RRE: A Game-Theoretic Intrusion Response and Recovery Engine

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

GOALS

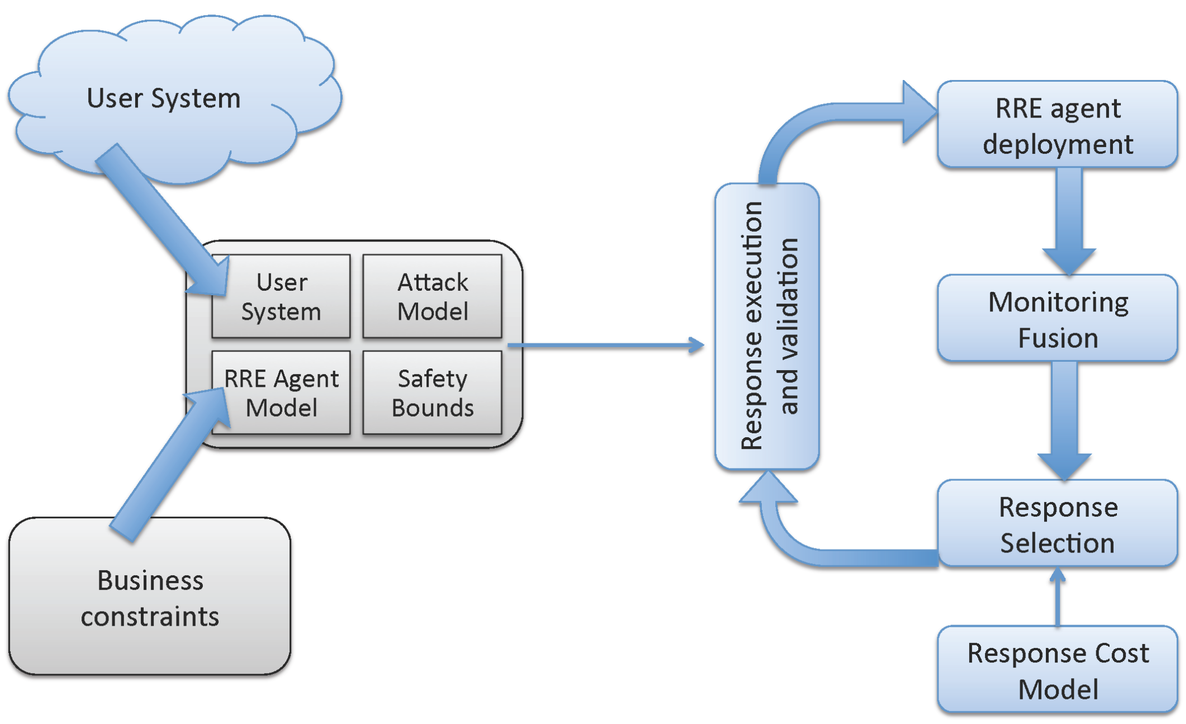
- Reactive response against adversarial attacks that uses knowledge about the power grid's current security state and its security requirements.
- Build a Response and Recovery Engine (RRE) as a distributed system that actively monitors systems and devises reactive and proactive responses.
- Use control-, game-, and graph-theoretic methods to find optimal response deployment.
- Adapt RRE to handle the scale of a large Advanced Metering Infrastructure (AMI).
- Model the smart grid as a cyber-physical system to study the cyber-physical interactions in detection and response. Interactions include how to detect a cyber attack from physical system indicators, and how a cyber response can help in an adverse physical situation.
- Implement a response and recovery system that is capable of effectively interfacing with a human operator.
- Verify safety of certain responses with respect to system invariants.

FUNDAMENTAL QUESTIONS/CHALLENGES

- How do we trust data coming from possibly compromised data sources?
- 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 in a manner independent of the technology used in the system.
- Accurately fuse information from diverse sources.

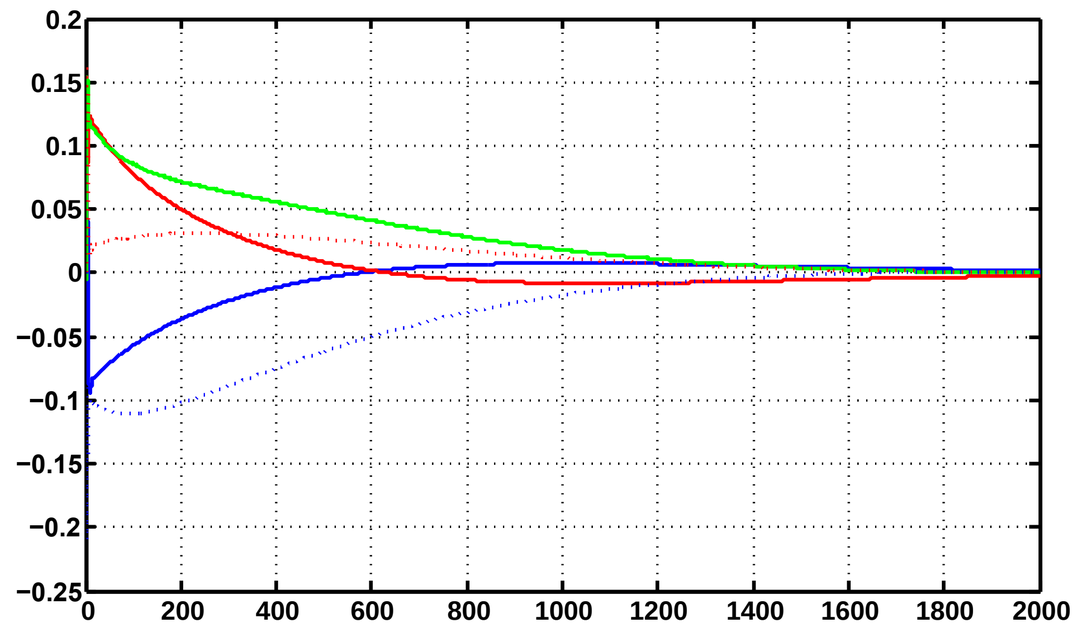
RESEARCH PLAN

- Use the cyber-physical topology language (CPTL) as a description of the system. CPTL will be used by RRE agents when computing optimal responses and fusing sensory data.
- Develop monitoring fusion algorithms that can detect high-level attack steps using diverse data sources. The diversity of data sources increases confidence that malicious events will be detected.
- Adapt several languages to express the responses in our response taxonomy. RRE agents use the response language to map high-level actions into low-level actions.
- Design several cost-sensitive response selection algorithms based on distributed control theory, game theory, and graph theory.



RESEARCH RESULTS

- Basic control-theoretic control responder.
- Distributed intrusion tolerance architecture suitable for the power grid.
- Are implementing a basic OpenFlow responder in a substation setting.



Performance of feedback controller for malware spread response

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 these from causing potentially catastrophic failures.

INTERACTION WITH OTHER PROJECTS

- Part of this work is being implemented using SEL's watchdog, an OpenFlow switch.
- We are building a response and recovery test-bed within the TCIPG test-bed.

FUTURE EFFORTS

- Design response selection algorithms using game theory, control theory, and graph theory.
- Design data fusion algorithms. The requirement is for the fusion algorithms to use diverse data sources.
- Design responses that stimulate a malicious entity, driving it to respond and thus enabling its detection.
- Implement RRE over SEL equipment.

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