IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 20, 2020, accepted June 9, 2020, date of publication June 19, 2020, date of current version June 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3003568

A Review of Machine Learning Approaches to Power System Security and Stability

OYENIYI AKEEM ALIMI[1], (Member, IEEE), KHMAIES OUAHADA[1], (Senior Member, IEEE), AND ADNAN M. ABU-MAHFOUZ[1,2], (Senior Member, IEEE)

[1]Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg 2006, South Africa
[2]Council for Scientific and Industrial Research, Pretoria 0184, South Africa

Corresponding author: Oyeniyi Akeem Alimi (alimioyeniyi@gmail.com)

This work was supported by the Council for Scientific and Industrial Research, Pretoria, South Africa, through the Smart Networks Collaboration Initiative and IoT-Factory Programme, funded by the Department of Science and Innovation (DSI), South Africa.

ABSTRACT Increasing use of renewable energy sources, liberalized energy markets and most importantly, the integrations of various monitoring, measuring and communication infrastructures into modern power system network offer the opportunity to build a resilient and efficient grid. However, it also brings about various threats of instabilities and security concerns in form of cyberattack, voltage instability, power quality (PQ) disturbance among others to the complex network. The need for efficient methodologies for quicker identification and detection of these problems have always been a priority to energy stakeholders over the years. In recent times, machine learning techniques (MLTs) have proven to be effective in numerous applications including power system studies. In the literature, various MLTs such as artificial neural networks (ANN), Decision Tree (DT), support vector machines (SVM) have been proposed, resulting in effective decision making and control actions in the secured and stable operations of the power system. Given this growing trend, this paper presents a comprehensive review on the most recent studies whereby MLTs were developed for power system security and stability especially in cyberattack detections, PQ disturbance studies and dynamic security assessment studies. The aim is to highlight the methodologies, achievements and more importantly the limitations in the classifier(s) design, dataset and test systems employed in the reviewed publications. A brief review of reinforcement learning (RL) and deep reinforcement learning (DRL) approaches to transient stability assessment is also presented. Finally, we highlighted some challenges and directions for future studies.

INDEX TERMS Classifiers, cyberattacks, deep reinforcement learning, intruder detection system, machine learning techniques, power quality disturbance, power system, reinforcement learning, test systems, transient stability assessment, voltage stability.

I. INTRODUCTION

Over the past few decades, power system operations are constantly being modernized so as to accommodate the integration of renewable energy and storage systems (RES), liberalized market, numerous measuring and communication technologies devices to name a few [1]. While the modernization contributed immensely to safer, reliable and cleaner energy distribution to users, the transition also brings along new challenges to the network's security and stability [2]. The overreliance of modern power system's applications such as state estimation, Supervisory Control and Data Acquisition (SCADA) systems, Phasor Measurement Unit (PMU) on open communication technologies including the internet have exposed the networks to various vulnerabilities and threats [3]. As a key critical infrastructure, the secure and stable operation of power system is usually treated with topmost priority by the governments and utility stakeholders as the various social, political, and economical activities are closely tied to the nation's power system. Adversaries can access network nodes and alter measurements including control commands, thereby destabilizing the operation, creating blackouts, financial losses and in some situations, national security can be put into jeopardy [4].

Furthermore, the geometric growth in energy demands, the introduction of certain disturbing loads, major changes in network topology, the increasing strains on transmission lines, etc. are dangerously pushing the power system towards and

The associate editor coordinating the review of this manuscript and approving it for publication was Ziang Zhang.

beyond stability limits, thus creating instabilities and power quality disturbances (PQD) problems [5], [6]. In recent times, these instabilities and disturbances concerns have drawn the attention of the industrial and academic communities as they are leading causes of outages, economic losses, equipment malfunctioning and failures. According to Electrical Power Research Institute (EPRI), power supply outages crisis created an economic loss estimates of $104 billion to $164 billion annually [7]. Several studies in the literature have discussed the threats, effects and impacts of these disturbances, insecurities and instabilities [8]–[11]. Monitoring the power system's status especially during load changes and post contingencies have always been a major concern to energy stakeholders and operators. Over the years, various statistical models and signal processing techniques [12]–[14] have been proposed in security and stability studies. Despite demonstrating satisfactory performances, the conventional methods have proven to be computationally inept, expensive and time-consuming as they struggle in addressing the emerging analytic needs of the complex modern power system.

In recent times, machine learning techniques (MLTs) have been vastly used in modelling and monitoring complex applications. Numerous MLTs such as Artificial Neural Network (ANN), Decision Tree (DT), Principal Component Analysis (PCA), etc. have been proposed in various capacities involving power system security and stability assessments. Unlike traditional methods, MLTs have proven to be computationally powerful, systematic and explicitly reliable when they are deployed in classification studies. In the literature, various simulation results in power system's research works have shown that MLTs have the capacity to learn and understand the changing characteristics of varying loads, network data, etc. that are peculiar to the dynamic nature of modern power system.

In line with the increasing concerns regarding power system security and stability, quite a number of review works in the literature have presented detailed description of the problems and notable solutions including machine learning approaches. Sun *et al.* [9] surveyed relevant cyber security studies with regards to dangers and solutions to improve the security of power grids. The work presented in [15] focused on surveying tools and techniques to uncover SCADA systems vulnerabilities. It also addressed different methods including machine learning algorithms for SCADA communication security. However, the study is only limited to SCADA communication aspect of the power system. In a similar study, Glauner *et al.* [16] reviewed different MLTs, features and datasets in detecting non-technical losses which includes electricity theft, defective meters and billing errors. Also, the study was limited to a specific domain as the authors did not include the study of MLTs on other key power system menaces. With regards to RES menaces, the authors in [17] presented a review on power grid protection especially with the challenges attributed to the numerous integration of RES. In the work, several MLTs deployed in the generation, forecasting and integration of RES into the power system were studied. Also, Saini and Kapoor [18] presented a survey on PQ classifications using machine learning and signal processing tools. The work focused only on power quality analysis.

To bridge the research gaps, we reviewed a wide range of machine learning architectures and explored the power system security and stability challenges that have benefitted from MLTs. This paper identifies four main power system security and stability domains: SCADA network vulnerability and threats, PQD studies, voltage stability assessment (VSA) and transient stability assessment (TSA) where MLTs have been extensively deployed. This review focuses on highlighting the methodologies, achievements and limitations in the classifier(s) design, dataset generation and test systems employed in the reviewed publications. A brief review of reinforcement learning (RL) and deep reinforcement learning (DRL) application especially in TSA studies is also presented. Conventional methods for power system security and stability solutions were not extensively reviewed in the paper as there are various works that have covered such approaches in the literature [19]–[21].

The review paper is intended for power system security and stability researchers with the intention of building analytics and/or artificial intelligence security solutions for power system infrastructure, using the current and emerging machine learning approaches. Different from the previous studies, this paper gathers together different approaches, strategies, procedures, limitations and research gaps on MLT application to power system security and stability studies. Specifically, the major contributions of this paper are stated briefly as follows:

- A comprehensive review of the most recent state-of-the-art ML approaches and the applicability in power system security and stability domain;
- The major power system security and stability domains (TSA, VSA, PQD and SCADA network vulnerability and threats) are extensively discussed;
- An elaborate review of several MLTs applied to power system security and stability problems as regards to the classifier(s) design, dataset generation, preprocessing techniques, optimization techniques and test systems deployed; and
- The challenges, limitations and research gaps of the current machine learning techniques' applications in power system security and stability studies and the directions for the successful deployment of MLTs in future power system security and stability applications.

Accordingly, the remainder of the paper is organized as follows; an overview of power system security and stability is presented in Section II. The section briefly discussed the TSA, VSA, PQ disturbances and SCADA network vulnerability analytics. Section III summarizes some of the power system stability and security solutions in the literature. Section IV presents a detailed analysis on MLTs for the power system stability and security menaces. Section V presents the

research gaps and future directions and Section VI concludes the paper.

II. OVERVIEW OF POWER SYSTEM SECURITY AND STABILITY

Ensuring that the power system is secured and stable especially after it has been exposed to varieties of strains and different contingencies is a major challenge that energy stakeholders are facing in today's world. Recent incidents worldwide have shown that the geographically dispersed power system are facing various security and stability crisis that warrants comprehensive protective and preventive measures. Historically, ensuring the security and stability of power system have always been a challenge. Operators of the old power system used to struggle in efficiently monitoring the network. In actual fact, operators usually expect reports on trips and faults from consumers [4]. However, despite the numerous innovations that epitomizes the modern power system in recent times, various evidences and reports have revealed that the modern power system globally are facing higher numbers of security and stability challenges. Also, the integration of numerous internet of things (IoT) infrastructures and other sophistically advanced gadgets affiliated with the modern power system are creating security and stability crisis to the network as some of the protocols and standards are highly vulnerable to cyberattacks and intrusion. In addition, the continuous quest for industrialization as well as the building of smart cities continue to create upsurge in unhealthy energy demand. The industrialization quest also creates the introduction of certain disturbing loads into the power system. The upsurge in energy demands is pushing generation and transmission facilities towards and beyond operational stability limits and the consequences are equipment failures, instabilities and PQDs.

Over the years, varieties of security and stability challenges have continued to plague the power system. Four major categories of power system menaces are identified as highly relevant to the stable and secured operation of the modern-day power system namely:

- Power Quality Disturbance (PQD)
- SCADA Network Vulnerabilities and Threats
- Transient Stability Assessment (TSA)
- Voltage Stability Assessment (VSA)

A. POWER QUALITY DISTURBANCE

Power quality disturbances can be defined as the sudden deviation manifested in voltage/current magnitude, phase angle and frequency from the standard rating. The disturbances are mostly created due to the introduction of non-linear loads, switching devices, rectifiers and inverters, etc. into the power system [7], [22], [23]. As explained by Wang and Chen [22], the continuous integrations of disturbing loads and RES are creating deterioration risks and malfunctioning of machineries at energy generation, transmission and consumption levels. Varieties of PQD effects include voltage sag, harmonic distortion, notch, flicker, spikes, etc. and they are capable of creating severe problems which include equipment malfunction, short life span and failures [24], [25]. According to EPRI, of all power supply outages crisis, PQ issues accounts for approximately 15% of the economic losses estimates of $104 billion to $164 billion annually [7]. Thus, the mitigation of PQD have continued to receive massive attention in the power system's research community.

B. SCADA NETWORK VULNERABILITIES AND THREATS

Critical infrastructures (CI) such as the power system, oil and gas pipelines, water distribution, etc. are monitored and controlled by SCADA systems which links the CI together as a network through advanced Information Technologies (IT) [26]. As shown in Fig. 1, the SCADA system architecture for the electricity grid basically consist of four major operational parts namely [27], [28]:

- The "Field" devices such as sensors for sensing the status of SCADA equipment under concern (power level, pressure, etc.) and control them according to the received commands.
- The "Remote Station" devices which include the Remote Terminal Units (RTUs) and Programmable Logic Controllers. They serve the purpose of sending and receiving digital data to and from the control centers and the field devices.
- The "Control Centre" devices consisting of the Master Terminal Units (MTU) that issues command to the remote station devices.
- Human Machine Interface (HMI): devices which present processed data to operators usually via graphic user interface. With the interface, operators can monitor and interact with SCADA processes.

Historically, when SCADA systems were first deployed, the major threat was sabotage through the physical destruction of the utility's hardware as the old SCADA systems had private and dedicated networks that are secured by traditional air gapped separations [29], [30]. However, over the past two decades, SCADA networks have been equipped with IoT devices that sometimes communicate over open channels which exposes the networks to numerous vulnerabilities and network based cyber-attacks [28]. These threats and attacks are projected to escalate in geometric rates in the nearest future as intruders/attackers find the energy infrastructures (arguably the most important of all CI) as a lucrative avenue to gain attention [31]. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) announced that, out of the 245 recorded cyber incidents on CI in 2014, 79 were targeted at the energy sector [2].

Based on the motives and the cause of attacks, SCADA threats and attacks can be categorized as [32]:

1. Internal/Malicious – operators, employees or contractors with intentional motives to cause disasters to the SCADA network. Example is the well-publicized stuxnet worm attack by a resentful engineer via a removable drive [15].

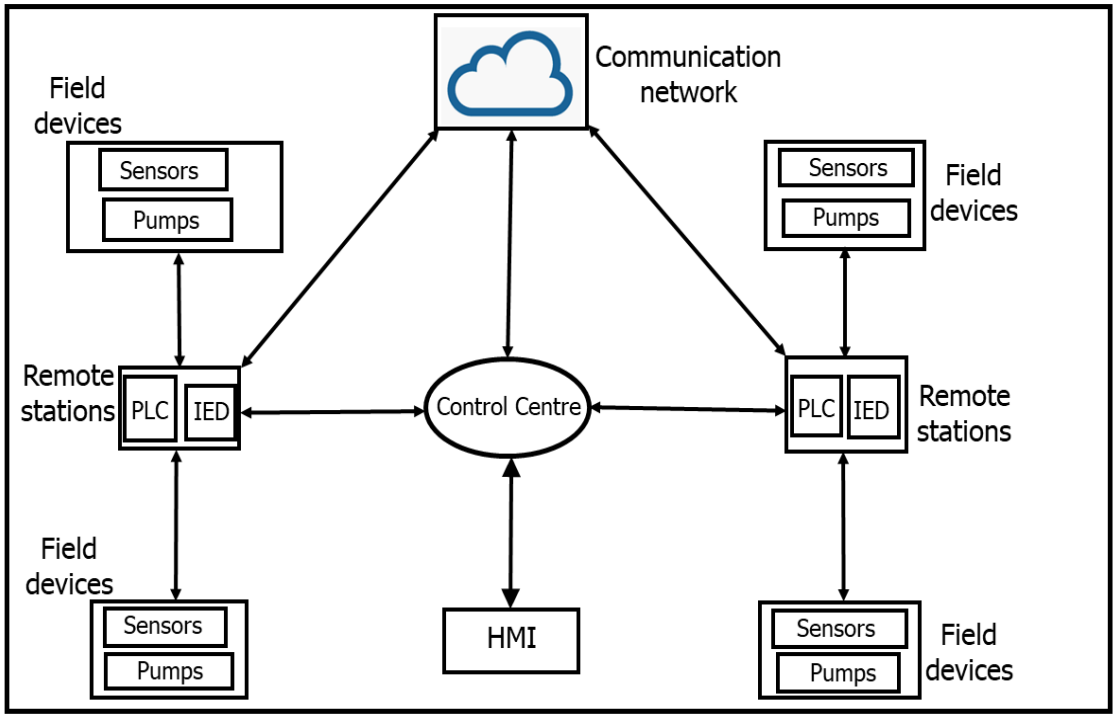

FIGURE 1. SCADA architecture [26].

2. Internal/Non-malicious – operator making an accidental mistake that causes harm to power system infrastructures. Example is the 2003 Ohio Davis-Besse nuclear plant ''Slammer'' worm infection that led to the plant being disabled for hours [33].
3. External/Opportunistic - hackers seeking a challenge or playing around.
4. External/Deliberate – this can be described as an attack by an external organized group that targets vulnerabilities in another nation/state power system such as the 2015 cyber-attack on Ukrainian power grid whereby the hackers were linked to Russia [34].

These experiences and several reported cases have showcased the immeasurable consequences of attacks on SCADA networks.

C. TRANSIENT STABILITY ASSESSMENT

Various incidences such as some specific blackouts in the United States, some European and Asian countries have shown that instabilities arising from RES, increasing energy demands and disturbances demands the necessity for improved tools in monitoring dynamic security of modern power system. According to [35], evaluating the capacity of a power system to withstand and survive a finite set of contingencies to an acceptable steady-state condition is termed dynamic security assessment (DSA). As shown in Fig. 2, transient stability, voltage stability and frequency stability are identified as the main DSA categories.

Transient stability assessment (TSA) provides system operators analytical judgment of the power system dynamic performance under various contingencies. As defined by James *et al.* [36], transient stability is the ability of all the generators to preserve synchronism after a severe disturbance such as a fault or sudden loss of generator/ load or other components. Transient instability is among the key causes of numerous power instability scenarios including islanding and widespread blackouts experienced recently in Iran and Russian [37]. According to the authors in [38], system operators must be able to evaluate the power system stability condition and, if needed, organize corrective actions to preserve the needed stability in order to avoid the blackouts and failures. Traditionally, TSA mathematically corresponds to solving a set of high-dimensional non-linear differential algebraic equations (DAE). Conventional TSA methods such as the time domain simulation (TDS) and direct methods (e.g. transient energy function (TEF) methods, the extended equal-area criterion (EEAC) and Lyapunov exponents have been widely proposed in numerous literature. Generally, the main limitation of these methods is the large computational effort to evaluate the swing curves for all the generators, for different load levels, faults and clearance times. Thus, the conventional TSA methods do not meet the requirements demanded by modern power system.

D. VOLTAGE STABILITY ASSESSMENT

While the attention has mostly focused on transient stability, another increasingly important dynamic security topic in

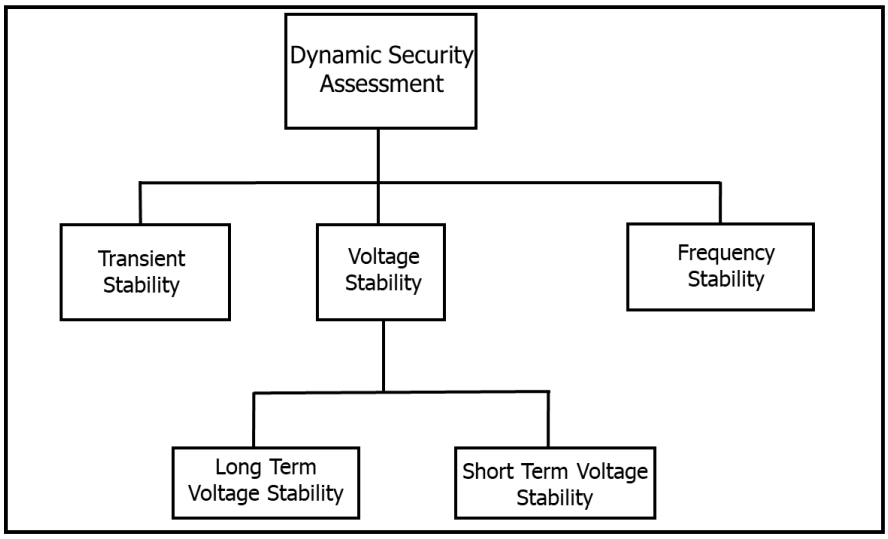

FIGURE 2. Dynamic security assessment architecture [35].

modern power system is voltage stability. Unlike transient stability that deals majorly with generators' synchronism, voltage stability is majorly tied to load dynamics as well as reactive power management [39]. Voltage stability denotes the power system's ability to maintain the bus voltages at acceptable values after a disturbance from a given operating condition [40]. The authors in [41], [42] explained that, the voltage profile of a power system is usually preserved within a stable range, however when the power system encounter a significant fault or disturbance, several incidents may occur. These incidents include: the voltage profile may lose stability thereby instituting the induction motors to decelerate radically, draws high reactive current and ultimately lead to a progressive and uncontrollable decline in voltage magnitudes. Apart from blackouts, other effects of voltage instability on the network includes the swift removal of generator(s) or transmission element(s) and low voltage supply [8]. Thus, a blackout may ensue within few minutes. Based on the time frame, voltage instability crisis can be categorized into short term and long term [43]:

- Short term voltage stability (STVS)- STVS problems occur within a short time frame (seconds) after the fault clearing. The short term voltage instability is mostly triggered by the dynamic characteristics of complex induction motor loads.
- Long term voltage stability- unlike the STVS, the time frame for long term voltage instability problems or collapse is longer (average of 0.5-30 minutes). Long term voltage instability problems are mostly experienced in heavily loaded power system. The long term voltage instability is mostly triggered by slow acting equipment, such as tap-changing transformers and current limiters [44].

The consequences of the voltage instability problems that were experienced in France, Tokyo and more recently in Israel have shown the economic and social significances of voltage instability, hence making voltage stability analysis one of the most discussed topics in the power system research world. Voltage stability analysis involves monitoring the power system reaction to continuous change in generator and load dynamics.

III. POWER SYSTEM STABILITY AND SECURITY SOLUTIONS

In the olden days, majority of power system stability and security challenges were judged on visual inspections based on operators' knowledge and experiences. However, more recently, several conventional methods have been proposed to maintain the steady operation of the heterogeneous power system. In the literature, numerous signal processing techniques have been proposed for PDQ studies over the years. Also, various mathematical formulations that focused on estimating the power system's margin towards voltage instability, time-domain simulations and direct methods have been proposed for DSA studies. Furthermore, as Intrusion Detection Systems (IDSs) are adjudged as the de-facto protection methodology for information technology systems, several statistical and theoretical formulations have been applied as models for various SCADA intrusion detection schemes down the years. However, due to varieties of factors, these statistical formulations are too rigid and computationally inept for some specific scenarios. Hence they are incapable of effectively protecting the modern heterogeneous systems [33], [45]. In addition, with the deployment of PMU devices into modern power system, significant progress has been made with regards to efficient measurement documentation as the PMU devices provide time synchronized phasor measurements thereby enhancing fast decision making and control actions which ultimately assist in creating a path for the successful realization of accurate and effective DSA. However, important factors such as the enormous data associated with PMU devices, the uncertainties associated with

measurement errors, intrusion on PMU devices and most importantly, the non-linearity and computational complexity of the current and future power system operations, etc. have exposed the limitations of conventional security and stability methods in effective mitigation. The need for proactive, well-calibrated, fast, reliable and advanced security and stability methods for modern-day power system have become essential to all energy stakeholders especially in the face of incessant blackouts and other power system menaces. In the last three decades, machine learning algorithms are proving extremely efficient in power system studies. MLTs have been widely proposed in power system studies involving the monitoring and classification of various power system menaces.

IV. MLTs FOR POWER SYSTEM MENACES

It is becoming increasingly challenging to protect the modern-day power system using conventional methods. MLTs and deep learning techniques are continuously proving to be a feasible option as they tick the various security factor boxes i.e. high performance, high speed of execution and efficiency. Machine learning methods have been widely proposed in power system literature for monitoring, intrusion detection, prediction and classification of various power system menaces. Based on the deployed learning mechanisms, Sharma and Wang [46] categorized existing MLTs and deep learning techniques into supervised learning, unsupervised learning and reinforcement learning. With regards to supervised learning, the learning techniques require the prior knowledge of a training dataset to learn a link between the input as well as the expected output. Examples of supervised learning techniques include NN, SVM, DT, etc. On the other hand, unsupervised learning techniques attempt to find hidden patterns in the data without the need of any labelled data, training dataset and expected output. Examples of unsupervised learning include K-Means, PCA, etc. With regards to reinforcement learning techniques, a learning agent observes and interacts with a system environment, alters the state of the environment by taking some control actions. Afterwards, they observe the effects of the actions in order to maximize the notion of cumulative reward [47]. Examples of RL algorithms include Q-learning, DQN, SARSA, DDPG, etc. [48]. From the conventional point of view, MLTs for power system studies are generally divided into three major phases: dataset generation, data preprocessing (feature selection/extraction) and evaluation/classification. In some studies, authors deployed various optimization techniques and ensemble multiple machine learning algorithms to boost the classification performances. The rest of this section explicitly discusses some of the power system studies that have been done using MLTs.

A. MLTs FOR POWER QUALITY DISTURBANCE CLASSIFICATION

In any real power system, there are multiple sources and types of power quality disturbances, hence the accurate detection and classifications of specific events are highly crucial [49]. Due to its massive success, various research works in the literature have proposed several combinations of machine learning algorithms and signal processing techniques for detecting and classifying PQD events. Basically, the combination follows the architectural framework shown in Fig. 3.

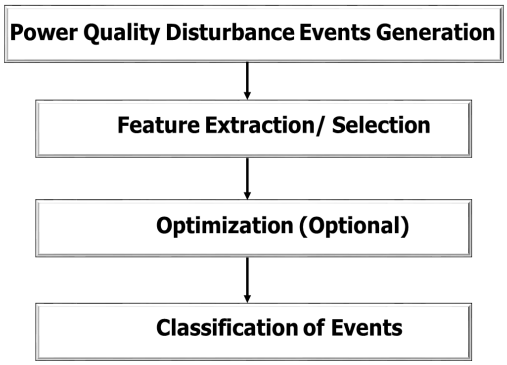

FIGURE 3. PQD classification steps.

1) PQD FEATURE EXTRACTION/SIGNAL ANALYSIS STAGE

In the literature, synthetic parametric equations of power quality disturbances based on IEEE standards are simulated using software such as MATLAB to generate single and multiple classes of large dimension feature dataset [23], [49]–[54]. The large dimension feature data generated is not ideal to be used as the input of the classifier as they will significantly increase computational time and reduce classification accuracy. Hence there is usually a need for the extraction of the dominant features for classification [53]. In the literature, several signal processing techniques have been deployed for extracting the dominant features of PQD waveforms. Various time domain signal processing techniques such as EMD [24], [55] and frequency domain techniques such as FT [56] have been successfully deployed for feature extraction in MLT based PQD studies. Despite the fact that the methods presented good performances, the fact that either frequency or time domain techniques cannot analyze signals at neither time nor frequency domain respectively is a massive limitation. As better options, several authors have deployed time-frequency domain techniques as they are capable of extracting features from both domains. The authors in [57]–[59] deployed wavelet transform as it offers good time-frequency characteristics and it is well known to have excellent ability in analyzing local discontinuities of signals [51]. In similar studies, Alshahrani *et al.* [60] and Naik *et al.* [61] opted for DWT and WPT respectively as they offer additional advantage with regards to fixed window size. Also, in order to boost the feature extraction performance and speed of extraction, Abdoos *et al.* [49] deployed VMD and ST signal processing as they have few tuning parameters in comparison to several other methods. As a widely used signal processing tool, WT have various mother wavelet filters and decomposition levels. Manimala *et al.* [54] explained that the choice of the mother

wavelet is crucial in wavelet analysis and it can affect the analysis results. The authors further explained that suitable mother wavelet can be determined based on properties such as PQ indices calculation, orthogonality, maximum number of vanishing moments, and compactness support. In the literature, the most frequently used mother wavelet class for PQD studies is the fourth order daubechies 4 wavelet (DB4) as it possesses the described characteristics and it is known to have a close similarity to power disturbance signal [51], Daubechies was deployed in studies such as the works in [23], [50], [57], [62]. With regards to feature vector decomposition modes, various authors have decomposed generated signal samples at various resolution levels to get wavelet coefficients that suits their classification specifications. Eristi and Demir [62] applied a 8-level wavelet decomposition to construct a nine-dimensional feature vector that suits their RBF kernel-based SVM classification study. Furthermore, at each decomposition level, different numbers of statistical methods such as standard deviation, mean, skewness, kurtosis, RMS, Shannon entropy, log energy entropy and norm entropy, etc. are calculated for feature vector which are used as the input vector for the MLT classification. Bosnic *et al.* [53] deployed mean, standard deviation, skewness, kurtosis, RMS, Shannon entropy, log energy entropy and norm entropy while Kanirajan and Kumar [63] used standard deviation, variance, norm, median, absolute deviation and mean absolute deviation as it suits the specification of their proposed classification models. For better performance, various authors have explored the use of multiple extraction techniques whereby the advantage of one signal processing tool is boosted by the ensemble partner. Using the combination of WT and MRA, Kanirajan and Kumar [63] argued that WT and MRA provides an excellent time frequency resolution as they provide a short window for high frequency components and long window for low frequency components. In a similar work involving two signal processing technique, Biswal *et al.* [64] used EMD to separate out intrinsic mode functions and applied HT on the intrinsic mode functions to extract instantaneous amplitude and frequency components.

2) PQD FEATURE SELECTION/OPTIMIZATION STAGE

In order to enhance the PQD event classification performances, various authors proposed the deployment of several feature selection/reduction and optimization techniques. The main objective of using these techniques is to eliminate redundant features such as noise in the extracted signals and to optimize the classifiers' performance accuracy [53]. Most feature selection methods for PQD feature vectors can be either wrapper based or filter based [49]. As explained Abdoos *et al.* [49] explained that wrapper based feature selection are time consuming but highly efficient while filter based are faster as they rank features based on intrinsic attributes. Ahila *et al.* [51] deployed a PSO based wrapper selection model to obtain the optimal number of hidden nodes and to select the beneficial subset of features in their PQD classification study. Despite the fact that the work in [50] did not deploy any feature selection method, the authors acknowledged that the use of optimization technique for feature selection creates better classification even though they may require huge computational resources, time and complex simulations. As a means to obtain optimal structure coupled with reduced feature vector dimension, Abdoos *et al.* [49] deployed sequential forward selection (SFS) and sequential backward selection (SBS) as wrapper based methods and Gram–Schmidt orthogonalization (GSO) as feature selection and optimization techniques respectively. Using the combinations, the authors were able to eliminate redundant features, reduce the computational cost and most importantly, improved the generalization capability of the deployed classifier in their PQD study. In a related work, Bosnic *et al.* [53] also deployed SFS to identify the most discriminative features in the PQD feature vector in their classification study. As GSO is well known for its numerical instability with respect to rounding error, Liquan *et al.* [57] opted for the highly rated particle swarm optimization (PSO) in optimizing the SVM parameters in their PQD classification study. In another work that involves the use of heuristic optimization technique, Khokhar *et al.* [23] used ABC algorithm to select optimal features in their PQD event classification study. In order to avoid combinational problems that are peculiar to some of the popular heuristic optimization techniques, the authors in [65] used ant colony optimization (ACO) as the feature selection/optimization technique in their PQD study. Similarly, Manimala *et al.* [54] used Genetic Algorithms (GA) and Simulated Annealing (SA) optimization techniques for the selection of the most dominant features for the SVM classifier deployed in their study.

3) CLASSIFICATION STAGE

In the literature, numerous machine learning and deep learning algorithms such as SVM [49], [53], [55], [57], [59], DT [64], [66], K-Means [67], various ANN types including Probabilistic Neural Network (PNN) [23], [68]–[70], Feed Forward Neural Network (FFNN) [51], [61], Radial basis function network (RBFNN) [63], [67] and deep neural networks such as Convolutional Neural Network (CNN) [22], [52], etc. have been employed in PQD classification. However, despite the numerous varieties of classifiers' proposed for PQD classification, SVM and PNN are the most widely deployed, owing to some of their attributes that makes them highly suitable for PQD classifications. Being a derivation of Bayesian and kernel fisher discriminant analysis algorithm, PNN are well known for their high accuracy and excellent classification performance in studies involving signal outliers. Khokhar *et al.* [23] and Huang *et al.* [69] explained that PNN is highly efficient in classifying PQD events as they do not require initial weight settings compared to other neural network models such as FFNN and RBFNN. Also, as a technique that is based on the Vapnik–Chervonenkis dimension theory of Statistical Learning Theory and structural risk minimization principle, SVM is highly rated as a powerful classifier. Various authors in the literature

have successfully deployed SVM in numerous power system studies. Abdoos *et al.* [49] used a RBF kernel SVM for classifying PQD events. In the study, the authors used improved ant colony optimization algorithm to determine the parameters of the RBF kernel. Eristi and Demir [62] also deployed RBF kernel SVM as the authors argued that the kernel type can behave like a linear kernel or a sigmoid kernel under different parameter settings. In a comparative study conducted in [54], the authors compared the result of rbf kernel SVM and polynomial kernel SVM. The authors achieved a better classification accuracy with RBF kernel compared to polynomial kernel. However, in another comparative study on a developed model involving three classifiers (DT, k-nearest neighbors (KNN) and SVM), Singh and Singh [65] adjudged DT as the most effective classifier as it presented the best result in terms of accuracy and classification time. In a work that involves neural network, Kanirajan and Kumar [63] deployed Gaussian functions for their RBFNN. In the study, the authors varied the weight by updating it at every iteration so as to boost the classification accuracy.

4) COMPARISON AND DISCUSSIONS OF MLT FOR PQD CLASSIFICATION

In Table 1, we summarize some recent works that involved the deployment of MLTs in the detection and classification of PQD events. The feature extraction techniques, optimization/feature selection technique(s) adopted and machine learning algorithm(s) that the authors deployed in the classification of PQD events are presented. As shown in Table 1, the ideas of MLT approaches to PQD events detection and classifications have been hugely successful. Furthermore, it can be observed from Table 1 that the most adopted machine learning tools is the SVM as it guarantees efficiency and high accuracy. In addition, it can be observed that the integrations of optimization techniques have positive influences on the classification results.

B. MLTs FOR SCADA NETWORK VULNERABILITIES AND THREATS

The widespread cyber presence especially in the form of advanced communication gadgets and IoT deployments in today's SCADA network have raised the power system's vulnerabilities to security threats, attacks and intrusions that conventional security measures such as whitelisting, encryption algorithms, authentication, antivirus programs, firewalls, traditional IDS, etc. are incapacitated as mitigation strategies [45], [71], [72]. In the past decade, the world have witnessed how various forms of cyberattacks on SCADA network have geometrically increased [3], [45]. It is increasingly imperative to devise effective IDSs that can efficiently detect attacks and intrusions in early stages. The ability of MLTs in autonomously learning, adapting to variations and acting without being pre-programmed have enhanced their reputation as credible methodologies for intelligent and efficient IDSs in recent times. Traditionally, MLTs approach for SCADA network IDSs involve three major stages: (1) dataset generation, (2) Data Preprocessing and (3) Classification/ Detection.

1) DATASET GENERATION STAGE

Traditionally, for an intruder to compromise a SCADA network, it is predictable that the intruder will somehow create a footprint or disruption no matter how marginal. SCADA network attack mitigation using MLTs involves the capture and analysis of SCADA network data traffic to build a training and testing dataset. Even though communication between SCADA components can be performed by different network protocols, the most widely deployed in the literature is the MODBUS over TCP/IP [3], [28], [45]. However, due to the unavailability of real-time SCADA dataset, researchers make use of publicly available datasets such as the simulated Mississippi State University (MSU) SCADA laboratory gas pipeline dataset [28], [73], [74] and KDD99 dataset [75]. Other notable public dataset include the cybergym dataset [3], UC Irvine machine learning repository dataset [73] and the University of Arkansas's National Center for Reliable Electric Power Transmission (NCREPT) testbed dataset [72]. It is worth mentioning that some authors such as Shitharth [76] and Gao *et al.* [45] simulated SCADA testbeds in their classification studies. Shitharth [76] designed a SCADA network structures that comprises of 100 sensor nodes using Network Simulator 2 to generate the SCADA datasets.

In a similar study, Gao *et al.* [45] simulated a SCADA testbed using virtual host Nova as MODBUS master and PLC by HoneyD as slaves to generate two separate datasets. In order to have a balanced dataset for the classifiers' training and evaluation, some intrusive actions in form of cyberattacks are usually integrated into the simulated testbeds. Typical intrusive attacks into SCADA testbeds including command injection, response injection and denial of service attack, man-in-the-middle attack, etc. are usually incorporated into the simulated testbed [3], [33], [46]. Sufficient network traffic that contains both normal traffic and the abnormal traffic (due to the intrusion) are captured as dataset for data preprocessing.

2) DATA PREPROCESSING STAGE

Preprocessing processes such as feature reduction, selection/ extraction, mapping and scaling are highly important for efficient SCADA intrusion classification [3], [74], [77]. The main purpose of deploying these preprocessing techniques is to have a well-organized dataset that can be used for efficient training, testing and validation at the classification stage. According to Ullah and Mahmoud [74], the preprocessing procedures assist in removing irrelevant and redundant features which can cause overfitting, skew predictions and misclassification. The preprocessing techniques also have positive influences on the classifications' computation time. Various preprocessing techniques such as categorical labelling, cleaning, scaling, extraction, selection, standardization and normalization are typically deployed on raw collected SCADA network dataset. To reduce the dimension

TABLE 1. Comparison of recently proposed MLT based approaches for PQD event classification using MLT.

Ref.	Feature extraction technique	Machine Learning Algorithm	Optimization/Feature selection technique	Accuracy achieved	Brief summary of the work's methodology
[49]	VMD + ST	SVM	SBS/SFS/ GSO	99.66%	Large feature vector involving 9 classes of events. 3 decomposition modes used. Few tuning parameters used for VMD and ST. SBS gave the best accuracy. Robust algorithm with good result in noisy environment.
[50]	DWT + MRA	SVM	-	94%	Used small dataset, Gaussian kernel SVM for feature mapping & classification, DB4 at 8-level of decomposition, Extracted features of energy, entropy & standard deviation. 27 dimensions of features, Limitation- algorithm was not used on large scale dataset and it may not yield good result with large data
[57]	WT	SVM	PSO	95.83%	DB4 wavelet as mother wavelet, 8 feature vectors as classifier input, PSO to optimize SVM classifier parameter. RBF kernel to classify wavelet energy difference. The RBF kernel function performed better compared to single kernel function
[23]	WT	PNN	ABC	99.875%	Used ABC for optimization as it converges rapidly, it has good memory, etc. PNN was used to select dominant features and spread constants and the selected features are evaluated using RBF and MLPNN. Limitation- some aspect of PQD such as inter-harmonic disturbances were not used in the study
[52]	CT	CNN	SSA	99.52%	Wrapping method used for extraction. Lag-covariance matrix of PQD waveform was constructed using trajectory matrix algorithm. CT and MSSA were used for waveform decomposition into 6 different levels. 6 frequency bands are used as features. Dropout technique to avoid overfitting, ReLu for CNN activation. Robust algorithm with excellent results even in noisy conditions.
[51]	WT	ELM	PSO	97.60%	Wrapping method of extraction based on PSO. Wavelet energy criterion used. DB4 used. Sampled signals decomposed with 13-level MRA.
[53]	WT	ECOC-SVM	SFS	98.69%	Voltage disturbance generated data used. WT used to decompose at 6-levels. 8 statistical methods to extract features. 200 instances for training and testing of SVM-ECOC classifier. Robust algorithm in noisy and noiseless conditions
[54]	WPT	SVM	GA	98.33%	WPT used to decompose at 4-levels. GA and SA to select dominant features out of 128 features for the RBF kernel SVM. 10-Fold validation used during evaluation.
[62]	WMRA	SVM	-	99.71%	ATP/EMTP used to generate PQ events. WMRA was used to extract features of a 3-phase voltage waveform. DB4 used. Data preprocessing involving normalization used. 10fold cross validation of SVM for kernel and penalty parameter were done during classification.
[67]	HHT	RBFNN	-	94%	HT and some statistical methods were used for extraction into real and imaginary features. During training, K-Means was first used for clustering. Algorithm performs well in noiseless environment
[64]	EMD+HT	BNT	-	97.90%	EMD was used to separate non-imaginary signal patterns into IMFs and also performs sifting. HT was used to extract amplitude and frequency feature patterns from the IMF. SD and entropy were taken as features for classification using BNT.
[63]	WT	RBFNN	PSO	97.85%	20 types of PQD events deployed. DB4 and symlet used. 4-level of decomposition used for analysis. Gaussian function used during classification. Classification result compared with FFML, LVQ, GRNN and PNN.
[70]	EMD+HT	RBFNN	PSO	97.85%	EMD was used to separate features into IMF. HT was applied to the first 3 IMF to acquire amplitude and phase that were used for feature vector construction. PNN was used for mapping and classification.

of dataset, Khan *et al.* [78] used PCA, CCA and ICA. To improve on the reduced data features, Khan *et al.* [78] further used bloom filter and AllKNN for balancing and re-sampling of the dataset deployed in their study. In a similar study, Mansouri *et al.* [73] deployed, PCA, ICA, GHA, SVD and SOM for dimension reduction to boost the NN

classification accuracy in their SCADA security study. With regards to feature extraction procedures, Kalech [3] deployed five feature extraction methods including feature extraction based on function code and feature extraction based on time factor, etc. In a related work, Wang *et al.* [75] deployed information gain for ranking dataset feature and for selecting dominant features before utilizing SVD to obtain a low-dimensional approximation of the original feature. Ullah and Mahmoud [74] also used information gain for ranking features, InfoGainAtributeEval as evaluator and ranker as search method and filter based approach for feature selection. In another related work, Perez *et al.* [28] used Gaussian Mixture Model (GMM), K-means cluster, Zero imputation & indicators and forward-filling techniques as data cleaning methods in their SCADA IDS study.

3) DETECTION AND CLASSIFICATION STAGE

Various MLTs such as SVM [28], [32], [77], K-Nearest Neighbour [78], [79], LR [75], various neural networks and deep neural networks including CNN [72], RNN [30], [45], etc. have been extensively deployed for SCADA network monitoring, intrusion prediction, detection and classification studies in recent times. Logically, most SCADA IDS models are binary classification, which makes them well suited for SVM models. Hence, numerous forms of SVM models have been proposed in the literature. Jiang and Yasakethu [32] and Maglaras and Jiang [80] successfully deployed K-Means clustered OCSVM in classifying data as normal and flagging the anomalies into clusters. Explaining the choice of OCSVM as the classifier deployed in their study, Maglaras and Jiang [77] argued that unlike several other MLTs, OCSVM do not need any labeled data for training. Hence making it ideal in SCADA IDS environment. In a similar study that adopted OCSVM, the author in [77] successfully used a RBF kernel for training the developed OCSVM classifier. In a comparative study, Da Silva *et al.* [81] compared the result of OCSVM with SVDD models in successfully detecting SCADA system cyberattacks. The authors revealed that both algorithms are well suited for the classification task. Another prominent machine learning algorithm that is well recognized in SCADA network IDS literature is the neural network models. Kalech [3] described the efficacy of SOM by combining it with HMM in successfully detecting temporal patterns on two different MODBUS datasets. In a related approach, Shitharith [76] deployed IWP-CSO in optimizing the input features for a Hierarchical neuron architecture based neural network (HNA-NN) classification model.

Several authors in the literature ensemble multiple machine learning algorithms as the limitation of one algorithm can be boosted by its partner thereby creating better classification algorithms that offer improved performances and robustness. Nader *et al.* [33] ensemble SVDD and KPCA for classifying intrusion on the MSU dataset. In a related work, the authors in [82] successfully deployed CNN and RNN for cyberattacks detection using a SWAT dataset. Also, Gao *et al.* [45] ensemble LSTM-RNN and FNN for detecting cyberattacks on a simulated SCADA testbed.

In order to identify which machine learning algorithm is better suited for a particular dataset, several authors explored different machine learning algorithms on the same dataset. Beaver *et al.* [83] explored the feasibility of different algorithms including NB, SVM, RF, OneR, J48, NNge in detecting command and data attack injections into SCADA network. From the achieved result, the authors acknowledged NNge and RF as the best performers compared to the other models. In a similar study, Qu *et al.* [84] deployed some supervised learning models including DT, KNN, SVM, RF, LR and OCSVM for SCADA network traffic IDS. From the result, the authors acknowledged OCSVM as the best performer. In a similar comparative study, Perez *et al.* [28] compared the performance of SVM and RF using Mean, standard deviation and min-max approaches in classifying both binary and a 7-class dataset that contains 20 features of MODBUS packet datasets.

4) COMPARISON AND DISCUSSIONS OF MLT APPROACH FOR SCADA NETWORK IDS

Table 2 presents the summary of some recent research works that deployed the use of MLTs for SCADA network intrusion detection schemes. In Table 2, we present a summarized description of the dataset simulation/deployed, the data preprocessing/ optimization technique(s) adopted and the machine learning algorithm(s) that some authors in recent literature deployed in the classification of SCADA dataset.

As shown in Table 2, the deployment of machine learning algorithms for SCADA network intrusion detection and classification studies have been successful. From Table 2, the accuracy achieved explained that most of the attacks that were integrated into the various systems have been reliably detected or classified. However, as most research works depend solely on simulated testbeds and open source datasets, most of the proposed schemes cannot be used to efficiently evaluate the potency of the model in practical real life systems.

C. MLTs FOR TSA

Power system stability monitoring and assessment with regards to its operation positioning neat stability margins is highly important for the efficient operation of the infrastructure [85]. The conventional TSA methods are computationally incompetent in handling large scale modern power system due to the enormous data involved. A report stated that an estimated 2500 PMU devices was installed in Chinese North Interconnection and each of them records more than 30 features every 20 milliseconds [84]. With such huge amount of data collected at high speed, using conventional TSA methods including time domain simulation and transient energy function alone are computationally intensive and may not meet the requirements of modern-day real-time TSA. Researchers in recent times have therefore turned to MLT, RL, DL and DRL approaches. These learning

TABLE 2. Comparison of recently proposed MLT based approaches for SCADA network protection.

Ref.	Dataset deployed	Data preprocessing/ Optimization techniques	Machine learning algorithm	Accuracy achieved	Brief summary of the work's methodology
[45]	Simulated Testbed	FE	FNN +LSTM	99.76%	Simulated SCADA testbed to generate 2 MODBUS datasets using virtual host Kali and PLC by HoneyD. Defense Wall was used to extract 19 features. Feature scaling was done using mean and standard deviation. Keras Tensorflow for MLT implementation. AdamOptimizer was used for training and softmax cross entropy was used as the loss function.
[28]	MSU data	FE	SVM-RF	99.58%	MSU gas pipeline data containing 274,628 instances with 20 features of MODBUS packets was used. Data cleaning done using GMM, K-Means, zero imputation & Indicators and Keep prior value. Mean, standard deviation and min-max methods were used as data transformation methods. Keras Tensorflow and Scikit Learn was used for classifier implementation.
[77]	Simulated data	RBF Kernel	OCSVM	98.87%	Model trained offline using network traces after data were extracted from a network dataset. Data scaling and mapping into numerical variables were done as preprocessing methods. RBF-kernel used.
[3]	Cyber-gym data and BGU data	FE	HMM-ANN	-	Five feature extraction methods including function code, time factor etc., used. The SOM-ANN algorithm was built using 100 neurons. The model showed excellent result on both datasets.
[76]	KDD 99	IWP-CSO	HNA-NN	93.1%	Designed network structure using NS2. The model comprises of 100 sensor nodes to generate packet data. IWP-CSO was used for feature optimization of the HNA-NN classifier. MATLAB was used for the classifier's implementation.
[33]	MSU data	FE	SVDD/KPCA	-	MSU gas pipeline data involving 6 different cyberattacks scenarios. 5 fold cross validation was used for the optimization of the parameters of the classifier.
[78]	MSU data	PCA, CCA, ICA, AllKNN	Boom filter + KNN	97%	MSU gas pipeline data involving 35 different cyberattacks scenarios. Categorical labelling, data normalization, dimension reduction balancing and re-sampling of data were all performed during preprocessing. RF, AdaBoost, MLPNN and QDA were used for training dataset. 10-fold cross validation used. Proposed method gave the best result in comparison with other methods.
[74]	MSU data	InfoGainAttributeEval	Bayes-Net +J48	99.5%	MSI gas pipeline data used. InfoGainAttributeEval was used as evaluator and ranker for feature processing. 5-fold validation was used for evaluation.
[73]	MSU data	PCA, ICA, GHA, SVD, SOM	MLPNN	97.5%	MSI gas pipeline dataset containing 3 categories of features used. Data contains 97019 samples out of which 96019 samples was used for training and the rest was used for testing. Feature reduction was done using PCA, ICA, GHA and SOM. Also, Greywolf algorithm was used for training the NN model. 10-fold cross validation was done. The result of the proposed model was compared with 24 other ML approach and the proposed model gave the best result.

techniques have been heavily deployed in recent studies peculiar to power system control problems including TSA studies. Different from conventional methods, these techniques have the capacity to process large amounts of PMU data, analyze them and classify the corresponding stability state of a system accordingly [86]. Malbasa *et al*. [87] explained that machine learning approach has the generalization ability whereby properly trained data-based model can make accurate stability predictions. The rest of this subsection first described the steps of MLTs approach to TSA. The subsection also briefly described a review of RL, DL and DRL approaches to TSA. With regards to MLTs approach, the steps for conventional methodologies are: feature generation, preprocessing and classification/prediction.

1) FEATURE GENERATION

The generation of input vector sets is identified as the first and the most important step in establishing reliable TSA model analysis [88]. Widespread use of phasor measurement units (PMU)- based wide area measurement system (WAMS) have assisted in the acquisition of synchronized measurements thus allowing the possibility of implementing advanced wide-area protection, decision making and control operations. Synchronously sampled power system variables provided by phasor measurement units (PMUs) collected before and/or immediately after clearing a fault have been utilized as data samples for TSA studies in numerous literature [89]–[92]. As the selection of the appropriate features is an important criteria for TSA, most studies involving MLT

approach to TSA usually resort to the generation/extraction of these feature sample data through TDS processes [89], [91], [93], [94]. As explained by Mosavi *et al.* [85], one major concern in TSA studies is the selection of proper trajectory features. In numerous studies, different trajectories such as terminal voltage amplitudes, rotor variables including angles and rotor speed [91], [95], [96] are used as predictors to judge whether the system is stable or not. Using a different approach to TDS, He *et al.* [97] utilized pattern identification strategy using dominant instability generator grouping based on shortest path algorithm for selecting input features. Similarly, Zhou *et al.* [5] used bootstrapping technique to generate dataset samples for the proposed prediction algorithm in their TSA study. To generate input data for their algorithm, Mosavi *et al.* [85] used a set of size and type independent trajectory features (s&tIFs) that measures suitable awareness level of the network status and its distance from instability.

2) FEATURE PREPROCESSING AND OPTIMIZATION

In order to remove redundancies and improve classification and prediction of transient instability, various authors have proposed numerous feature reduction, selection and optimization techniques that fits the type of datasets and classification algorithms they proposed. In the TSA study conducted by Li and Yang [90] using PMU post fault data, the authors were able to reduce the features of their dataset to one-third using binary jaya feature selection technique. In a similar study, Li *et al.* [94] deployed a feature selection method based on kernelized fuzzy rough sets (KFRS) and memetic algorithm. Also, the authors in [98] chose Sequential Forward Selection (SFS) as feature selection method for their proposed TSA algorithm. In another related work, Zhang *et al.* [99] argued that PSO has better optimization ability and better searching efficiency compared to other conventional optimization techniques, hence the authors deployed PSO in the ELM prediction based TSA study.

3) CLASSIFICATION/PREDICTION

Usually, MLT based TSA studies in the literature usually adopt the 'offline training, online application' model [95], [99] whereby the training model is performed offline and the TSA testing is done online. In order to minimize misclassification cost, He *et al.* [100] deployed boosting algorithms to build the classification model as a weighted voting of multiple DTs. In another study, Wang *et al.* [86] used core vector machines for its offline training procedure. In a similar study, Mahdi and Genc [101] used a generated dataset to train a multilayer perceptron offline before it was deployed for online TSA testing. In most recent studies in the literature, the testing of the various proposed schemes for transient stability studies are conducted using the IEEE 39-bus test system popularly known as the New England test system [5], [89]–[91], [96]. Various generators and loads variation are usually modelled, with various considered contingencies which include three-phase to ground short-circuit faults etc. and fault clearing times are varied in cycles. Despite the numerous success that have been achieved using the 'offline training, online application' model', Li and Yang [90] argued that the 'offline training, online application' is inapplicable in the real world as offline generated training sets cannot exhibit all the attributes expected of the time-varying modern power system. Furthermore, the authors explained that when a model is not satisfied with some of the sample data during the online application, the offline training is conducted all over.

Historically, since Sobajic and Pao [102] employed ANN for critical fault clearing 30 years ago, numerous authors have deployed varieties of ANN for successful TSA classifications [96], [103]. Notably, some other MLTs such as SVM [5], [95], KNN [97], DT [92], Bayesian [91], etc. have also been successfully deployed for TSA classifications in the literature. Owing to its capability to map nonlinear relationship between inputs and outputs, Lin [103] claimed that neural networks are superb classifiers for transient stability studies as their outcomes can be continuous such that the margins and boundaries for transient stability can appear smoother. Conversely, He *et al.* [100] argued that DTs are excellent choices for building online DSA classifier as they have good interpretability which makes them well suited for TSA studies. Similarly, Kamwa *et al.* [104] also explained that DTs are good classifiers as they perform well with regards to cluster problems. As a viable alternative, the application of SVM for TSA studies have been mentioned repeatedly in the literature. Supporting the motion that SVM are excellent classifiers for TSA, Zhou *et al.* [5] explained that apart from the good prediction guaranteed using SVM, SVM can calculate the ''distance'' between an instance and stable boundary, which can be further used to define the confidence index. However, Tian *et al.* [105] clarified that despite the numerous advantages that SVM brings, their deficiency lies with the parameter selection and a wrong choice will result in poor classification. On the other hand, Random forest based TSA is another area that is showing a lot of promise as RF models can calculate feature weights and sort features in ranking order according to the weights [93]. Compared to other learning algorithms, the authors in [106] and [107] explained that ELM has superb generalization performance with quicker learning speed. Also, the authors in [36] used LSTM in their TSA study.

As ensemble paradigm are known to present more accurate classification models compared to single MLTs, Zhou *et al.* [5] and Yuanhang *et al.* [108] presented ensemble classifiers using multiple SVMs. In a related TSA work that involves ensemble approach, Xu *et al*. [109] used an ensemble structures of multiple ELMs for TSA training and classification. Deploying a different approach. Baltas *et al.* [88] presented a comparative study using three different algorithms

(DT, SVM and ANN) with the aim of suggesting which algorithms is more suited for the deployed data.

4) REVIEW OF RL AND DRL APPROACHES TO TSA

The past few years have seen increasing efforts concentrated on the application of RL and DRL in various decision making and control problems such as power system studies most especially with regards to TSA and emergency control [47], [99]. As explained by Yang *et al.* [110], the modelling of RL is synonymous to the process of human learning knowledge. Thus, RL algorithms do not necessarily require the complete dynamics of an environment in order to learn, they can learn self-improvement sorely by judging the feedback from its own experience in the environment. Various power system security and stability devices such as power system stabilizer have been modelled based on RL algorithms. Similarly, Glavic [111] designed a resistive brake controller that is based on RL algorithm. According to the authors in [47], the architectural structure of the application of RL in power system stability and control studies involves two stages namely: learning and execution. While the learning stage refers to the usual RL implementation, the execution stage deploy the knowledge acquired from the learning stage for decision making. As TSA crisis can be considered as a wide-area control systems' (WAC) crisis, Druet *et al*. [112] investigated the deployment of RL using Monte Carlo control to define the switching control law for tripping generators in order to avoid loss of synchronism.

However, due to scalability challenges, traditional RL algorithms struggle especially with regards to large scale power system. As viable alternatives, RL have been combined with DL to form DRL algorithms which can implement varieties of tasks requiring high dimensional raw input and policy control [48]. As explained in [113] the rise of DRL is linked to the evolution of the powerful deep neural networks. The authors in [114]–[116] designed various Wide Area Control (WAC) strategies to boost transient stability using various RL and DRL methods. Using a modified IEEE 68 bus as test system, Yousefian *et al.* [116] proposed a WAC design using RL and NN, which optimizes the closed-loop performance of a wind integrated power grid through Approximate Dynamic Programming (ADP). From the simulation result achieved, the authors were able to provide transient stability index which guarantees the system's convergence to post-fault equilibrium. Similarly, Zhang *et al.* [89] used RBM to extract trajectory cluster features which as set as inputs for a DBN classifier.

5) COMPARISON AND DISCUSSIONS OF MLT APPROACH FOR TRANSIENT STABILITY ASSESSMENT

Table 3 presents the summary of some recent research works that deployed the use of MLTs for TSA. In Table 3, we present a summarized description of the test system, the preprocessing/optimization technique(s) adopted and machine learning algorithm(s) that some authors in recent literature deployed in TSA studies.

D. MLTs FOR VOLTAGE STABILITY ASSESSMENT

Various blackout events have shown how crucial the management of reactive power and more importantly the monitoring and evaluation of voltage stability status is a key issue for maintaining global stability of modern power system [117], [118]. Conventional methods of analyzing voltage stability such as the calculation of the P-V and Q-V curves at selected load buses using numerous numbers of load flows in traditional models have shown worrying limitations [43].

Sajan *et al.* [119] and Velayati *et al.* [117] explained that, apart from the fact that some of the traditional methods disregard the dynamic behaviors of modern power system, the methods require comparatively large computations [120] and they do not provide a detailed practical information on the stability problems [43]. In recent years, the use of MLTs have been identified as a promising alternative for overcoming the various shortfalls of the conventional voltage stability methods [118], [121]. The process of MLT approach to VSA is divided into two main stages.

1) FEATURE GENERATION AND SELECTION PROCESS

As explained by Goh *et al.* [43], power system can be classified as being in the voltage stability region if it can maintain steady acceptable voltages at all buses in the system under normal operating conditions and after being subjected to a disturbance. Conventionally, the typical input vectors for MLT based VSA are retrieved as voltage phasor from PMUs.

Similar to TSA, the input vectors are usually used to train the classifier's algorithms mostly through offline training and the output vector is the Voltage Stability Margin Index (VSMI) [119], [120], [122]. Diao *et al.* [123] pre-trained a DT algorithm offline using a voltage security analysis conducted using the past representative and forecasted daily operating conditions that involves 29 different scenarios for an American Electric Power (AEP) test system. In the study, synchronized feature attributes are obtained in real time using PMU devices and compared with the offline thresholds determined by the DTs to assess stability status. As voltage stability monitoring models are highly nonlinear complex models with large volume of dataset involved, the need for feature selection and reduction is highly important. Mohammadi and Dehghani [124] explained that the large quantities of power system attributes are not appropriate to be used directly as classifier's inputs. Hence, several feature extraction methods have been proposed in the literature. In an effort to boost the efficiency and accuracy of a developed SVM based VSA approach, the authors in [125] deployed multi-objective optimization for the selection of features for the SVM training. Similarly, the authors in [124] deployed both PCA and correlation analysis techniques as feature reduction and feature selection technique respectively in their DT based voltage stability study. In another related study, Bahmanyar and Karami [6] reduced a developed ANN inputs significantly using GSO. In a similar study, Xu *et al.* [121] chose

TABLE 3. Comparison of recently proposed MLT based approaches for voltage stability TSA.

Ref.	Test system	Preprocessing and Optimization Techniques	Machine learning algorithm	Accuracy achieved	Brief summary of the work's methodology
[5]	New England 68 bus	Min-max normalization	Ensemble of SVM	100%	Feature generation using bootstrap sampling. 12900 samples containing 6739 stable and 6161 unstable sample generated. Min-Max normalization as preprocessing method. 5-fold cross validation of the ensemble classifiers involving multiple SVM.
[94]	New England 39 bus	KFRS, Memeric algorithm	ELM	95.2%	PMU data used. Feature selection was done using KFRS and memeric algorithm. The algorithm was tested using New England 39-bus system and the Southern Hubei province power system.
[85]	IEEE 24 bus	-	TSVMNN	86.27%	Size and type independent features trajectory was used as dataset. The features were used to generate 414 samples for training and testing. The deep neural network based TSVMNN was used to eliminate computational complexity of kernel tricks. Contingency samples of SAVNW, IEEE 24 and Brazilian test system were used for training while new England 39-bus system was used for testing.
[91]	New England 39 bus	-	Bayesian Multiple Kernel learning	98.18%	PMU data used. TDS simulation was performed to generate feature samples. Polynomial and Gaussian Kernel functions are used and compared. Results showed that the proposed method outperformed other ML models.
[90]	New England 39 bus and Liaoning province system	BinJaya FS	OS/ELM	98.24%	Post fault PMU data generated for study. Angle modulation for binary jaya feature selection deployed. The feature reduction reduced the dataset to one third of initial volume. Sigmoid function was used as activation function for the classifier.
[97]	West East Lines	-	KNN	90%	Deployed a steady state information such as topology and operating states as features. DIGG strategy was done to select input features based on shortest path algorithm. The model has an advantage of simple training process. KNN was used for clustering analysis.
[92]	New England 39 bus	-	DT	95.1%	PMU dataset involving post fault disturbance used. DT was used for classification. Results showed the robustness of the model
[89]	New England 39 bus	RBM	DBN	98.83%	PMU data used. 27 trajectory cluster features were extracted using RBM and they are used as model input. 4-fold validation was used during evaluation. Sigmoid activation function used. 4 layer of DBN deployed. Results showed the robustness of the model

RELIEF algorithm as the feature selection technique for a developed NNRW training.

Furthermore, to improve the accuracy, reduce generalization error and training time, various optimization techniques have been deployed to optimize machine learning parameters in VSA studies. Owing to its excellent performance with regards to generalization errors, GA has been widely deployed in the literature for VSA. While Sajan *et al.* [126] deployed GA to boost the performance of a modelled SVM parameter, the authors in [120] used GA to improve the parameter tuning of a modelled ANN. As an alternative to GA, the author in [119] opted for ICA for tuning the ANN meta-parameters in their VSA study. In another work, Jayasankar *et al.* [8] deployed linear optimization for the modelled FFBPN.

2) CLASSIFICATION OF VOLTAGE STABILITY MARGIN INDEX

Prominent machine learning algorithms such as NN [39], [119], [120], [122], [127] and DT [123], [124] have been deployed in various voltage stability studies most especially in predicting the voltage stability margin index (VSMI). Zhang *et al.* [41] explained that, by learning from a voltage-stable database, the nonlinear mapping relationship between the power system operating parameters (input) and the voltage stability margin (output) can be mined and reformulated efficiently using neural networks. Also, Jayasankar *et al.* [8] described the computation time for ANN as very small and it gives incredible VSMI accuracy values. However, ANN have limitations, Zhang *et al.* [41] argued that traditional neural networks learning algorithms usually suffer from excessive training and the parameter tuning can be worrisome, then leading to substandard generalization performance. As a viable alternative, ELM have been deployed by some authors as they can learn faster and predict VSMI more accurately. Velayati *et al.* [117] and Zhang *et al.* [41] successfully deployed ELM in classifying VSM. In a related study, while deploying NNRW for short term voltage instability problem, Xu *et al.* [121] argued that NNRW are better options compared to traditional NN as they have efficient tuning mechanisms which makes them highly

TABLE 4. Comparison of recently proposed MLT based approaches for voltage stability assessment.

Ref.	Test system	Preprocessing and Optimization Techniques	Machine learning algorithm	Accuracy achieved	Brief summary of the work's methodology
[43]	IEEE 9 bus and IEEE 14	-	FFBP	99.4%	System variable based VSI was used as it requires less computational time. The 6 line VSI implemented are Lmn index, LQP index, FVSI index, VCPI (power), VCPI (Loss) and LCPI index. The classifier made use of 2 layer FFNN with error back propagation.
[87]	WECC system	-	FFBP	90.01%	Synthetic data obtained using a simulated power system model was used. Three class data containing individual samples of 5078, 2540 and 2529 labelled OC was used to generate a total of 10147 samples was deployed for classification. 1000 sample each of the individual OC was taken as testing data. SVM, FFBP and RF was used for classification. RF gave the best result.
[123]	AEP system data	-	DT	95.45%	PMU data used. 29 Operating Condition (OC) generated which involves 163 contingencies to create 9454 sample set. Hourly updated DT are initially trained offline using features of past representative and forecasted 24hour OCs.
[121]	New England 39 bus	Relief algorithm	NNRW	99.2%	In a study focusing on STVS. various dynamic load components were modelled using PSS/E. PMU data used. Offline training was conducted using forecasted OC (a day ahead method) and the corresponding voltage collapse status for VSI was used for online testing. Relief algorithm was used to select the dominant 136 features. During online testing, classifiers are updated using latest OCs. 100 individual NNRW was used for the ensemble classifier model as it presents fast training speed.
[118]	IEEE 14 &30 bus	-K-Means	SVM	99%	Instead of using large number of OCs, offline identification of Voltage stability pattern was done using K-Means. Parameter choosing of online training of SVM was also done offline. Testing was done using updated SVM. CBGA and 5fold validation was done during evaluation.
[129]	IEEE 30 bus	CBR	PFDT	94%	IEEE 30 bus used for evaluation. 300 different load variations at each buses and the varying of real and reactive power were considered as contingencies. Probabilistic fuzzy decision tree and case based reasoning were used for predicting voltage stability

suited for VSM classification. As alternatives to various neural networks methods, numerous studies in the literature has successfully deployed DT for VSA studies. Mohammadi and Dehghani [124] clarified that, with regards to less dataset samples, DT has simpler splitting rules and performs excellently in online voltage assessment classification. Another possibility is the prospect of SVM for VSA studies. By using the same dataset, Sajan *et al.* [126] compared the results of an optimized SVM with two modelled neural network and conveniently achieved better result from the optimized SVM approach. In another comparative study involving SVM, neural network and Adaptive Neural Fuzzy Inference System (ANFIS) models in a load-ability margin estimation study, Suganyadevi and Babulal [128] achieved the best result from the developed SVM model.

3) COMPARISON AND DISCUSSIONS OF MLT APPROACH FOR VOLTAGE STABILITY ASSESSMENT

Table 4 presents the summary of some recent research works that deployed the use of MLTs for the prediction, monitoring and analysis of voltage stability assessment. Table 4 presents a summarized description of the test system employed, the data preprocessing/optimization technique(s) adopted, machine learning algorithm(s) that some authors in recent literature deployed in VSA studies.

V. RESEARCH GAPS AND FUTURE DIRECTIONS

Despite the astonishing accomplishments that have been achieved in the application of MLTs for power system security and stability studies, a number of challenges still remain unsolved. The prediction and detection accuracy of MLTs are known to depend majorly on the quality and quantity of the dataset and test systems employed. However, due to the non-availability and inadequacy of realistic power system data from real power stations and field devices, scholars and researchers have been restricted to the use of simulated datasets, open source datasets and the development of scalable testbeds which have shown inconsistency in predictions and classifications. Also, apart from the number of input dataset, another important factor that is peculiar to machine learning applications is the tuning of the parameters. The rigorous events performed in tuning the parameters so as to achieve desired results means the MLT approaches requires a high level of expert interaction and they can sometimes be time consuming. Furthermore, most articles in the literature usually assume that PMU data are complete, trustworthy and

available for online use. In the real world, the measurements may not always be available due to jamming, malfunctioning or even attacks.

With regards to MLT approaches to SCADA network intrusion mitigation, most research works typically train the developed algorithms using network traffic from open source datasets which mostly are outdated and are no longer relevant with regards to new cyberattack trends. With the high rate of newly developed sophisticated cyberattacks being witnessed worldwide, creating a solution to an outdated problem can be irrelevant.

Furthermore, the dependency on traditional schemes such as TDS for feature extractions in MLT based TSA is recognized as a strong determinant in TSA accuracy. However, being a conventional method, TDS is well-known for its computational complexity especially with regards to large scale power system. Better and faster means of feature extractions for machine learning approach to stability studies can be a focus for future research works.

Also, the issue of offline training and online testing that is peculiar with MLT based stability approach can be a huge liability. Conventionally, most research works deploy static post faults power flows for classifier training offline. However, it is well known that modern power system is robust and they have various measures in place to control, protect and restore the systems especially after suffering a disturbance. Therefore, class imbalance crisis cannot be overlooked as it is unrealistic to depend on only the static post fault data in evaluating the stability of the systems. The training samples generated during offline simulations may not be a relevant representation of the current or future status of the power system. Hence, deploying the offline training process may inevitably lead to a poor applicability of the trained model when it is deployed for online TSA testing.

Future research work on MLT based approach to power system security and stability menaces should focus on detailed validation of the approaches using large scale test system which have similar characteristics as modern power system.

TABLE 5. Definitions of all acronyms mentioned in the paper.

Abbreviations	
DBN	Deep Belief Network
DWT	Discrete Wavelet Transform
MRA	Multiresolution Analysis
WT	Wavelet Transform
CT	Curvelet Transform
HHT	Hilbert-Huang Transform
HT	Hilbert Transform
ABC	Artificial Bee Colony
SSA	Static Single Assignment
FFS	Forward Feature Selection
GA	Genetic Algorithm
ELM	Extreme Learning Machine
CCA	Canonical Correlation Analysis
ICA	Independent Component Analysis
TSVMNN	Twin convolutional support vector machine
SVD	Singular value decomposition
SOM	Self-Organizing Map Neural Network
OCSVM	One class support vector machine
ECOC-SVM	Error-correcting output code-support vector machine
SWAT	Secure Water Treatment testbed
LSTM	Long term short memory
IWP-CSO	Intrusion weighted Particle based Cuckoo Search Optimization
BNT	Balanced Neural Tree
NNRW	Neural Network with Random Weight
WPT	Wavelet Packet Transform
VMD	Variational Mode Decomposition
ST	S-Transform
PMU	Phasor Measurement Unit
EPRI	Electrical Power Research Institute
HNA-NN	Hierarchical Neuron Architecture Based Neural Network
DQN	Deep Q Net
LR	Logistic Regression
SVDD	Support Vector Data Description
KPCA	Kernel principal component analysis
IoT	Internet of Things
CI	Critical Infrastructure
TDS	Time domain simulation
DDPG	Deep Deterministic Policy Gradients
IM	Induction Motor
EMD	Empirical mode decomposition
FT	Fourier Transform
SARSA	State–Action–Reward–State–Action
FFBP	FeedForward BackPropagation

VI. CONCLUSION

In recent times, power system security and stability has been a major concern to all energy stakeholders especially the operators. Operators must be well equipped in timely recognition of potential intrusion, attacks, disturbances, and situational awareness. The deployment of conventional methods has shown flaws especially in terms of resiliency and adaptation to the trends of current and future power system. To address these problems, this paper presents a comprehensive review of the most recent MLT based approaches to addressing the dominant power system menaces: power quality disturbance, SCADA network vulnerability and threats, transient stability assessment and voltage stability assessment. Unlike many of the previously published works, the paper addresses the methodologies applied, the limitations, drawbacks and future directions of the most recent trends in MLT applications to power system security and stability solutions.

APPENDIX

Table 5 presents all the acronyms used in the paper.

REFERENCES

[1] G. N. Baltas, C. Perales-Gonzalez, P. Mazidi, F. Fernandez, and P. Rodriguez, "A novel ensemble approach for solving the transient stability classification problem," in *Proc. 7th Int. Conf. Renew. Energy Res. Appl. (ICRERA)*, Oct. 2018, pp. 1282–1286.

[2] O. A. Alimi, K. Ouahada, and A. M. Abu-Mahfouz, "Real time security assessment of the power system using a hybrid support vector machine and multilayer perceptron neural network algorithms," *Sustainability*, vol. 11, no. 13, p. 3586, Jun. 2019.

[3] M. Kalech, "Cyber-attack detection in SCADA systems using temporal pattern recognition techniques," *Comput. Secur.*, vol. 84, pp. 225–238, Jul. 2019.

[4] O. A. Alimi and K. Ouahada, "Security assessment of the smart grid: A review focusing on the NAN architecture," in *Proc. IEEE 7th Int. Conf. Adapt. Sci. Technol. (ICAST)*, Aug. 2018, pp. 1–8.
[5] Y. Zhou, J. Wu, Z. Yu, L. Ji, and L. Hao, "A hierarchical method for transient stability prediction of power systems using the confidence of a SVM-based ensemble classifier," *Energies*, vol. 9, no. 10, p. 778, Sep. 2016.
[6] A. R. Bahmanyar and A. Karami, "Power system voltage stability monitoring using artificial neural networks with a reduced set of inputs," *Int. J. Electr. Power Energy Syst.*, vol. 58, pp. 246–256, Jun. 2014.
[7] T. Chakravorti, N. R. Nayak, R. Bisoi, P. K. Dash, and L. Tripathy, "A new robust kernel ridge regression classifier for islanding and power quality disturbances in a multi distributed generation based microgrid," *Renew. Energy Focus*, vol. 28, pp. 78–99, Mar. 2019.
[8] V. Jayasankar, N. Kamaraj, and N. Vanaja, "Estimation of voltage stability index for power system employing artificial neural network technique and TCSC placement," *Neurocomputing*, vol. 73, nos. 16–18, pp. 3005–3011, Oct. 2010.
[9] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018.
[10] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.
[11] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2016.
[12] X. Wang, X. Luo, M. Zhang, and X. Guan, "Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers," *Int. J. Electr. Power Energy Syst.*, vol. 110, pp. 208–222, Sep. 2019.
[13] J. Zhang and X. Wang, "Quickest detection of time-varying false data injection attacks in dynamic linear regression models," 2018, *arXiv:1811.05423*. [Online]. Available: http://arxiv.org/abs/1811.05423
[14] Y. Huang, H. Li, K. A. Campbell, and Z. Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test," in *Proc. 45th Annu. Conf. Inf. Sci. Syst.*, Mar. 2011, pp. 1–6.
[15] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Comput. Secur.*, vol. 70, pp. 436–454, Sep. 2017.
[16] P. Glauner, J. A. Meira, P. Valtchev, R. State, and F. Bettinger, "The challenge of non-technical loss detection using artificial intelligence: A survey," 2016, *arXiv:1606.00626*. [Online]. Available: http://arxiv.org/abs/1606.00626
[17] K. S. Perera, Z. Aung, and W. L. Woon, "Machine learning techniques for supporting renewable energy generation and integration: A survey," in *Proc. Int. Workshop Data Anal. Renew. Energy Integr.*, 2014, pp. 81–96.
[18] M. K. Saini and R. Kapoor, "Classification of power quality events—A review," *Int. J. Electr. Power Energy Syst.*, vol. 43, no. 1, pp. 11–19, Dec. 2012.
[19] P. Kundur, N. J. Balu and M. G. Lauby, *Power System Stability and Control*. New York, NY, USA: McGraw-Hill, 19947.
[20] P. Jokar, N. Arianpoo, and V. C. M. Leung, "A survey on security issues in smart grids," *Secur. Commun. Netw.*, vol. 9, no. 3, pp. 262–273, Feb. 2016.
[21] W. U. Guangyu, J. Sun, and J. Chen, "A survey on the security of cyber-physical systems," *Control Theory Technol.*, vol. 14, no. 1, pp. 2–10, 2016.
[22] S. Wang and H. Chen, "A novel deep learning method for the classification of power quality disturbances using deep convolutional neural network," *Appl. Energy*, vol. 235, pp. 1126–1140, Feb. 2019.
[23] S. Khokhar, A. A. M. Zin, A. P. Memon, and A. S. Mokhtar, "A new optimal feature selection algorithm for classification of power quality disturbances using discrete wavelet transform and probabilistic neural network," *Measurement*, vol. 95, pp. 246–259, Jan. 2017.
[24] M. Lopez-Ramirez, L. Ledesma-Carrillo, E. Cabal-Yepez, C. Rodriguez-Donate, H. Miranda-Vidales, and A. Garcia-Perez, "EMD-based feature extraction for power quality disturbance classification using moments," *Energies*, vol. 9, no. 7, p. 565, Jul. 2016.
[25] M. Valtierra-Rodriguez, R. de Jesus Romero-Troncoso, R. A. Osornio-Rios, and A. Garcia-Perez, "Detection and classification of single and combined power quality disturbances using neural networks," *IEEE Trans. Ind. Electron.*, vol. 61, no. 5, pp. 2473–2482, May 2014.
[26] M. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "SCADA system testbed for cybersecurity research using machine learning approach," *Future Internet*, vol. 10, no. 8, p. 76, Aug. 2018.
[27] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *Proc. eCrime Researchers Summit*, 2010, pp. 1–9.
[28] R. Lopez Perez, F. Adamsky, R. Soua, and T. Engel, "Machine learning for reliable network attack detection in SCADA systems," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 633–638.
[29] E. Chikuni and M. Dondo, "Investigating the security of electrical power systems SCADA," in *Proc. AFRICON*, Sep. 2007, pp. 1–7.
[30] C. Feng, T. Li, and D. Chana, "Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2017, pp. 261–272.
[31] S. Parthasarathy and D. Kundur, "Bloom filter based intrusion detection for smart grid SCADA," in *Proc. 25th IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, Apr. 2012, pp. 1–6.
[32] J. Jiang and L. Yasakethu, "Anomaly detection via one class SVM for protection of SCADA systems," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Oct. 2013, pp. 82–88.
[33] P. Nader, P. Honeine, and P. Beauseroy, "Intrusion detection in SCADA systems using one-class classification," in *Proc. 21st Eur. Signal Process. Conf. (EUSIPCO)*, 2013, pp. 1–5.
[34] R. M. Lee, M. J. Assante, and T. Conway, "TLP: White analysis of the cyber attack on the Ukrainian power grid," E-ISAC, Washington, DC, USA, Tech. Rep., 2016. [Online]. Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
[35] A. Sharifian and S. Sharifian, "A new power system transient stability assessment method based on type-2 fuzzy neural network estimation," *Int. J. Electr. Power Energy Syst.*, vol. 64, pp. 71–87, Jan. 2015.
[36] J. J. Q. Yu, D. J. Hill, A. Y. S. Lam, J. Gu, and V. O. K. Li, "Intelligent time-adaptive transient stability assessment system," *IEEE Trans. Power Syst.*, vol. 33, no. 1, pp. 1049–1058, Jan. 2018.
[37] N. Amjady and S. F. Majedi, "Transient stability prediction by a hybrid intelligent system," *IEEE Trans. Power Syst.*, vol. 22, no. 3, pp. 1275–1283, Aug. 2007.
[38] J. J. Q. Yu, A. Y. S. Lam, D. J. Hill, and V. O. K. Li, "Delay aware intelligent transient stability assessment system," *IEEE Access*, vol. 5, pp. 17230–17239, 2017.
[39] S. I. Suliman and T. K. A. Rahman, "Artificial immune system based machine learning for voltage stability prediction in power system," in *Proc. 4th Int. Power Eng. Optim. Conf. (PEOCO)*, Jun. 2010, pp. 53–58.
[40] Z. Nie, D. Yang, V. Centeno, and K. D. Jones, "A PMU-based voltage security assessment framework using hoeffding-tree-based learning," in *Proc. 19th Int. Conf. Intell. Syst. Appl. Power Syst. (ISAP)*, Sep. 2017, pp. 1–6.
[41] R. Zhang, Y. Xu, Z. Yang Dong, P. Zhang, and K. Po Wong, "Voltage stability margin prediction by ensemble based extreme learning machine," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2013, pp. 1–5.
[42] O. B. Adewuyi, R. Shigenobu, K. Ooya, T. Senjyu, and A. M. Howlader, "Static voltage stability improvement with battery energy storage considering optimal control of active and reactive power injection," *Electr. Power Syst. Res.*, vol. 172, pp. 303–312, Jul. 2019.
[43] H. H. Goh, Q. S. Chua, S. W. Lee, B. C. Kok, K. C. Goh, and K. T. K. Teo, "Evaluation for voltage stability indices in power system using artificial neural network," *Procedia Eng.*, vol. 118, pp. 1127–1136, Jan. 2015.
[44] S. Johansson, "Long-term voltage stability in power systems-alleviating the impact of generator current limiters," Chalmers Univ. Technol., Gothenburg, Sweden, 1998.
[45] J. Gao, L. Gan, F. Buschendorf, L. Zhang, H. Liu, P. Li, X. Dong, and T. Lu, "Omni SCADA intrusion detection using deep learning algorithms," 2019, *arXiv:1908.01974*. [Online]. Available: http://arxiv.org/abs/1908.01974
[46] S. K. Sharma and X. Wang, "Toward massive machine type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 426–471, 1st Quart., 2020.

[47] M. Glavic, R. Fonteneau, and D. Ernst, "Reinforcement learning for electric power system decision and control: Past considerations and perspectives," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 6918–6927, Jul. 2017.

[48] D. Zhang, X. Han, and C. Deng, "Review on the research and practice of deep learning and reinforcement learning in smart grids," *CSEE J. Power Energy Syst.*, vol. 4, no. 3, pp. 362–370, Sep. 2018.

[49] A. A. Abdoos, P. K. Mianaei, and M. R. Ghadikolaei, "Combined VMD-SVM based feature selection method for classification of power quality events," *Appl. Soft Comput.*, vol. 38, pp. 637–646, Jan. 2016.

[50] F. Jandan, S. Khokhar, S. Abid, and F. Abbasi, "Recognition and classification of power quality disturbances by DWT-MRA and SVM classifier," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 3, pp. 368–377, 2019.

[51] R. Ahila, V. Sadasivam, and K. Manimala, "An integrated PSO for parameter determination and feature selection of ELM and its application in classification of power system disturbances," *Appl. Soft Comput.*, vol. 32, pp. 23–37, Jul. 2015.

[52] H. Liu, F. Hussain, Y. Shen, S. Arif, A. Nazir, and M. Abubakar, "Complex power quality disturbances classification via curvelet transform and deep learning," *Electr. Power Syst. Res.*, vol. 163, pp. 1–9, Oct. 2018.

[53] J. A. Bosnic, G. Petrovic, A. Putnik, and P. Mostarac, "Power quality disturbance classification based on wavelet transform and support vector machine," in *Proc. 11th Int. Conf. Meas.*, May 2017, pp. 9–13.

[54] K. Manimala, K. Selvi, and R. Ahila, "Optimization techniques for improving power quality data mining using wavelet packet based support vector machine," *Neurocomputing*, vol. 77, no. 1, pp. 36–47, Feb. 2012.

[55] Z. Liu, Y. Cui, and W. Li, "A classification method for complex power quality disturbances using EEMD and rank wavelet SVM," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1678–1685, Jul. 2015.

[56] U. Singh and S. N. Singh, "Application of fractional Fourier transform for classification of power quality disturbances," *IET Sci., Meas. Technol.*, vol. 11, no. 1, pp. 67–76, Jan. 2017.

[57] Z. Liquan, G. Meijiao, and W. Lin, "Classification of multiple power quality disturbances based on the improved SVM," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2017, pp. 2625–2628.

[58] C. Chunling, X. Tongyu, P. Zailin, and Y. Ye, "Power quality disturbances classification based on multi-class classification SVM," in *Proc. 2nd Int. Conf. Power Electron. Intell. Transp. Syst. (PEITS)*, Dec. 2009, pp. 290–294.

[59] D. De Yong, S. Bhowmik, and F. Magnago, "An effective power quality classifier using wavelet transform and support vector machines," *Expert Syst. Appl.*, vol. 42, nos. 15–16, pp. 6075–6081, Sep. 2015.

[60] S. Alshahrani, M. Abbod, B. Alamri, and G. Taylor, "Evaluation and classification of power quality disturbances based on discrete wavelet transform and artificial neural networks," in *Proc. 50th Int. Universities Power Eng. Conf. (UPEC)*, Sep. 2015, pp. 1–5.

[61] C. Naik, F. Hafiz, A. Swain, and A. K. Kar, "Classification of power quality events using wavelet packet transform and extreme learning machine," in *Proc. IEEE 2nd Annu. Southern Power Electron. Conf. (SPEC)*, Dec. 2016, pp. 1–6.

[62] H. Erişti and Y. Demir, "A new algorithm for automatic classification of power quality events based on wavelet transform and SVM," *Expert Syst. Appl.*, vol. 37, no. 6, pp. 4094–4102, Jun. 2010.

[63] P. Kanirajan and V. Suresh Kumar, "Power quality disturbance detection and classification using wavelet and RBFNN," *Appl. Soft Comput.*, vol. 35, pp. 470–481, Oct. 2015.

[64] B. Biswal, M. Biswal, S. Mishra, and R. Jalaja, "Automatic classification of power quality events using balanced neural tree," *IEEE Trans. Ind. Electron.*, vol. 61, no. 1, pp. 521–530, Jan. 2014.

[65] U. Singh and S. N. Singh, "A new optimal feature selection scheme for classification of power quality disturbances based on ant colony framework," *Appl. Soft Comput.*, vol. 74, pp. 216–225, Jan. 2019.

[66] M. Biswal and P. K. Dash, "Detection and characterization of multiple power quality disturbances with a fast S-transform and decision tree based classifier," *Digit. Signal Process.*, vol. 23, no. 4, pp. 1071–1083, Jul. 2013.

[67] T. Jayasree, D. Devaraj, and R. Sukanesh, "Power quality disturbance classification using Hilbert transform and RBF networks," *Neurocomputing*, vol. 73, nos. 7–9, pp. 1451–1456, Mar. 2010.

[68] R. Kumar, B. Singh, and D. T. Shahani, "Recognition of single-stage and multiple power quality events using Hilbert–Huang transform and probabilistic neural network," *Electric Power Compon. Syst.*, vol. 43, no. 6, pp. 607–619, Apr. 2015.

[69] N. Huang, D. Xu, X. Liu, and L. Lin, "Power quality disturbances classification based on S-transform and probabilistic neural network," *Neurocomputing*, vol. 98, pp. 12–23, Dec. 2012.

[70] S. Shukla, S. Mishra, and B. Singh, "Empirical-mode decomposition with Hilbert transform for power-quality assessment," *IEEE Trans. Power Del.*, vol. 24, no. 4, pp. 2159–2165, Oct. 2009.

[71] L. Zhou, C. Su, Z. Li, Z. Liu, and G. P. Hancke, "Automatic fine-grained access control in SCADA by machine learning," *Future Gener. Comput. Syst.*, vol. 93, pp. 548–559, Apr. 2019.

[72] H. Yang, L. Cheng, and M. C. Chuah, "Deep-learning-based network intrusion detection for SCADA systems," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–7.

[73] A. Mansouri, B. Majidi, and A. Shamisa, "Anomaly detection in industrial control systems using evolutionary-based optimization of neural networks," *Commun. Adv. Comput. Sci. Appl.*, vol. 2017, no. 1, pp. 49–55, 2017.

[74] I. Ullah and Q. H. Mahmoud, "A hybrid model for anomaly-based intrusion detection in SCADA networks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 2160–2167.

[75] H. Wang, T. Lu, X. Dong, P. Li, and M. Xie, "Hierarchical online intrusion detection for SCADA networks," 2016, *arXiv:1611.09418*. [Online]. Available: http://arxiv.org/abs/1611.09418

[76] S. Shitharth and W. D. Prince, "An enhanced optimization based algorithm for intrusion detection in SCADA network," *Comput. Secur.*, vol. 70, pp. 16–26, Sep. 2017.

[77] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," in *Proc. Sci. Inf. Conf.*, Aug. 2014, pp. 626–631.

[78] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," *IEEE Access*, vol. 7, pp. 89507–89521, 2019.

[79] A. Almalawi, X. Yu, Z. Tari, A. Fahad, and I. Khalil, "An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems," *Comput. Secur.*, vol. 46, pp. 94–110, Oct. 2014.

[80] L. A. Maglaras and J. Jiang, "OCSVM model combined with K-means recursive clustering for intrusion detection in SCADA systems," in *Proc. 10th Int. Conf. Heterogeneous Netw. Qual., Rel., Secur. Robustness*, Aug. 2014, pp. 133–134.

[81] E. G. da Silva, A. S. Da Silva, J. A. Wickboldt, P. Smith, L. Z. Granville, and A. Schaeffer-Filho, "A one-class NIDS for SDN-based SCADA systems," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jun. 2016, pp. 303–312.

[82] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *Proc. Workshop Cyber-Phys. Syst. Secur. PrivaCy (CPS-SPC)*, 2018, pp. 72–83.

[83] J. M. Beaver, R. C. Borges-Hink, and M. A. Buckner, "An evaluation of machine learning methods to detect malicious SCADA communications," in *Proc. 12th Int. Conf. Mach. Learn. Appl.*, Dec. 2013, pp. 54–59.

[84] H. Qu, J. Qin, W. Liu, and H. Chen, "Instruction detection in SCADA/modbus network based on machine learning," in *Proc. Int. Conf. Mach. Learn. Intell. Commun.*, 2017, pp. 437–454.

[85] A. B. Mosavi, A. Amiri, and S. H. Hosseini, "A learning framework for size and type independent transient stability prediction of power system using twin convolutional support vector machine," *IEEE Access*, vol. 6, pp. 69937–69947, 2018.

[86] B. Wang, B. Fang, Y. Wang, H. Liu, and Y. Liu, "Power system transient stability assessment based on big data and the core vector machine," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2561–2570, Sep. 2016.

[87] V. Malbasa, C. Zheng, P.-C. Chen, T. Popovic, and M. Kezunovic, "Voltage stability prediction using active machine learning," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 3117–3124, Nov. 2017.

[88] N. G. Baltas, P. Mazidi, J. Ma, F. de Asis Fernandez, and P. Rodriguez, "A comparative analysis of decision trees, support vector machines and artificial neural networks for on-line transient stability assessment," in *Proc. Int. Conf. Smart Energy Syst. Technol. (SEST)*, Sep. 2018, pp. 1–6.

[89] R. Zhang, J. Wu, M. Shao, B. Li, and Y. Lu, "Transient stability prediction of power systems based on deep belief networks," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, Oct. 2018, pp. 1–6.

[90] Y. Li and Z. Yang, "Application of EOS-ELM with binary Jaya-based feature selection to real-time transient stability assessment using PMU data," *IEEE Access*, vol. 5, pp. 23092–23101, 2017.

[91] X. Gu and Y. Li, "Bayesian multiple kernels learning-based transient stability assessment of power systems using synchronized measurements," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2013, pp. 1–5.

[92] Y. Yang, Y. Huang, J. Liu, Y. Liu, T. Liu, and Y. Xiang, "Measurement-based cell-DT method for power system transient stability classification," *CSEE J. Power Energy Syst.*, vol. 3, no. 3, pp. 278–285, Oct. 2017.
[93] C. Zhang, Y. Li, Z. Yu, and F. Tian, "Feature selection of power system transient stability assessment based on random forest and recursive feature elimination," in *Proc. IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Oct. 2016, pp. 1264–1268.
[94] Y. Li, G. Li, and Z. Wang, "Rule extraction based on extreme learning machine and an improved ant-miner algorithm for transient stability assessment," *PLoS ONE*, vol. 10, no. 6, Jun. 2015, Art. no. e0130814.
[95] W. Hu, Z. Lu, S. Wu, W. Zhang, Y. Dong, R. Yu, and B. Liu, "Real-time transient stability assessment in power system based on improved SVM," *J. Mod. Power Syst. Clean Energy*, vol. 7, no. 1, pp. 26–37, Jan. 2019.
[96] E. A. Frimpong, P. Y. Okyere, and J. Asumadu, "On-line determination of transient stability status using MLPNN," in *Proc. IEEE PES PowerAfrica*, Jun. 2017, pp. 23–27.
[97] C. He, L. Guan, and W. Mo, "A method for transient stability assessment based on pattern recognition," in *Proc. Int. Conf. Smart Grid Clean Energy Technol. (ICSGCE)*, Oct. 2016, pp. 343–347.
[98] S. Kalyani and K. S. Swarup, "Binary SVM approach for security assessment and classification in power systems," in *Proc. Annu. IEEE India Conf.*, Dec. 2009, pp. 1–4.
[99] Y. Zhang, T. Li, G. Na, G. Li, and Y. Li, "Optimized extreme learning machine for power system transient stability prediction using synchrophasors," *Math. Problems Eng.*, vol. 2015, Nov. 2015, Art. no. 529724.
[100] M. He, J. Zhang, and V. Vittal, "Robust online dynamic security assessment using adaptive ensemble decision-tree learning," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4089–4098, Nov. 2013.
[101] M. Mahdi and V. M. I. Genc, "Artificial neural network based algorithm for early prediction of transient stability using wide area measurements," in *Proc. 5th Int. Istanbul Smart Grid Cities Congr. Fair (ICSG)*, Apr. 2017, pp. 17–21.
[102] D. J. Sobajic and Y.-H. Pao, "Artificial neural-net based dynamic security assessment for electric power systems," *IEEE Trans. Power Syst.*, vol. 4, no. 1, pp. 220–228, Feb. 1989.
[103] Y.-J. Lin, "Comparison of CART- and MLP-based power system transient stability preventive control," *Int. J. Electr. Power Energy Syst.*, vol. 45, no. 1, pp. 129–136, Feb. 2013.
[104] I. Kamwa, S. R. Samantaray, and G. Joos, "Catastrophe predictors from ensemble decision-tree learning of wide-area severity indices," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 144–158, Sep. 2010.
[105] F. Tian, X. Zhou, Z. Yu, D. Shi, Y. Chen, and Y. Huang, "A preventive transient stability control method based on support vector machine," *Electr. Power Syst. Res.*, vol. 170, pp. 286–293, May 2019.
[106] Y. Li and X. Gu, "Power system transient stability assessment based on online sequential extreme learning machine," in *Proc. IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Dec. 2013, pp. 1–4.
[107] I. B. Sulistiawati, A. Priyadi, O. A. Qudsi, A. Soeprijanto, and N. Yorino, "Critical clearing time prediction within various loads for transient stability assessment by means of the extreme learning machine method," *Int. J. Electr. Power Energy Syst.*, vol. 77, pp. 345–352, May 2016.
[108] D. Yuanhang, C. Lei, Z. Weiling, and M. Yong, "Multi-support vector machine power system transient stability assessment based on relief algorithm," in *Proc. IEEE PES Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Nov. 2015, pp. 1–5.
[109] Y. Xu, Z. Y. Dong, J. H. Zhao, P. Zhang, and K. P. Wong, "A reliable intelligent system for real-time dynamic security assessment of power systems," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1253–1263, Aug. 2012.
[110] T. Yang, L. Zhao, W. Li, and A. Y. Zomaya, "Reinforcement learning in sustainable energy and electric systems: A survey," *Annu. Rev. Control*, vol. 49, pp. 145–163, Apr. 2020.
[111] M. Glavic, "Design of a resistive brake controller for power system stability enhancement using reinforcement learning," *IEEE Trans. Control Syst. Technol.*, vol. 13, no. 5, pp. 743–751, Sep. 2005.
[112] C. Druet, D. Ernst, and L. Wehenkel, "Application of reinforcement learning to electrical power system closed-loop emergency control," in *Proc. Eur. Conf. Princ. Data Mining Knowl. Discovery*, 2000, pp. 86–95.
[113] M. Glavic, "(Deep) reinforcement learning for electric power system control and related problems: A short review and perspectives," *Annu. Rev. Control*, vol. 48, pp. 22–35, Oct. 2019.
[114] R. Yousefian and S. Kamalasadan, "Energy function inspired value priority based global wide-area control of power grid," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 552–563, Mar. 2018.
[115] R. Yousefian and S. Kamalasadan, "A Lyapunov function based optimal hybrid power system controller for improved transient stability," *Electr. Power Syst. Res.*, vol. 137, pp. 6–15, Aug. 2016.
[116] R. Yousefian, R. Bhattarai, and S. Kamalasadan, "Transient stability enhancement of power grid with integrated wide area control of wind farms and synchronous generators," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4818–4831, Nov. 2017.
[117] M. H. Velayati, N. Amjady, and I. Khajevandi, "Prediction of dynamic voltage stability status based on hopf and limit induced bifurcations using extreme learning machine," *Int. J. Electr. Power Energy Syst.*, vol. 69, pp. 150–159, Jul. 2015.
[118] S. M. Pérez-Londoño, G. Olivar-Tost, and J. J. Mora-Florez, "Online determination of voltage stability weak areas for situational awareness improvement," *Electr. Power Syst. Res.*, vol. 145, pp. 112–121, Apr. 2017.
[119] K. Sajan, V. Kumar, and B. Tyagi, "ICA based artificial neural network model for voltage stability monitoring," in *Proc. TENCON IEEE Region 10 Conf.*, Nov. 2015, pp. 1–3.
[120] K. S. Sajan, B. Tyagi, and V. Kumar, "Genetic algorithm based artificial neural network model for voltage stability monitoring," in *Proc. 18th Nat. Power Syst. Conf. (NPSC)*, Dec. 2014, pp. 1–5.
[121] Y. Xu, R. Zhang, J. Zhao, Z. Y. Dong, D. Wang, H. Yang, and K. P. Wong, "Assessing short-term voltage stability of electric power systems by a hierarchical intelligent system," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1686–1696, Aug. 2016.
[122] S. Kamalasadan, D. Thukaram, and A. K. Srivastava, "A new intelligent algorithm for online voltage stability assessment and monitoring," *Int. J. Electr. Power Energy Syst.*, vol. 31, nos. 2–3, pp. 100–110, Feb. 2009.
[123] R. Diao, K. Sun, V. Vittal, R. J. O'Keefe, M. R. Richardson, N. Bhatt, D. Stradford, and S. K. Sarawgi, "Decision tree-based online voltage security assessment using PMU measurements," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 832–839, May 2009.
[124] H. Mohammadi and M. Dehghani, "PMU based voltage security assessment of power systems exploiting principal component analysis and decision trees," *Int. J. Electr. Power Energy Syst.*, vol. 64, pp. 655–663, Jan. 2015.
[125] H. Mohammadi, G. Khademi, M. Dehghani, and D. Simon, "Voltage stability assessment using multi-objective biogeography-based subset selection," *Int. J. Electr. Power Energy Syst.*, vol. 103, pp. 525–536, Dec. 2018.
[126] K. S. Sajan, V. Kumar, and B. Tyagi, "Genetic algorithm based support vector machine for on-line voltage stability monitoring," *Int. J. Electr. Power Energy Syst.*, vol. 73, pp. 200–208, Dec. 2015.
[127] A. Maiorano and M. Trovato, "A neural network-based tool for preventive control of voltage stability in multi-area power systems," *Neurocomputing*, vol. 23, nos. 1–3, pp. 161–176, Dec. 1998.
[128] M. Suganyadevi and C. Babulal, "Fast assessment of voltage stability margin of a power system," *J. Electr. Syst.*, vol. 10, no. 3, pp. 305–316, 2014.
[129] S. R. Nandanwar, M. L. Kolhe, S. B. Warkad, N. P. Patidar, and V. K. Singh, "Voltage security assessment by using PFDT and CBR methods in emerging power system," *Energy Procedia*, vol. 144, pp. 170–181, Jul. 2018.

OYENIYI AKEEM ALIMI (Member, IEEE) received the Bachelor of Technology degree (Hons.) in electronics and electrical engineering from the Ladoke Akintola University of Technology, Nigeria, in 2011, the Master of Technology degree in electrical engineering from the University of Johannesburg, South Africa, in 2017, where he is currently pursuing the Ph.D. degree. He has published some papers in reputable journals and conference proceedings. His current research interests include power systems security, energy management and optimization, smart grid, machine learning and data science, and data privacy and security. He is a member of remarkable professional organizations, which include the South African Institute of Electrical Engineers (SAIEE) and the Engineering Council of South Africa (ECSA).

KHMAIES OUAHADA (Senior Member, IEEE) received the B.Eng. degree from the University of Khartoum, Sudan, in 1995, and the M.Eng. and D.Eng. degrees from the University of Johannesburg, South Africa, in 2002 and 2009, respectively.

He was with Sudatel, Sudanese National Communications company. He is currently a Professor with the University of Johannesburg. He is also the Founder and the Chairman of the Centre for Smart Communications Systems, Faculty of Engineering and the Built Environment, University of Johannesburg. He is a rated researcher with the National Research Foundation, South Africa. His research interests include information theory, coding techniques, power-line communications, visible light communications, smart grid, energy demand management, renewable energy, wireless sensor networks, reverse engineering, and engineering education. He is a Senior Member of the IEEE Information Theory and Communications societies and SAIEE Society. He is also a member of the IEEE South Africa Information Theory Society Chapter.

ADNAN M. ABU-MAHFOUZ (Senior Member, IEEE) received the M.Eng. and Ph.D. degrees in computer engineering from the University of Pretoria. He is currently a Principal Researcher with the Council for Scientific and Industrial Research (CSIR), a Professor Extraordinaire with the Tshwane University of Technology, a Visiting Professor with the University of Johannesburg, and an Extraordinary Faculty Member with the University of Pretoria. He is also the Founder of the Smart Networks Collaboration Initiative that aims to develop efficient and secure networks for the future smart systems, such as smart cities, smart grid, and smart water grid. He has participated in the formulation of many large and multidisciplinary research and development successful proposals (Principal Investigator or main author/contributor). His research interests include wireless sensor and actuator networks, low-power wide area networks, software defined wireless sensor networks, cognitive radio, network security, network management, and sensor/actuator node development. He is a member of many the IEEE Technical Communities. He serves as an Associate Editor for IEEE Access, the IEEE Internet of Things, and the IEEE Transaction on Industrial Informatics.