Abstract

Hierarchical controllers for direct current (DC) microgrids and alternating current (AC) microgrids have gained popularity due to their layer-wise control structure. Distributed controllers at the secondary layer of these microgrids, using distributed communication, enable voltage and frequency restoration along with proportional power-sharing. Distributed controlled microgrids are highly subjected to cyber-attacks due to the sensor feedback and distributed communication. Though cyber-attacks are a low-probability event in the distributed controlled microgrids, they significantly disrupt microgrid operation and the controller's objectives and sometimes may lead to a total system shutdown due to the fast-acting power electronic converters and associated control system. The resiliency against cyber-attacks in microgrids has become the need of the hour, especially for defense, shipboard, remote island microgrids, etc. This thesis focuses on modeling, detecting, and mitigating sophisticated false data injection (FDI) cyber-attacks in microgrids.

First, a stealth FDI attack modeling on the output current measurement of distributed energy resource (DER) in DC microgrids is presented where the attacker's presence is hidden from the system operator. Due to the lack of global information monitoring in the distributed controlled DC microgrids, detecting stealth FDI attacks has become a challenge. This thesis proposes a discordant element (DE)-based attack detection to detect attacked nodes. The proposed detection method is simple to implement and uses local and neighboring DERs inductor current references from the device level control and computes the DE values. Any non-zero value of DE of DER during the DC microgrid operation indicates the presence of an FDI attack.

Cyber-attackers may target to disrupt the microgrid operation or control objectives without the system operator's notice. For this, the second chapter in the thesis proposes localized attack detection and event-driven mitigation to make distributed controlled DC microgrids resilient against FDI attacks. An attack impact analysis is presented to determine the deviation in average voltage and output current caused from its pre-attacked values due to the FDI attack. Based on the analysis, the global control objectives are derived for the resilient DC microgrid operation. A localized attack detection based on the error between sensor measurement value and artificial neural network (ANN) estimated value is used to detect the FDI attack. Further, an event-driven resiliency is developed to mitigate the attack, where the attacked measurements are replaced with ANN-based estimated values.

Further, the resiliency of the microgrid can be enhanced by decreasing the number of variables communicated in the communication links, so the number of attack-prone elements is effectively reduced. However, it is a challenge to realize the distributed control with a reduced number of variables while achieving the average voltage restoration and proportionate power-sharing simultaneously in the DC microgrid. For this, a distributed control with reduced communication variables is proposed, along with event-based resiliency for communication variable attacks.

In AC microgrids, any false data injection (FDI) in the communicated variables used in distributed secondary control leads to frequency and voltage deviations. A steady-state FDI attack impact analysis on the conventional distributed controller is carried out to determine the deviations in attack magnitude and controller parameters. Further, to mitigate the deviations, the auxiliary variables are incorporated into the conventional cooperative active and reactive power loops. The cooperative errors derived from the auxiliary variables are used to nullify the attack impacts on frequency and voltages. A steady state impact analysis is also presented for the proposed distributed control with an FDI attack to show the convergence of frequency and average voltage of the AC microgrid to its nominal values. The presented impact analysis, proposed detection, and mitigation strategies throughout the thesis have been validated in simulations and hardware experimental setups for various case studies showing satisfactory performance.

Finally, the significant findings and proposed method implications are concluded, along with the future scope that can pave the way forward for this thesis.