U.S. DEPARTMENT OF
ENERGY

OFFICE OF
Cybersecurity, Energy Security,
and Emergency Response

Cybersecurity Center for Secure, Evolvable Energy Delivery Systems (SEEDS)

University of Arkansas

H. Alan Mantooth, Qinghua Li

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- R&D cybersecurity technologies, tools, and methodologies that will advance the energy sector's ability to survive cyber attacks and incidents while sustaining critical functions.
- Scope of work: cybersecurity of power electronics, data, operation and control systems, and operation networks in energy delivery systems.

Schedule

- Project start/end dates: 10/01/2015 – 12/31/2021.
- Deliverables: cybersecurity technologies well designed, implemented, and tested.
- Security capabilities that result from research projects of this center: threat and risk assessment; incident prevention, detection, mitigation, and response; defense in depth against dynamic threats; security management and decision support.

Total Value of Award:	$12,226,504+$3,082,610
Funds Expended to Date:	82%
Performer:	University of Arkansas
Partners:	Florida International, Carnegie Mellon, U. Arkansas Little Rock, MIT, Arkansas Electric Cooperative Company

Advancing the State of the Art (SOA)

- **State of the art (SOA)**
  - Power grid control and operation systems and operation technology infrastructure need better and customized protection against cyber threats.
  - New power grid components and services are usually deployed first and then security is validated and added later.
  - Cybersecurity management is mostly manual.
  - Gap between fundamental research and technology transfer to industry.
- **Our approach**
  - Provides protection against cyber attacks based on computing methods and the physics of energy delivery systems.
  - Industry inputs throughout the R&D cycle (define, research, alpha, beta, transition).
  - Yearly solicitation of security problems from industry and proposals from faculty.
- **Why our approach is better than the SOA**
  - Customized protection for energy delivery systems.
  - Builds security into the design of new power grid components and services.
  - Security management automation to tackle the high complexity and volume of security data.
  - Our security solutions are more practical for deployment.

Advancing the State of the Art (SOA)

- **Feasibility of approach**
  - Involvement of industry in the entire cycle, including needs solicitation, project selection, feedback to research, and beta testing.
  - Technology intentionally made easy-to-integrate into the existing system, e.g., avoiding interruption of service.
- **How the end user will benefit**
  - All research is industry-driven and research solution efficacy is validated for transition to practice and commercialization.
  - Research university partners have testing facilities to evaluate cybersecurity tools prior to deployment.
  - Research is beta tested with an energy industry partner.
  - The intense research and development focus allows for the involvement of students from all partner institutions to help provide industry a robust cybersecurity workforce.
- **How our approach will advance the cybersecurity of energy delivery systems**
  - Improve situational awareness through *security data analytics and anomaly detection.*
  - Protect integrity of operation and control by *hardening hardware, detecting tempering of data and devices.*
  - Secure communication network infrastructure by *designing secure extensions to standard communicatio. protocols and detecting network attacks.*
  - Advance security management by *providing automation technologies and decision support.*

Progress to Date (1/2)

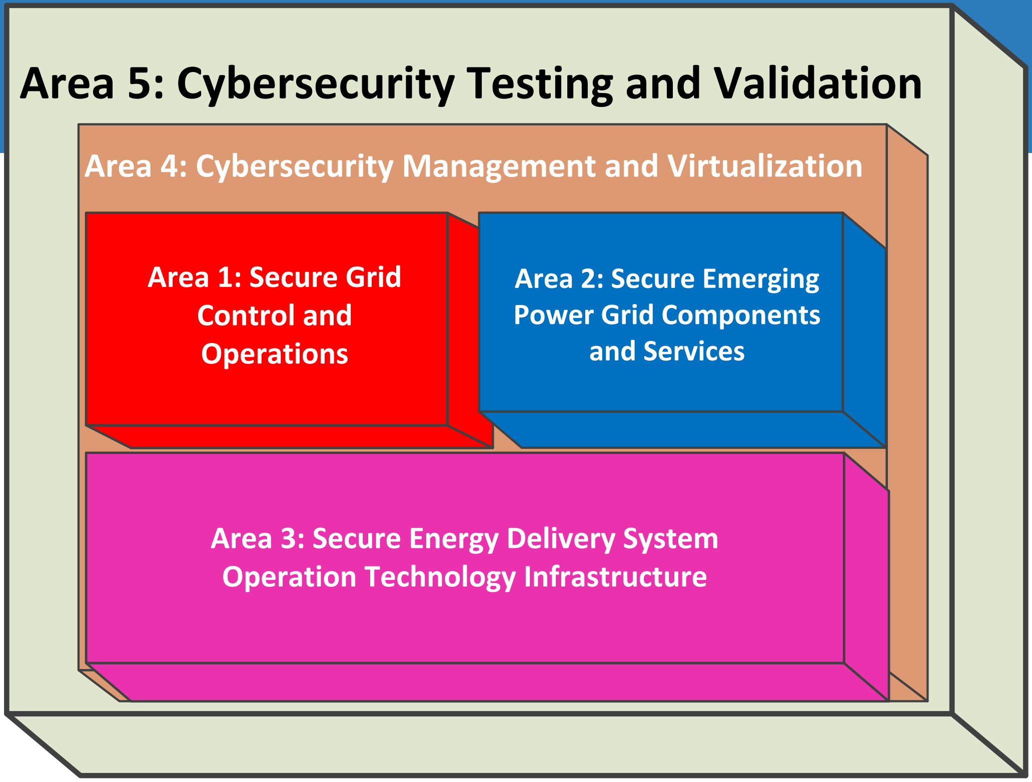
Major Accomplishments

- 24 cybersecurity tools developed and tested
- 9 inventions disclosed
- 50 journal publications
- 64 conference publications
- 7 more papers in submission
- 10 invited talks
- 1 cybersecurity special section at IEEE Journal of Emerging and Selected Topics in Power Electronics
- 1 Cybersecurity Session at IEEE ECCE 2016
- Collaboration with ORNL to organize a cyber conference
- 6 industry engagement meetings
- Evaluative methodology for project selection
- 8 Industrial Board Members as a paying organization - to fund additional efforts
- 60 organizations that SEEDS has interacted with
- 48 students

Progress to Date (2/2)

Major Accomplishments

- Cyber testbed
- Automating remediation action analysis, mitigation information localization, and risk analysis for security vulnerabilities
- Extended cybersecurity threat information sharing
- A tri-modular framework for an intelligent visualization of smart grid cyber attacks
- HELOT-Hunting Evil Life in Operational Technology
- Detecting compromised devices
- Detecting and localizing data falsification attacks in AGC through learning-based and physics-based methods
- Detecting and localizing topology attacks through hypothesis testing
- Early insider threat detection
- Quickest detection of sparse false data injection attacks



Area 5: Cybersecurity Testing and Validation
Area 4: Cybersecurity Management and Virtualization
Area 1: Secure Grid Control and Operations
Area 2: Secure Emerging Power Grid Components and Services
Area 3: Secure Energy Delivery System Operation Technology Infrastructure

- Cyber-secure power router
- Sequence hopping-based fast authentication for IEC 61850 GOOSE messages
- Detecting intelligent, stealthy delay-increasing attacks in time-critical communications
- Bloom filter-based public key management for smart meter networks
- Lightweight key management for low-bandwidth legacy environments in smart grid

Challenges to Success

Challenge 1: Solutions need knowledge from both cybersecurity and power systems, and from both academe and industry.

- Bridge the gap between industry and academia.
- Interdisciplinary team across cybersecurity, computer science, and power systems.

Challenge 2: Difficult to obtain industry data.

- Involving industry partners more closely.
- Working with industry to sanitize data.
- Sending student interns to industry partners.

Challenge 3: Integration into existing systems without interrupting service.

- Account for the impact of solutions on the existing system in design and evaluation.
- Beta testing at industry partners or over industry-shared data.

Challenge 4: Center sustainability.

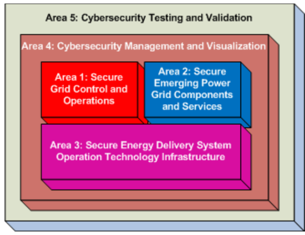
- Continue to provide benefits that convince industry to join the center.
- Multi-tier membership structure to provide flexibility to members.

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

- Targeted end user for the technology
  - Vendors: One current start-up licensing a SEEDS technology.
  - Facility owners: AECC, SPP, Today's Power
- Plans to gain industry acceptance?
  - Project topics were proposed by industry and proposal selections were suggested by industry
  - Many technologies have been alpha-tested (at university facilities) and/or beta-tested (at industrial facilities)
  - Beta-testing partners include EPRI, AECC, and SPP
  - Hardware and software demonstrations were carried out at annual center meetings and with company partners.
  - Multiple patents were filed and brought up to IAB members for technology transfer.
  - Other patents are being managed by universities and commercialization plans are under development.
- Timeline for demonstration and sector adoption
  - SPARTAN Technology has already been tested and demonstrated extensively sector adoption is imminent.
  - CSPR has been tested extensively and is currently being demonstrated. Sector adoption is expected within one year.

Next Steps for SEEDS (1/3)


Area 5: Cybersecurity Testing and Validation

Area 4: Cybersecurity Management and Visualization

Area 1: Secure Grid Control and Operations

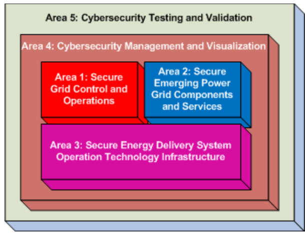
Area 2: Secure Emerging Power Grid Components and Services

Area 3: Secure Energy Delivery System Operation Technology Infrastructure

Approach for the next year or to the end of project

- Detecting Compromised Devices
- Detecting and localizing data falsification attacks in AGC through learning-based and physics-based methods
- Topology Attacks
- Quickest Intrusion Detection
- Cyber-Secure Power Router

Next Steps for SEEDS (2/3)


Area 5: Cybersecurity Testing and Validation
Area 4: Cybersecurity Management and Visualization
Area 1: Secure Grid Control and Operations
Area 2: Secure Emerging Power Grid Components and Services
Area 3: Secure Energy Delivery System Operation Technology Infrastructure

Approach for the next year or to the end of project

- Sequence hopping algorithms for secure IEC 61850 Layer 2
- Lightweight Key Management for Low-bandwidth Legacy Environments in Smart Grid
- Detecting intelligent, stealthy delay-increasing attacks in time-critical communications
- Automated Security Vulnerability and Patch Management
- Extended Cybersecurity Threat Information Sharing
- A Tri-Modular Framework for an Intelligent Visualization of Smart Grid Cyber-Attacks
- HELOT-Hunting Evil Life in Operational Technology

Next Steps for SEEDS (3/3)

- Transition of mature tools to practice.
- We have expanded collaboration with industry, national labs in proposal submissions and will continue collaborations in various ways.
- NSF I/UCRC effort for sustainability with CREDC (UIUC).

Cyber Secure Power Router

Objective: Develop Cyber Physical System that is cyber-hardened by design

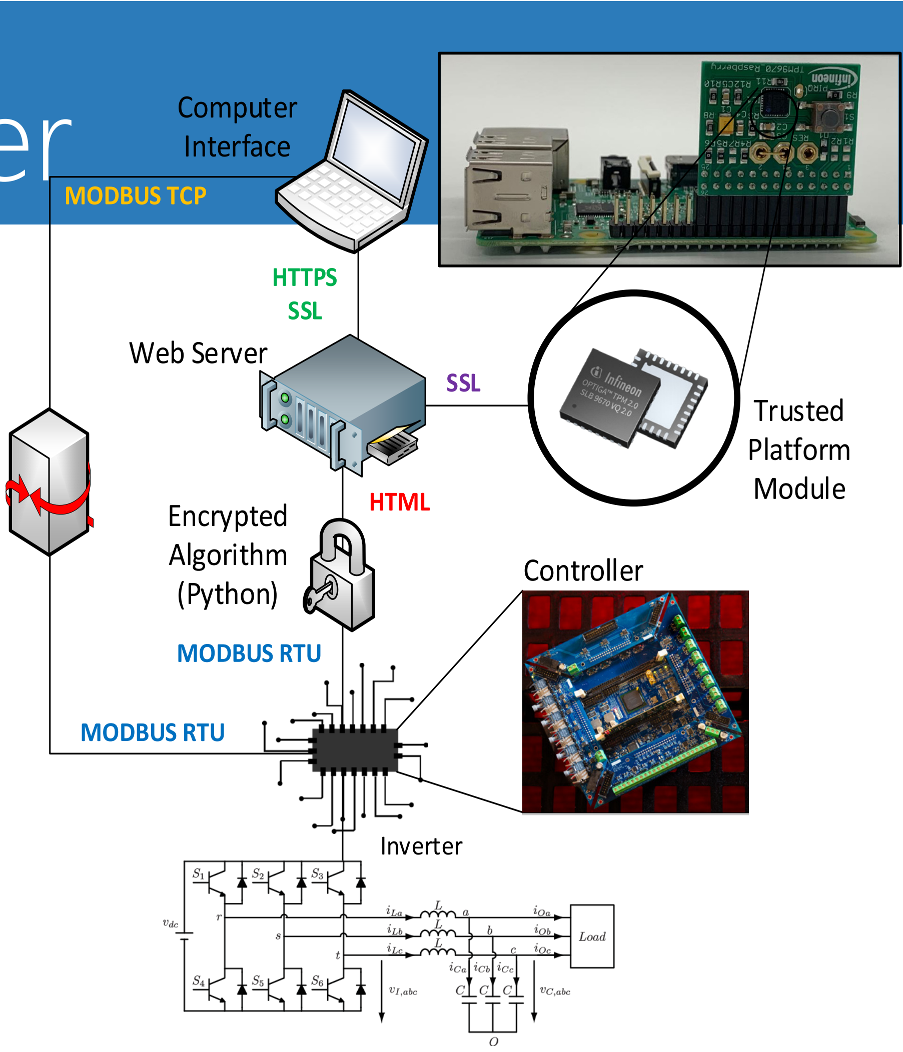
- Detect and mitigate cyberattacks at the communication layer, control layer and hardware layer.
- Effectively distinguish between cyberattacks and load changes.

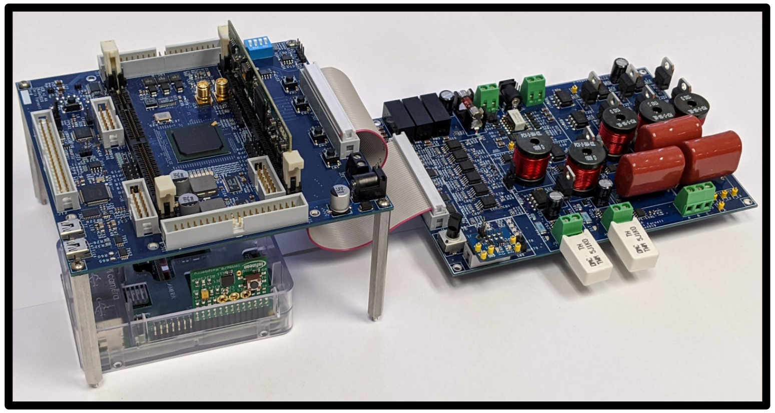
Innovations:

- Prevent software theft of encryption keys through the integration of a TPM into the cyber-physical system.
- Developed shoot-through protections and ensured the integrity of the data at hardware level through polling of voltage values at hardware layer.

Products: Cyber Secure Power Router Pre-Production prototype.

- Webserver to interface with CSPR board.





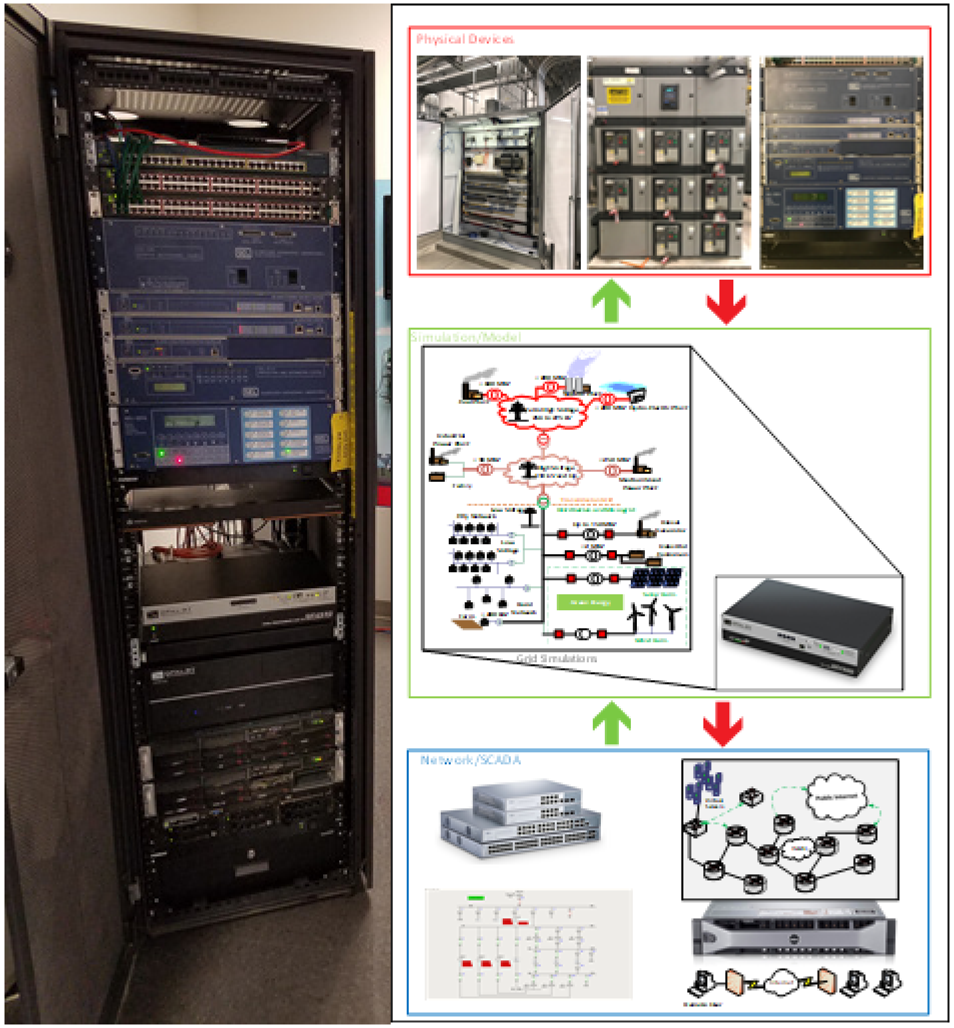
SEEDS Advanced Testbed Project

Objective: Large-Scale Control Cybersecurity Testing based on an Extended Testbed

- Allow for Alpha testing in a realistic environment.
- Utilize industry standard protocols and equipment.
- Both simulated and real-world power flows.

Innovations:

- Developed virtual protection relay models.
- Integrated HIL assets/simulations with physical devices.
- Emulated Inter and Intra communication networks.



Products: Cybersecurity Testbed

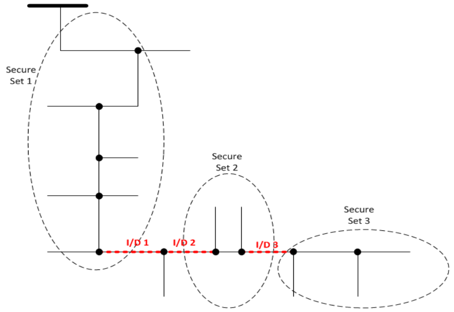
- Testing resource for researchers.
- Data collection of realistic network traffic.
- Remotely accessible testing environment.

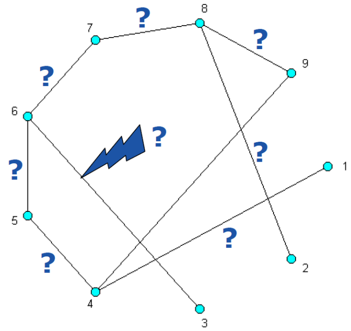
Topology Attacks: Detection and Localization
PI: Soummya Kar, Carnegie Mellon University

Objective

- A topology attack occurs when the assumed network structure is incorrect.

Goals:
- ❑ detect and isolate topological inconsistencies
- ❑ scalable, decentralized topology monitoring
- ❑ unified approach: transmission and distribution





Schedule

- 09/2019 --- 12/2020
- Developed algorithms and software, and performed validation.
- This project develops a framework for power system topology monitoring and attack detection, based on optimal sensor placement, measurement data integration and fast decentralized attack analysis algorithms. The tools developed can be integrated with existing utility system modules, to enable reliable state and topology monitoring, protection and outage analysis in the face of malicious cyber attacks.

Total Value of Award:	**$230,021.36**
Funds Expended to Date:	**93%**
Performer:	**Carnegie Mellon University**
Partners:	

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Topology Attacks: Detection and Localization

	Current Methods	Our Software and Methods
Detection Strategy	Mostly centralized	Distributed
Computation burden	Slow and inefficient	Fast and efficient detection
Scalability	Complexity increase with scale	Scalable without increasing the complexity
Objective	Failure and outage detection	Topology attacks, failure and outage detection
Scope	Mostly power transmission networks	Transmission & distribution networks
Structure exploitation	Not exploited efficiently	Leveraged to increase the effectiveness of solution where applicable

PowerWatch: Detection of Compromised Devices in the Smart Grid

PI: Selcuk Uluagac, FIU

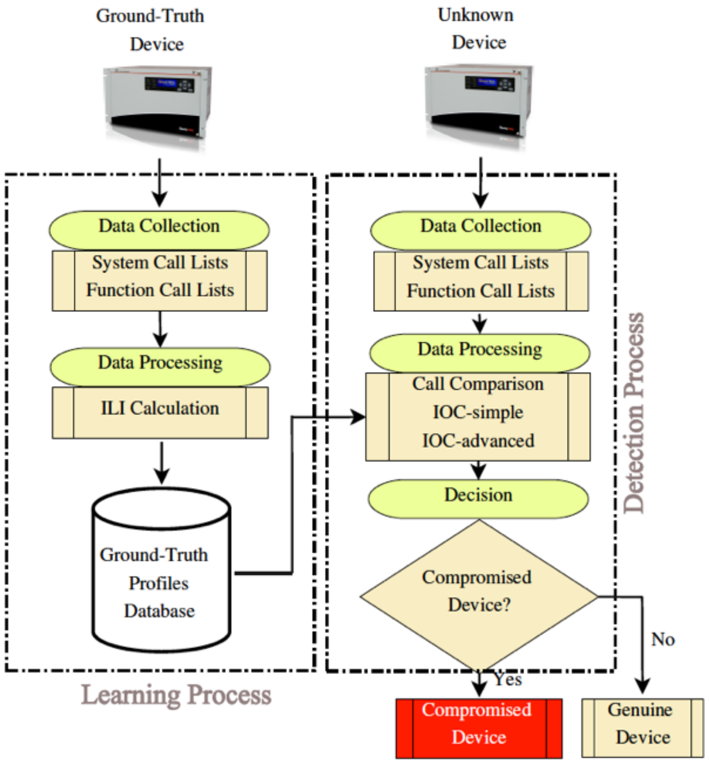
Objective

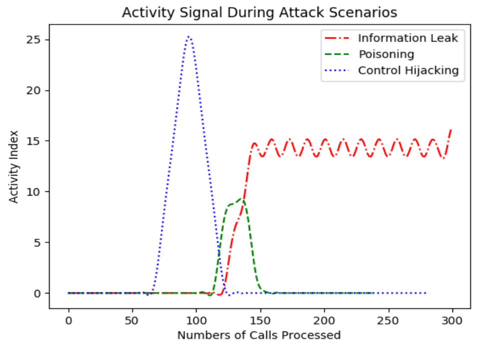
- The use of untrusted compromised smart grid devices (e.g., IEDs, PLCs, PMUs) poses a real problem to the reliable two-way communications in the grid.
- Consequences of propagating false or malicious data, as well as stealing valuable user or smart grid state information from compromised devices are costly.
- Hence, early detection of compromised devices is critical for protecting smart grid's components and users.
- To address these concerns, in this project, we propose a system called PowerWatch that utilizes system call tracing, library interposition, statistical, and machine learning techniques for monitoring and detection of compromised smart grid devices.

Schedule

- Year-1: Initial testbed built.
- Years 2-3: Initial algorithms and PowerWatch framework built and evaluated.
- Years 3-4: Improved the framework with more detection algorithms and tested it.
- Years 4-5: Decentralized capability built (in collaboration with the UARK team).

Project Overview





PowerWatch is able to detect compromised devices with %95.1 accuracy at %0.03 false positive rate.

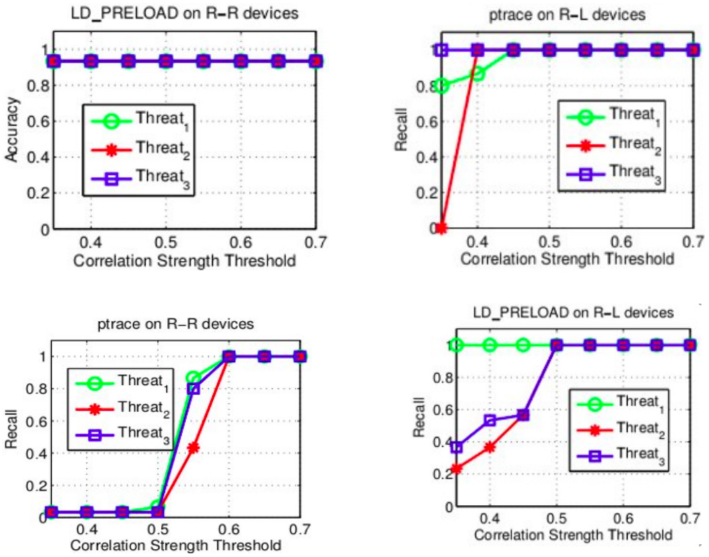
PowerWatch: Project 1.7 Detection of Compromised Devices in the Smart Grid

PI: Selcuk Uluagac, FIU

Project Highlights and Impact

Outcome & Impact

- We are the first team to investigate compromised devices in the smart grid context and furthermore successfully explored the integration our solution with the Cybersecure Power Router Project (PI: Mantooth).
- So far, we have developed a lightweight method to detect compromised devices, extended this method to be more comprehensive and implemented a version that is able to run on a prototype energy management system, as well as distributed systems.
- As a result, our work have been recognized with **3 patents** (2 awarded, 1 pending), **5 journal papers** (some under review), **4 conference papers**, **2 posters**, **6 invited talks**, **1 invited live demo**, **2 best demo awards**. In addition, our PhD student Leonardo Babun has been awarded a prestigious NSF/DHS scholarship for his work in the project.



Initial Talks with Industry

- **PowerWatch is ready to be deployed**, and we are actively seeking to collaborate with the industry. We are already in talks with AECC, EPRI, and Bedrock Industries for testing, feedback, and application of our ideas.
- **Benefits to Industry:** (1) Open source, (2) Configurable, (3) Minimal overhead, (4) Comprehensive threat model, (5) High detection rate, (6) Applicable beyond smart grid.

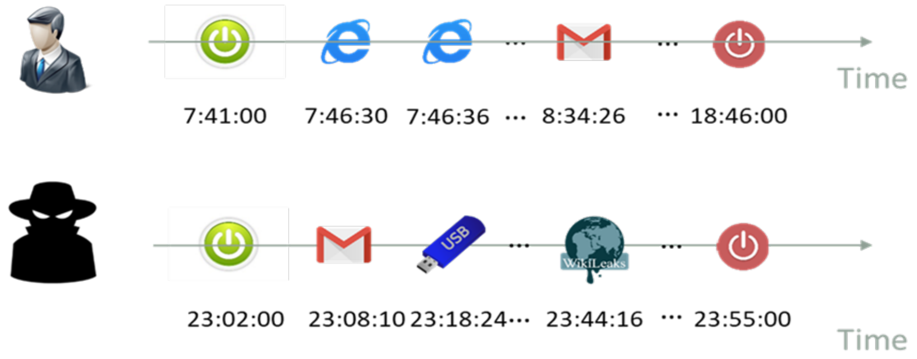
BEDROCK OPEN SECURE AUTOMATION

Arkansas Electric Cooperative Corporation
We Are Arkansas

EPRI ELECTRIC POWER RESEARCH INSTITUTE

U.S. DEPARTMENT OF ENERGY | OFFICE Cybersecurity, Energy Security, and Emergency Response

Early Insider Threat Detection
PI: Xintao Wu, University of Arkansas



➢ It addresses challenges

- Heterogeneous data
- Time dynamics
- No or few labeled insider records in training dataset

➢ A suite of novel algorithms for insider threat detection

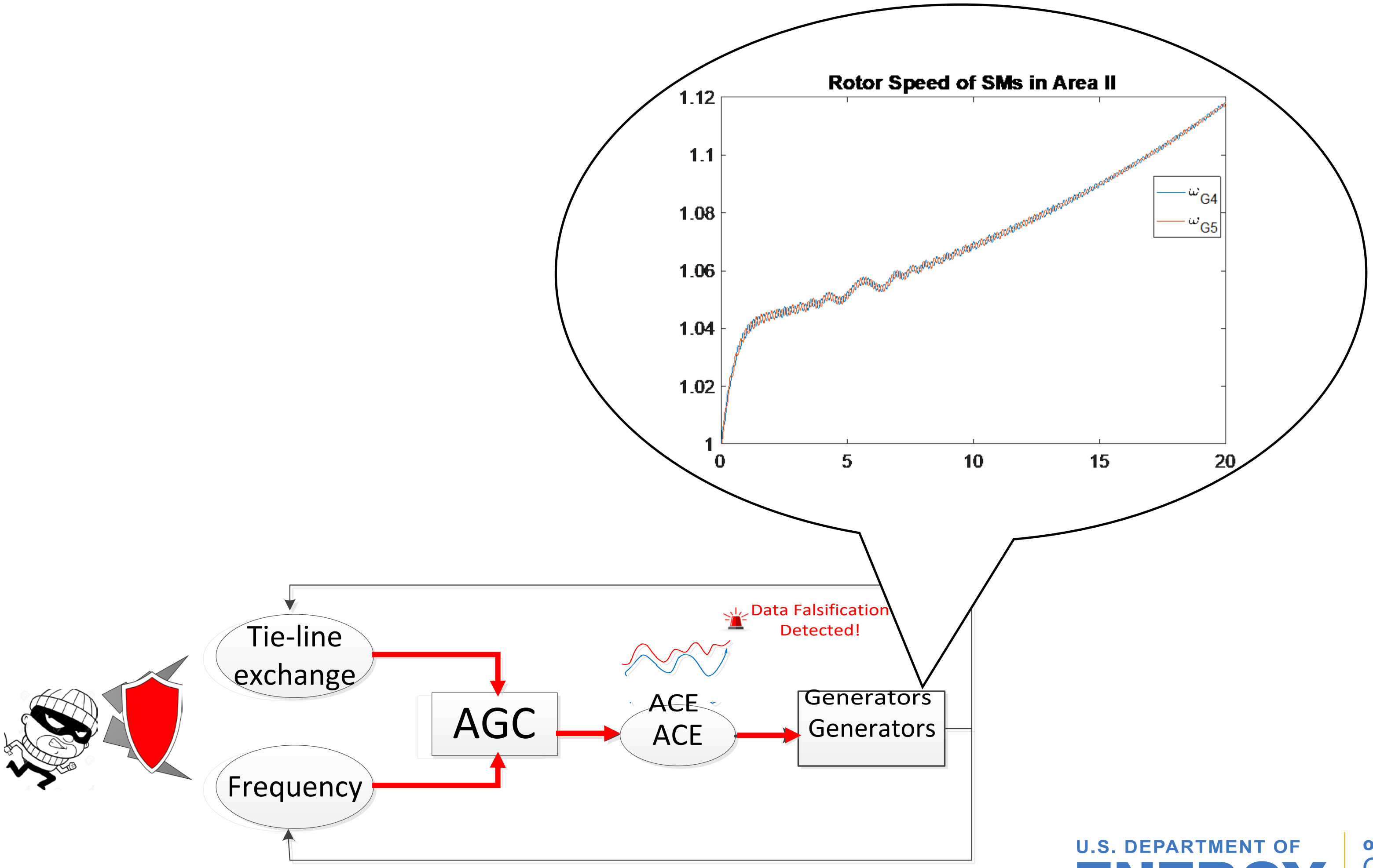
- Multi-Source LSTM
- Hierarchical Neural Temporal Point Processes
- One Class Generative Adversarial Networks
- Few Shot Learning

➢ Publications

- Shuhan Yuan, Panpan Zheng, Xintao Wu, Qinghua Li. "Insider Threat Detection via Hierarchical Neural Temporal Point Processes". Proceedings of IEEE International Conference on Big Data (BigData), Los Angeles, CA, USA, Dec 9-12, 2019.

Cyber-Physical Methods for Detecting and Localizing Data Falsification Attacks in Automatic Generation Control
PI: Marija Ilic (MIT), Co-PI: Qinghua Li (UA)

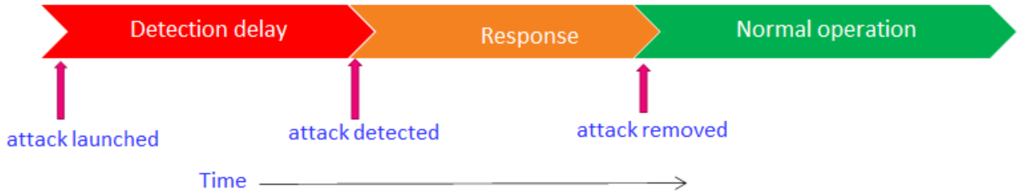
- **Problem addressed**
  - Data falsification in AGC → incorrect generation & power grid instability.



Cyber-Physical Methods for Detecting and Localizing Data Falsification Attacks in Automatic Generation Control
PI: Marija Ilic (MIT), Co-PI: Qinghua Li (UA)

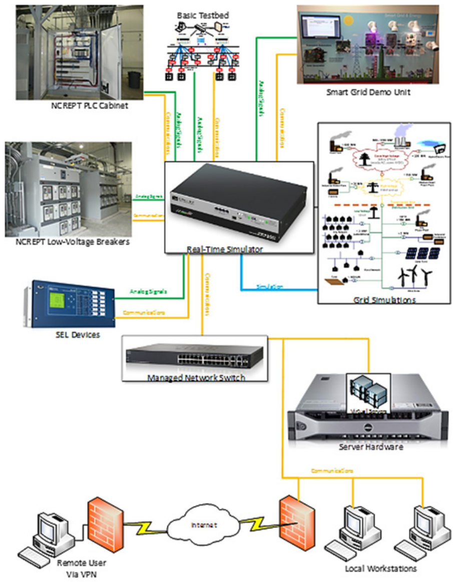
- **Project accomplishments**
  - A learning-based technology for detecting and localizing data forgery based on neural networks.
  - A physics-based technology for detecting and localizing data forgery based on Interaction Variables (IntVar).
  - Easy to deploy and no interruption of energy delivery.
  - Tests of prototype system over real ACE data of SPP and PJM and simulated AGC systems showed high accuracy (>95%).
  - 3 publications, 1 award, 1 invited talk, and 2 paper submissions.
- **Next Steps**
  - Comprehensive assessment of the impact of AGC data forgery attacks to the power grid.
  - Tests on real AGC operation data.
  - NDA being signed for accessing the AGC data of a utility partner.
- **Tech transfer**
  - Work with utility partner or open-sourcing.

Quickest Intrusion Detection
PI: Jingxian Wu, University of Arkansas



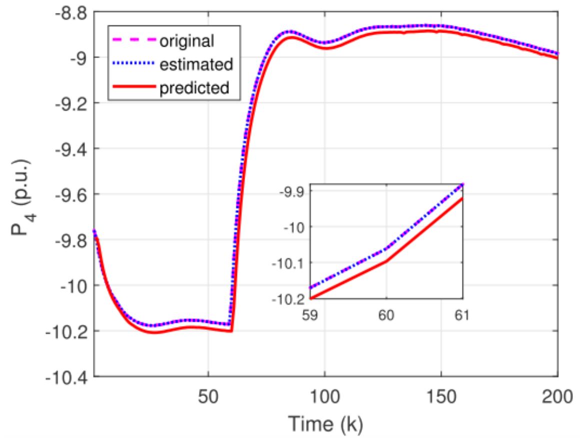
Objective: minimizing detection delay

- Detect cyberattacks and sudden load changes in real time with minimum delays.
- Effectively distinguish between cyberattacks and load changes.



Innovations:

- Minimizing detection delay while maintaining high detection accuracy.
- Transient analysis with dynamic models to track power grid state transition in real time.



Products: Quickest intrusion detection algorithms

- OMP-CUSUM
- EKF-GLRT
- Rao-CUSUM

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Sample Project: Sequence Hopping Algorithm for Secure GOOSE Messages [PI: Osama Mohammed, FIU]

What is the product?

Sequence Hopping Algorithm to protect IEC 61850 GOOSE messages against attacks.

Deployment

Alpha tested V1.0 of Sequence Hopping Algorithm for protecting Layer 2 GOOSE Messages at FIU Smart Grid Testbed.

Beta tested V1.0 of Sequence Hopping Algorithm for protecting Layer 2 GOOSE Messages at Electric Power Research Institute (EPRI), in Knoxville, TN.

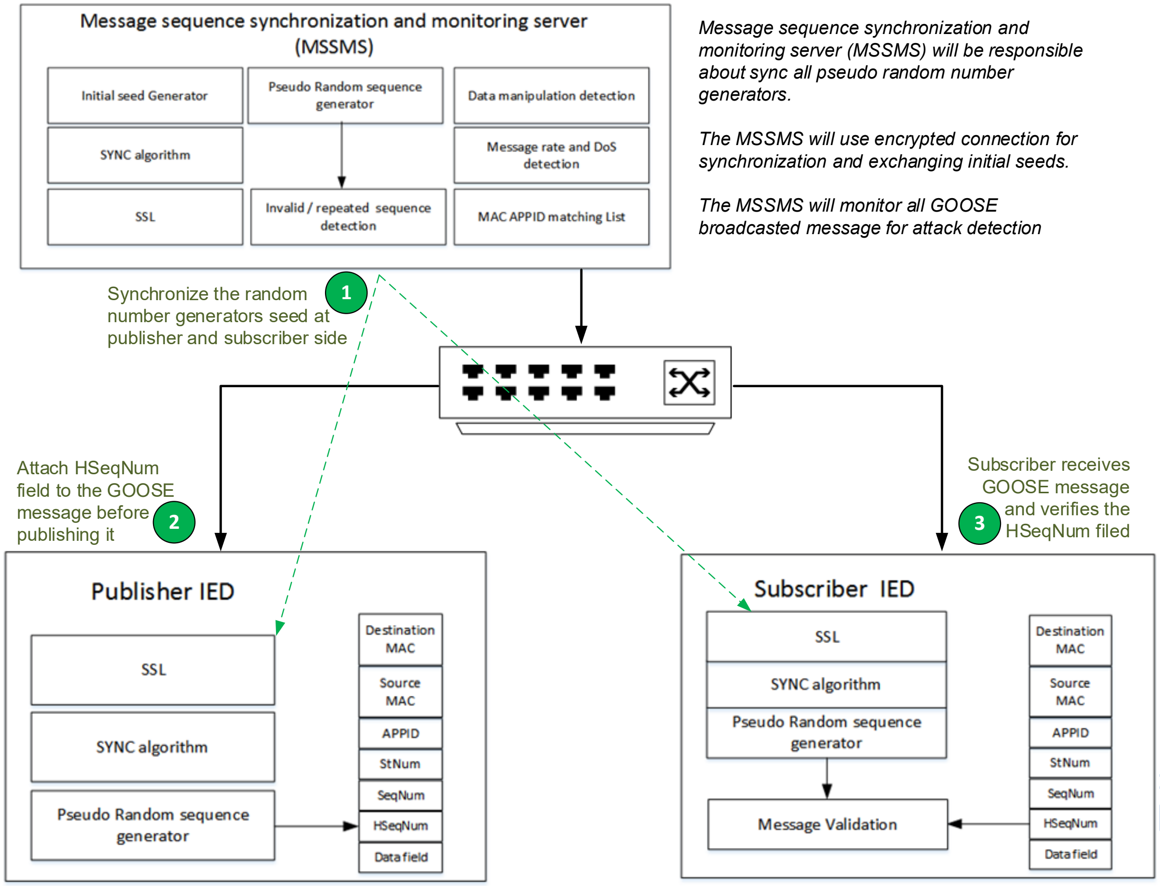
A US Patent (9894080) has been awarded for the efforts completed so far.

This solution could be deployed through a firmware update to IEDs or as a bump-in-the-wire device.

Industry Relevance

Addressing the security of critical IEC 61850 GOOSE messaging protocol, which is a widely accepted standards.

Presented the research efforts in the IEC TC57 WG15 meeting.



Message sequence synchronization and monitoring server (MSSMS)

Initial seed Generator

Pseudo Random sequence generator

Data manipulation detection

SYNC algorithm

Message rate and DoS detection

SSL

Invalid / repeated sequence detection

MAC APPID matching List

Message sequence synchronization and monitoring server (MSSMS) will be responsible about sync all pseudo random number generators.

The MSSMS will use encrypted connection for synchronization and exchanging initial seeds.

The MSSMS will monitor all GOOSE broadcasted message for attack detection

1 Synchronize the random number generators seed at publisher and subscriber side

2 Attach HSeqNum field to the GOOSE message before publishing it

3 Subscriber receives GOOSE message and verifies the HSeqNum filed

Publisher IED

SSL

SYNC algorithm

Pseudo Random sequence generator

Destination MAC

Source MAC

APPID

StNum

SeqNum

HSeqNum

Data field

Subscriber IED

SSL

SYNC algorithm

Pseudo Random sequence generator

Message Validation

Destination MAC

Source MAC

APPID

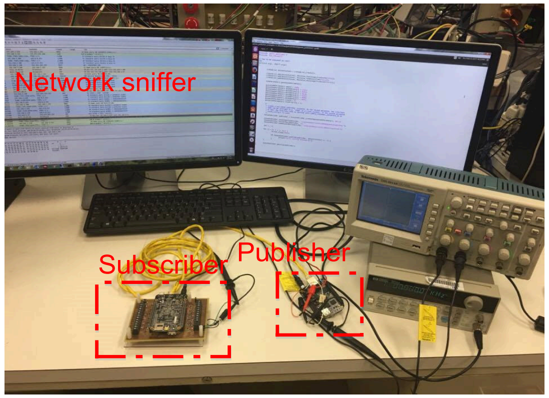
StNum

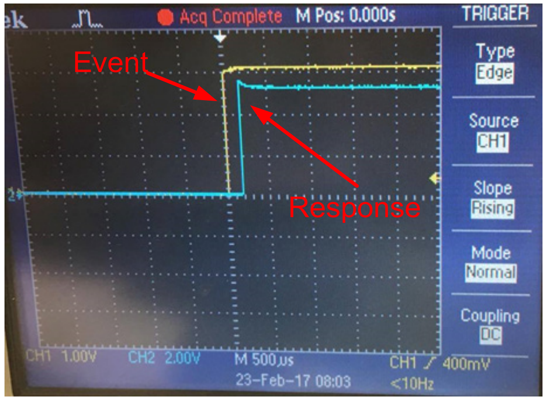
SeqNum

HSeqNum

Data field

Experimental Validation





End-to-end delay time for the embedded sequence hopping implementation is **250 micro seconds**

Lightweight Key Management for Low-bandwidth Legacy Environments in Smart Grid
PI: Kemal Akkaya Florida International University

Objective

- Integrating key management solutions with the current legacy equipment and communication infrastructure of power grid to ensure security services while not compromising the performance.

Schedule

- 8/15/2019 – Ongoing.
- Protocol Software and testbed for evaluations.

Total Value of Award:	**$ 91,106.00**
Funds Expended to Date:	**% 90**
Performer:	**FIU**
Partners:	**NA**

Lightweight Key Management for Low-bandwidth Legacy Environments in Smart Grid
PI: Kemal Akkaya Florida International University

Advancing The State of The Art (SOA)

- Current key management standards such as TLS and IPSec are not suitable for Power Grid environments with legacy infrastructures.
  - They bring communication overhead which may eventually risk actual data transfers.
- Our approach considers the traffic types and characteristics of power grid devices to bring same key management features without impacting the operations of the grid devices.
- Our approach reduces the symmetric key management communication overhead 4-fold even in the worst case.
- The proposed approach can be used by remotely deploying the software on the field devices.
- Through this approach, the same level of security is achieved as the Internet and keys are renewed in the ideal frequency to prevent any compromise.
- Since the infrastructure for a power grid is still legacy in most places, this approach is crucial and easily deployable.

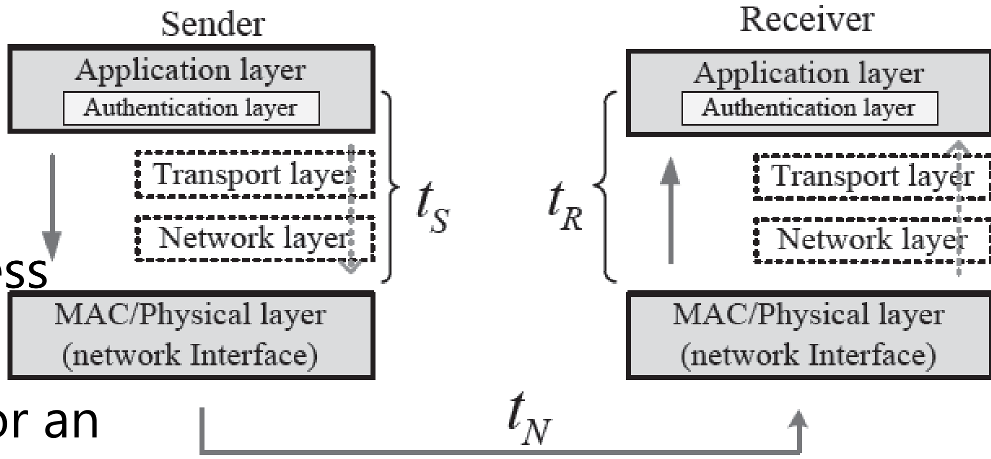
Lightweight Key Management for Low-bandwidth Legacy Environments in Smart Grid
PI: Kemal Akkaya Florida International University

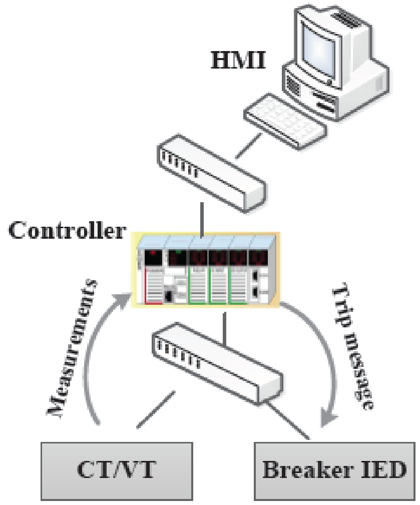
Major Accomplishments

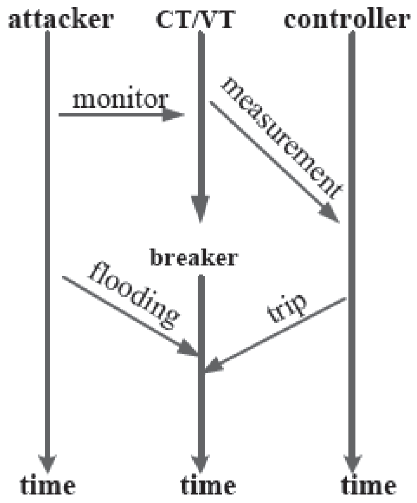
- A novel symmetric key management protocol geared for legacy power grid systems is designed and implemented.
- The protocol achieves at least 4-fold delay reduction while being resilient to any of the existing cybersecurity attacks.
- Preliminary results of the paper are published in one of the flagship conferences, IEEE GLOBECOM in Dec. 2019.
- Another version is applied to DNP3 and has been accepted to be published as part of DOE Resilience Week in Oct. 2020.
- A LoRa-based testbed was developed to test the approach at FIU in a realistic setting. The code is available to be deployed and used for real environments.
- A journal submission and a patent disclosure are being prepared.
- The student who was involved in this project graduated with a PhD degree and has been hired as a tenure track faculty in the US.

Secure Time-Critical Communications
PI: Qinghua Li, University of Arkansas

- **Problem addressed**
  - Substation communications have stringent time constraint (e.g., 3ms)
  - Attacks make message delays exceed the limit
- **Project accomplishments**
  - Experimentally assessed the resilience of wireless and switched Ethernet against flooding attacks
  - Developed a bait-based detection technique for an intelligent, stealthy delay-increasing attack
  - Easy to deploy in network security device/software
  - One publication
- **Next Steps and Tech Transfer**
  - Detection in multi-attacker scenarios
  - Field test at EPRI
  - Seeking for industry partners for tech transfer



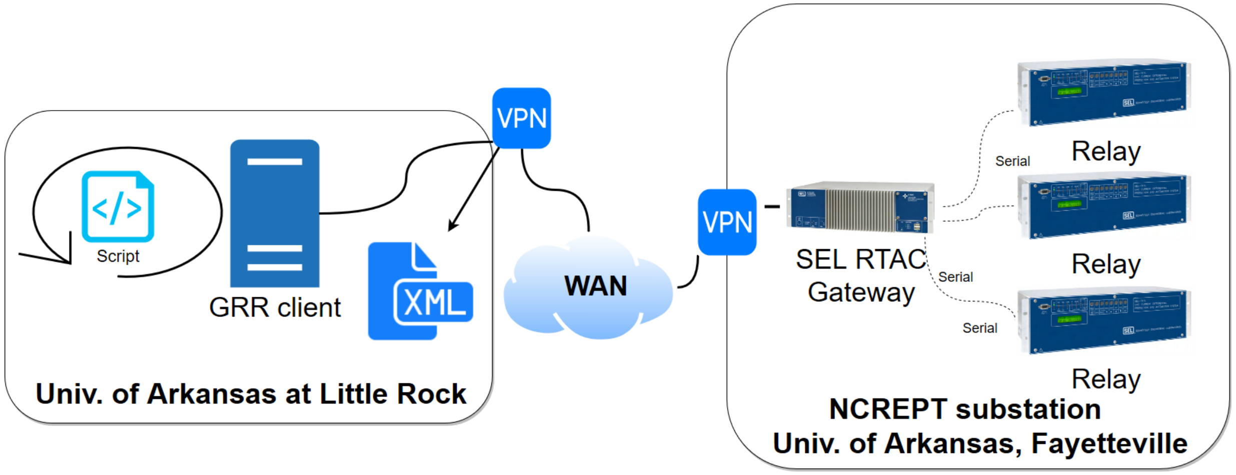




HELOT-Hunting Evil Life in Operational Technology
PI: Jan Springer, University of Arkansas, Little Rock

Life forensics in combined OT/IT environments

- Minimal security logs and storage for OT devices
- Geographically dispersed devices
- Service downtime undesired
- How to capture forensic artifacts?

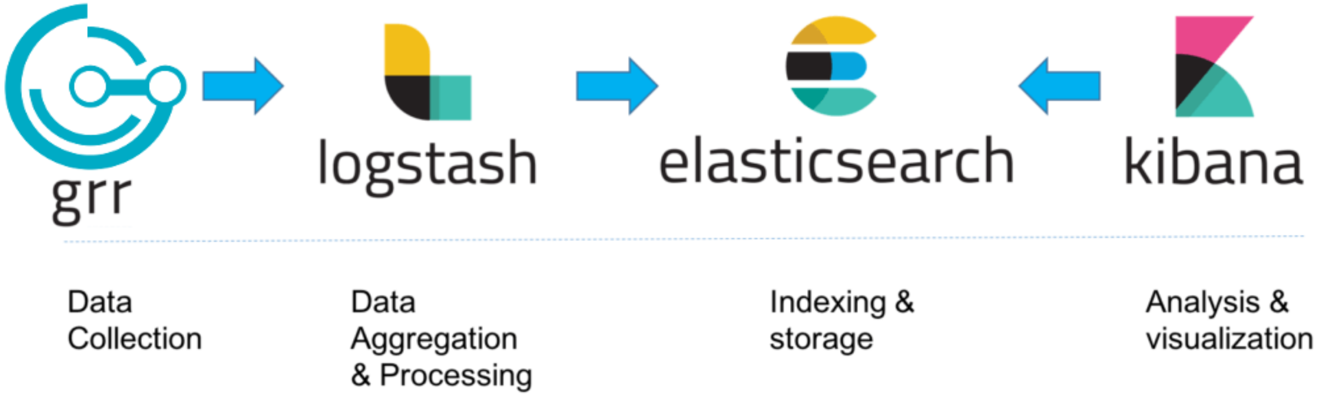


Innovation

- Live forensics pipeline of configuration data and network traces
- Artifact specification for each OT device
- Light client, client-less connection spanning wide area networks

Next steps

- Multi-vendor OT device support
- Large-scale testing at EPRI
- Real-world testing at regional utility
- Back-end machine learning analytics



Technology transfer

- OT device specs to be included w/ GRR
- Apache License 2.0

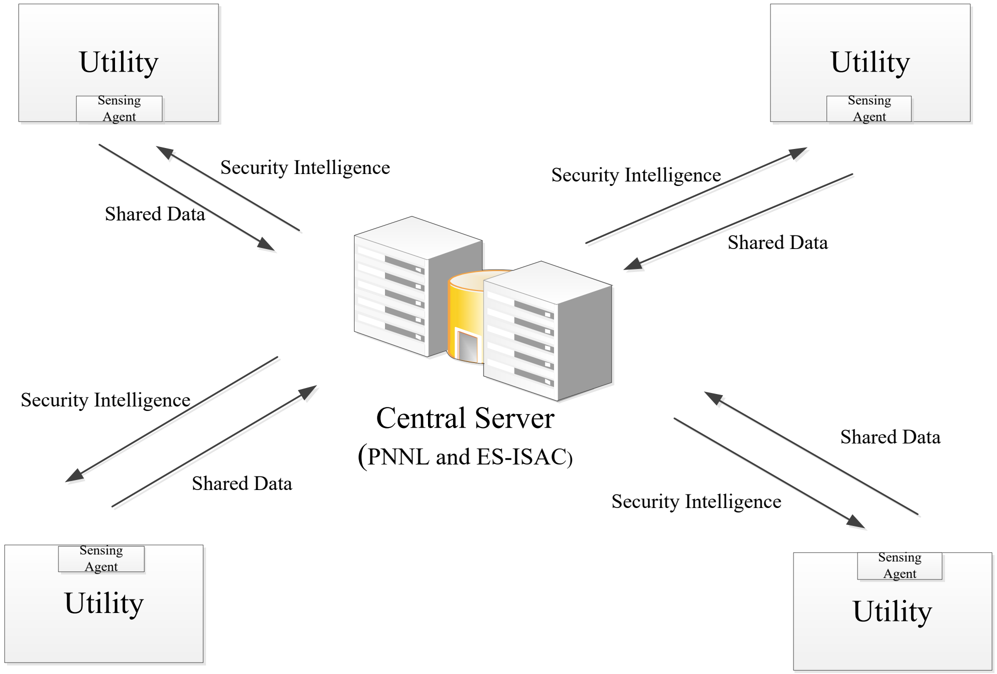
EPRI ELECTRIC POWER RESEARCH INSTITUTE

Electric Cooperatives of Arkansas
Your Local Energy Partners

U.S. DEPARTMENT OF ENERGY
OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Extended Cybersecurity Threat Information Sharing
PI: Qinghua Li, University of Arkansas

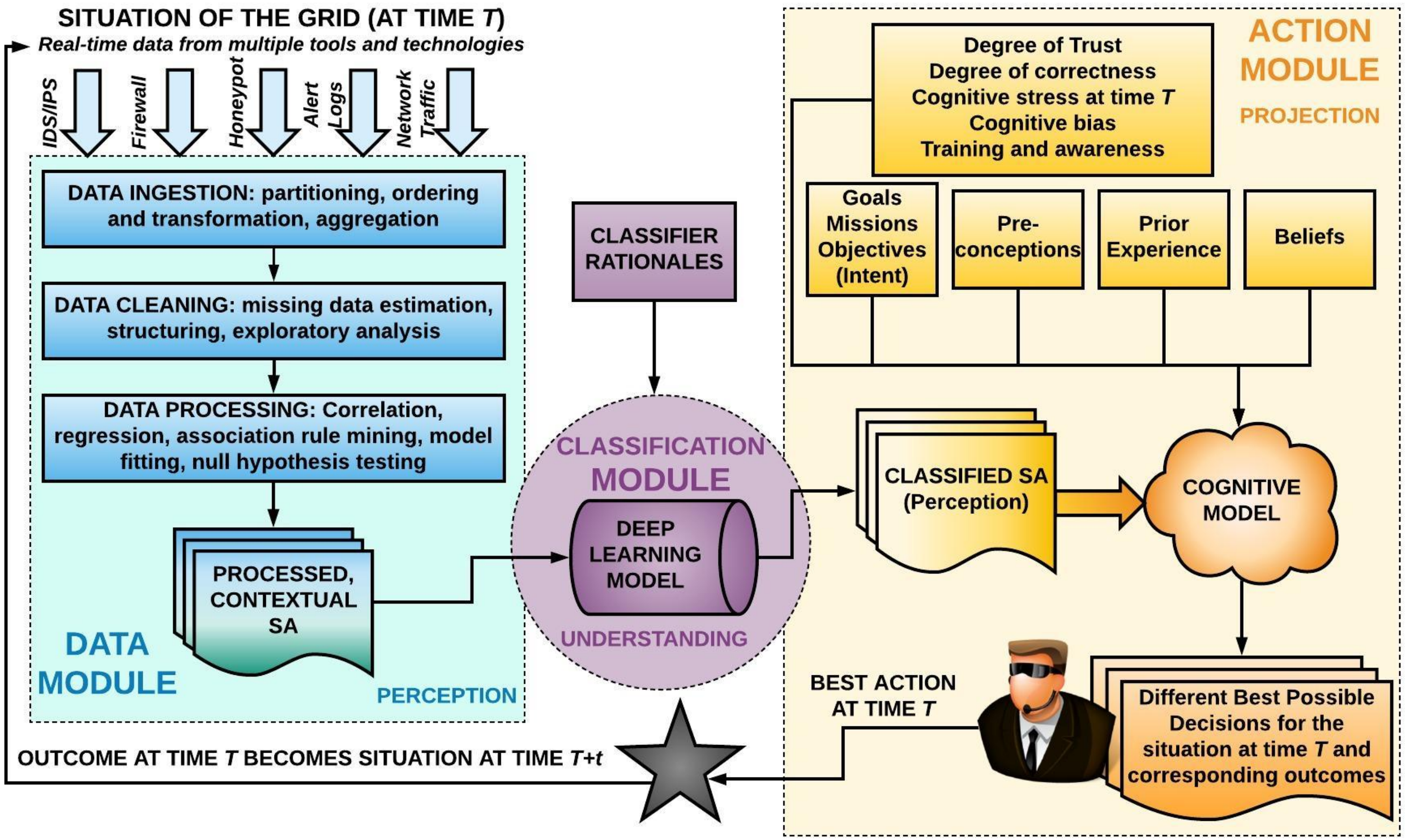
- **Limitations of existing sharing**
  - Deployed at boundary of utility networks
  - Only share IP headers
  - Expensive collection sensor
- **Project accomplishments**
  - Advancing state of the art: sharing internal traffic & sharing application-layer data & low-cost sensing agent
  - Identified data types to share
  - Identified data not to share
  - Identified methods for perturbing sensitive data
  - Implemented a software agent for collecting data
- **Next Steps and Tech Transfer**
  - Refine application data collection
  - Field test
  - Collaboration with CRISP for tech transfer



U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Tri-Modular Framework
PI: Arif Sarwat, Florida International University

Data management and analysis framework for Network Operating Center and Security Operating Center


SITUATION OF THE GRID (AT TIME *T*)
Real-time data from multiple tools and technologies
IDS/IPS
Firewall
Honeypot
Alert Logs
Network Traffic
DATA INGESTION: partitioning, ordering and transformation, aggregation
DATA CLEANING: missing data estimation, structuring, exploratory analysis
DATA PROCESSING: Correlation, regression, association rule mining, model fitting, null hypothesis testing
PROCESSED, CONTEXTUAL SA
DATA MODULE
PERCEPTION
CLASSIFIER RATIONALES
CLASSIFICATION MODULE
DEEP LEARNING MODEL
UNDERSTANDING
ACTION MODULE
PROJECTION
Degree of Trust
Degree of correctness
Cognitive stress at time *T*
Cognitive bias
Training and awareness
Goals Missions Objectives (Intent)
Pre-conceptions
Prior Experience
Beliefs
CLASSIFIED SA (Perception)
COGNITIVE MODEL
BEST ACTION AT TIME *T*
Different Best Possible Decisions for the situation at time *T* and corresponding outcomes
OUTCOME AT TIME *T* BECOMES SITUATION AT TIME *T+t*

Rapid Response formulation

- By enhancing the Situational Awareness of employees.
- Providing intuitive visual queues about un-folding events in the smart grid.
- Reducing cognitive stress in time-critical scenarios.

Derive knowledge and wisdom from data streams

- Using the Classification Module (CM) to correct false positives from security tools.
- Layer Artificial Intelligence on-top of traditional threat detection.

Data Module, False Data Injection Detector, and Detection of Suspicious Network Traffic

The data module functionality includes:

- **data storage**
- **correlation of input variables**
- **regression for prediction of time-series**
- **other functions to create a perception of the wide-area cyber-physical system state from the incoming data incoming**

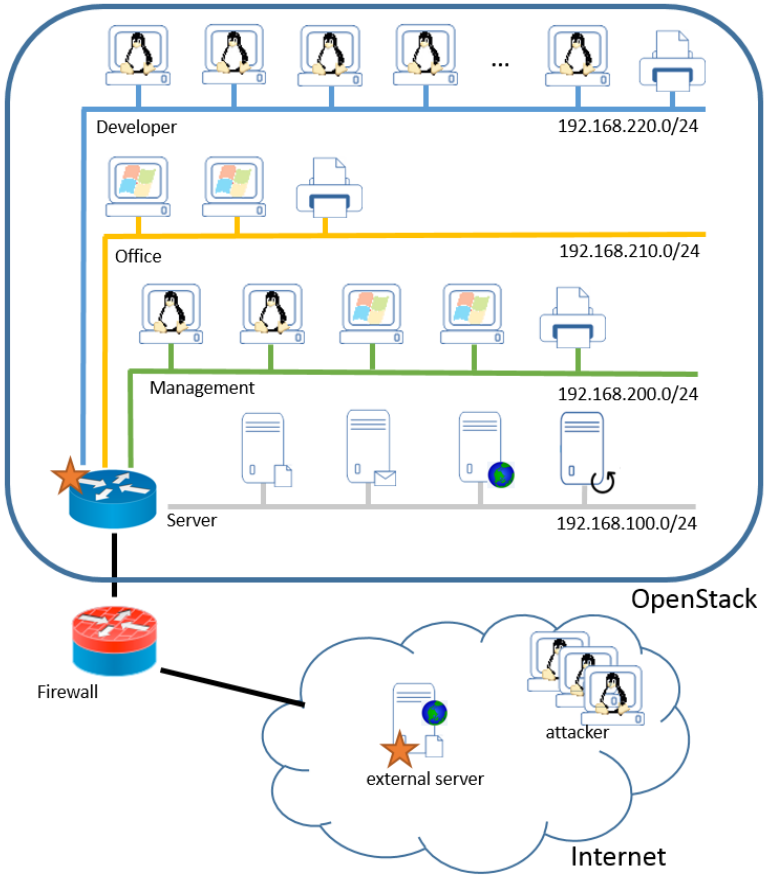
It uses computer clustering to enable scalability of the system meet demand [1]

Comprehensive cyber-security computational framework:

- **a holistic approach to cyber-security**
- **addresses the data management and machine learning aspects**
- **addresses the human element and the cognitive dissonance between the security personnel and the data to be parsed**
- **approach is of 'human-on-the-loop' as opposed to the traditional 'human-in-the-loop' security that does not consider the human cognitive performance in cyber-security [2]**

Ongoing work towards publication of a technique for false data injection attack detection at photovoltaic production net meter

Recent efforts are on the development of the CM and testing scenarios.



Cyber network in the Coburg Intrusion Detection Data Sets malicious network activity dataset

[1] "Cluster-based Module to Manage Smart Grid Data for an Enhanced Situation Awareness: A Case Study," A. Sundararajan, H. Riggs, A. Jeewani, and A. I. Sarwat. IEEE Resilience Week 2019.
[2] "A Tri-Modular Framework to Minimize Smart Grid Cyber-Attack Cognitive Gap in Utility Control Centers," A. Sundararajan, L. Wei, T. Khan, A. I. Sarwat, and D. Rodrigo, Resilience Week 2018.

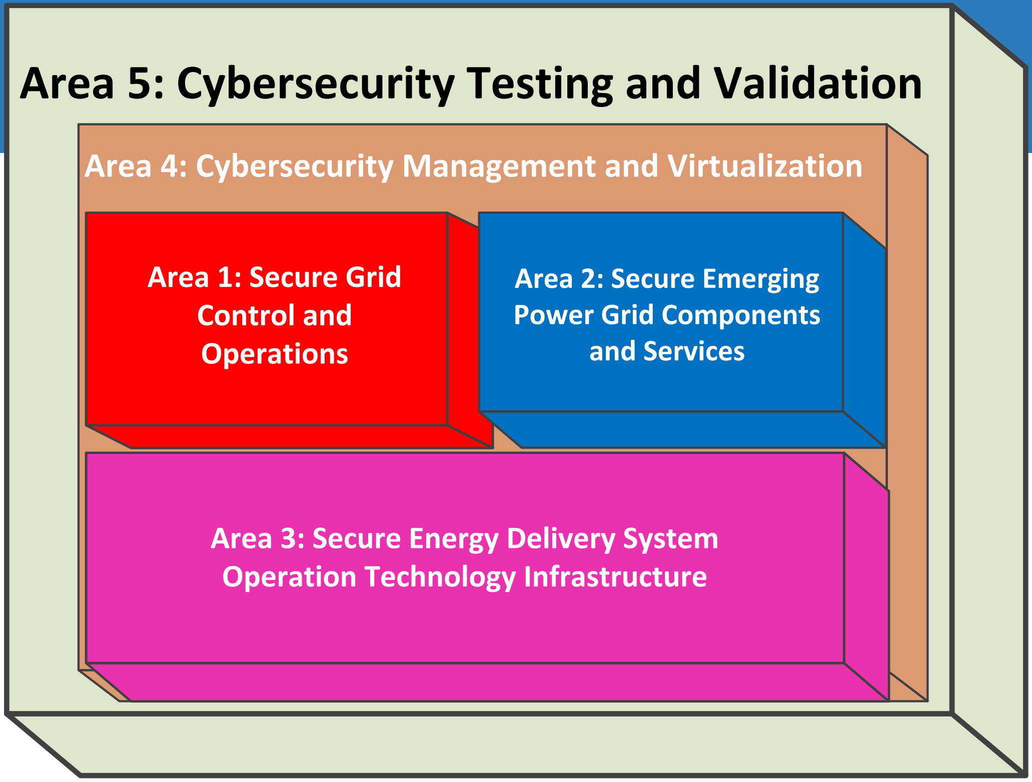
Security Patch Automated Remediation Tool Analyzing the NVD (SPARTAN)
PI: Qinghua Li (UA), Co-PI: Philip Huff (UA Little Rock)

- **Problem addressed**
  - Many security vulnerabilities + heavily manual operations in vulnerability risk analysis and decision making → long delay in remediation & poorer security & high cost.
- **Project accomplishments**
  - An AI-based tool for automated prediction of remediation actions for vulnerabilities.
  - An AI-based tool for automated estimation of risk levels for vulnerabilities.
  - A natural language processing-based tool for automated identification mitigation strategies from online resources.
  - Field tests at four electric utility partners.
  - 1 patent filed, 1 technology disclosed, 3 publications, multiple talks.
- **Tech transfer:** commercialization via a startup in process.

Progress to Date (2/2)

Major Accomplishments

- Cyber testbed
- Automating remediation action analysis, mitigation information localization, and risk analysis for security vulnerabilities
- Extended cybersecurity threat information sharing
- A tri-modular framework for an intelligent visualization of smart grid cyber attacks
- HELOT-Hunting Evil Life in Operational Technology
- Detecting compromised devices
- Detecting and localizing data falsification attacks in AGC through learning-based and physics-based methods
- Detecting and localizing topology attacks through hypothesis testing
- Early insider threat detection
- Quickest detection of sparse false data injection attacks


Area 5: Cybersecurity Testing and Validation
Area 4: Cybersecurity Management and Virtualization
Area 1: Secure Grid Control and Operations
Area 2: Secure Emerging Power Grid Components and Services
Area 3: Secure Energy Delivery System Operation Technology Infrastructure

- Cyber-secure power router
- Sequence hopping-based fast authentication for IEC 61850 GOOSE messages
- Detecting intelligent, stealthy delay-increasing attacks in time-critical communications
- Bloom filter-based public key management for smart meter networks
- Lightweight key management for low-bandwidth legacy environments in smart grid