

# Attack-resilient Control for Optimal Protection Coordination of Microgrid

Masoud Barati

ECE Department, University of Houston

Houston, TX, USA

[mbarati@uh.edu](mailto:mbarati@uh.edu)

*Abstract* – The development of a trustworthy smart grid increases the effective attack surface available to an adversary and exposes the control applications that depend on it. Hence, in addition to improving cyber security of the communication network, it becomes imperative to develop control system algorithms that are both, attack resilient and tolerant. Cyber physical attack in the microgrid will change the normal operating point of the system; therefore the self-healing process takes action to remove the attacked points or zones. The overcurrent relay protection schemes would be changed by changing the topology of the microgrid. We present basic concepts of attack resilient control by designing adaptive overcurrent relay coordination as a defense algorithm in presence of the cyber-physical-attacks. On the occurrence of a fault or abnormal condition by attacker such as intentional faults, bad data injection on AMI system, the adaptive protection system must be capable of detecting it immediately in order to isolate the affected section or re-coordination of protective relays, thus permitting the rest of the microgrid to remain in service and limiting the possibility of damage to other equipment. The defense algorithms must be developed with the assumption that the attacker has knowledge of system operation. In the proposed algorithm, bad data injection, faulty zone and components are detected as an assumption. The resilient control scheme is optimally designed taking into account both modes of operation (grid-connected and islanded). The problem has been formulated as a master problem and subproblem and is solved using the CPLEX algorithm. Master problem minimize the total microgrid operation cost. Self-healing process is embedded in the master problem in case of feeder or transformer outages. The value of short circuit near-end and the far-end fault currents can be obtained by using the impedance matrix of the new topology of network. To achieve optimal coordination of the relays, their settings are chosen for their minimum operation time. Subproblem minimizes the total time delay of protective relays. The proposed approach is tested on two networks: a typical HRDS distribution system and on the IEEE 30-bus looped power distribution system equipped with directly connected conventional synchronous generators. Developing this adaptive setting technique is a step toward introducing attack- resilience control of protection systems.