ABSTRACT

Phasor measurement units, also known as synchrophasor devices, constitute an integral part of the modern smart grid. Compared to the conventional supervisory control and data acquisition (SCADA) systems, they provide situational awareness by sending time-stamped, real-time measurements from different parts of the smart grid to data centers and thus ensuring proper grid visibility and monitoring with improved accuracy. While this progress has been enormous, significant issues have evolved due to their widespread use, particularly in data quality.

This work considers two PMU data integrity attacks, namely, Time Synchronization Attack (TSA) and Man-in-the-Middle (MitM) attacks, both of which potentially compromise the PMU measurements and cause severe impact on the grid are analyzed. Signal processing techniques are used to correct these compromised measurements. Specifically, we propose a novel method based on an alternate expectation-maximization framework to mitigate the effects of these attacks on the state estimation process. To validate the presented technique, numerical experiments are performed on IEEE-14 and 30 bus systems with various attack scenarios. Without any hardware modifications, the proposed approach provides accurate estimations without any knowledge of the number of attacks or the location of the attack. In terms of state estimate accuracy, the suggested method outperforms the traditional weighted least square method.