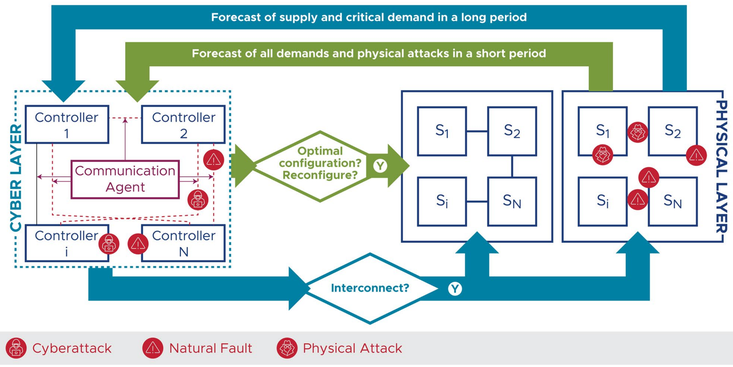
Peer-to-Peer Communication Control for Resilient Operations of Networked Cyber-Physical Systems | Thrust 2

Long Vu (PI), Sayak Mukherjee, Ankit Singhal

RESILIENT NETWORK CONTROL VISION

Multi-layered, multi-timescale co-controlling of communication network and physical links of networked cyber-physical systems (CPSs) to respond to ongoing and coordinated cyber-physical attacks and natural faults.



Resilient network control capability: Enable networks of CPSs—such as electric, gas, or water networks—to self-assemble to adaptively respond to cyber-physical attacks and faults, while supporting critical demand.

OBJECTIVE

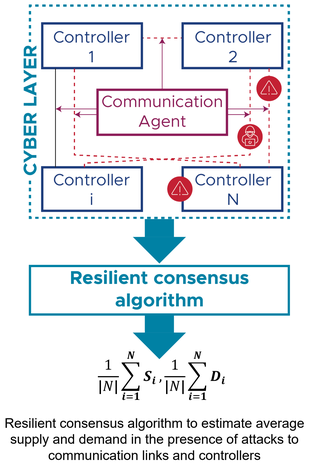
Networked CPSs are exposed to cyber-physical attacks and faults, yet existing sensing and control systems are not designed for resilience. This project aims to enable networks of CPSs to make self-assembling decisions to support the end-use demand in a way resilient to cyber-physical attacks and natural faults.

ACHIEVEMENTS

- A submission to the 2022 IEEE Conference on Decision and Control
- Advanced Grid Modeling proposal in forming resilient grid (in a collaboration with Clarkson University and New York Power Authority)
- Initial interaction for invention disclosure

APPROACH

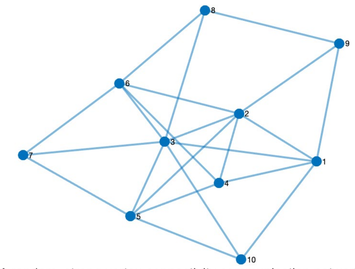
- Exploit the flexibility in both physical and communication interconnections
- Use peer-to-peer communication among controllers for decision-making to avoid one-point failure
- Co-design of communication network and resilient consensus/optimization algorithms for self-interconnecting and self-reconfiguring physical networks of CPSs
- Demonstrate on networked microgrids



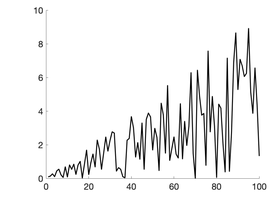
Resilient consensus algorithm to estimate average supply and demand in the presence of attacks to communication links and controllers

FY22: Self-Interconnection Framework

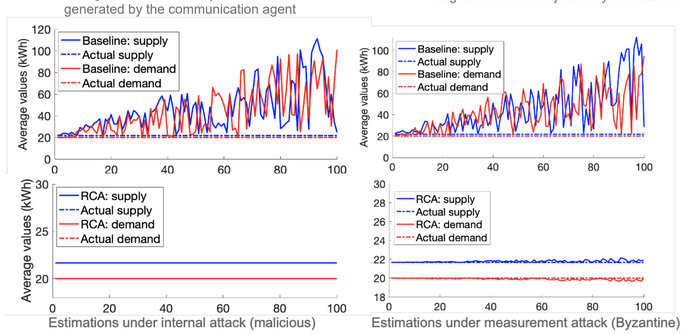
- Interconnection criterion: energy supply meets critical demand, i.e., $\sum_{i=1}^{N} S_i > \sum_{i=1}^{N} D_i$
- Resilient consensus algorithm (RCA) was utilized to help each controller robustly estimate the total supply and demand in the presence of attacks to controllers and communication links, through exchanging information with other controllers in a strong vertex-connectivity peer-to-peer communication network.
- Graph algorithms were developed for the communication agent to randomly generate strong vertex-connectivity peer-to-peer communication networks, while reducing the success of cyberattacks to communication links.



A random, strong vertex-connectivity communication network generated by the communication agent



Magnitude of error injected by the attacks



Estimations under internal attack (malicious)

Estimations under measurement attack (Byzantine)

RESULTS

- RCA was tested and compared with the baseline approach (average CA) on two types of attacks: (i) malicious attack on controller's calculation, and (ii) attack on the measurement one controller sends to its neighbors
- Communication agent can quickly generate random strong vertex-connectivity communication network
- RCA can robustly estimate average supply and demand in both types of attacks and allow controllers to evaluate the interconnection criterion, while the baseline approach cannot

IMPACT

- The interconnection and reconfiguration framework brings in a resilient energy/power control architecture for networked microgrids

- The framework can also enable resilient decision of networks of CPSs modeled in the supply/demand context:
  - Gas network (e.g., supporting critical users)
  - Water network (e.g., reserve/demand balance)
  - Transportation network (e.g., congestion reduce)

U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

8/18/2022 | PNNL-SA-174894

Pacific Northwest NATIONAL LABORATORY
www.pnnl.gov