TCIPG

RRE: A Game-Theoretic Intrusion Response and Recovery Engine

S. Zonouz, R. Berthier, H. Khurana, K. Joshi, K. Rogers, A. Fawaz, R. Bobba, T. Overbye, T. Yardley, W. H. Sanders

Goals

- Cyber-physical security-state estimation using cyber-side Intrusion Detection Systems (IDSes) and power-side Power Measurement Units (PMUs).
- A system security metric to assess and measure, at each time instant, the system-wide security level of the power grid.
- Reactive response against adversarial attacks that uses knowledge about the power grid's current security-state and its security level.

Fundamental Questions/Challenges

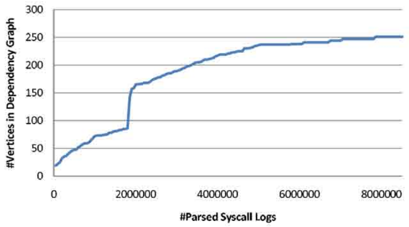
- How to handle and fuse overwhelming information from various data sources deployed in the cyber and power sides of the grid.
- How to rank the security incidents regarding their criticality level, and present them to system operators in a meaningful and concise manner.
- How to realistically reason about and predict attackers' behavior in the future.

Research Plan

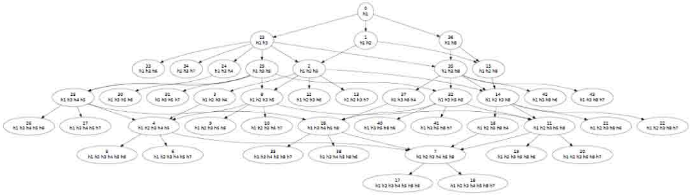
- To make use of machine learning algorithms to automatically capture dependencies among the power grid subsystems in order to minimize the human involvement in the information fusion process.
- To use the automatically learned system dependency model along with efficient and scalable belief propagation techniques to deduce how critical each security incident is globally.
- To design and develop a scalable game-theoretic decision-making solution to come up with optimal response and recovery actions in real-time for large-scale power grid networks.

Research Results

- Automated generation and learning of system-wide dependency graph and adversary-driven attack graph for large-scale power grid networks.
- Automated calculation of the system security using the Gibbs Sampler method.



- (Semi-)automated response against attackers.



Broader Impact

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

Interaction with Other Projects

- We have been working with Prof. Overbye and his student Kate Rogers on scalable bad-data detection algorithms that ignore corrupted data while fusing sensory information.
- Our group is planning to make more intensive use of the TCIPG test-bed room, as a shared resource, to collaborate with other research groups.

Future Efforts

- The major next step of the project will be to add a response capability to our test-bed implementations that we demonstrated in Nov. 2010.

Trustworthy Cyber Infrastructure for the Power Grid ▪ www.tcipg.org

University of Illinois ▪ Dartmouth College ▪ Cornell University ▪ UC Davis ▪ Washington State University