Abstract

Modern control centers adopt state estimation algorithms to define the current operating scenario of the grid as critical grid operations like economic load dispatch, load scheduling, and load monitoring are inherently dependent on it. With the large-scale inclusion of renewables and plug-in electric vehicles, a need for real-time monitoring of the grid is essential. To ensure the aforesaid, rapid adoption of modern industrial internet of things technology (IIOT) within the power sector has been furnished which promotes enhanced reliability. Such enhanced grid automation with modern IIOT devices comes with its inherent vulnerabilities. Recently, a rapid increase in cyber-attacks by undermining the critical vulnerabilities of the remote terminal units, sensors, meters, and communication channels has led to rise in mal-operations and critical scenarios of the power sector. This thesis undertakes a study of one such advanced cyber-attack strategy on the grid, namely the false data injection attack. Such attacks have recently demonstrated their harmful potential against the state estimation algorithms within the energy management systems in the control center by compromising the measurements of several meters, and sensors, i.e., by corrupting the wide-area measurements and the monitoring systems, hence leading to the formulation of biased estimation of the operating states. Although detection of such attacks is a critical issue, nevertheless novel attack vector formulation schemes must be presented to test the prevalent identification policies. This thesis presents effective attack vector formulation policies by undertaking the low-rank subspace of the topology matrix. In particular, it is seen that under some specific constraints, attack vectors defined on the low-rank subspace are bound to bypass the statistical residue test as adopted by the bad data detectors in the control center. A critical comparison of low-rank approximation algorithms for defining stealthy attack vectors under ideal, noisy conditions along with the presence of outliers within the topology matrix has also demonstrated the efficacy of the proposed approaches. All the aforesaid propositions are validated on the

standard IEEE 14-bus test bench. For an efficient determination of such attacks, this thesis furnishes a novel, real-time, scalable state forecasting-based attack detection policy within the raw measurements by incorporating advanced deep learning models followed by anomaly detection schemes. The proposed deep learning model furnishes a nonlinear structure with minimal performance indices like root mean squared error, mean squared error, and mean absolute error while the anomaly detection schemes are based on the error vector and the error covariance matrix developed due to the forecasted and the estimated set of operating states at the control center. The demonstrated approaches when tested on the standard IEEE 14-bus system define a robust determination of the presence of attacks within the raw measurements under varying noise and attack scenarios. Nevertheless, most of the recent studies in the detection of such a class of attacks promote an efficient presence detection policy within the acquired set of measurements whereas their exact intrusion points remain unknown. To mitigate this issue, this thesis also presents a novel strategy for the detection of the presence of such a class of attacks within the acquired measurements along with its respective locations of intrusions by incorporating advanced deep learning models working as multilabel classifiers. Such classifiers furnish a cost-effective, model-free, and real-time attack detection scheme. Moreover, when tested over large-scale systems like IEEE 118-bus, the undertaken deep learning and machine learning models furnish a robust performance under a varying range of noise, outliers, and attack scenarios.