Motivation

- For the Smart Grid to be resilient, wide-area monitoring and control is a necessity.
- Local control loops, do not depend on wide-area information exchange for their operations, which makes them less vulnerable in the face of cyber security threats.
- Due to the lack of observability in local measurements, local control schemes will not be able to deliver the expected performance and reliability for future power grid.
- Use of wide-area measurements for control design, will transform power system control structure from “islands of automation” to highly interconnected networked control systems.
- Although, these advancements will greatly improve the overall power system performance, they also present an increased dependency on cyber resources, which may be vulnerable to attack.

Future control framework for power grid should be able to provide the required performance and reliability, while minimizing the cyber security concerns introduced from wide-area measurements and communication infrastructure.

Distributed vs. Conventional Control

- **Conventional control** design problem assumes that all controllers in the system have access to the same information.
- In **Distributed Control**, the decision maker is composed of several interconnected units. Each local decision maker can only access a subset of the global information (e.g., sensor measurements, model parameters) and actuate on a subset of the inputs.

\[
\min_{\hat{K}} \int_0^\infty (\hat{x}(\tau)')Q\hat{x}(\tau) + \hat{u}(\tau)\hat{R}\hat{u}(\tau) d\tau
\]

subject to

- dynamics: \( \hat{x}(t) = \hat{A}\hat{x}(t) + \hat{B}\hat{u}(t) \)
- feedback control: \( \hat{u}(t) = \hat{K}\hat{x}(t) \)
- stability: \( \hat{A} + \hat{B}\hat{K} \) is Hurwitz
- communication: \( \hat{K} \in \mathbb{R}^{N}_{n,m}(\mathcal{G}) \)
- initial condition: \( \hat{x}(0) = \hat{x}_0 \)

Fundamental Challenges

- **Theoretical Challenges:**
  - Distributed control design is a NP-hard problem.
  - Two main approaches that have been proposed for solving distributed control problem: 
    1. Identifying sub-optimal solutions.
    2. Identifying special conditions or information patterns under which the problem can be solved.

- **Implementation Challenges:**
  1. Implementation of a robust communication network
  2. IEEE Standards Privacy in data sharing agreements
  3. Cyber security concerns and …

Research Results

- **No Control**
- **Centralized Control**
- **Distributed Control**
- **Decentralized Control**

Conclusion and Future Work

- In distributed control, only limited amount of communication between few controllers is exploited and the information provided to each decision maker is also limited. Thus, distributed architecture results in a framework, which is less vulnerable to cyber threats compared to centralized schemes.
- While local controllers cannot deliver the expected performance for the future grid and centralized-type wide-area controllers are challenging to implement securely, distributed controllers can achieve a trade-off between performance and cyber security.
- Future research is focused on comparing and quantifying the impact of cyber attacks for local, distributed and centralized control structures.