SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

University of Arkansas

H. Alan Mantooth
Qinghua Li

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

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

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

Objective

- Research and develop cybersecurity technologies, tools, and methodologies that will advance the energy sector's ability to survive cyber attacks and incidents while sustaining critical functions

Schedule

- Project start/end dates: 10/01/2015 – 09/30/2020
- Deliverables: cybersecurity technology delivered in three phases in Sep. 2017, Mar. 2019, and Sep. 2020
- Security capabilities that will result from 20 projects of this center: threat and risk assessment; incident prevention, detection, mitigation, response, recovery, and analytics/forensics; defense in depth against dynamic threats; security management and visualization

Performer:	University of Arkansas
Partners:	Arkansas Electric Cooperative Corporation Carnegie Mellon University Florida International University Lehigh University Massachusetts Institute of Technology University of Arkansas, Little Rock
Federal Cost:	$12,226,504
Cost Share:	$3,082,610
Total Value of Award:	$15,309,114
Funds Expended to Date:	15%

Advancing the State of the Art (SOA)

- **State of the art (SOA)**
  - Power grid control and operation systems and operation technology infrastructure need customized protection against security threats
  - New power grid components and services are usually deployed first and then security is validated and added later
  - Cybersecurity management is mostly manual
- **Our approach**
  - Addresses new problems or provides better solutions for existing challenges
  - Industry inputs throughout the R&D cycle (define, research, alpha, beta, transition)
- **Why our approach is better than the SOA**
  - Provides customized protection against security attacks
  - Builds security into the design of new power grid components and services
  - Security management automation to deal with the complexity and large quantity of security data
  - Our security solutions are more practical for deployment
- **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

Advancing the State of the Art (SOA)

- **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
  - All 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 *detecting forged data and compromised devices*
  - Secure communication network infrastructure by *detecting botnet in SCADA networks*
  - Advance security management by *configuration management and visualization*

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 academe
  - Interdisciplinary team across cybersecurity, computer science and power systems
- **Challenge 2: Difficult to obtain industry data**
  - Development of a secure server
  - Involving industry partners more closely
- **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 partner AECC
- **Challenge 4: Center sustainability**
  - Continue to provide benefits that convince industry to join the center

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Targeted end user for the technology: both facility owners and vendors
  - Facility owners: cybersecurity management and visualization tools, situational awareness tools, configuration and patch management tools
  - Vendors: customized intrusion detection technologies, data forgery detection tools, security data analytics tools
- Plans to gain industry acceptance
  - Security needs take input from industry
  - Project selection suggested by industry
  - Technology design takes feedback via industry focus group activities
  - Beta testing of technologies conducted at industry partner AECC
  - Communications to industry through avenues in addition to academic publications

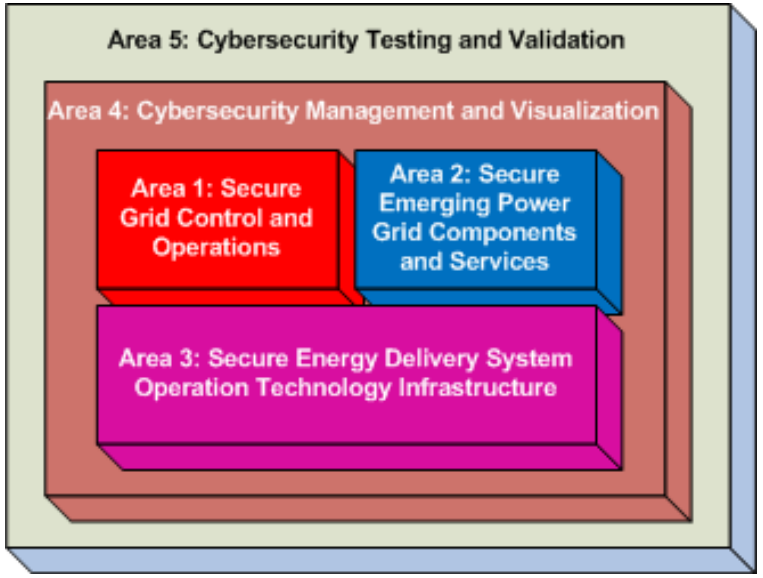
First Year Accomplishments

- 3 journal papers
- 11 conference papers
- 3 conference posters
- 2 invited talks
- 3 non-technical articles
- 1 cybersecurity special session at ECCE
- 3 industry-focused workshops
- 12 more paper submissions
- Began webinar series
- Evaluative methodology for project selection

Progress to Date

Major Accomplishments

- Detecting data integrity attacks for resilient power state estimation
- Detecting topology attacks through hypothesis testing
- Detecting data falsification attacks in AGC through deep learning
- Detecting time synchronization attacks against PMU data
- Detecting compromised devices through activity profiling
- Assessing risks of AMI hacking and Demand Response
- Cross-layer moving target defense to mitigate network attacks
- Post-disaster network resilience via software-defined networking



- Assessing the vulnerability of time-critical communications
- Detecting P2P Botnet in SCADA networks
- Designing an intelligent agent system for threat identification
- Development of NCREPT-based security testbed

Next Steps (1/2)

Approach for the next year

- Model-free detection of anomalous PMU data
- Detecting unidentifiable attacks
- Detection models for pricing attacks and impact assessment
- Mitigating DoS attacks for time-critical communications
- Algorithms to detect DSM misuse
- Co-design of security-aware microgrid
- Design of optimization tool for allocating security resources
- Cybersecurity management through a correlation framework
- Visualization for security data analytics
- Software tool implementation for proposed technologies
- Alpha and Beta test a set of technologies
- Transfer one set of technologies to the industry

Next Steps (2/2)

Technologies to be delivered in Phase I

- Detecting data integrity attacks
- Detecting and localizing topology attacks
- Detecting unidentifiable attacks
- Detecting data falsification in AGC
- Detecting anomalous PMU data
- Algorithms to detect DSM misuse
- Cross-layer MTD technology
- Security recovery mechanism for post-disaster networks
- Correlated cybersecurity management
- Visualization for security data analytics

Test Facilities at SEEDS

NCREPT at UA

- 7000 sq. ft.
- 6 MVA – 15 kV
- Host cyber testbed

Facilities at FIU

Facilities at Lehigh

Sample Project: Detecting Data Falsification Attacks in Automatic Generation Control (AGC) [PI: Qinghua Li, UA]

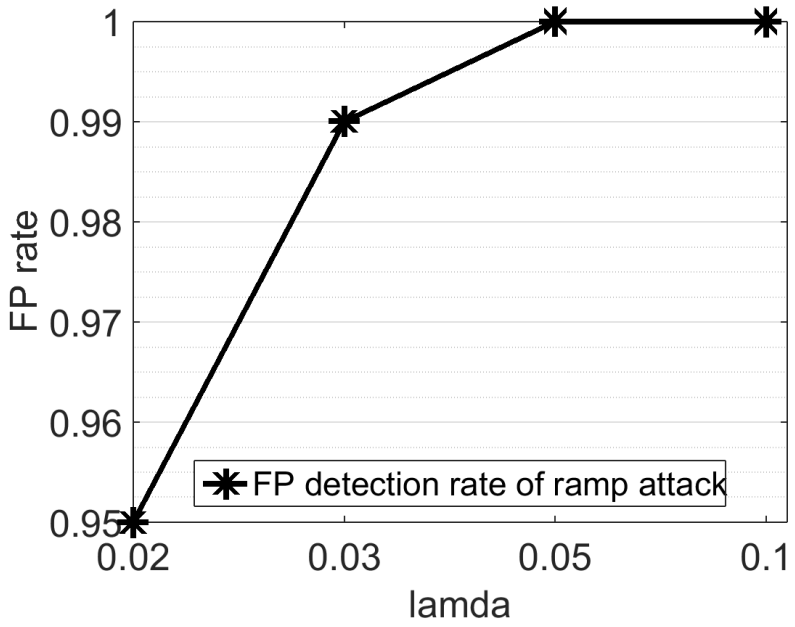
Problem: Injection of falsified measurement can cause miscalculation of Area Control Error (ACE) in AGC

Solution: Long Short Term Memory (LSTM) Neural Network is used to learn the normal patterns of ACE sequence and predict future ACE sequence. The predicted ACE is compared with the measured ACE to detect attacks

Results:

True positive (TP) rate: ≥95%

False positive (FP) rate: ≤5%



Sample Project: Detecting Time Synchronization Attack (TSA) in PMU Data [PI: Rick Blum, Lehigh]

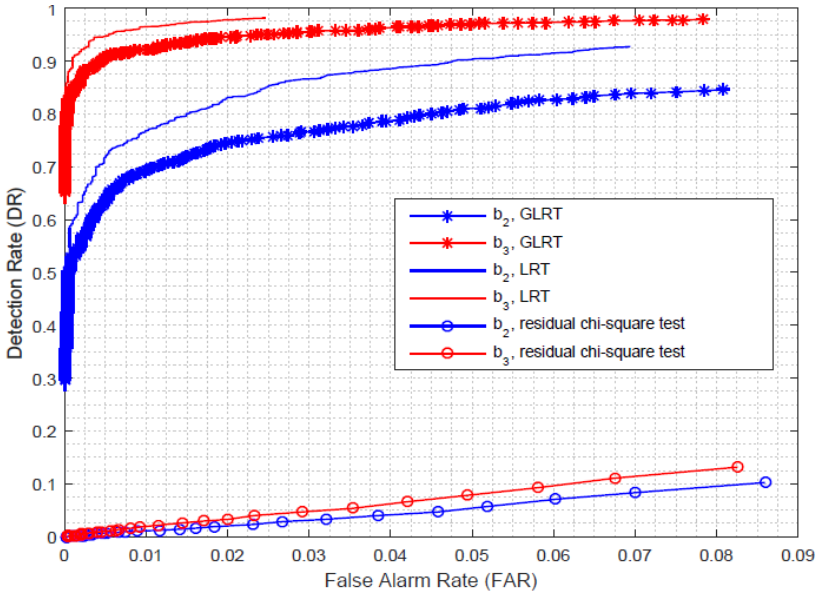
Problem: TSA alters the time synchronization of phasor readings and the measurement matrix in power system

Solution: To detect changes in measurement matrix, a generalized likelihood ratio hypothesis testing is used to estimate the measurement matrix and detect attacks

Results:

Detection rate: 96%

False alarm rate: 5%



Sample Project: Detecting Compromised Devices
[PI: Selcuk Uluagac, FIU]

Problem: Compromised devices can be used by adversaries to steal data and compromise other devices

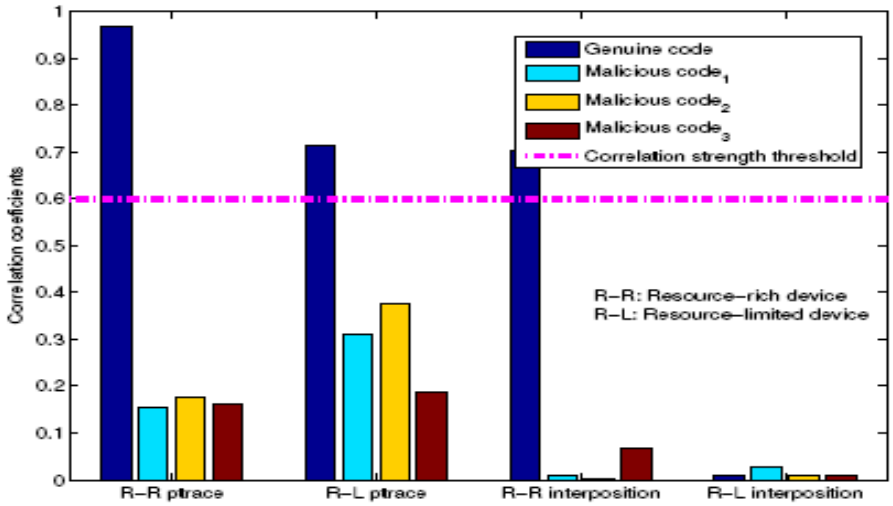
Solution: Build a system-level configurable framework and detect compromised devices based on system call activities

- Two types of devices: resource-rich devices and resourc-limited devices
- Three threats: open communication channels to adversaries, inject false data, store data in hidden files

Results

- Technique 1: detects all malicious codes for *ptrace*, but only detects malicious code1 for *interposition*
- Technique 2: detects all malicious codes

	Type of call	Gen.	Mal. 1	Mal. 2	Mal. 3
ptrace	*mmap2*	1	2.4	4.4	2.4
	mprotect	1	2.8	1.1	1
	munmap	1	1	2	13
	open	1	1	1	5
	rt_sigaction	1	1	3	3
Interposition	*mmap*	1	12.5	1	1
	mprotect	1	12.5	1	1
	pthread_create	1	12.5	1	1
	sendto	1	4.3	~1	~1
	signal	1	24	1	1



Sample Project: Detecting Data Integrity Attacks and Resilient State Estimation using Bayesian Method [PI: Bruno Sinopoli, CMU]

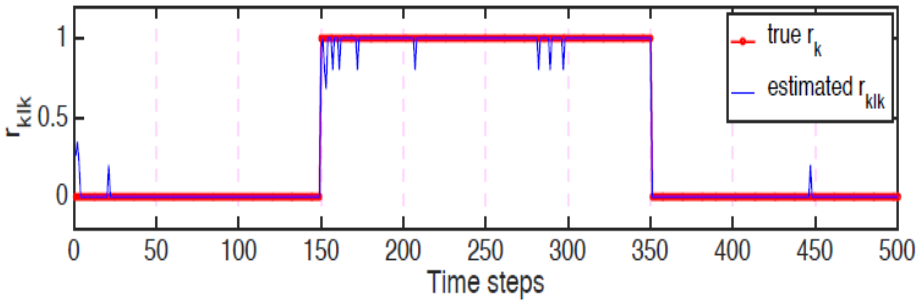
Problem

- Detect a signal attack (on sensor/actuator data) and jointly estimate the attack and the state of the cyber-physical system with the presence of extra fake measurement injection

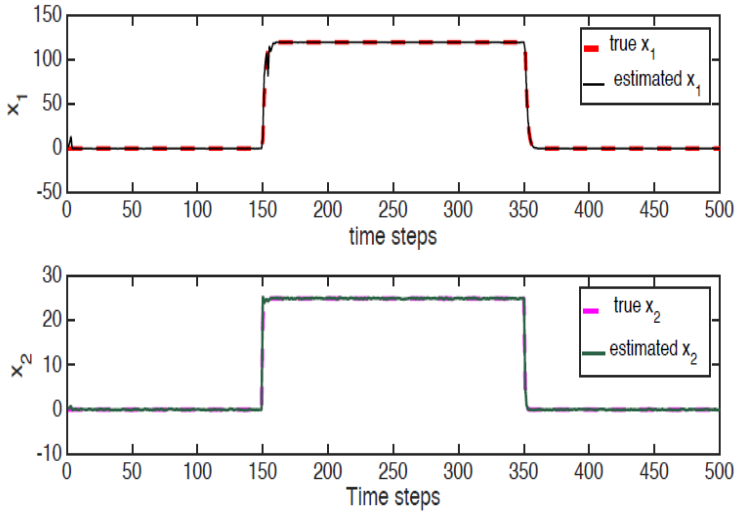
Solution: The formulated Bayesian framework is used to update in real-time:

- The joint posterior density of the signal attack and of the state (i.e. at each time instant we obtain an estimate of the signal attack and of the state of the system)
- The probability of existence of the signal attack

Results:



Attack detection



State estimation