UCI University of California, Irvine

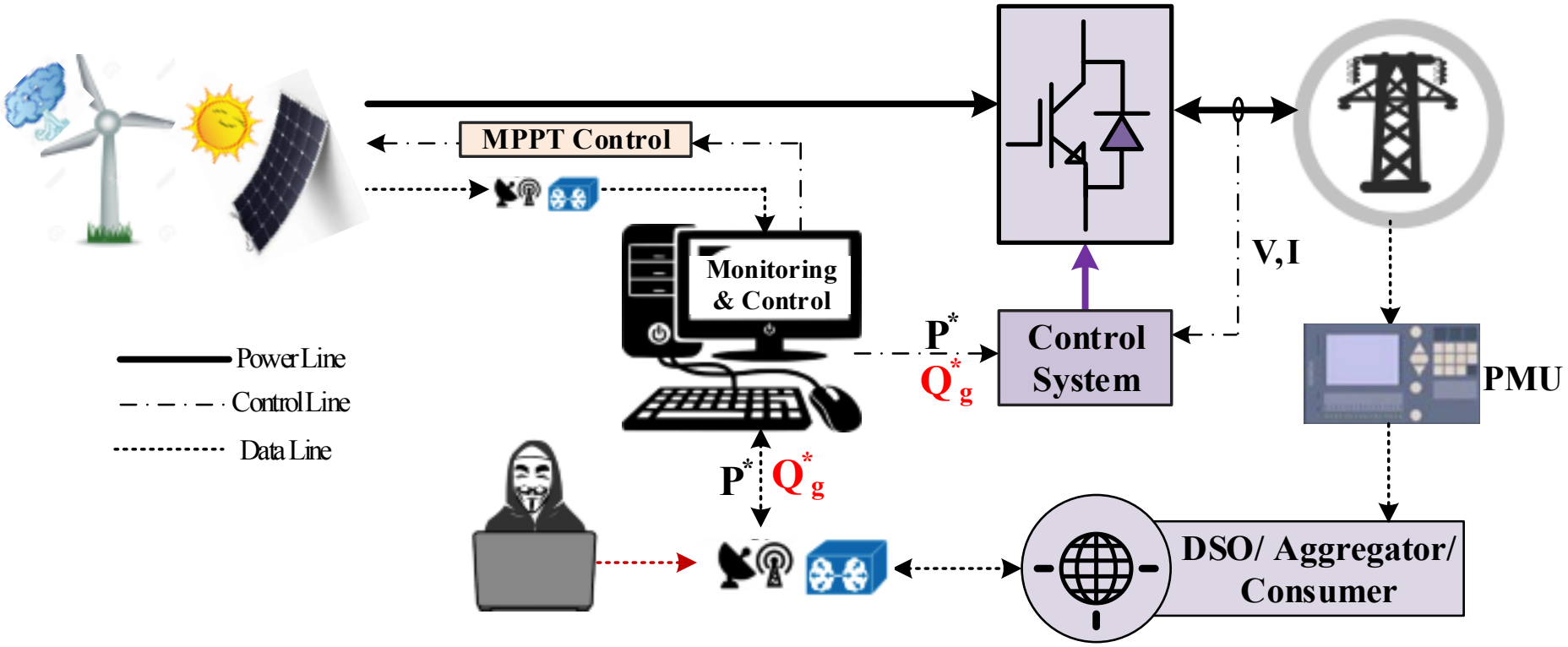
Progress Report *(March 2018 - March 2019)*

Research Project on

UC–Lab Center for Electricity Distribution Cybersecu

Keyue Smedley, Mohammad Al Faruque, Marco Levorato, Anto Josep
Arnav Malawade, Anomadarshi Barua, Peyman Tehrani, Igor Burago

March 08


MPPT Control
Monitoring & Control
P*
Q*g
Control System
V,I
PMU
Power Line
Control Line
Data Line
P*
Q*g
DSO/ Aggregator/ Consumer

rview

Research Achievements

- *Transient and Power Flow* Study during Cyber-attack on Distributed Power System.
- Secure-by-Design & Self-Secured Control with *Anomaly Detection* in Smart Grid.
- *Hierarchal Decision Making* in Smart Grid Under Cyber Security Attacks.

esearch Achievement

nsient and Power Flow Study during Cyber-attack on Distributed stem

Dynamics of distributed power system (DPS) during the interruption of DER, cap banks, loads, and switchgears.

- Lead to increase/decrease the grid voltage, LTC change, relay trip.

Dynamic behavior of DER when the reactive power set point is hacked.

- lead to reduce the active power feed-in and could trip the DER off DPS.
- Lead to voltage transients in buses.

Reactive Power Controller (Switched capacitors, Reactive power set-point in DER significant risky component in DPS.

Research Achievement

cure-by-Design & Self-Secured Control with Anomaly Detection in Smart

A new co-simulation platform (Secure Grid Simulator) to simulate new and ex cyber-physical attack methodologies.

- Identified common vulnerabilities/attack methodologies and their effects on di components of the smart grid.
- Impact of attack on physical infrastructure at distribution level

Self-Secured Control with Anomaly Detection and Recovery in BMS.

- CGAN will capture the dynamic behavior of the control loop in order to detect any anomaly r from attacks, and to recover from the attacks by predicting the correct state of system.

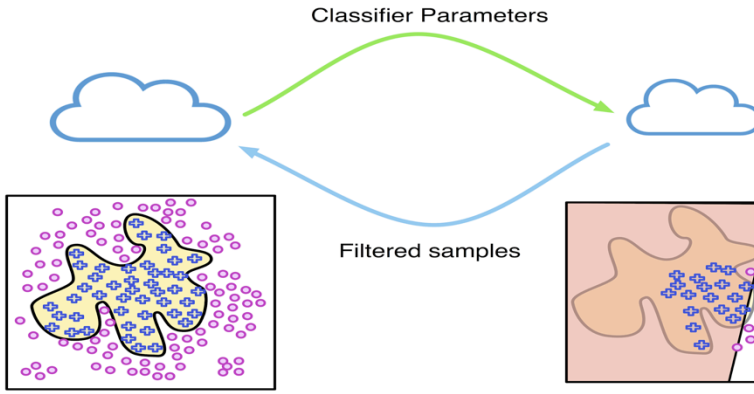
Research Achievement

rarchal Decision Making in Smart Grid Under Cyber Security Attacks

Review of the combined grid/communication system attacks.

Distributed classification technique resilient to combined grid/communication s attacks.

- To minimizes the information flow from sensors to attack detectors by dynamically (and contin training simple classifiers used as filters at the sensor level.



verables

M. A. Al Faruque et al., "Self Secured Control with Anomaly Detection and Recove Automotive Cyber-Physical Systems", *IEEE/ACM Design Automation and Test in Eu (DATE'19),* Florence, Italy, March 2019 (Accepted).

I.Burago and M. Levorato, "Randomized Edge-Assisted On-Sensor Information Selectio Bandwidth-Constrained Systems", Published in *Fifty-second Asilomar Conference on Sig Systems and Computers*, Asilomar, CA, Oct. 28-30, 2018.

I.Burago and M. Levorato, "Cloud-Assisted On-Sensor Observation Classification Constrained Decision-Making in Latency-Impeded IoT Systems", Submitted to *IEEE 2019*, July 7-12 2019, Paris, France.

e Research Work

Transient Study during Cyber-attack on Distributed Power System and and defense methods.

- Coordinated attack scenarios will be studied.
- Investigate the cascaded failures in distributed power system with respect to a attack in the unit.
- Simulation of DVC defense system to combat major scenarios of cyber attacks: optimal location and capacity fo placement for protection of given system.

Secure-by-Design & Self-Secured Control with Anomaly Detection in Smart Grid.

- Continue further development of Secure-Grid-Simulator to handle Distributed Coordinated attacks on Smart Grid.
- Development of new architecture for Self Healing of the DERs and their controllers from physical attacks.
- Combine Physics based modelling of the smart grid with the machine learning to make it robust.

Hierarchal Decision Making in Smart Grid Under Cyber Security Attacks.

- Integration of adaptive learning/filtering techniques in attack detection.
- Development of simulative case study scenarios and modeling techniques where the dynamics of the syste determined by contextual variables.
- Development of distributed, communication-aware, detection algorithms embedding the notion of state and context.

Thank you!