CPS: Medium: Cyber Attack-Defense Modeling, Risk and Contingency Analysis for the Power Grid using Game Theory

PIs: Manimaran Govindarasu and Sourabh Bhattacharya

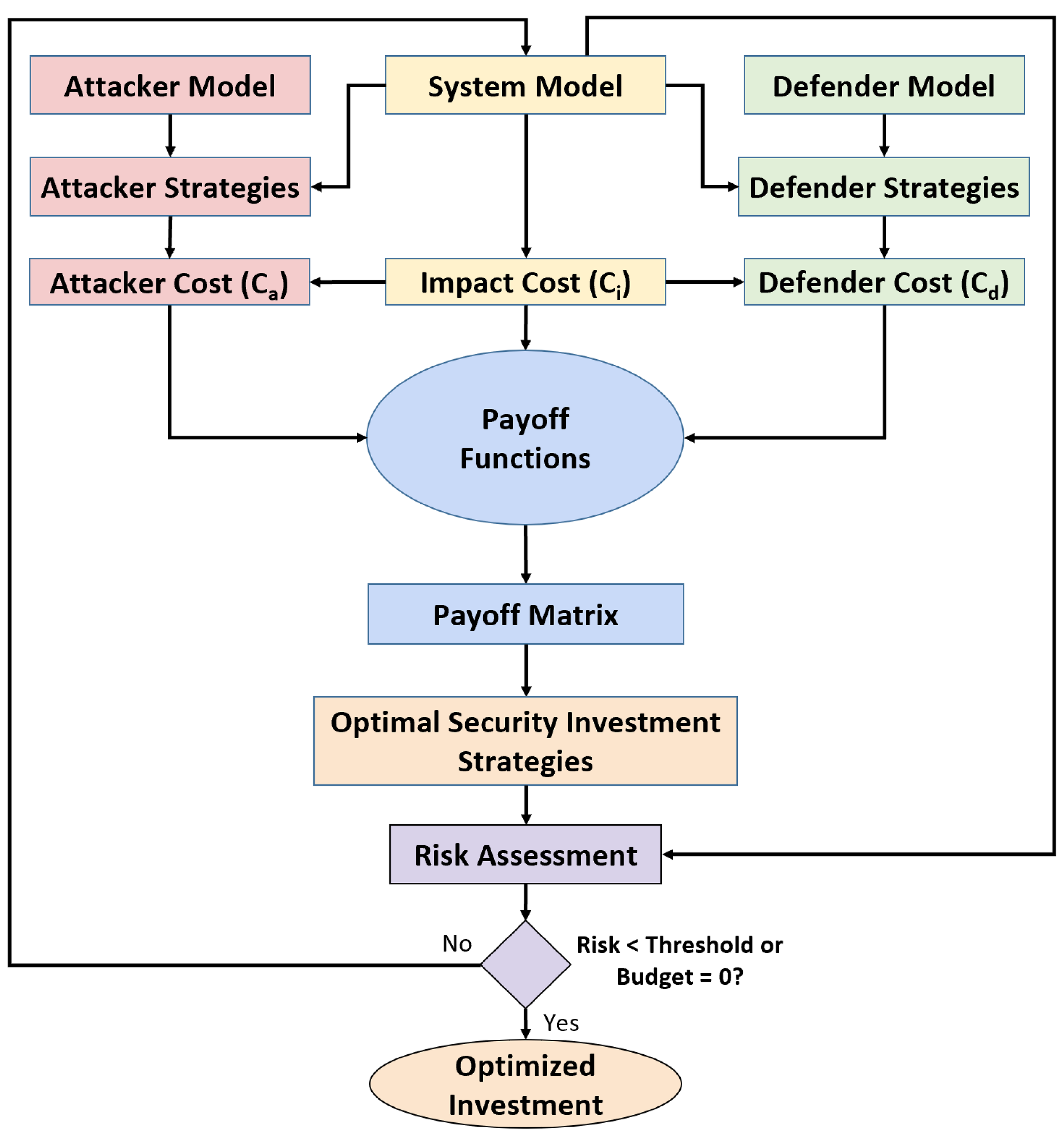
Researchers: Burhan Hyder, Hamid Emadi, and Joseph Clanin

IOWA STATE UNIVERSITY

Objective and Research Tasks

This project will develop a scientific methodology, algorithms, and tools for cyber risk assessment, attack-defense modeling, and cyber contingency analysis by leveraging game theoretic tools and solution strategies with the following research tasks: (1) To develop fundamental game-theoretic formulations and models for cyber-physical systems; (2) To develop cyber risk assessment and mitigation methodology which optimizes the security investments to defend the grid against attacks; (3) To develop real-time operational planning strategies to handle multiple contingencies due to coordinated attacks; (4) To evaluate the effectiveness of the proposed models and defense algorithms on a CPS security testbed; (5) To integrate research outcome into education & outreach activities

Risk Assessment-based Cybersecurity Investment Optimization[1,5]



N-k CPS Contingency Analysis and Optimal Resource Allocation

Problem Formulation: Zero-Sum Additive Security Game

- Graph model of power grid: $G(\mathrm{V},\mathrm{E}), |\mathrm{E}| = m$; $\emptyset_e$: edge failure impact values
- Attacker's action set X, $|X| = n_a$, $n_a = \binom{m}{k_a}$; Attacker attacks $k_a < m$ links
- Defender's action set Y, $|Y| = n_{d,}$ $n_d = \binom{m}{k_d}$; Defender defends $k_d < m$ links
- Cost matrix has an additive property: A_{ij} = sum of costs of successfully attacked links
- Solution concept: Saddle-point equilibria

Challenges:

- Combinatorial Explosion: Cost matrix size increases exponentially.
- How to efficiently compute an optimal defender resource allocation?

Solutions:

- Linear Time Algorithm to Compute Optimal Defender Resource Allocation[3]
  - Leverages structural properties[2] of saddle-point equilibria in additive security games
- Generalized non-zero-sum additive security game model[4]
  - Models attackers with diverse incentives
  - Optimal solutions may be computed in quadratic time

Evaluation:

- Test cases: Modified IEEE 5 bus, IEEE 9 bus, IEEE 14 bus, and IEEE 39 bus systems
- Computational complexity reduction from exponential to linear time

Broader Impacts

- Cyber Risk Assessment Tool that helps to systematically quantify cyber risks and helps to make cost-optimal security investment decisions.
- CPS contingency analysis methodology, metrics, and proof-of-concept studies showing their benefit and efficacy in smart grid's energy management system (EMS).
- Broader applicability of the game-theoretic models, metrics, and methodology to model cyber risk, investment analysis, and CPS contingency analysis in other CPS critical infrastructure systems.
- Workforce development: Graduate education (course work and thesis research) and undergraduate senior design project(s).

1. B. Hyder and M. Govindarasu, "Optimization of Cybersecurity Investment Strategies for the Smart Grid Using Game Theory", IEEE ISGT 2020
2. Emadi, H. and Bhattacharya, S. On the Characterization of Saddle Point Equilibrium for Security Games with Additive Utility. International Conference on Decision and Game Theory for Security. Springer, Cham, 2020.
3. Emadi, H., Clanin, J., Hyder, B., Khanna, K., Govindarasu, M. and Bhattacharya, S. "An Efficient Computational Strategy for Cyber-Physical Contingency Analysis in Smart Grids", IEEE PESGM 2021
4. Emadi, H., Clanin, J., Bhattacharya, S. "Structural Characterization of Nash Equilibria in Two-Player Security Games with Additive Utility", IEEE CDC '21 (Submitted)
5. Kush Khanna and M. Govindarasu, "Cyber-Physical Risk Assessment and Investment Planning for Power System". (To be submitted for journal publication)

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: ECCS 1739969