**ABSTRACT**

The immense increase in the demand for electrical energy has become a challenge not only for production but also for its distribution. This growing demand along with the advancement in technology has led to the remote control and monitoring of power grids through supervisory control and data acquisition (SCADA) system and automation at substations which decreases the cost of power transmission and increases efficiency. Any interruption in the transmission, like widespread blackouts, will cause irreparable effects on different aspects of society. However, this opportunity also may lead to a threat if cyber security is met with a lack of attention in smart grids. Transmitting data from IEDs leaves them vulnerable to cyber-attacks. Attackers can inject false data into the power system control center and thereby prevent the operators from obtaining the true operating conditions of the system. Thus is highly necessary to separate naturally occurring conditions from cyber-attacks to confirm the grid’s reliability. Automatically and accurately detecting cyber-attacks in the power system remains a big challenge within the field of intelligent fault diagnosis. In this paper, we employ machine learning algorithms to differentiate cyber-attacks from naturally occurring conditions in a power system.