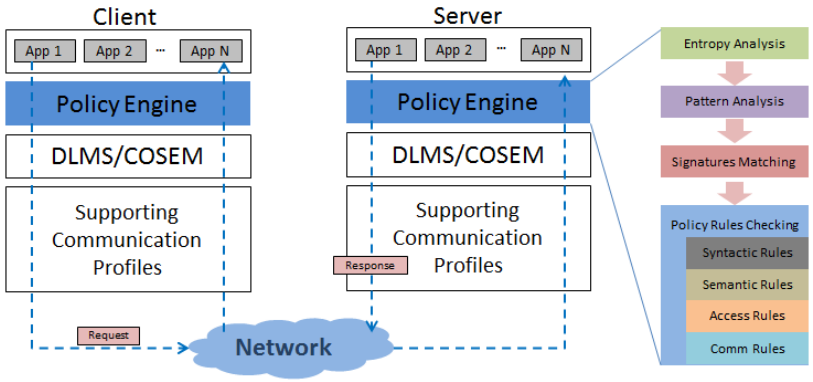
Malware can disrupt the operation of services in advanced metering infrastructure (AMI), which is at risk because of connectivity with the global Internet. In motion, malware may hide within the data payloads of legitimate AMI control traffic, implying the need for deep packet inspection. Some of the inspections one may make look for consistency with respect to data available only at the application layer, requiring one to position the analysis high in the protocol stack. Towards that end, we propose a policy engine that examines both ingress and egress traffic to the AMI application layer.

Research Objectives

- Identify malware propagation threats in AMI networks.
- Design a host-based architecture for the policy engine that supports various malware detection algorithms.
- Design entropy identification, pattern analysis, signature-based analysis, and rule-checking mechanisms.
- Derive an analytical model to study the effectiveness of the policy engine.
- Experiment with ARM binaries and C12.22 meter data to test the policy engine.
- Implement the policy engine with an open-source AMI application.
- Evaluate performance overhead.
- **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 or packed content that might be part of malware.
- Detect the binary executable carried in the traffic with structured patterns.
- Use signatures to represent the byte-level characteristics of executable contents and identify malware using a multiple-signature matching approach.
- Extend the existing policy-checking mechanism that is built in the AMI application with more categories of rules, including syntactic, semantic, access control, and communication rules.



Results and Benefits

- Created policy engine to enable host-based security research in AMI network.
- Created various rules to establish a legitimate profile of AMI traffic.
- Found multiple signatures that are able to identify ARM executables.
- Conducted experiments on evaluating the effectiveness and efficiency of the policy engine.
- Implemented the policy engine with an open-source DLMS/COSEM application.
- Controlled the performance overhead below 0.3%.
- Partnerships and External Interactions: Electronics and Telecommunications Research Institute (ETRI).
- **Technology Readiness Level:** Concept proved; implanted as open-source project; 1 publication from this activity.

Researchers

- David M. Nicol, dmnicol@illinois.edu
- Huaiyu Zhu, hzhu10@illinois.edu

Industry Collaborators

- Cheolwon Lee, Electronics and Telecommunications Research Institute (ETRI)

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

Overview and Problem Statement

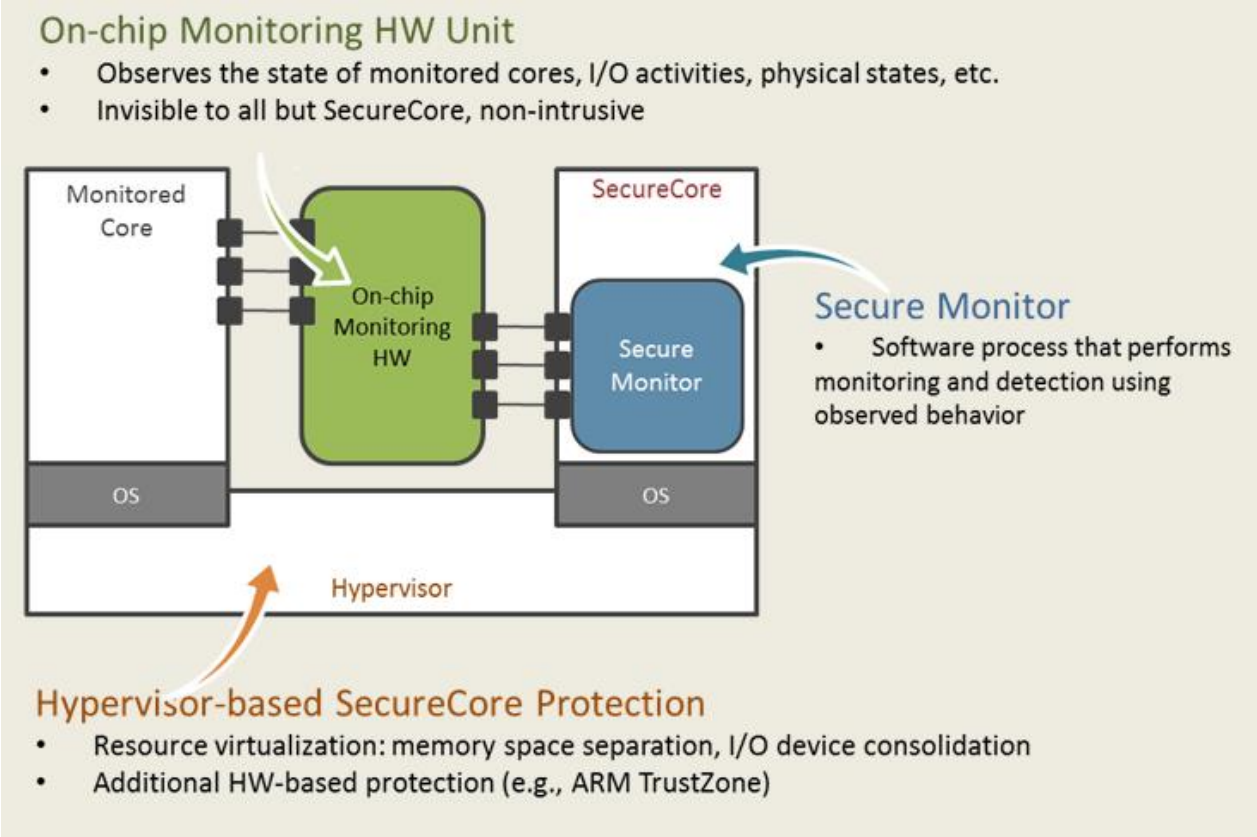
We aim to tackle the problem of detecting intrusions in power grid components with real-time properties; most components that require a safety-critical model of operation fall under this category. We will do so by behavioral analysis of such devices to find anomalies in certain properties (e.g., execution time, memory, 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 their detection and removal using our techniques. That 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 successfully intrude 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.
- On detection, transfer control away from the main controller to the trusted hardware module; the main controller is either shut down gracefully or analyzed by engineers. Either way, the physical control system is not harmed.
- **Smart Grid Application Area:** Security for components with real-time properties in the smart grid; 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 will be successful because most computational components in cyber-physical systems have deterministic properties that can be monitored for anomalies. For this activity, we are starting with *execution time* and *control* behavior and then, time permitting, will follow up with other system states, such as memory and I/O traffic.
- Hence, we are working on the development of timing-based analysis models for real-time control systems, both for exact timing and for statistical methods.
- We will then implement the timing models and monitoring platforms to detect anomalies in smart grid components such as IEDs.
- Time permitting, we intend to evaluate other analysis/monitoring signals, such as memory profiles and I/O flows, and integrate them into our iMonitor framework.
- We are also developing secure hardware-based monitoring platforms; the image on the reverse page shows the high-level design using a multicore platform (which we call "SecureCore").



Results and Benefits

- Increased security for individual computational nodes in the power grid (e.g., IEDs and smart meters).
- Ability for 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.

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

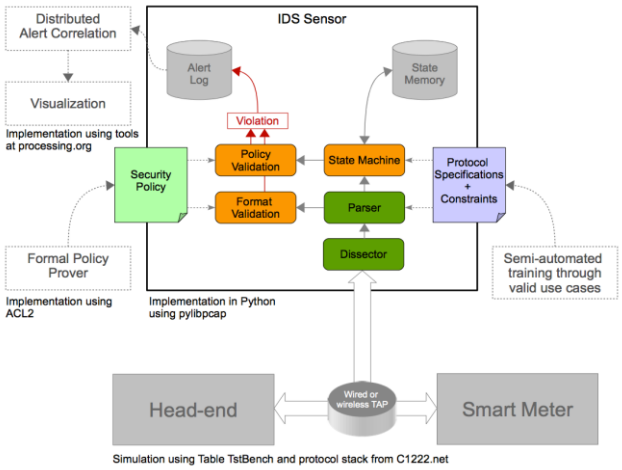
To ensure the security and reliability of a modernized power grid, the current deployment of millions of smart meters requires the development of innovative situational awareness solutions to prevent compromised devices from impacting the stability of the grid and the reliability of the energy distribution infrastructure. To address this 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 12,000-meter AMI.

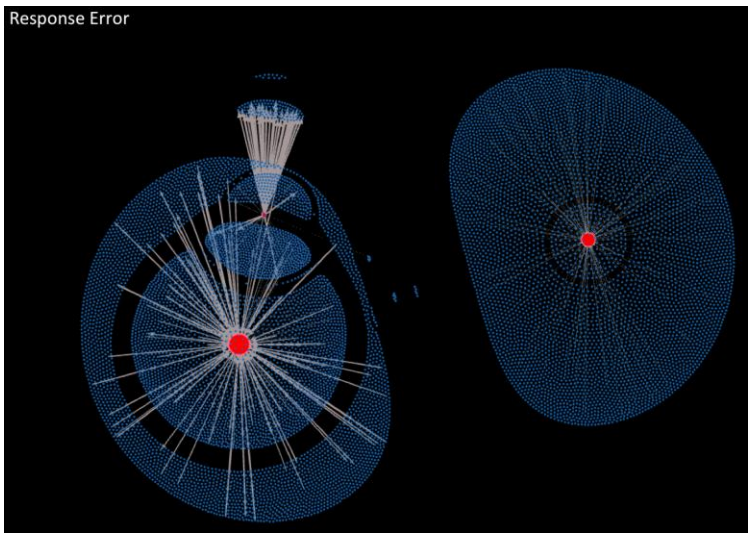
Research Objectives

- 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.





Results and Benefits

- Definition of a rigorous process utilities and vendors can use to develop a comprehensive monitoring architecture.
- Integration of formal methods in a practical framework to offer strong security guarantees.
- Deployment of an Amilyzer sensor in collaboration with FirstEnergy to monitor 12,000 meters.
- **Partnerships and External Interactions**: In collaboration with EPRI, FirstEnergy, and Itron.
- **Technology Readiness Level**: Prototype.

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, Marcus Noel, and Nathan Sterrett
- Fujitsu: Jorjeta Jetcheva and Daisuke Mashima
- UT Dallas: Alvaro Cardenas
- Sandia National Labs: David Grochocki

Specification-based IDS for the DNP3 Protocol

Overview and Problem Statement

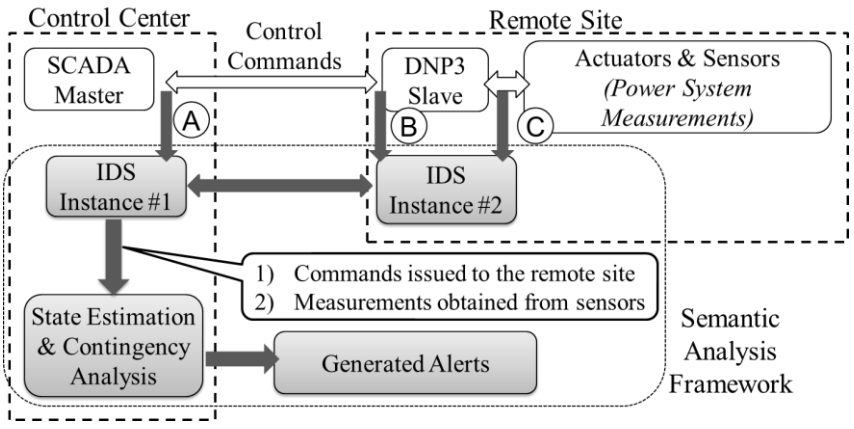
Modern SCADA systems are increasingly adopting Internet technology to control industrial processes. With security vulnerabilities thus exposed to public networks, attackers may be able to penetrate control systems to issue malicious control commands that drive remote facilities into an unsafe state, 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 activities. To overcome that challenge, we introduce a semantic analysis framework based on a distributed network of IDSes. The framework combines system knowledge of both cyber and physical infrastructure in power grids to help IDSes estimate execution consequences of control commands, thus revealing attackers' malicious intentions.

Research Objectives

- Design and implement a dedicated network analyzer and integrate it with the Bro intrusion detection system.
- Augment Bro IDS with power flow assessment tools to perform run-time state estimation to predict the consequences of executing a (potentially maliciously crafted) control command that is transmitted by run-time network packets.
- Develop attack scenarios that demonstrate an attacker's capability to make a wide range of system changes with a single DNP3 command.
- Experiment to establish the feasibility of the proposed semantic framework.

Technical Description and Solution Approach

- Design and implement Bro IDS at the control center.
  - Distinguish critical commands from noncritical ones, e.g., commands that can change system states instantly.
  - Collect measurements from all substations.
  - Include state estimation & contingency analysis components to estimate the execution consequence of the command.
- Design and implement Bro IDS at the remote site.
  - Use local IDS to obtain measurements directly from sensors (trusted measurements under our threat model).
  - Confirm that measurements are not corrupted at other locations.



Results and Benefits

- Through integration of power flow analysis modules, the deployed Bro IDS is able to detect malicious commands transmitted by legitimate network packets.
- Experiments can estimate how an attacker introduces physical violations in the power grid with a small number of network packets.
    - E.g., increase generation, increase load demands, or open transmission lines.
- Can estimate execution time needed to estimate execution consequences of network commands.
    - Analyze feasibility of such analysis at runtime in SCADA networks.

Researchers

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

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 responses 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.
-

<table>
<tr><td>Symbols: 8</td><td>2</td><td colspan="2">2</td><td>variable</td></tr>
<tr><td>Preamble
0x00000000</td><td>SFD
0xA7</td><td>Frame length
(7 bits)</td><td>Reserved</td><td>PSDU</td></tr>
<tr><td colspan="2">SHR</td><td colspan="2">PHR</td><td>PHY payload</td></tr>
</table>

IEEE 802.15.4 standard 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

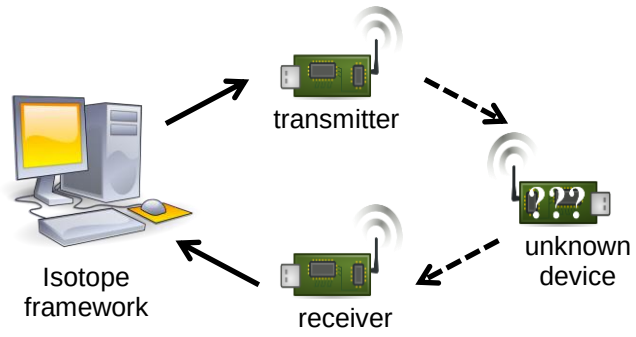
- Insert a variable number of 0xF symbols between the preamble and SFD

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

- Preliminary results suggest unique identification of Moteiv Tmote Sky and Atmel RZUSBstick devices.
- Fingerprinting framework, Isotope, introduced.
- 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; engaged in collaborative use and developed extensions to Api-do with River Loop Security.
- **Technology Readiness Level:** Beta; tools in ongoing development; more experimental results to come.

Researchers

- Sergey Bratus, sergey@cs.dartmouth.edu
- Rebecca Shapiro, bx@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 trend in the smart grid evolution. 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 noises from 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 these physical and cyber challenges.

Research Objectives

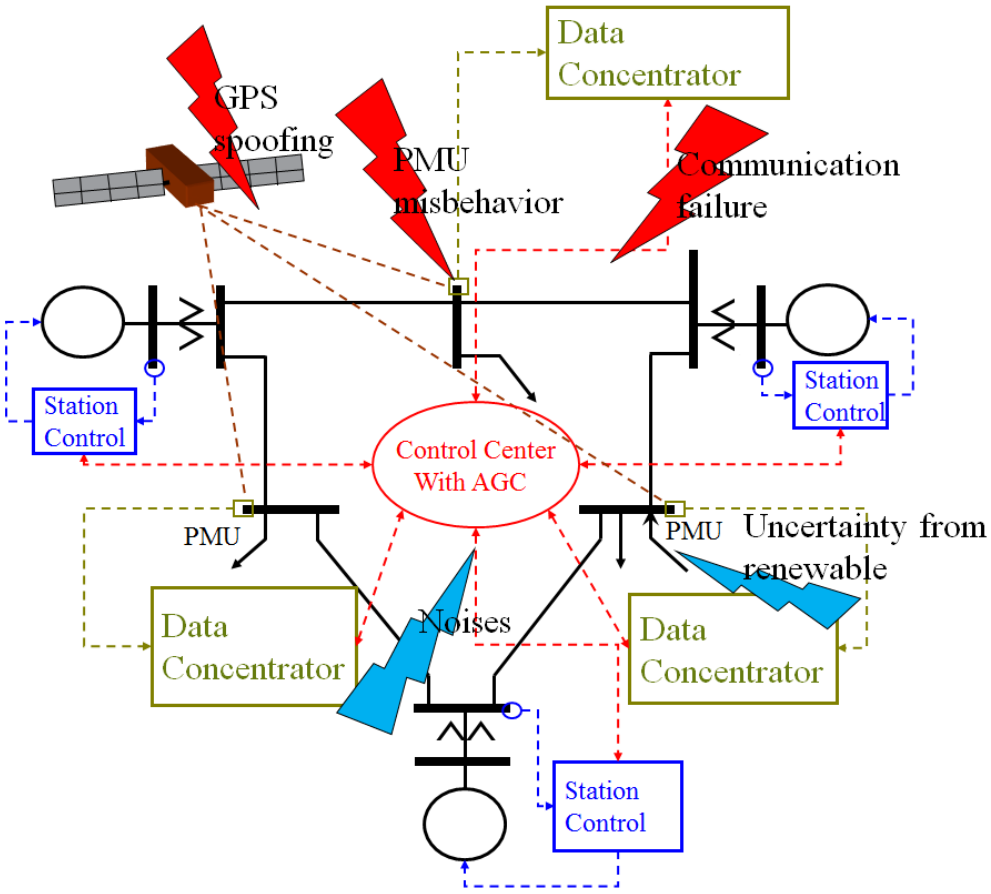
- Develop an exhaustive taxonomy of uncertainty factors in both cyber and physical components in a power grid:
    - Physical-related uncertainty factors: potential faults in physical infrastructure for generation and transmission, and uncertainties from renewable energies;
    - Cyber-related uncertainty factors: potential faults, attacks, and noises in cyber infrastructure for measuring, communication, and control.
- Construct appropriate models to quantify the impacts of uncertainties defined on 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.
- Characterize the effect of those faults on system monitoring.
    - Develop analysis tools to monitor system stability and reliability by utilizing information from advanced cyber components, e.g., phasor measurement units (PMU);
    - Identify the impact of the misbehaviors of cyber components on system awareness performance.
- Assess the impact on overall system dynamic performance and reliability of the uncertainties affecting system operations and control, through tools from switched/hybrid system analysis.

Results and Benefits

- Different methods of attack on PMU synchronization have been developed and simulated. The impact on system awareness performance has been evaluated.
- Uncertainty on renewable-based generation, noises, and potential continuous attacks on communication networks are properly modeled as stochastic processes.
- A framework to evaluate the impact of various uncertain 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, and the impact of uncertain factors on performance metrics is being provided through sensitivity analysis.



- We have proposed a variety of system communication network attack scenarios that would adversely affect power system performance metrics. A tool to evaluate the impact of general attacks is being developed.
- Partnerships and External Interactions: N/A
- **Technology Readiness Level:** Ongoing research. Preliminary results are being obtained as expected on test systems.

Researchers

- Alejandro D. Domínguez-García, aledan@illinois.edu
- Xichen Jiang, xjiang4@illinois.edu
- Jiangmeng Zhang, jzhang67@illinois.edu
- Peter Sauer, psauer@illinois.edu
- Lee DeVille, rdeville@illinois.edu
- D. Apostolopoulou, apostol2@illinois.edu

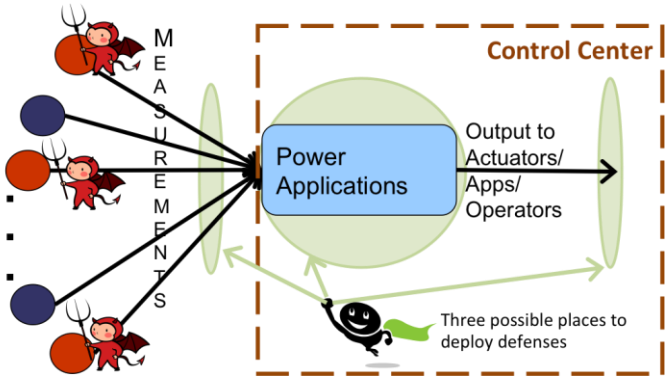
Security and Robustness Evaluation and Enhancement of Power System Applications

Overview and Problem Statement

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



Technical Description and Solution Approach

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

- Design effective ways to combine and use knowledge about both cyber infrastructure security state and power system electrical state during power system operations for increased robustness against cyber attacks.
- 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 (to appear in *IEEE Transactions on Smart Grid*, 2013).
- 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 are investigating defenses (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:** Collaborating with researchers at KTH Royal Institute of Technology in Sweden; collaborating with TCIPG alumni at PowerWorld and University of Miami.
- **Technology Readiness Level:** This technology is currently in the research and design phase.

Researchers

- Rakesh B. Bobba, rbobba@illinois.edu
- Robin Berthier, rgb@illinois.edu
- Erich Heine, eheine@illinois.edu
- Miao Lu, mlu20@illinois.edu
- Tom Overbye, overbye@illinois.edu
- William H. Sanders, whs@illinois.edu
- Pete Sauer, psauer@illinois.edu

- **External Researchers:** Saman Zonouz (Univ. of Miami), György Dán and Ognjen Vuković (KTH Royal Institute of Technology)
- **Past Researchers:** Himanshu Khurana, Kate Morrow, Klara Nahrstedt, Tom Overbye, Qiyan Wang, and Zheming Zheng

Industry Collaborators

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

Synchrophasor Data Quality

Overview and Problem Statement

Synchrophasor data are envisioned as a key technology enabling real-time power grid situational awareness and control.

More than 1000 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 error, 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 synchrophasor measurement device (also known as a *phasor measurement unit*); understand the challenges of measuring, processing, synchronizing, and integrating synchrophasor data. Research the application of synchrophasor data to power systems.

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+ phasor measurement units. Kleitsch is the operations lead for the ATC DOE Synchrophasor Project, which involves

the addition of 45 Phasor Measurement Units (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 activity has demonstrated a PMU developed using National Instruments' LabVIEW software and C-RIO hardware (compact reconfigurable I/O (RIO) architecture). The PMU produces 10 voltage phasors per second. The PMU is being integrated with an uninterruptible power supply to enable transient measurements during power outages. Synchrophasor data are buffered and transferred each hour to a remote Linux web server via an FTP connection.
- TCIPG PMU cost is approximately $1000 per unit; work is underway to use NI hardware due to be released in Nov '13 to reduce the per-unit cost 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. Work to date has focused on application of MATLAB visualization tools.
- **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
- Andy Yoon, yoon62@illinois.edu
- Kenta Kirihara, kirihar1@illinois.edu
- Matthew Harvey, harvey16@illinois.edu
- Peter Sauer, psauer@illinois.edu
- Hao Zhu, haozhu@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 reclosers, that are distributed all across their service area. Those devices are often mounted on utility poles in both remote and densely populated areas, and have little physical security outside of the cabinet in which they are placed. However, these 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 the utility would like to detect when one of its devices is being tampered with, and cut off that device's network connection, 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 when a technician is sent to service a device.
- The utility may also want to leave the connection open in the event of a natural disaster, to simplify and expedite recovery effects.

While there's been a great deal of research in the tamper detection field, it all falls short for a number of reasons:

- Most tamper protection systems are geared towards protecting data at an individual node, but we wish to protect operations across a multi-node system.
- Tamper-evident systems are often easy to defeat and do not account for non-malicious intrusions, such as when a technician services a device during an emergency.
- Tamper-resistant systems may be too costly to use when retrofitting older cabinets.
- Tamper detection/response systems do not always work in extreme environment conditions, and may not have enough information to differentiate between a malicious attack and an emergency situation such as a natural disaster.
- Tamper detection/response systems also generally have a single course of action to follow (e.g., delete its secret data), but a system should change its response based on the kind of tampering it detects.
- Standard security guidelines (such as FIPS 140-2) are not wholly applicable.

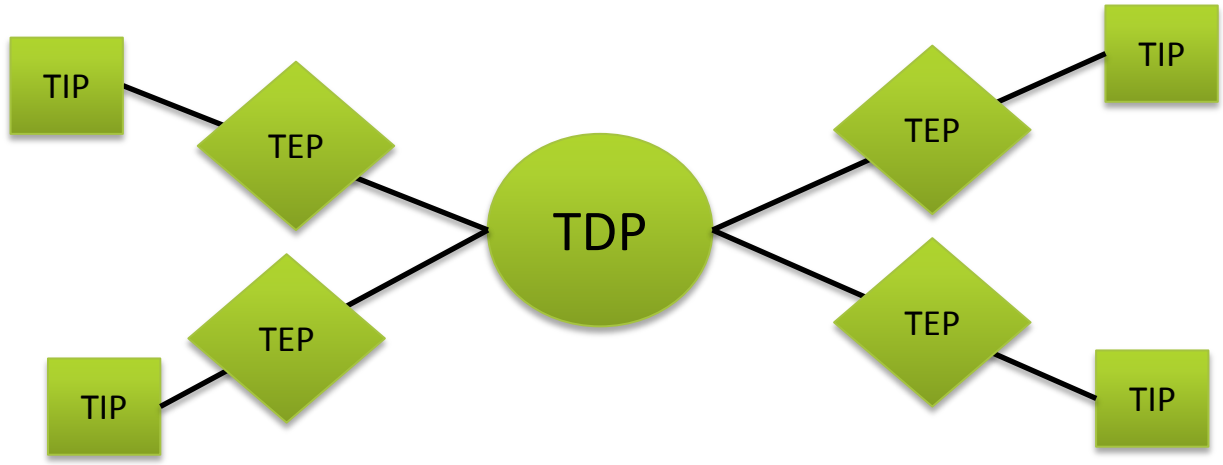
Research Objectives

- 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 represents malicious activity, benign activity (e.g., a technician is servicing the device), or 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 (such as reclosers) that are spread throughout a utility's service area.

Technical Description and Solution Approach

We propose a *distributed* approach to tamper detection, where tamper responses for a single device are based on the status of all of the enabled devices in the network.

- *Tamper Information Points* (TIPs) 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) act on tamper decisions by either destroying secret data or cutting off network access.
- T*amper Decision Points* (TDPs) reside in a higher-security area of the network, collect information from the TIPs within its network, and send tamper decisions to the TEPs in its network.



- Some initial thoughts:
  - We will need some sort of "heartbeat" exchange between the TDP and each TIP to ensure that they stay connected to the network. Connection loss is treated as an attack on the TIP.
  - The TDP will also need an interface that allows control center personnel to specify times when tamper signals from particular devices should be ignored (e.g., when a technician is scheduled to service the devices).
  - If the TDP receives a tamper signal, it should query or listen for similar reports from the other TIPs it manages. If the information received by the TDE fits the profile of a natural disaster, no action is taken. Otherwise, the TDP's tamper signal is considered legitimate, and the TEPs are signaled to take protective measures (delete secret data, cut off network access, etc.).

Researchers

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

Acknowledgments

- Ryan Bradetich, Jason Dearien, Dennis Gammel, and Rhett Smith, Schweitzer Engineering Laboratories
- Elaine Palmer, IBM Watson
- Steve Weingart, Atsec

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

Overview and Problem Statement

To integrate new kinds of green power generation and support wide-area monitoring and efficient demand response, many promised smart-grid management ideas require the scalability, computing resources, and economy of scale only cloud computing can offer. However, there are still many concerns (such as lack of security, reliability, and real-time guarantees) that make current cloud technology unsuitable for the power-grid. As new solutions and techniques are being researched to address the features required to make cloud computing suitable in the power industry, we are contributing by developing tools, methods, and procedures to experimentally evaluate and quantify the resiliency that cloud-based power grid management needs.

Research Objectives

- Experimentally evaluate the reliability and security of cloud infrastructure and cloud-based power-grid applications.
- Build a cloud testbed for evaluating cloud-based power grid applications.
- Study past failure data to understand the failure modes in cloud infrastructure.
- Build a scalable, distributed fault injection framework capable of creating realistic failures in a cloud environment as well as recording and analyzing the fault injection result.
- Develop procedures to systematically explore the failure scenarios in a cloud system.
- Integrate the fault injection framework and evaluation procedure into a cloud-based fault injection service.
- **Smart Grid Application Area:** Develop tools to enable experimental evaluation of the reliability and security of cloud infrastructure and cloud-based smart grid applications.

Technical Description and Solution Approach

This research is addressing ways to ensure the reliability and security of cloud-based smart grid solutions. Our approach is to build a fault injection service for cloud systems in order to experimentally evaluate the robustness of the system by creating planned failures on an ongoing basis. Our solution approach consists of the following three stages:

Stage 1:

- Set up a cloud testbed for experimental evaluation of cloud-based smart grid solutions.
- Design and implement a scalable and distributed fault injection framework.
- Study past cloud failures to understand the common failure modes and what fault injection capabilities are needed to create realistic cloud failures.

Stage 2:

- Develop a systematic approach to exploring failure scenarios in a cloud system and methods to reduce the fault space to a reasonable size.
- Integrate the cloud testbed with the TCIPG testbed to simulate a realistic power system operating environment.
- Set up real smart grid applications on the cloud testbed to evaluate our proposed fault injection approach.

Stage 3:

- Study how cyber asset failure might affect a physical power grid.
- Demonstrate the feasibility of failure as a service on the testbed.
- Set up a failure knowledge base to collect failure data for future failure analysis.

Results and Benefits

- Our research will produce a tool to provide a scalable, minimally intrusive, and small-footprint fault injection framework in order to evaluate the reliability and security of the cloud infrastructure and cloud applications by creating planned actual failures, such as power failures and network failures.
- We envision the integration of the fault injection framework into the cloud infrastructure in order to provide ongoing and periodic evaluation of the cloud system and to create benchmarks for the reliability and security of cloud-based smart grid applications.
- The fault injection result will also be collected into a knowledge database that can be used to quickly identify potential failure causes based on the observed failure symptoms.
- **Technology Readiness Level:** Ongoing development of the fault injection framework.

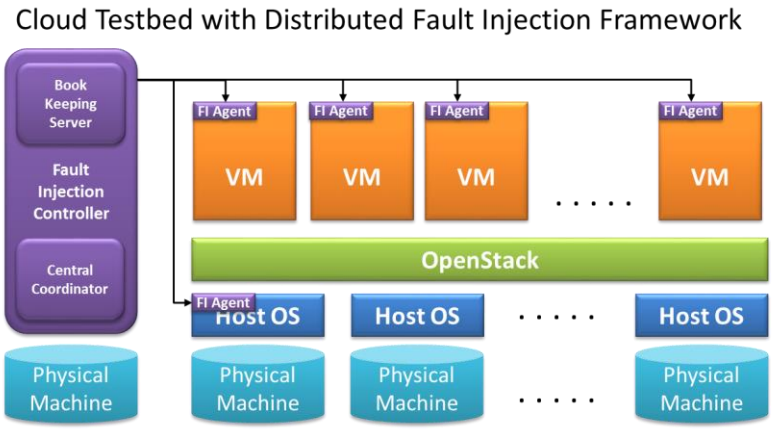


Figure 1. Cloud Testbed Setup

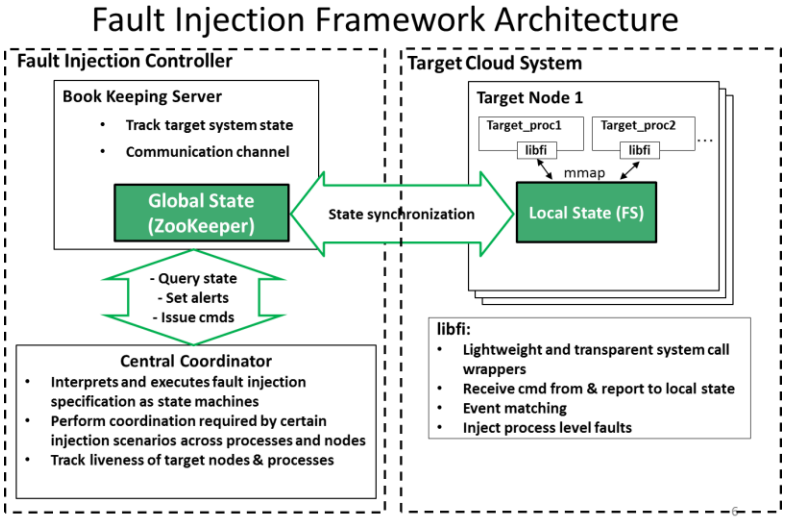


Figure 2. Fault Injection Framework Architecture

Researchers

- Daniel Chen, dchen8@illinois.edu
- Cuong Pham, pham8@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.

Research Objectives

- Control systems can be served by policies and mechanisms considerably **more restrictive** of allowed computation than those of general-purpose systems. We aim to develop such mechanisms **throughout all layers** of a control system, and keep the mechanisms **lightweight** & **maintainable.**
- We aim to develop **concise** policies that capture a programmer's **intent** at every architectural layer of a control system without burdening the programmer with additional policy tasks (as in, e.g., SELinux).
- We aim to capture **intent-level semantics** in control applications, standard libraries, kernels, and network- and bus drivers, for maximal reduction in unintended (malicious or exploitable) computation.
- **Smart Grid Application Area:** Hardening of SCADA control platforms and systems.

Technical Description and Solution Approach

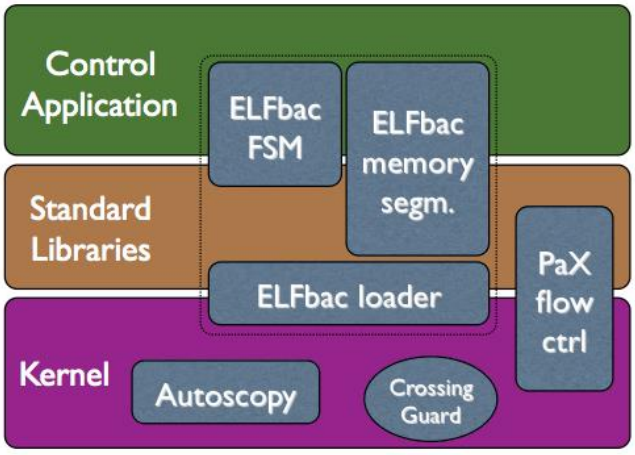
Our "Stack of Trust: A Multi-Layered Protection Strategy" is described in the table.

Stack of Trust: A Multi-Layered Protection Strategy

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

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

Relationship and placement of Trusted Control Stack system components.



Results and Benefits

- The network-layer solution YASIR is complete and tested. In testing that used 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.
- Lightweight kernel intrusion detection research has been completed and a prototype developed. This has informed the design and implementation of a secure control system at an industry partner.
- A prototype port of the PaX technology has been completed and awaits testing in conjunction with other components (tested with Autoscopy).
- ELFbac kernel component is in beta-stage testing. Design and implementation are described in Dartmouth Technical Report **TR2013-727, ELFbac: Using the Loader Format for Intent-Level Semantics and Fine-Grained Protection,** Julian Bangert, Sergey Bratus, Rebecca Shapiro, Michael E. Locasto, Jason Reeves, Sean W. Smith, and Anna Shubina.
- CrossingGuard is in development; preliminary results have been published at the Workshop on Embedded Systems Security (WESS) and are featured on a separate poster.
- **Technology Readiness Level:** varies by project/component, see 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
- Sean W. Smith, sws@cs.dartmouth.edu

Industry Collaborators

- Schweitzer Engineering Laboratories (kernel hardening)
- **Industry collaborators sought!**

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 this 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.
- Several assumptions can be made in the case of a PMU (e.g., stationarity of the unit), which can possibly be exploited to detect a spoofing attack.
- We will implement and test a GPS simulator (in cable) capable of spoofing a PMU to test and improve its resiliency to various spoofing vectors.

Results and Benefits

- Simulation of GPS spoofing has been carried out in MATLAB.
- A literature survey of general spoofing attacks and mitigation strategies has been conducted.
- A hardware-based testbed is being created to investigate effects of spoofing on PMUs.
- **Technology Readiness Level:** Ongoing research.

Researchers

- Jonathan J. Makela, jmakela@illinois.edu
- Grace Gao, gracegao@illinois.edu
- Alejandro Domiguez-Garcia, aledan@illinois.edu
- Rakesh Bobba, rbobba@illinois.edu
- Thomas Gehrels, gehrels2@illinois.edu
- Xichen Jiang xjiang2@illinois.edu
- Liang Heng heng@illinois.edu

Education and Engagement

Testbed Initiatives

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

Education and Engagement

Overview

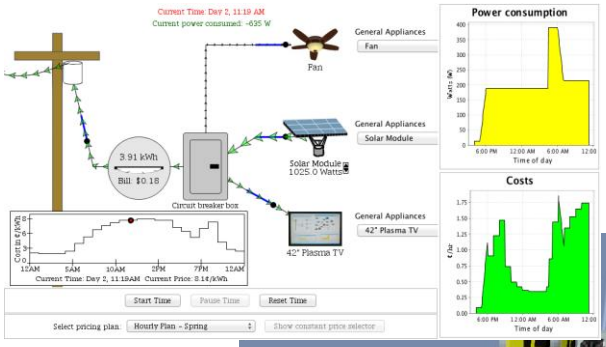
Members of the TCIPG Education team work with teachers, informal educators, industry, and other TCIPG researchers to develop a variety of educational opportunities. Our activities are designed to engage learners of all ages. We develop curriculum materials that involve young people in virtual power system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

Objectives

- Link researchers, educators, 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 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.

Solution Approach

- Create literacy-enhanced, hands-on learning opportunities.
- Correlate hands-on explorations with virtual simulations.
- Incorporate the science of electricity and the historical and economic development of the electric grid into a video game virtual world.



- 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, and hands-on activities.
- Interactive app for iPad and other touch tablet devices.
- Partnerships and External Interactions:
  - Illinois Energy Education Council
  - National 4-H SET Initiative
  - KidWind and WindWise Education
  - IEEE
  - Project Lead the Way pre-engineering curriculum
  - National Science Teachers Association (NSTA)
  - ASEE
  - Illinois Solar Schools

Researchers

- Jana Sebestik, sebestik@illinois.edu
- George Reese, reese@illinois.edu
- Jason Mormolstein, jmormol2@illinois.edu
- Andrew Gazdziak, gazdzia1@illinois.edu
- Rebecca Byrd, rabyrd2@illinois.edu
- Brendan McDonnell, brendan.r.mcdonnell@gmail.com
- Mark Talbot, mark.talbot12@gmail.com

Industry Collaborator

- Rod Hilburn, RHilburn@ameren.com

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 and 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 the testbed capabilities, features, and functionality through strategic integration of equipment.
  - Provide integration glue that provides unique capabilities in the testbed environment.
  - Leverage existing and emerging research from other areas when it can advance the goals of the testbed effort.
- **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)
- GPSs, 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, IDSs.
- 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 Lab, Siemens AG, SISCO, Space Time Insight, Trilliant