Quantification of Cyber-Physical Security Risk and Probability of Rare Failures

Estimation of Risk and Rare Events

Mardavij Roozbehani and Munzer Dahleh

GOALS

- The objective of this task is to provide tools based on model approximation and relaxation methods in optimization to compute tight bounds on probability of rare events in critical energy infrastructure.
- Early detection of risk emergence is key to containing it. Such emergence of risk can be characterized by an increased correlation between certain relevant states, cascaded failures of parts of the system, or simply a rate of growth of certain endogenous variables of the system.
- We are interested in expanding such research to represent a wider class of networked systems to embrace cyber-physical systems and, specifically, power systems.

FUNDAMENTAL QUESTIONS/CHALLENGES

- The fundamental analysis question in risk is the computation of the probability that the networked system will enter a forbidden region defined in terms of the states of its nodes. Typically, such an event is a rare event, which presents serious challenges in terms of computation using sampling methods.
- Past research has demonstrated that the emergence of fragility in networks occurs in a specific pattern that is due to the topology of the network and the distribution of disturbances.
- Analytically, such a computation is extremely hard, as it depends on the network structure, the evolution mechanisms, and the decision strategies of the nodes. Techniques from large deviation theory, hidden Markov models, and uncertainty quantification address such an analysis problem for simple models.

RESEARCH PLAN

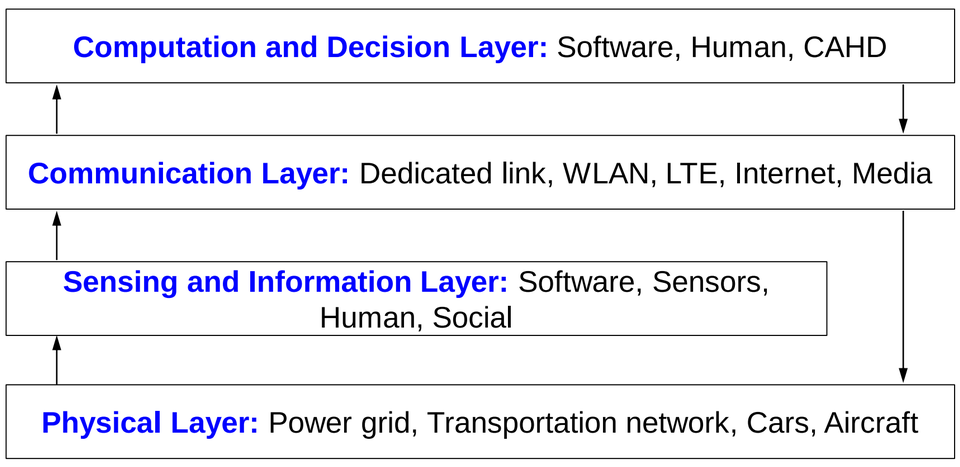

Fig. 1. A layered abstraction of a cyber-physical system.

We take a systematic approach for creating computational models that can address the aforementioned challenges.

1. Representation of the different components of a system via finite-state models.
2. Aggregation of the individual finite-state models in a global finite-state model for the entire system.
3. Also incorporating stochastic models for exogenous disturbances, hidden states, and unmodeled dynamics.
4. Complexity reduction via model reduction and aggregation techniques.
5. Distributed computation of risk over finite-state models.
6. Validation with data.

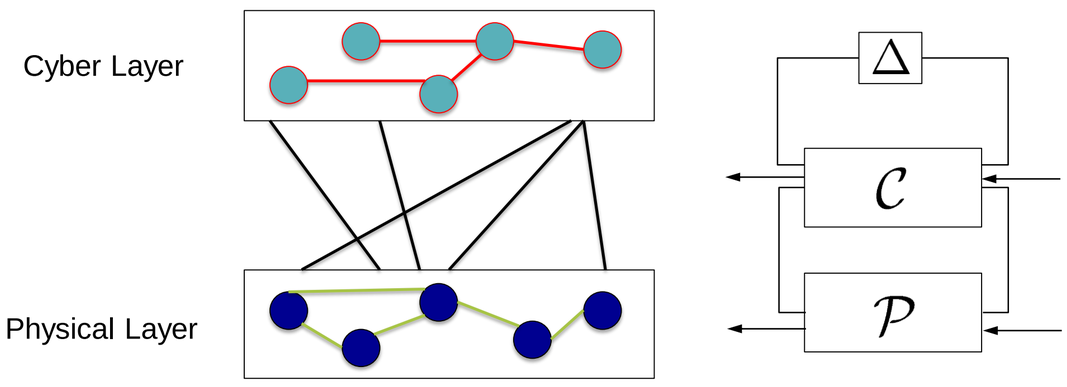

Fig. 2. Cyber-physical system model based on interconnection of finite-state system models.

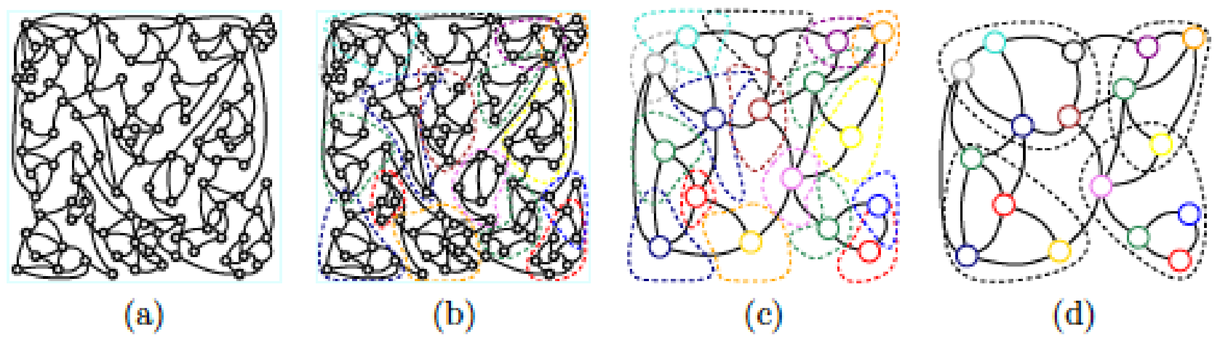

Fig. 3. Schematic representation of the steps for model reduction and structural complexity reduction using hierarchical aggregation: (a) initial system with highly detailed models; (b) identification of clusters in the network; (c) realization of local reduced order models based on the identified clusters; (d) clustering of the second layer of models.

CASE STUDY

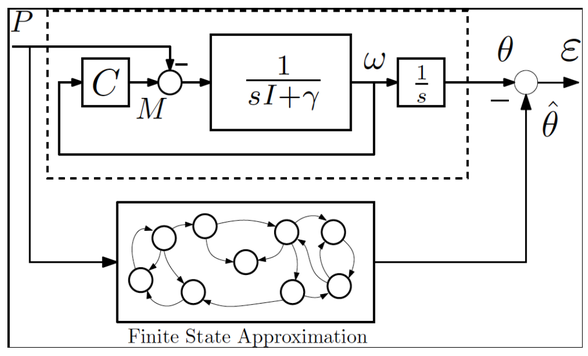

Fig. 4a. Finite-state system approximation of a continuous model of a synchronous generator.

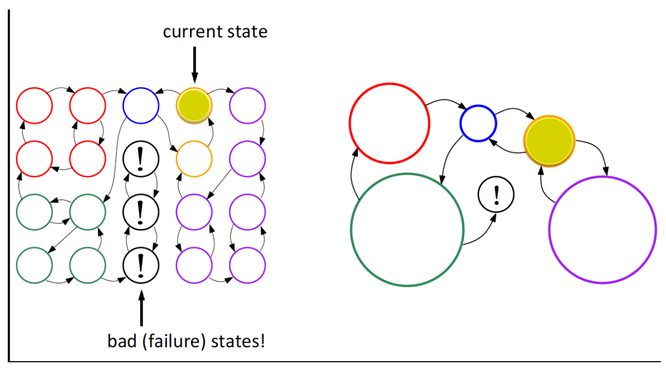

Fig. 4b. For complexity reduction, states are aggregated in macrostates according to the transitions between them. Critical states need to be preserved in the aggregation process, in order to recognize them in the reduced model.

Lyapunov techniques are used to construct certificates of safety of the system, in the sense that starting from some initial conditions, the system will not reach the unsafe states with some guaranteed probability. If such a certificate cannot be produced, the dual notion of density function can be used to identify the most probable path from initial states to unsafe states.

RESEARCH RESULTS

Even with accurate system models, Bayesian inference in a rare observation regime is extremely fragile (sensitive to small noise), and it cannot be used in security applications..

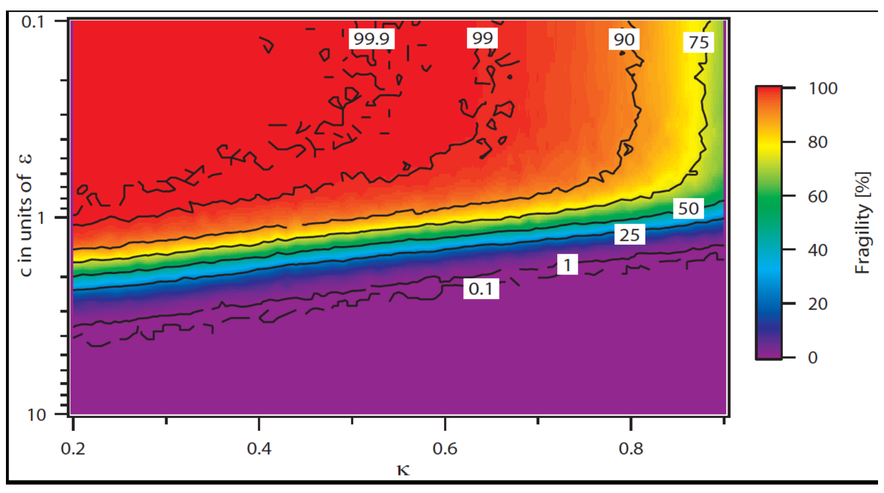

Fig 5. Upper left corner: rare observations; extremely fragile. Lower right corner: more probable observations; robust.

BROADER IMPACT

- Recent advances in data sciences and technologies point to the methodological gap that exists in transferring large amounts of offline and real-time data from the grid to computationally tractable models of risk in critical infrastructure.
- This is likely to lead to development of fundamental knowledge on design principles and architecture of secure cyber-physical systems. The abstract framework sets a foundational framework that will prove valuable in many application areas of interest.

FUTURE DIRECTION

Characterize limitations of Bayesian inference in rare observation regimes and develop non-Bayesian framework for risk estimation.

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY