A Verifiable Framework for Cyber-Physical Attacks and Countermeasures in a Resilient Electric Power Grid

ASU Team: Lalitha Sankar, Kory W. Hedman, and Oliver Kosut

Industry Collaborators: Robin Rodmore, IncSys, Marck Robinson, PowerData

Email: *lsankar@asu.edu* , *oliver.kosut@asu.edu*, and *kory.hedman@asu.edu*

Electric Grid Cyber-security

- The electric power system is a physical network monitored and controlled by sensors and actuators (cyber layer).
- Cyber layer: data collection, processing, distributed sharing, control and actuation.
- **Cyber layer vulnerable to all attacks on information systems** (e.g., data integrity, man-in-the-middle, malware, Trojans, …)
- Well-designed attacks can have severe consequences (blackouts, cascading failures).

State of the Art

- Attacks focused predominantly on tractable models for specific cyber modules.
  - Essential preliminary work.
- **Does not capture system complexity**
- **Cannot clarify effect of attacks on the system as a whole**.
  - e.g., can 'unobservable' attacks be detected in an ensuing module or via existing system-wide resiliency mechanisms?

Scope of Proposed Work

- **Challenge**: **lack of access** to detailed and accurate models for grid energy management system (EMS) (proprietary)
- **Approach: Collaborate with industry experts in power system simulation** to develop high-fidelity models for end-to-end cyber operations (EMS).
- Objectives of collaborative effort:
  - Temporal consequences of cyber-attacks and develop countermeasures;
  - Distributed grid operations and develop resilient data sharing protocols;
  - **Verifiable software framework (academic) to model attack consequences, evaluate countermeasure, and develop resilient protocols;**
  - **High fidelity EMS simulator in collaboration with IncSys Inc. and PowerData to test attacks and countermeasures.**

Proposed Work

- Spatio-temporal modeling of Energy Management Systems (EMS)

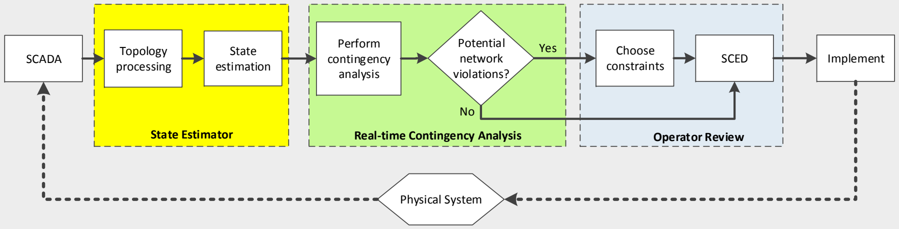

Fig. 1. Typical functions of an Energy Management System functionality
Unobservable attacks in one function can often be observed across EMS operations.

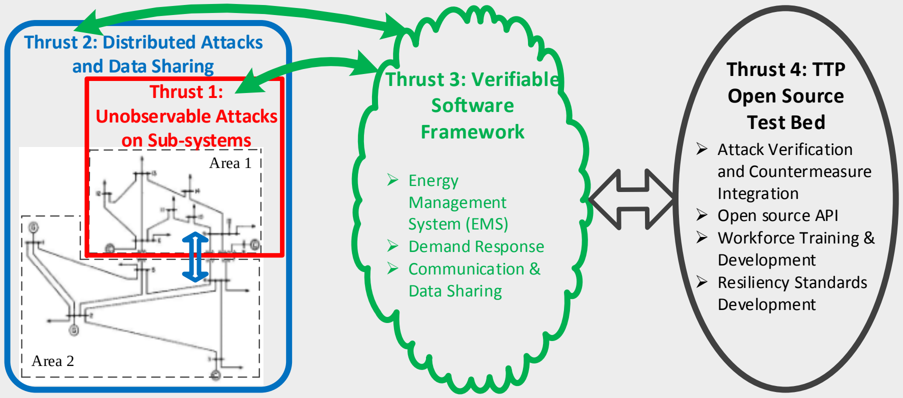
Thrust 2: Distributed Attacks and Data Sharing
Thrust 1: Unobservable Attacks on Sub-systems
Area 1
Area 2
Thrust 3: Verifiable Software Framework
Energy Management System (EMS)
Demand Response
Communication & Data Sharing
Thrust 4: TTP Open Source Test Bed
Attack Verification and Countermeasure Integration
Open source API
Workforce Training & Development
Resiliency Standards Development

Fig. 2. The four research goals and their interrelationships.
Green arrows: interdependency between Thrusts 1 & 2 and software framework (Thrusts 3 and 4).
Black arrow: knowledge exchange between (academic effort) Thrust 3 and testbed of Thrust 4.

Countermeasures

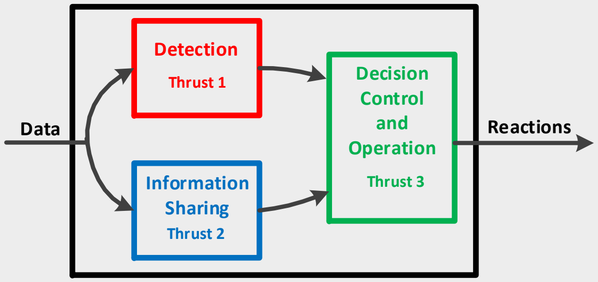

Fig. 3. The three interdependent features of countermeasures spanning Thrusts 1, 2, and 3.

Transition to Practice

- **Development of high fidelity open source commercial grade EMS software**.
- Collaboration with NAE member Dr. Robin Podmore (CEO, IncSys) and power systems software developer PowerData.
  - Access to power system simulation knowledge-base, NERC certification process, and workforce training.
- Testing of attacks and countermeasures in the open source software environment:
  - Unobservable attacks and machine learning countermeasures;
  - MitM attacks on distributed EMSs and information sharing countermeasures;
  - Attack implications and response via real-time contingency analysis (RTCA) tool;
  - Generator attacks and countermeasures;
  - False data attacks and demand response;
- Ability to develop NERC certified cyber-security-inclusive operator training curriculum.

Preliminary Results

Recent results:

- J. Liang, O. Kosut, and L. Sankar. "Cyber attacks on AC state estimation: unobservability and physical consequences," IEEE PES General Meeting, July 2014.
- J. Zhang, L. Sankar, and K. Hedman. "Implications of cyber attacks on distributed power systems operations," CIGRE National Committee, 2014 US Grid of the Future Symposium, Oct. 2014.