RRE: A Game-Theoretic Intrusion Response and Recovery Engine

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

Goals

- Reactive response against adversarial attacks that uses knowledge about the power grid's current security state and its security requirements.
- Adapt RRE for Automated Metering Infrastructure (AMI) to handle the size of AMI and the special responses.
- Model the cost of a response in AMI to reflect the cost due to the underlying distribution grid and include the cost to the customer as well.
- Verify safety properties of selected responses.

Fundamental Questions/Challenges

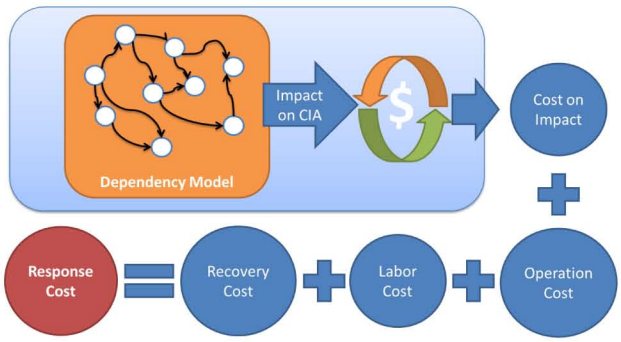
- How to accurately model the cost of responses and attacks, to capture the costs due to the physical system.
- How to optimize RRE to get real-time responses that track the attack steps while scaling for the massive size of an AMI.
- How to define safety properties in the distribution and transmission grid and prove that responses fall within the safety limits.
- How to realistically reason about and predict attackers' behavior in the future.

Research Plan

- Define a custom response action taxonomy for AMI.
- Model accurately the cost of responses and attacks based on the cyber and physical states of the power grid using dependency graphs and the state of the distribution grid.
- Use hybrid automata to model the power grid and prove that responses fall within the safety boundaries of a system.
- Design and develop a scalable game-theoretic decision-making solution to provide optimal response and recovery actions in real-time for large-scale power grid networks.

Research Results

- Currently working on implementing RRE for AMI.
- Implementing the cost model using a realistic AMI simulated from real GSI data and the Gridlab-d application.
- Proposed a taxonomy of response actions for AMI that aided in the generation of a set of response actions.
- Proposed a cost model for responses and actions in AMI that uses the dependency graph to compute the effects on CIA and convert those to a financial cost.



Broader Impact

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

Interaction with Other Projects

- Deployed Itron's Openway AMI system in the TCIPG testbed.

Future Efforts

- The next major step of the project will be to add a response capability to our AMI deployment in the testbed.