NETWORKED MICROGRIDS FOR CYBER-PHYSICAL SYSTEMS SECURITY

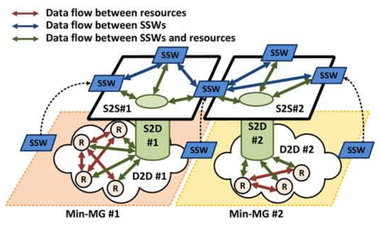
Reconfigurable and Resilient Operation Against Cyber and Physical Disturbances

Bo Chen (bo.chen@anl.gov) , **Feng Qiu** (fqiu@anl.gov), **Jianzhe Liu, Yichen Zhang, Shijia Zhao**
Center for Energy, Environmental, and Economic Systems Analysis (CEEESA)
Argonne National Laboratory

ABSTRACT

Evolving electric power systems feature increasing intelligent power sources (e.g., microgrids) and advanced communication capabilities, which enable microgrids to be potentially networked and support many innovation operation paradigms.

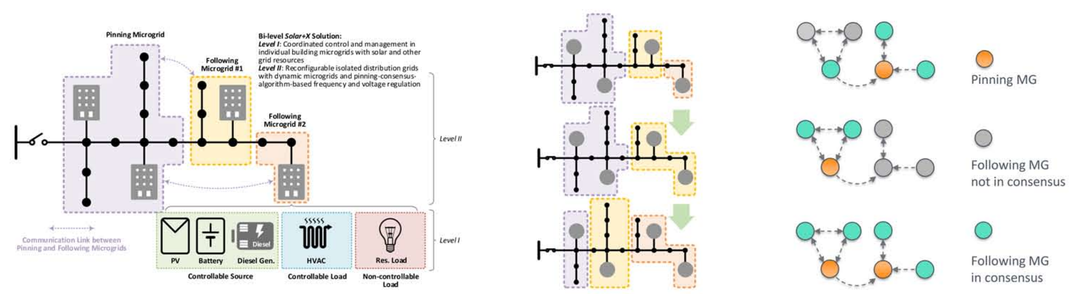
Our existing work explores the utilization of networked microgrids (NMGs), which are tightly-coupled cyber-physical systems, for future transmission and distribution grids. Specifically, we develop optimal operation solutions to protect the power system from severe cyber and physical disturbances.



- Cyber security enhancement through pinning-based distributed control
  - Real-time distributed control using only a select fraction of grid assets (pinning nodes) to achieve system-wise control objectives
  - Reduce computational and communication burden
  - Robust to physical and communication network changes
- Resilient operation against extreme weather events
  - Risk quantification of extreme weathers: hurricane, flood and winter storms
  - Pre-event resource planning and allocation: crew, mobile generator, etc.
  - Post-event restoration: Microgrid formation and energy management, crew dispatch

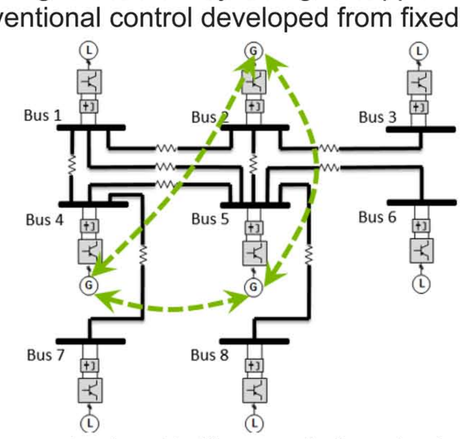
MOTIVATION

- As the penetration level of distributed energy resources (DERs) increases rapidly, a resilient, reliable and stable operation on cyber-physical coupled power system is urgently needed to modernize electric grids and ensure operation continuity. As an effective entity of integrating DERs and local loads, microgrids have been widely deployed. The concept of networked microgrids is an emerging operation paradigm, in which multiple microgrids are coordinated through intelligent control and flexible operation methodologies to further improve grid resilience and renewable integration. In addition to single and individual microgrids, networked and dynamic microgrids with controllable and effective interconnections have been deployed and studied to advance resiliency enhancement, especially for critical infrastructures.



PINNING-BASED DISTRIBUTED CONTROL

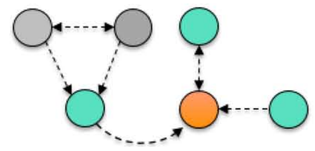
- Communication/physical topology can be maliciously maneuvered
  - Certain grid assets may lose grid supporting capability unexpectedly
  - Conventional control developed from fixed physical/commu. topology can fail



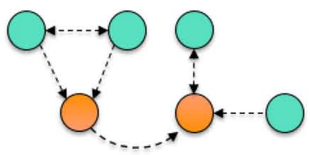
An example microgrid with communication network

Adversary
Communication network varies due to attacks

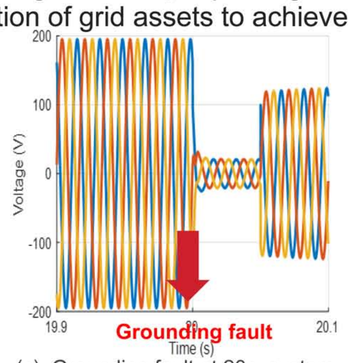
- Pinning based distributed control is more resilient against cyber events
  - Online assess controllability of grid assets, improving situational awareness
  - Capable of using only a fraction of grid assets to achieve system-wise goals



(a) Assessment of controllability



(b) Pinning control design

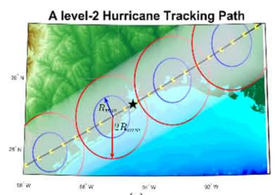


(c) Grounding fault at 20s, system cannot be restored w/ fixed control

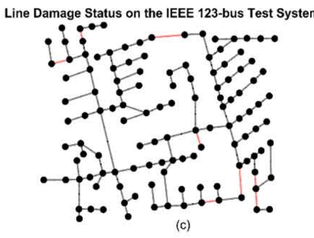
(d) System restoration from faults via changing pinning nodes

RESILIENT OPERATION AGAINST EXTREME WEATHERS

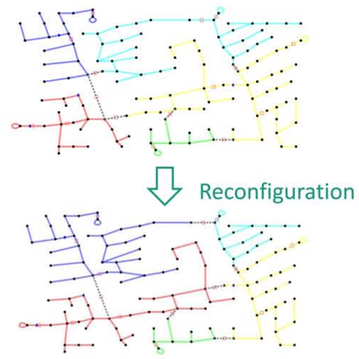
- The developed tool can provide
  - Visualization of weather metrics of extreme weathers (hurricane, flood, winter storm)
  - Reconfigurable and resilient operation against physical disturbances
  - Large-scale test system (>10,000 nodes) and close to practical scenarios
  - Failure probability of system components based on fragility functions
  - Damage status of system components subject tot weather impacts
  - Graphic UI with layer control to demonstrate selected outputs

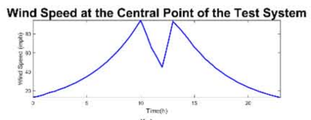


(a)

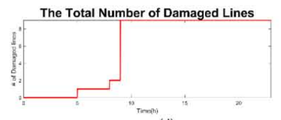


(c)

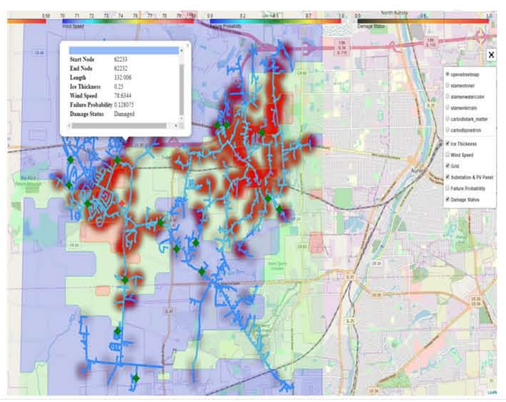




(b)



(d)



CONCLUSIONS

- Networked microgrids to improve security of cyber-physical systems
  - Novel conceptual framework as a CPS
  - Reconfigurable and resilient operation against cyber and physical disturbances
  - Provide significant operation flexibility
- Pinning-based distributed control
  - Physical and cyber attacks may jeopardize the system's resilience, w/ fixed controller design
  - Pinning-based control selects control nodes according to real-time physical/cyber conditions

FUTURE DIRECTIONS

- Co-simulation
  - Integrate physical and cyber coupled models in one composite simulation
  - Emulate multi-timescale operations, including physical/cyber network planning and control.
- Hardware-in-the-loop testing
  - Online fault injection similar to red team exercise
  - Utilize real-time simulator to conduct attack-defense testing of the proposed approach
- Tool Development
  - Algorithms and models put into implementations
  - User-friendly and adapt to user-defined systems

- Report and presentation of 2 DOE-SETO funded projects.
  - "Optimization Framework for Solar Energy Integrated Resilient Distribution Grid"
  - "Reconfigurable and Resilient Operation of Network-Controlled Building Microgrids with Solar Integration"
- Yuhua Du, Xiaonan Lu, Jianhui Wang, and Srdjan Lukic. "Distributed Secondary Control Strategy for Microgrid Operation with Dynamic Boundaries." IEEE Transactions on Smart Grid (2018).
- Yuxi Men, Xiaonan Lu, Jianzhe Liu, Chen Chen, Bo Chen, "Reconfigurable and Dynamic Distribution Systems Enabled Using Self-Sustainable Minimal-Microgrids with Region Based Stability Guarantees." IEEE Energy Conversion Congress and Exposition (ECCE), 2019.
- Jianzhe Liu, Xiaonan Lu, Chen Chen, Bo Chen, "Leader Selection in Robust Pinning-based Distributed Control for Islanded Microgrids." IEEE Energy Conversion Congress and Exposition (ECCE), 2019.

THE UNIVERSITY OF CHICAGO
U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.
SMU
TEMPLE UNIVERSITY
IOWA STATE UNIVERSITY
ILLINOIS INSTITUTE OF TECHNOLOGY
United Technologies Research Center
Argonne NATIONAL LABORATORY