CRII: CPS: Noninvasive Security Analysis for Smart Grid Energy Management System

Mohammad Ashiqur Rahman, Florida International University
https://acyd.fiu.edu/crii-cps/

Problem Overview:

- Cyber technologies are increasingly used in physical systems like power grids to offer smarter services, real-time demand responses, and economic advantages (Figure 1).
- This cyber and physical integration makes power grids more vulnerable to cyber attacks (e.g., tampered data) that can cause improper controls and lead to serious damages.
  - Adversaries can evade existing outlier-based bad data detection mechanisms used in EMS.
- It is crucial to analyze the potential attacks and impacts on the system in a non-invasive manner.

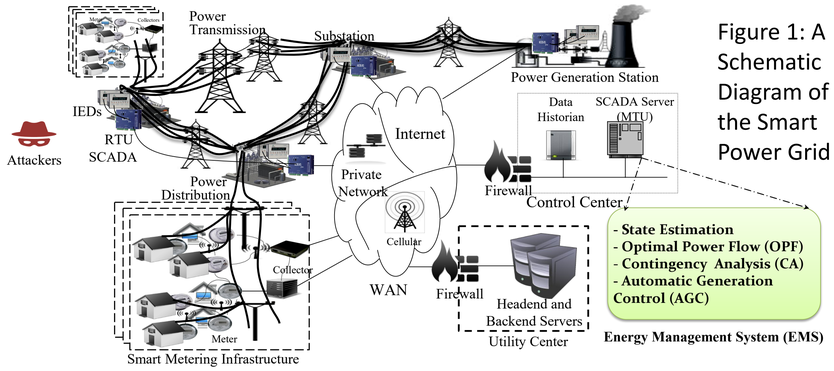

Figure 1: A Schematic Diagram of the Smart Power Grid

Challenges:

- It requires to model a complex threat characteristic exhibiting in a grid:
  (i) Interactions between cyber and physical layers through control routines
  (ii) Interdependency between different control modules run by EMS
- A large, distributed infrastructure making the attack space enormous.

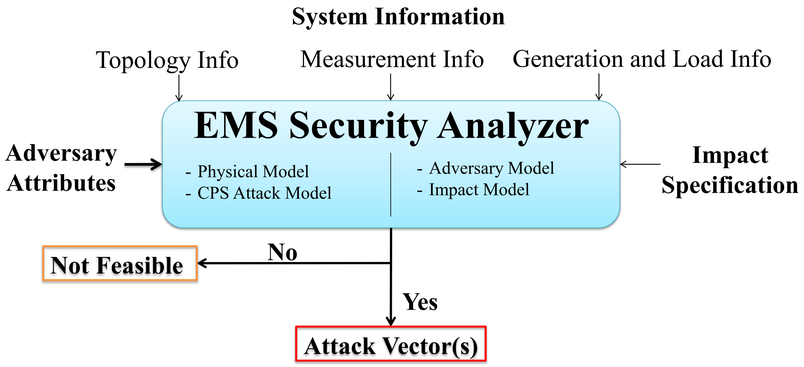

Figure 2: the EMS security analytics framework

CPS Contribution

- A noninvasive approach to identify the potential attacks of the system
  - A provable and time-efficient manner
  - Provide the system's risk under flexibly chosen attack capabilities
- Equally applicable for CPSs that utilize measurement-based estimation.

Technical Approach:

- Formal analytics to synthesize impact-aware stealthy false data injection attacks on EMS control operations (Figure 2).
  - Constraint satisfaction problem modeling
  - Satisfiability Modulo Theories (SMT)
- Flexible adversary model
  - Knowledge, accessibility, resource
  - Attack target/impact (e.g., OPF cost increase)
- To deal with nonlinear control logics, hybrid approaches are adopted. E.g.,
  - MATLAB Simulink is integrated with SMT
  - SMT provides the test cases to be systematically inspected by Simulink for further assessment.
  - Parallelism to explore the attack space.
- Various performance metrics are evaluated.
  - Simulations on standard test bus systems
  - Real-time emulations (RTDS)

Research Outcomes and Technological Impact:

- CPS that is resilient to attacks will ensure crucial services and encourage investments for sophisticated applications.
- Potential stakeholders include energy providers, utilities, vendors, and federal agencies.

Education and Outreach

- Used in graduate and undergraduate level course modules on CPS/IoT security.
- Graduate student training
- Research experience opportunities for undergraduate students

Results and Dissemination:

- The project's outcome has resulted in 9 publications (3 journals, 6 conference papers).
- It partially supported 1 PhD and 3 MS students.
- Three undergraduate students (two of them are Hispanic) have participated in this project.

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: 1929183