RRE: A Game-Theoretic Intrusion Response and Recovery Engine

A. Fawaz, R. Berthier, and W. H. Sanders

GOALS

- Reactive response against adversarial attacks that uses knowledge about the power grid's current security state and its security requirement.
- Build RRE as a distributed system that actively monitors systems and devises responses.
- Adapt the Response and Recovery Engine (RRE) to handle the scale of a large Automated Metering Infrastructure (AMI).
- Model the smart grid as a cyber-physical system to study the cyber-physical interactions in detection and response.
- Verify safety properties of possible responses.

FUNDAMENTAL QUESTIONS/CHALLENGES

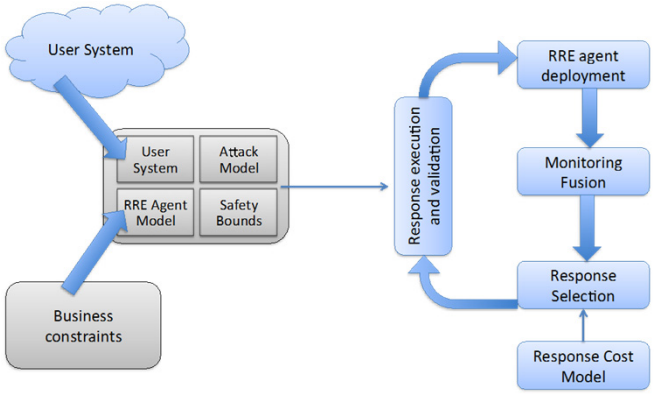
- Model a CPS without using simulation software or linearized models of the power flow equations.
- Select effective responses without running into state-space explosion issues.
- Express responses independent of the technology used in the system.
- Accurately fuse information from different sources, such as IDS, logs, and physical sensors, to detect attacks in the power grid.

RESEARCH PLAN

- Devise a new modeling method for cyber-physical systems that takes into account detection and response interactions. The goal is to avoid the current layered approaches for CPS models that use a simulation or linearization of the power flow equations to model the grid while ignoring the real cyber interactions.
- Develop monitoring fusion algorithms that can detect high-level attack steps based on low-level information, such as from IDS alerts, firewall logs, syslog, dtrace, and other sources.
- Adopt several languages to express the responses in our response taxonomy. Those languages include SDN (OpenFlow) and Mandatory Access Control (SELinux).
- Design several cost-sensitive response selection algorithms based on distributed control theory.

RESEARCH RESULTS

- Distributed intrusion tolerance architecture suitable for the power grid.
- Implemented a basic OpenFlow responder in a substation setting.



BROADER IMPACT

- The ultimate goal of providing an automated response capability to power grid control rooms is to enable quick reaction against security attacks and failures, thus preventing them from causing potentially catastrophic failures.

INTERACTION WITH OTHER PROJECTS

- Part of this work is being implemented using SEL's watchdog, an OpenFlow switch.

FUTURE EFFORTS

- Design response selection algorithms.
- Design data fusion algorithms.
- Implement RRE over SEL equipment.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T