Electrical Engineering (2021) 103:813–824
https://doi.org/10.1007/s00202-020-01118-z

ORIGINAL PAPER

Real-time dynamic security analysis of power systems using strategic PMU measurements and decision tree classification

Rituparna Mukherjee[1] · Abhinandan De[1]

Received: 16 February 2020 / Accepted: 1 October 2020 / Published online: 20 October 2020

Abstract

Fast and accurate online dynamic security analysis (DSA) is the key enabler for secure operation of modern power systems. Real-time assessment of the current power system operating state and increased awareness about plausible future insecurity can enable necessary operational and control measures to ensure secure operation. This paper proposes an ensemble decision tree (DT)-based online DSA method for large-scale interconnected power system networks using wide area measurement (WAMS) with phasor measurement units (PMU). A novel attribute selection method has been demonstrated for optimizing PMU installation at strategic buses in large-scale power networks. Multi-stage screening of the initial measurements has been done to minimize the data acquisition cost and computation overhead, which are the key challenges in real-time DSA. The ensemble DT classifier was trained offline using data from the operational model of the power system under different system loading and contingency conditions. The trained classifier provides online security assessment and classifies the power system's current operating state as secure or insecure based on real-time measurements of the key attributes by selective PMUs. The proposed scheme was tested on IEEE 118-bus system, and the results demonstrate that it has the potential to be used as a reliable online DSA method.

Keywords Power system transient stability · Dynamic security analysis · Pattern classification · Ensemble Decision Tree

1 Introduction

Modern power systems are often less secure than the systems of the past due to various reasons like operation of the power system near its security limits, unpredictable power transfer driven by market activities, increased intermittency due to integration of renewable energy sources and adoption of special protection systems and complex controls, which often result unusual system behaviour. Further, power systems recurrently experience disturbances like outage of generating units and other power supply equipment (contingencies), short-circuits in power transmission lines (faults) and combination of these events, which have the potential to risk power system security. Security analysis is therefore imperative to assess, how robust a system is, relative to large variety of severe, yet plausible disturbances [1]. Power system security studies can be broadly categorized as: static security analysis (SSA) and dynamic security analysis (DSA) [2]. Since change in operating condition (state) is imminent after any major contingency, it is important that the system finally settles to a new state of operation, which is stable. In SSA, transition to new stable operating state is presumably accomplished and the analysis is focused on assessment of whether any physical and/or security constraints were violated in the post-contingency steady-state operating condition [3]. However, in the event of a severe disturbance, fast transition to a new steady-state operating point is infeasible. This may result in quasi-stable system operation for substantially long duration of time, which can trigger unintended operation of system protection and control devices, eventually leading to cascaded tripping and outages and disrupting system security. Online dynamic security assessment (DSA) is one solution to ensure security of the power system in near real time [4, 5]. The major difficulty against online and real-time assessment of dynamic security is the computation complexity. Insecure states of operation of electric power system, which can potentially lead to large-scale blackouts, are often unique, and there is no single algorithm to effectively

✉ Rituparna Mukherjee
ritu.gnit1@gmail.com

[1] Department of Electrical Engineering, Indian Institute of Engineering Science and Technology, Shibpur, Howrah, West Bengal 711103, India

reveal such insecure conditions fast enough, to be useful in real-time security assessment. Therefore, there is an acute need for developing a fast and reliable method for real-time security monitoring and assessment of the current security level of large power systems.

1.1 Existing DSA methods

Nonlinear time-domain simulation (TDS) is considered one of the most accurate methods for dynamic security analysis under large disturbances (transient stability) [5]. The method requires mathematical modelling of a power system by sets of nonlinear time-domain differential/algebraic equations, which can represent the dynamic behaviour of the generators and other power system components. These equations are then solved using numerical integration methods to assess the dynamic behaviour of a system under credible sets of disturbances and to ascertain whether transient stability would be maintained or lost, for a given disturbance. The major criticism against TDS is the requirement of intensive time- and resource-consuming numerical integrations, making it difficult to use online. A recent work in [6], however, reported a novel methodology to calculate transient stability at the earliest time using TDS. Relative stability of a power system is often considered more important than assessing absolute stability. For example, degree of severity of a given contingency (contingency ranking) can be judged by its impact on system security relative to others. TDS can provide different metrics such as critical clearing times (CCTs), or maximum swing under different scenarios and these metrics can be used for calculating degree of severity of a given contingency. TDS method is computationally intensive, but still it is the most trusted method for DSA in the electric power industry at present [7, 8].

An alternative approach to transient stability analysis is the direct method, which uses transient energy function [9, 10] to determine the stability of the post-contingency operating point of a power system. The direct method is less computationally demanding compared to the numerical integration approach, but considered less accurate than TDS as it uses reduced order modelling of the post-contingency system. A recent approach in [11] generalized the idea of energy methods and extended the concept of energy function to a more general Lyapunov functions family (LFF) to alleviate some of the drawbacks of classical energy method. Until recent time, direct method used to be considered impractical for large-scale power system stability analysis. However, [12] reported a real-world application of direct methods for online DSA of large-scale power system. This evaluation study is the largest in terms of system size, involving 14,500-bus, 3000 generators.

Some pioneering research works in the late 1980s [3, 13] adopted artificial intelligence (AI) and machine learning methods (ML) to develop 'fast' and 'intelligent' DSA systems by mapping the inherent relationship between system operating conditions and the dynamic security state of the system. Once such relationships were successfully mapped, new dynamic stability cases could be assessed and operating pre-conditions, which led to potential system insecurity could be traced back with minimal computational efforts. Decision tree and learning method was used in [14, 15]. In a recent paper [16], 'cascaded convolution neural network' was proposed for 'fast transient stability' assessment, while a 'deep learning framework' for transient stability assessment has been suggested in [17]. Another recent paper [18] has used an 'improved SVM' for real-time transient stability assessment of power system. These research works established that use of AI and ML can effectively alleviate the real-time computing burden and make online dynamic security assessment feasible.

While existing research proves that application of the machine learning for DSA is promising, the methods still lack rigorous support for their feasibility and reliability. One aspect which is critically important for the ML/pattern recognition (PR)-based DSA systems to be commercially viable is that the data acquisition cost (PMU installation) and computation overhead must be reasonable for real-time power systems. The motivation of this work is derived from critical review of the publishes researches till recent time, which reveals that while researches on online DSA have been primarily focused on the deployment of newer and more powerful ML/PR techniques, little attention has been given to optimize the measurement and data acquisition cost. For example, a continuous 'online monitoring system (OMS)' for power system stability based on PMU measurements has been proposed in [19], where the proposed OMS assumed PMU measurements of all the generator buses available at a central location, which is cost inefficient and may be infeasible for a large-scale system. Another recent work [20] described a new DSA model, termed as: 'multi-branch stacked denoising autoencoder (MSDAE)'. The case study on IEEE 50-machine system demonstrated in this paper again considered voltage trajectories of all the 50 generator buses obtained by PMU measurements, which can be slow, inefficient and costly. A more recent work in [21] proposed a 'hierarchical deep learning' model for online transient stability prediction. The case study on IEEE 39-bus system demonstrated in this paper again considered that raw PMU measurements and PMU-based dynamic state estimation at all generator buses are available. Review of these research works reveal that there is scope for optimizing the measurement and acquisition of power system attributes to improve the online DSA performance and its cost effectiveness.

1.2 Contribution

The main contribution of this paper is the novelty in the optimal selection and precise location of the PMUs whose measurements are critical for the online DSA. This effort is primarily aimed at reducing the data acquisition or PMU installation cost and to reduce the computation overhead and was achieved by discovery of the 'most dominant' variables or 'critical attributes' to be measured by the PMU's through step-by-step screening of the initial measurements. Further, the present paper addresses two critical issues involved in ML-based online DSA that can result in inaccurate security prediction. First, the PMU measured operating conditions can be dissimilar to those simulated offline, due to inaccurate modelling of the power system. Second, change of network topology can occur due to the outage of generators, transformers or transmission lines. To develop robust ML-based online DSA schemes, efforts have traditionally been given to prepare the initial knowledge (operating condition) base as exhaustive and realistic as possible. Limited efforts, however, have been reported in dealing with variation in operating conditions and topology change. Reference [22] proposed to build a completely new DT or replace a sub-tree of the DT with newly built corrective DT if the existing DT fails to recognize the variation in operating conditions correctly, while [23] used adaptive ensemble learning to re-train the DT adaptively by adding new training cases to the knowledge base to handle the changes in operating condition or system topology. Both the approaches require tracking network topology change in real time, which is impractical for large system.

This present paper suggests a novel method to create an exhaustive knowledge base that can handle variations in system topology by using a correlation-based approach in selecting the attributes that are independent of topology. As such it is almost impossible to find a common set of attributes having same degree of correlation with system's dynamic security under all probable operating condition and topology. An acceptable solution to this dilemma was arrived by deploying an efficient attribute selection method to optimally choose the most critical set of system-wide variables, directly measurable by PMU's, which can be perceived as the 'common useful features' with high average correlation with system's dynamic security, independent of initial condition and system topology. The proposed attribute selection method is highly beneficial in optimizing PMU installation in large power networks. If the system-wide critical variables can be identified, PMU's can be installed only at specific buses for a given system to monitor only these critical variables, independent of operating condition and system topology. This significantly reduces the data acquisition cost and computation overhead for online DSA and improves prediction accuracy and reliability of the online DSA.

PMU-based measurement has been used in this paper due to several advantages of synchrophasor technology over asynchronous and slower 'supervisory control and data acquisition (SCADA)'-based measurements. Fastness of measurement is critically important in DSA, where decision making needs to be as fast as a few cycles to maintain system stability. Further, DSA requires post-fault dynamic state information and measurement of dynamic system variables, such as frequently changing bus voltages and relative voltage angles. Many post-fault control actions, such as the response of fast exciters, play crucial role in determining the post-fault system dynamics, which further influence the system's transient stability. Even though the static features are available through SCADA, the dynamic state information of post-fault power systems can only be acquired by PMUs.

Ensemble decision tree (DT) classifier has been proposed [23, 24]. The reason for choosing ensemble DT as the security predictor is its proven capability of DT's to form reliable decision rules for fast and accurate prediction of power system's operating states in a real-time and online environment and high interpretability of the classification decisions [14, 15, 22]. The underlying offline analysis has been made as extensive as possible, by training the classifier offline using results obtained from the most tedious and accurate TDS. The ensemble DT classifier trained with exhaustive set of power system pre-contingency operating conditions and large variety of credible contingencies outperformed other equivalent classifiers such as method of least square (MLS), neural network (NN), vector quantization (VQ) and support vector machine (SVM)-based classifiers when implemented in IEEE 118-bus system, owning to its novel framework and efficient selection of attributes that are critically important to predict future dynamic state of a power system.

2 Background of Ensemble Decision Tree

Ensemble decision tree (DT) is a collaborative assembly of individual decision trees, where each single tree structure is built on classification and regression models [14, 25]. A decision tree may be perceived as a method of dissecting data sets into more minute subsets with increase in the depth of a hypothetical tree. A tree usually comprises of 'decision nodes' and 'leaf nodes' where numerous branches may fall on each decision node. A classification or decision is represented by a leaf node. The node corresponding to the best predictor is termed as the root node. A single decision tree can, however, rarely generalize the data it was not trained on. Combining the predictions of large number of decision trees can result in very accurate predictions. Such method of combining individual decision trees is known as an 'ensemble method'. Mathematically speaking, a decision tree has low bias and high variance. Ensemble of many decision trees reduces the variance while maintaining the same low bias. The ensemble approach can be viewed as an extension of the bagging idea [26, 27]. Bagging tries to implement parallel learning of similar learners on small sample populations and then takes a mean of all the predictions. A collective decision is finally obtained by using an elementary 'committee' method which classifies an object according to the decision of most of the base learners. One of the progressive bagging-based approaches is the method called random forest [23]. 'Boosting' is another popular technique [27, 28] for improving the accuracy of a predictor by applying the prediction repeatedly in a series and then combining the weighted output of each predictor, so that the total error of the prediction is minimized. In many cases, the prediction accuracy of such a series greatly exceeds the accuracy of the base predictor used alone. The tree boost algorithm [27] is used for improving the accuracy of models built on decision trees. Research [28] has shown that models built using tree boost are among the most accurate of any known decision tree models. The tree boost algorithm is functionally similar to 'Decision Tree Forests' [23, 29] because it creates a tree ensemble, and it uses randomization during the tree creations. However, a random forest [24] builds the trees in parallel and they 'vote' on the prediction, whereas 'tree boost' creates a series of trees, and the prediction receives incremental improvement by each tree in the series.

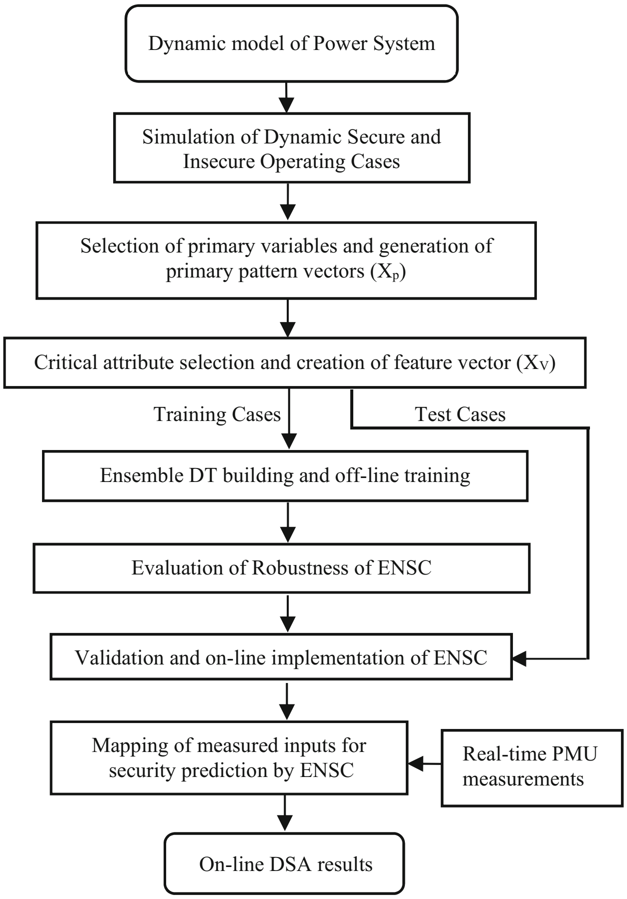
Dynamic model of Power System
Simulation of Dynamic Secure and Insecure Operating Cases
Selection of primary variables and generation of primary pattern vectors (Xp)
Critical attribute selection and creation of feature vector (Xv)
Training Cases
Test Cases
Ensemble DT building and off-line training
Evaluation of Robustness of ENSC
Validation and on-line implementation of ENSC
Mapping of measured inputs for security prediction by ENSC
Real-time PMU measurements
On-line DSA results

Fig. 1 The conceptual model of the developed scheme for real-time power system dynamic security assessment

3 Proposed ensemble DT-based online DSA scheme

The objective behind the development of an online DSA scheme is to enhance system operator's awareness about the current operating condition by assessing its potential to make a system transiently unstable in the events of fault or major outage. For this purpose, an 'ensemble DT security classifier (ENSC)' has been trained offline to recognize the present dynamic operating condition from real-time measurement of system attributes via PMU and classify the system's dynamic states into secure or insecure classes in near real time.

A secure class represents the set of operating conditions without possibility of existence of any 'critical line faults', which can cause potential instability. An insecure class, on the other hand, represents those operating states, which have at least one (or more) 'critical line fault' having the potential to cause dynamic instability. A critical line fault is usually a 3-phase line fault (or in some case any other asymmetrical fault) that may enforce dynamic instability in at least one of the generators present in the system. Figure 1 depicts the conceptual diagram of the proposed ENSC.

4 Illustrative example of implementation of the proposed scheme

The main steps of implementing of the proposed online DSA scheme, including knowledge-base preparation, critical attribute selection for strategic PMU measurement and offline ensemble training, have been demonstrated in this section using a test system. Finally, the results of robustness test under changed operating conditions have been presented.

The IEEE 118-bus test system is chosen as an illustrative medium to large-scale system considering its topological spread and intricacy. The test system contains 54 generators including 35 synchronous condensers, 186 lines, 9 transformers and 91 load buses. A schematic single line diagram of the system is presented in "Appendix".

4.1 Knowledge-base preparation for the ENSC

The success of the proposed method largely depends on adequacy of training, in terms of both 'quality' and 'quantity' of training exemplars. 'Quality' refers to the following:

(a) Consideration of diverse and well-dispersed operating conditions including topology changes due to contingency. The operating points must effectively represent the whole operating space of the power system including base case and contingencies, keeping in mid the fact that the machine learning approaches are usually more efficient in interpolation rather than extrapolation of data.
(b) Accurate modelling of the post-fault dynamic behaviour of the system given the fact that the system moves away from the pre-fault equilibrium point and experiences transient post-fault dynamics. A realistic model of power system should include dynamics of the generator excitation system, nonlinearity of the network and dynamic response of the load against changing voltage and frequency.
(c) Judicious choice of attributes which can represent dynamic characteristic of the system and are correlated with post-fault system security. This usually refers to a set of variables representing current state of the system (such as load-generation level, line flows, bus voltage magnitudes and bus voltage angles). PMU measurements allow synchronized monitoring of these variables and their variation with changing system conditions, and therefore, they are considered good candidates to represent dynamic state of a power system.

'Quantity', on the other hand, refers to the total number of observations or number of samples used for training, where each observed sample corresponds to a unique pre-contingency operating condition. Though there is no guideline regarding how many observations should be considered 'adequate' for a given problem, the rule of thumb is to start with sample size, at least 10 times the number of features present in the data, and update the sample size incrementally, if the training accuracy is not up to the expectation.

A dynamic model of the IEEE 118-bus test system was created in PSAT [30] for simulation of operating conditions and contingencies. Dynamics of the generator excitation system and dynamic voltage and/or frequency dependent load models were considered. However, nonlinearity of the network elements could not be considered due to inadequate information. Creation of large number of diverse and well-dispersed operating points was achieved by multiple load-flow simulations with variable initial conditions such as generation and load variations, as well as with changed network topologies due to generator, line and transformer outages and their combinations. This illustration considers only 54 number (*N-1*) generator contingencies and 186 number (*N-1*) line and transformer contingencies. In real-time deployment, a contingency list can be prepared by the grid operator to account for probable (*N-k*) contingencies depending on system size and criticality of the contingency and the new cases can be incrementally added in the knowledge base. Figure 2 demonstrates how offline simulation was used to create the knowledge base for the ENSC.

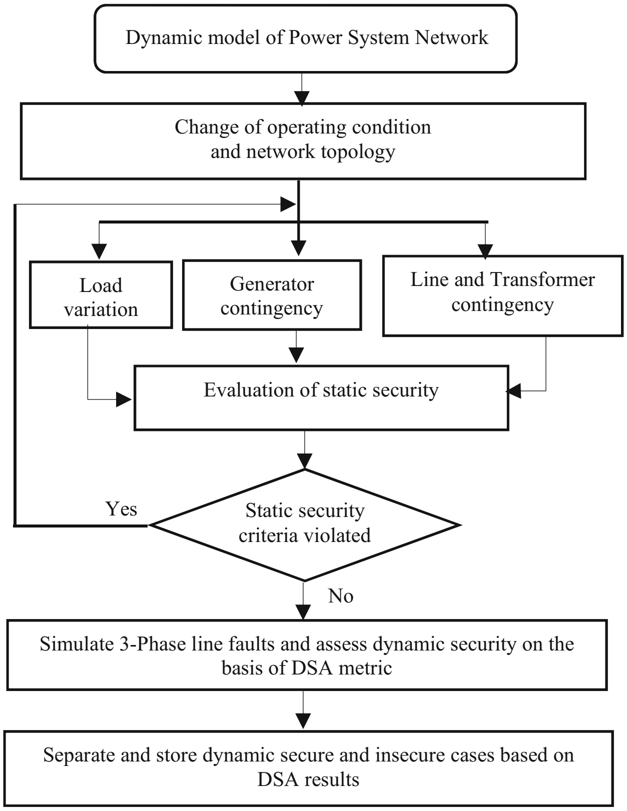
Dynamic model of Power System Network
Change of operating condition and network topology
Load variation
Generator contingency
Line and Transformer contingency
Evaluation of static security
Yes
Static security criteria violated
No
Simulate 3-Phase line faults and assess dynamic security on the basis of DSA metric
Separate and store dynamic secure and insecure cases based on DSA results

Fig. 2 Knowledge-base creation for the ENSC through offline computer simulation

4.1.1 Simulation of operating conditions and contingencies

In order to simulate the most credible operating scenarios, load-change was considered in approximately 14% of the total number of system load buses simultaneous. Out of the total 91 load buses, set of 13 buses were randomly selected as candidates for simultaneous load-change in 5 discrete steps of 0.5, 0.75, 1.0, 1.25 and 1.5 p.u. of the base loads at these buses. The process was recurrently followed for further sets of 13 randomly chosen buses which are not common with either of the previously selected buses, until all the system buses were considered. This generated 5 × 7=35 distinct, well-dispersed and yet credible load-generation cases. Each of these 35 load-generation conditions was then combined with single-generator outage cases. Considering 54 number generators in the IEEE 118-bus system, and 'no generator outage' as yet another scenario, a total of 35 × 55 = 1925 unique load-generation-generator outage scenarios were simulated. Single line-outage cases were also considered for the 186 lines/transformers on these lines, and taking

Table 1 Distribution of dynamic stable and unstable operating cases in the knowledge base of ENSC

ENSC knowledge-base	Data count	Distribution	
Total OCs	8470	NA	
Discarded static insecure OCs	3735	NA	
Qualifying Static secure OCs	4715	🟩 59%	🟥 41%
Dynamic secure OCs	2826	🟩 100%	
Dynamic insecure OCs	1889	🟥 100%	
Training OCs (2/3rd)	3143	🟩 59%	🟥 41%
Test OCs (1/3rd)	1572	🟩 59%	🟥 41%

* OC: operating case dynamic secure OCs: 🟩
dynamic insecure OCs: 🟥

‘no line-outage’ as one more condition and combining 186 single line-outage cases with 35 load-generation patterns, 187 × 35 = 6545 exclusive combinations load-generation-line-outage conditions were simulated. Thus, all together 1925 + 6545 = 8470 mutually exclusive, yet credible operating cases were simulated for representation of the complete operational space of the IEEE 118-bus test system. Rigorous TDS revealed that out of these 8470 cases, 3735 load-generation-outage combinations caused generator and line loading limit violations or voltage level violations (static security criteria) and hence they were disregarded as credible operating points. Finally, the 4715 remaining qualifying operating cases (OCs) were considered as candidates for the knowledge base of ENSC.

4.1.2 Simulation of dynamic secure and insecure cases

After the 4715 initial conditions referred above (and their corresponding 898 operating variables listed in Table 2) were archived in the knowledge base, 3-phase line faults were simulated in each of the 186 lines of the test system, and dynamic security of the post-fault system in each case was assessed by TDS and using the DSA metric explained in Sect. 4.3B. Table 1 summarizes the results of the TDS and the distribution of dynamic stable and unstable operating cases in the knowledge base of the ENSC.

All numerical simulations were performed on a computer with an Intel Core i7 CPU working at 3.4 GHz and 8 GB RAM. The overall ENSC knowledge-base creation time is estimated as follows: TDS over 20-s horizon for checking limit violation for each of the 8470 initial OCs took on average 2–5 s, totalling approximately 7 h. Further post-fault DSA by TDS for the 186 three-phase line faults over 10-s horizon and step size 10 ms for each of the 4715 knowledge-base candidate cases took 20 s on average, totalling another 26 h. There is scope for reducing the simulation time proportionately by using parallel computation on multiple CPU’s or distributed computing, since each simulation is independent.

4.2 Dynamic security assessment criteria

The post-fault rotor angle deviation has been used as the indicator of dynamic stability of the power system. Rotor angle trajectory of all the generator buses during fault and post-fault clearance were obtained by TDS for each of the 4715 operating cases. The dynamic stability status was evaluated by observing the absolute values of bus voltage angle difference between any two generator buses in the system over the chosen TDS horizon [0, t_s]. The system is considered dynamically unstable if the angle separation between any two generator buses in (1) exceeds a certain threshold at any TDS time-step.

$$\Delta\delta_{ij} = \left|\delta_i - \delta_j\right| > \delta\text{max}; \quad i,\ j \in B_G \text{ and } i \neq j \tag{1}$$

where δ is the bus voltage angle, $\mathrm{B_G}$ is the set of generator buses, and $\delta_{\max}$ is the predetermined threshold or maximum allowable generator rotor angle separation for secure operation. $\delta_{\max}$ was set to 120 degree [31]. TDS horizon t_{s} was chosen as 10 s, and 10 ms step size was chosen for each TDS. A dynamic security index (SI) is proposed in (2) to assess the relative criticality of an operating condition following a disturbance

$$\mathrm{SI} = 1 - \frac{\delta\text{max} - \delta_{ij}(t_s)}{\left|\delta\text{max} + \delta_{ij}(t_s)\right|} \tag{2}$$

where $\delta_{ij}(t_s)$ is the final rotor angle separation between any two generators at the end of TDS horizon. Finally, *SI*-based DSA criteria can be defined as: SI < 1: secure and SI ≥ 1: insecure.

4.3 Selection of critical attributes for strategic PMU measurement

Choice of input is crucial to effectively train the ENSC. As mentioned earlier, the biggest challenge in developing a robust online DSA system is handling frequent variations in operating conditions like change of load, re-scheduling of generators and occasional topology changes due to the forced outage of generators, transformers or transmission lines. While some attributes or variables may be critical in deciding system security under one operating scenario, the same attributes may not be equally important in changed situations. Selecting proper variables for training and real-time measurement of those variables for DSA has a number of challenges: first, how to decide critically important variables for DSA under a given operating condition and topology? For a large system, it is impractical to consider that every system bus will have measuring devices like PMUs pre-installed; second when criticality of attributes changes under new operating conditions and changed topology, how to practically measure the new set of critical variables with fixed installation of PMUs?; and third how to re-train the ML-algorithm adaptively with new inputs every time? The present paper suggests a novel approach to deal with the above challenges.

First, a correlation-based feature screening approach is used in selecting optimal set of attributes which have highest correlation with system's dynamic security under a given operating condition and topology (case specific optimization).

Second, the optimization is extended for all probable operating condition and topology to obtain a globally optimum set of attributes that are independent of operating condition and topology. It is unlikely that a common set of attributes will have same degree of correlation with system's dynamic security under all probable operating condition and topology. It is therefore important to optimally choose the most critical set of system-wide variables, which have high average correlation with system's dynamic security, independent of operating condition and topology by deploying an efficient attribute screening method and train the proposed ENSP with these globally optimum set of attributes.

When a global set of critical variables is identified, it is not difficult to decide the strategic buses where PMUs need to be installed for measurement of these critical variables independent of operating condition and system topology. The method therefore suggests a practical way to decide optimal installation of PMU for reliable online DSA and significantly reduces the data acquisition cost and computation overhead. The following section illustrates a practical method of feature screening for selection of critical attributes. The sequence of steps implemented for the proposed attribute selection is illustrated in Fig. 3.

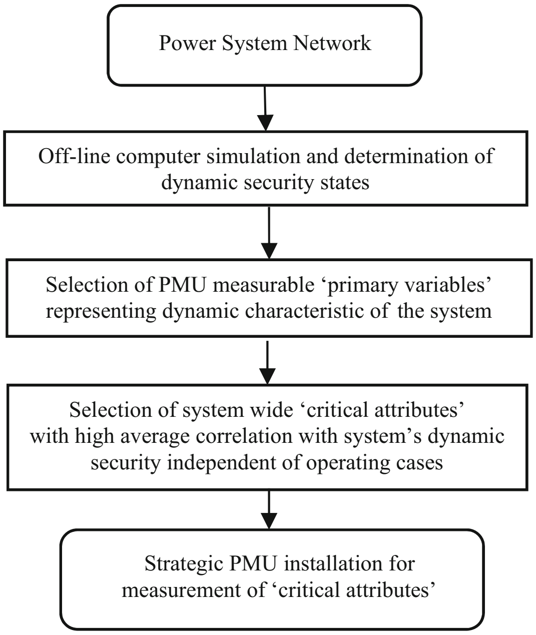
Power System Network
Off-line computer simulation and determination of dynamic security states
Selection of PMU measurable 'primary variables' representing dynamic characteristic of the system
Selection of system wide 'critical attributes' with high average correlation with system's dynamic security independent of operating cases
Strategic PMU installation for measurement of 'critical attributes'

Fig. 3 The sequence of steps implemented for critical attribute selection for strategic PMU measurement

4.3.1 Selection of primary variables

Primary variables are those which can adequately represent dynamic characteristic of the system and have correlation with post-fault system security. These selected variables should preferably be PMU measurable or derivable from PMU measurements obviating the need of extensive computation for fast online DSA. Based on experience of the previous researchers [32, 33], a set of PMU-measurable variables S was created with the initial attributes:

Active generation	:	$\{P_{Gi};\ i\in B_P\}$
Reactive generation	:	$\{Q_{Gi};\ i\in B_P\}$
Active load power	:	$\{P_{Li};\ i\in B_P\}$
Reactive load power	:	$\{Q_{Li};\ i\in B_P\}$
Bus voltage magnitude	:	$\{V_{Bi};\ i\in B_P\}$
Bus voltage angle	:	$\{\delta_{Bi};\ i\in B_P\}$
Line active power flow	:	$\{P_{ij};\ i, j\in B_P\}$ and $i>j$
Line reactive power flow	:	$\{Q_{ij};\ i, j\in B_P\}$ and $i>j$

where B_P is the set of buses having PMU. Initially, B_P contains every system bus. Exact candidate buses for B_P are decided later on the basis of attribute screening result. Table 2 illustrates the 898 primary variables constituting the set $S=\{P_{Gi}, Q_{Gi}, P_{Li}, Q_{Li}, V_{Bi}, \delta_{Bi}, P_{ij}, Q_{ij}\}$ for the IEEE 118-bus system. These variables are calculated by solving PF for each of the 4715 operating cases and passed on to feature screening algorithm for selection of globally optimum set of critical variables referred earlier.

Table 2 The initial pre-selected primary system variables

Primary system variables	Symbol used	Number of variables
Active generation	P_{G}	54
Reactive generation	Q_{G}	54
Active load power	P_{L}	91
Reactive load power	Q_{L}	91
Bus voltage magnitude	V_{B}	118
Bus voltage angle	δ_{B}	118
Line active power flow	P	186
Line reactive power flow	Q	186
Total		898

4.3.2 Critical attribute selection

The critical set of global attributes with high average correlation with system's dynamic security independent of operating condition and topology was selected by 'Gini Index (GI)' [34]-based feature screening method. 'Feature' refers to the distinctive attributes which can broadly represent a system. GI uses a correlation-based criterion, which attempts to estimate a feature's ability to aid classification. The method finds wide use as a splitting criterion in many decision tree algorithms [35]. The Gini split criterion can be described as:

$$GI(t_K) = \sum_i P\left(\frac{t_k}{C_i}\right)^2 \cdot P\left(\frac{C_i}{k}\right)^2 \tag{3}$$

where $P\left(\frac{t_k}{C_i}\right)$ is the probability that the feature t_k occurs in category C_i and $P\left(\frac{C_i}{k}\right)$ refers to the conditional probability that the feature t_k belongs to the category C_i when the feature t_k occurs. The method proposes to choose the feature t_k if it produces highest impurity reduction in the next split.

4.3.3 Strategic PMU installation

Since the correlation of critical variables change with change in operating condition, topology and faults., it was therefore necessary to compute 'average correlation' of the 898 primary variables in *'S'* for all probable operating conditions, topology and fault and finally select a minimal set of 'n' (n∈S) globally optimized variables, which can be perceived as the '*common critical variables'* with high average correlation with system security under all operating conditions. 'n' needs to be decided by a trade-off between PMU installation/data acquisition cost and reliability/accuracy of the online DSA. An illustrative example of relative criticality of the variables is presented in Fig. 4 with the highest correlated variable scaled to 100%. As such, no heuristic or analytical algorithms were used to optimize the selection, and rather the selection was based on meticulous review of the average correlation of the variables as in Fig. 4. Since the average correlation of the 15th variable (VB89) already fell to just 8% in a scale of 0–100%, choosing $n > 15$ was not considered prudent, as the variables with still lesser correlation would hardly benefit the DSA classification, while unnecessarily increasing the computation load. Therefore, $n = 15$ was used in this illustrative case study. There exists scope for using heuristic or analytical algorithms to optimize 'n' and it may be possible that $n < 15$ also provide 'satisfactory results'. However, such optimization further needs to consider 'observability' of the system and 'PMU contingency'. Since out of these 15 critical variables, 8 are dynamic variables (7 relative bus voltage angles and one bus voltage magnitude, which keep changing frequently in post-fault scenario), for online DSA, synchronized measurement with PMUs are necessary. PMUs are required to be installed at strategic buses to monitor these final set of critical variables, independent of operating condition and system topology. For practical PMU installation, additional constraints like 'observability' of the system and 'PMU contingency' needs to be taken into consideration. The 'critical attribute vector' C={C_1, C_2, C_3, … C_{15}} is finally formed with each critical variable (C_k) as member of C for preparing the knowledge base of the ENSC.

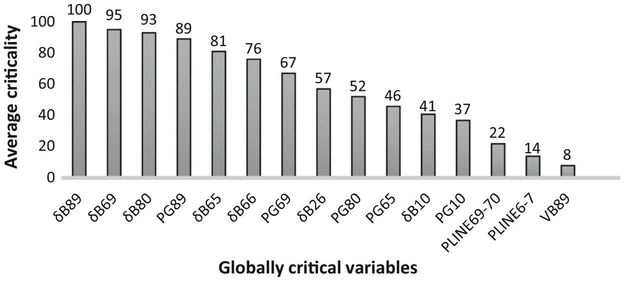

Fig. 4 Correlation of the critical variables with system security

4.4 Offline DT building and training

The ENSC was developed in Python, scikit-learn by ensemble of DTs, where individual DTs were built upon classification and regression tree (CART) model [36]. The DTs were trained using a training set and a test set to classify the operating cases (OCs) into 'secure' and 'insecure' classes (for two-class classification). The classification may be extended to (I + 1) classes if 'insecure' class needs to be sub-divided further into I classes depending on relative criticality of the insecure operating cases. Initially, 2/3rd of the operating cases (3143 OCs in Table 1) served as the training set for a single decision tree. For each of the 3143 training OCs, individual DTs were trained with corresponding unique 'critical attribute vector' C. Each of these individual decision trees can vote in favour of one output class ('secure' or 'insecure') for a given operating case.

Pre-selection of the critical attributes (in Sect. 4.3.2) and use of the critical attribute vector 'C' of reduced dimension n = 15 (Sect. 4.3.3) in lieu of all the 898 primary variables in *'S'* offered significant performance benefit during offline DT building and training. There was noticeable advantage both in terms of the commutation overhead and time. With the 3143 training OCs and 'C' as input, the Intel Core i7 3.4 GHz CPU accomplished DT training and met the misclassification error criteria in 3707 epochs taking a total time of 5.6 h with average run time of 5.4 Sec/epoch. In comparison, the DT building and training took 5233 epochs to meet the same misclassification error criteria, when all the 898 variables in 'S' were used as input and took a total training time of over 57 h with average run time of 39.3 Sec/epoch. Thus, training time decreased by more than 90% when using reduced order critical attribute vector 'C' as input in lieu of full set of primary variables 'S'.

Final class prediction then follows the 'majority voting' principle, where the class receiving maximum number of votes by individual decision trees is finally considered as the output security class for the operating case under consideration. In the second stage, assessment of correctness of the decisions made by various DTs in the ensemble of DTs was done by calculating misclassification rate. This assessment was performed on the remaining 1/3$^{\text{rd}}$ data (1572 OCs in Table 1) to estimate prediction error and focus was to minimize the misclassification rate. If the results were unsatisfactory, or splitting data into just two parts (2/3rd and 1/3rd) did not result good prediction, cross-validation [37] was used to improve prediction accuracy. Tenfold cross-validation was used in this illustration to determine optimal tree height and optimal number of DTs. The training data were randomly partitioned during training into 10 subsets of equal size. For a given tree height and given number of trees, the classifier model was trained with $10 - 1 = 9$ data subsets and tested with the remaining one subset. The training process was then repeated 10 times with each of these 10 subsets used once and only once as test subset. The overall misclassification error was calculated by averaging the prediction error of 10 training instances. The final optimal values of tree height and number of trees were accepted when the average misclassification error dropped below 1%.

5 Performance of different DT Models in offline DSA

Performance of different trained DT models in the offline DSA was evaluated and compared for the 1572 test OCs in Table 1 containing 927 (59%) secure and 645 (41%) insecure cases, with the objective to select the better performing dynamic security predictor model for the IEEE 118-bus system. Among the 'boosting-DT' models [27], the 'stochastic gradient boosting (SGB)' [38] was considered, where in each iteration a sub-sample of the training data was drawn at random from the full data set without replacement. The randomly selected sub-sample was then used to train the individual base learners [23]. In the 'adaptive boosting-DT' category, the 'Ada Boost (AB)' [39] model was tested, which is an ensemble model that attempts to create a 'strong classifier' from a number of 'weak classifiers' [15]. In the 'bagging' [27] category, 'random forest (RF)' was tested, which is a decision tree model where individual trees have structural similarities, but the algorithm trains the sub-trees in a manner that reduces the correlation between the prediction results of the individual sub-trees. The confusion matrix [40] for each DT model is presented in Table 3 for the training cases and in Table 4 for the test cases, which illustrate the results of the security classifier over several trials against the actual known security classes of the items in the data set, and thus offers a convenient way to evaluate which dynamic security classes are being correctly/incorrectly classified. Among the trained DT models, RF is found to perform better in this illustration.

Table 3 Confusion matrix for the 3143 knowledge-base training cases

Actual	Classified as					
	Secure			Insecure		
	RF	AB	SGB	RF	AB	SGB
Secure	1745	1702	1681	109	152	173
Insecure	64	71	76	1225	1218	1213

Table 4 Confusion matrix for the 1572 test cases

Actual	Classified as					
	Secure			Insecure		
	RF	AB	SGB	RF	AB	SGB
Secure	880	848	833	48	95	116
Insecure	31	32	34	613	597	589

The classification decisions are of the following types: (1) *CS* (correct secure): A secure OC is correctly classified as secure; (2) *WS* (wrong secure): A secure OC is wrongly classified as insecure; (3) *CIS* (correct insecure): An insecure OC is correctly classified as insecure and (4) *WIS* (wrong insecure): An insecure OC is wrongly classified as secure. The composite classification accuracy '*CCA*' of the classifier is defined as the probability of a correct classification decision, which is the ratio of the number of correct classifications (correct secure + correct insecure) to the total number of test OCs:

$$\mathrm{CCA} = (\mathrm{CS} + \mathrm{CIS})/N_{\mathrm{OC}} \quad (4)$$

where N_{OC} is the total number of test OCs. The misclassification rate can be defined as: $e = 1 - \mathrm{CCA}$ which is the probability of making an incorrect classification. A number of other metrics have also been used to evaluate the performance of the security classifier:

$$\text{Secure misclassification rate:}\ \ \mathrm{SMR} = \mathrm{WS}/(\mathrm{CS} + \mathrm{WS}) \quad (5)$$

$$\text{Insecure misclassification rate :}\ \mathrm{IMR} = \mathrm{WIS}/(\mathrm{CIS} + \mathrm{WIS}) \quad (6)$$

In power system security classification, misclassification of secure OCs only raises false alarm without much harm to normal system operation. But, misclassification of insecure OCs is potentially hazardous, as it results in lack of remedial actions and plausible system outage. It is, therefore, important to design a security classifier to keep *IMR* at minimal. Table 5 illustrates the performance of different ensemble DT classifiers in terms of the metrics defined in (4)–(6) and

Table 5 Comparison of performance different classification methods

Classification methods	Classifier performance metrics		
	CCA (%)	SMR	IMR
Ensemble methods			
RF	94.97	0.034	0.07
AB	91.92	0.036	0.137
SGB	90.45	0.039	0.164
Single learner methods			
SVM	88.6	0.063	0.177
MLS	86.9	0.079	0.195
LVQ	85.6	0.083	0.21
PNN	83.4	0.089	0.24
KNN	81.2	0.097	0.31

compares the classification results with results of different single learner classification methods, such as 'support vector machine (SVM)' [41], 'method of least squares (MLS)' [42], 'learning vector quantization (LVQ)' [43], 'probabilistic neural network (PNN)' [44] and 'Kohonen's neural network (KNN)' [45]. It is apparent from these classification results that the use of a reduced order critical attribute vector 'C' for DT building and training did not have any noticeable impact on the classification performance, but the suggested technique significantly reduced computational overhead and training time.

6 Conclusion

The paper presented a real-time dynamic security assessment scheme for large-scale power systems based on ensemble decision tree using selective PMU measurement data. An ensemble decision tree (DT) classifier was developed and trained offline to recognize the present dynamic operating condition of the power system from real-time measurement of important system attributes by PMUs and classify the system's current dynamic state into secure or insecure class. The scheme identified a critical set of PMU-measurable attributes with high average correlation with system's dynamic security independent of operating condition and topology and accordingly suggested a practical method for strategic PMU installation in wide area power system networks considering the trade-off between PMU installation/data acquisition cost and reliability/accuracy of the online DSA. The scheme was tested on IEEE 118-bus system under wide range of operating conditions and credible set of contingencies. The test results demonstrated that the ensemble decision tree (DT)-based classification method is more accurate, reliable and computationally efficient than other equivalent methods built upon 'support vector machine (SVM)', 'method of least squares (MLS)', 'learning vector quantization (LVQ)', 'probabilistic neural network (PNN)' and 'Kohonen's neural network (KNN)' classifiers in offline simulation.

Acknowledgements Not applicable.

Authors' contributions All the authors participated and contributed equally in the analysis and interpretation of the results and data, drafting the article or revising it critically and preparing the final version.

Funding The authors declare that they have not availed any funding from any source for this research work.

Availability of data and material (data transparency) The data sets used and/or analysed during the current study are available from the corresponding author on reasonable request.

Code availability (software application or custom code) The custom code used in the current study is available from the corresponding author on reasonable request.

Compliance with ethical standards

Conflicts of interest The authors declare that they have no competing interests.

Appendix

See Fig. 5.

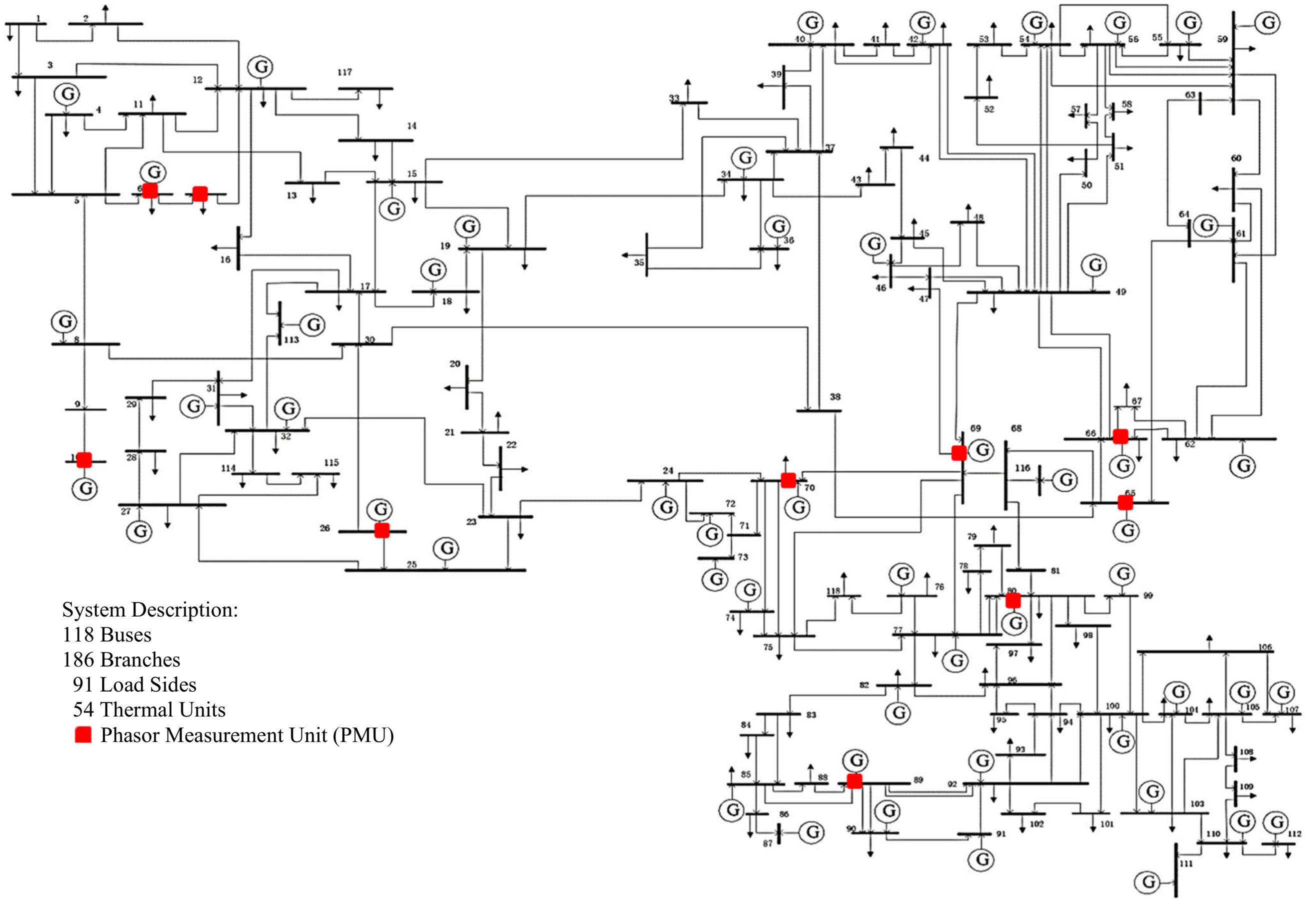

Fig. 5 IEEE 118-bus power system with strategic PMU installations

References

1. Kundur P (1994) Power system stability and control. McGraw-Hill Education, New York
2. Kundur P, Paserba J, Ajjarapu V, Andersson G, Bose A, Canizares C, Hatziargyriou N, Hill D, Stankovic A, Taylor C, Cutsem VT, Vittal V (2004) Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions. IEEE Trans Power Syst 19(3):1387–1401
3. Wehenkel L, Cutsem VT, Ribbens-Pavella M (1989) An artificial intelligence framework for online transient stability assessment of power systems. IEEE Trans Power Syst 4(2):789–800
4. Sauer WP, Pai AM (1998) Power system dynamics and stability. Prentice-Hall, New Jersey
5. Laufenberg JM, Pai AM (1998) A new approach to dynamic security assessment using trajectory sensitivities. IEEE Trans Power Syst 13(3):953–958
6. Chang DH, Chu CC, Cauley G (1995) Direct stability analysis of electric power systems using energy functions: theory, applications, and perspective. Proc IEEE 83(11):1497–1529
7. Chiang DH, Wang SC, Li H (1999) Development of BCU classifiers for on-line dynamic contingency screening of electric power systems. IEEE Trans Power Syst 14(2):660–666
8. Zhang R, Xu Y, Dong YZ, Wong PK (2015) Post-disturbance transient stability assessment of power systems by a self-adaptive intelligent system. IET Gener Transm Distrib 9(3):296–305
9. Fouad A, Vittal V (1988) Power system transient stability analysis using the transient energy function method. Int J Electr Power Energy Syst 10(4):233
10. Hiskens I, Hill D (1989) Energy functions, transient stability and voltage behaviour in power systems with nonlinear loads. IEEE Trans Power Syst 4(4):1525–1533
11. Morteza S, Wu EN, Bay SJ (2018) Transient stability assessment of large lossy power systems. IET Gener Transm Distrib 12(8):1822–1830
12. Chiang DH, Li H, Tong J (2013) On-line transient stability screening of a practical 14,500-bus power system: methodology and evaluations. High performance computing in power and energy systems. Springer, Berlin, pp 335–358
13. Hansen KL, Salamon P (1990) Neural network ensembles. IEEE Trans Pattern Anal Mach Intell 12(10):993–1001
14. Kamwa I (2010) Catastrophe predictors from ensemble decision-tree learning of wide-area severity indices. IEEE Trans Smart Grid 1(2):144–158
15. He M, Zhang J, Vittal V (2012) A data mining framework for online dynamic security assessment: decision trees, boosting, and complexity analysis. In: Proceedings of IEEE PES Innovative Smart Grid Technologies, ISGT 2012
16. Yan R, Geng G, Jiang Q, Li Y (2019) Fast transient stability batch assessment using cascaded convolutional neural networks. IEEE Trans Power Syst 34(4):2802–2813
17. Tan B, Yang J, Tang Y, Jiang S, Xie P, Yuan W (2019) A deep imbalanced learning framework for transient stability assessment of power system. IEEE Access 7:81759–81769

18. Hu W, Zongxiang L, Shuang W, Weiling Z, Yu D, Rui Y, Baisi L (2019) Real-time transient stability assessment in power system based on improved SVM. J Modern Power Syst Clean Energy 7(1):26–37
19. Gupta A, Gurrala G, Sastry SP (2019) An online power system stability monitoring system using convolutional neural networks. IEEE Trans Power Syst 34(2):864–872
20. Zhu Q, Chen J, Zhu L, Shi D, Bai X (2018) A deep end-to-end model for transient stability assessment with PMU data. IEEE Access 6:65474–65487
21. Zhu L, Hill JD, Lu C (2020) Hierarchical deep learning machine for power system online transient stability prediction. IEEE Trans Power Syst 35(3):2399–2411
22. Rovnyak S, Kretsinger S, Thorp J, Brown D (1994) Decision trees for real-time transient stability prediction. IEEE Trans Power Syst 9(3):1417–1426
23. Banfield R, Hall L, Bowyer K, Kegelmeyer W (2007) A comparison of decision tree ensemble creation techniques. IEEE Trans Pattern Anal Mach Intell 29(1):173–180
24. Jana S, De A (2020) Structured approach to downsize data administration and improve fault recognition accuracy for large power systems. IET Gener Transm Distrib 14(14):2731–2739
25. Chiang DH, Wu FF, Varaiya PP (1988) Foundations of the potential energy boundary surface method for power system transient stability analysis. IEEE Trans Circuits Syst 35(6):712–728
26. Geeganage J, Annakkage DU, Weekes T, Archer AB (2015) Application of energy-based power system features for dynamic security assessment. IEEE Trans Power Syst 30(4):1957–1965
27. Mason L, Baxter J, Bartlett LP, Frean RM (1999) Boosting algorithms as gradient descent. Neural information processing systems. Springer, Berlin, pp 512–518
28. Niculescu-mizil A, Caruana R (2005) Obtaining calibrated probabilities from boosting. In: Proceedings of 21st Conference Uncertainty in Artificial Intelligence, AUAI Press
29. Freund Y, Schapire R (1997) A decision-theoretic generalization of on-line learning and an application to boosting. J Comput Syst Sci 55:119–139
30. Kaplan (2019) PSAT/NMSQT Prep 2019: 2 Practice Tests + Proven Strategies + Online (Kaplan Test Prep)
31. Powertech Labs, DSATools: Dynamic Security Assessment Software. http://www.dsatools.com
32. Sun K, Likhate S, Vittal V, Kolluri V, Mandal S (2007) An online dynamic security assessment scheme using phasor measurements and decision trees. IEEE Trans Power Syst 22(4):1935–1943
33. Diao R, Sun K, Vittal V, Keefe OR, Richardson M, Bhatt N, Stradford D, Sarawgi S (2009) Decision tree-based online voltage security assessment using PMU measurements. IEEE Trans Power Syst 24(2):832–839
34. Zonoobi D, Kassim AA, Venkatesh VY (2011) Gini index as sparsity measure for signal reconstruction from compressive samples. IEEE J Sel Top Signal Process 5(5):927–932
35. Shang W, Qu Y, Huang H, Zhu H, Lin Y, Dong H (2010) Complete gini-index text (GIT) feature-selection algorithm for text classification. In: 2nd international conference on software engineering and data mining, SEDM 2010
36. He M, Zhang J, Vittal V (2013) Robust online dynamic security assessment using adaptive ensemble decision-tree learning. IEEE Trans Power Syst 28(4):4089–4098
37. Setiono R (2001) Feedforward neural network construction using cross validation. IEEE Trans Neural Comput 13(12):2865–2877
38. Ding H, Li G, Dong X, Lin Y (2018) Prediction of pillar stability for underground mines using the stochastic gradient boosting technique. IEEE Access 6:69253–69264
39. Mukherjee I, Rudin C, Schapire ER (2013) The rate of convergence of AdaBoost. J Mach Learn Res 14(1):2315–2347
40. Ohsaki M, Matsuda K, Wang P, Katagiri S, Watanabe H (2015) Formulation of the kernel logistic regression based on the confusion matrix. In: 2015 IEEE congress on evolutionary computation, pp 2327–2334
41. Gomez F, Rajapakse A, Annakkage U, Fernando I (2011) Support vector machine-based algorithm for post-fault transient stability status prediction using synchronized measurements. IEEE Trans Power Syst 26(3):1474–1483
42. Lilley WR (1990) Demonstration of MLS advanced approach technique. IEEE Aerosp Electron Syst Mag 5(5):41–46
43. Xu W, Nandi KA, Zhang J (2003) Novel fuzzy reinforced learning vector quantisation algorithm and its application in image compression. IEE Proc Vis Image Signal Process 150(5):292
44. Franti P, Kaukoranta T, Sen FD, Chang SK (2000) Fast and memory efficient implementation of the exact PNN. IEEE Trans Image Process 9(5):773–777
45. Aghamohammadi RM, Mahdavizadeh F, Bagheri R (2009) Power system dynamic security classification using Kohenen neural networks. In: IEEE/PES power systems conference and exposition