2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

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

Award #: CNS 1929183 [January 2019 – April 2022]

PI: Mohammad Ashiqur Rahman, Florida International University

Challenge:

- An adversary can alter measurements to corrupt the EMS estimation and thus the control decisions.
  - –Can evade the existing bad data detection mechanism in EMS.
- It is important to perform proactive and efficient identification of potential threats and their impacts for cost-efficient mitigation planning.
  - –It needs to model interdependency between control modules and consider
  - –The large, distributed physical/control infrastructure makes a large attack space.

Solution:

- Formal analytics to synthesize impact-aware stealthy false data injection attacks on EMS control operations (Figure 1).
  - –Constraint satisfaction problem modeling
  - –Satisfiability Modulo Theories (SMT)
- 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 (Figure 2).
  - –Parallelism to explore the attack space..
- Various performance metrics are evaluated.
  - –Simulations on standard test bus systems
  - –Real-time emulations (RTDS)

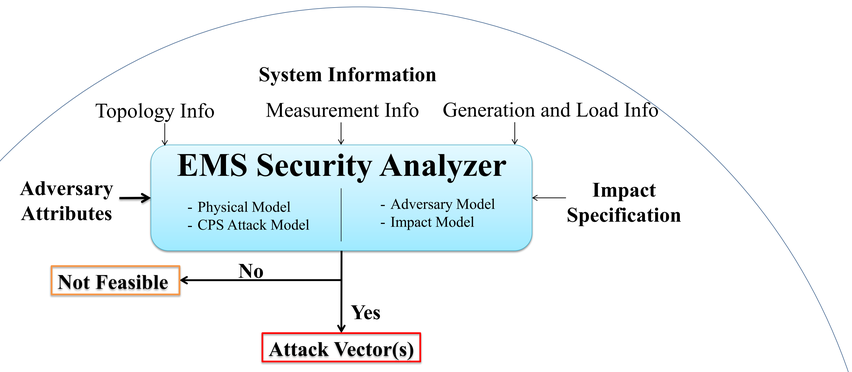

Figure 1: the EMS security analytics framework

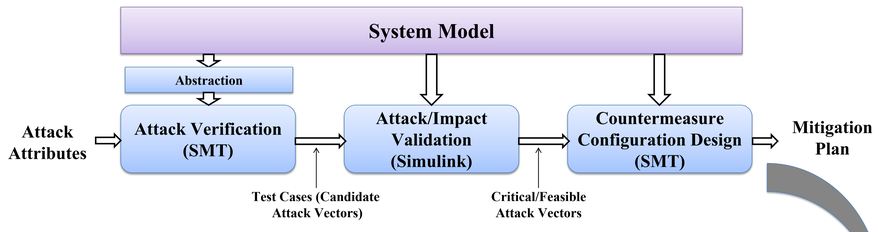

Figure 2: A high-level architecture of integrating Simulink model with SMT verification for impact analysis.

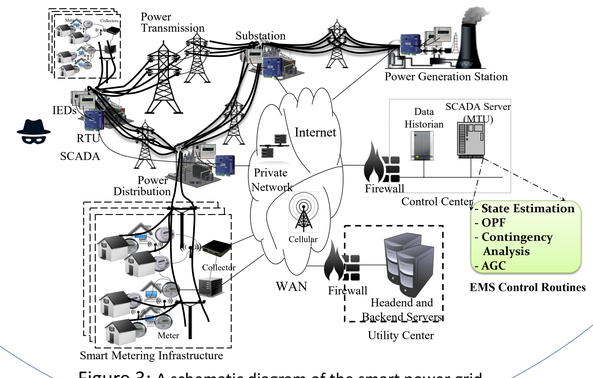

Figure 3: A schematic diagram of the smart power grid.

Mohammad Ashiqur Rahman
Assistant Professor, Florida International University
Email: marahman@fiu.edu
Website: https://rahman.eng.fiu.edu/

Scientific Impact:

- Integrates different theories, such as formal verification, model simulation, data and control flow, and security concepts, into the CPS components.
- A noninvasive, provable approach to identify the potential attacks on the system comprehensively
  - –An extendable framework considering various cyber-threat models, adversary attributes, and control dependencies.
- This research targets EMS in smart grids.
  - –The approach is broad enough to be generalized for other CPS control loops that utilize measurement-based estimation.

Broader Impact:

- With the wake of cyberwarfare, the critical infrastructures like power grids have become more vulnerable.
  - –Power grid attack incidents in Ukraine in 2015, 2016
  - –This research addresses the urgent need of analyzing and hardening power grid security (Figure 3).
- Potential stakeholders include energy providers, utilities, vendors, and federal agencies.
- The project produces contents on CPS/IoT security for graduate/undergrad level courses.
- The project's outcome has resulted in 9 publications (3 journals, 6 conference papers).
- It has partially supported 1 PhD and 3 MS students.
- Three undergrad students (two of them are Hispanic) have participated in this project.