The Journal of CPRI,
Vol. 10, No. 4, December 2014 pp. 673-680

Decision tree approach to dynamic security assessment

Nikhil Valluru* and Shanti Swarup K**

Dynamic Security Assessment (DSA) of power systems is an important study for real time application in control centers. Historically, various numerical, methods have been adopted for carrying out DSA. These are time consuming and computationally intensive. So faster and easily computable methods for Security Assessment are the need of the hour. With the advances in technology, several new methods which are more effective than the earlier adopted methods have been developed. One of them is the use of Decision Trees (DTs) for Dynamic Security Assessment. The real time system data can be obtained which helps in identifying current system operating condition and hence used it in predicting whether the system is dynamically secure or not.As a result, making accurate predictions for the power system operating conditions is an important task for the current power system research. The research mainly interests in checking if the operating conditions are acceptable after contingencies.

Keywords: *Power System Security; energy management system, on-line control, dynamic security assessment (DSA); decision Trees (DT).*

1.0 INTRODUCTION

The he 2012 blackouts which affected 22 Indian states has indicated that the operation and control of the power system needs to be improved. Even though the operators have access to a huge amount of data, they were not able to take the proper actions in time to prevent the blackouts. Motivated by this harsh reality, this paper is focused on empowering the operators by helping them take decisions easily by predicting the security of the power system. Instead of using a model of the power system to estimate the state, measured variables are used as input data to the algorithm. The algorithm classifies secure from insecure states of the power system using the measured variables directly. The algorithm is trained before hand with data from a model of the power system.

This paper uses Decision Trees to classify whether the power system can withstand the (n-1) contingencies during variety of operation conditions. The decision tree once generated can be deployed online and used to predict when the system is going into an insecure state, thus helping the operators at any early stage and enable them to take proper evasive actions.

2.0 POWER SYSTEM SECURITY

Power system security is usually assessed on the basis of security standards, i.e., the relationship between outages of generation and transmission plant and the level of any acceptable loss of demand. An 'N-1' security standard requires the system to work satisfactorily following loss of any one of its N elements.

* Indian Institute of Technology, Madras, Chennai – 600 036, India. E-mail: vvnikhil@gmail.com
** Power System Engineering Division, Indian Institute of Technology, Madras, Chennai – 600 036, India. E-mail: swarup@ee.iitm.ac.in

TABLE 1
FACTORS AFFECTING POWER SYSTEM SECURITY

Characteristics	Potential Impact
Aging transmission infrastructures	Increased probability of component failures and malfunction leading to system disturbances
Lack of new transmission facilities	Overloading of transmission facilities leading to protection operation or contributing to phenomena such as voltage collapse
	Bottlenecks in key transmission corridors leading to congestion
Cutbacks in system maintenance	Component failures and disturbances such as flashovers to trees
Increased dependence on controls and special protection systems	Increased probability of inadvertent/incorrect operation of protections Increased unpredictability of cascading events
Large number of small and distributed generators	Increased difficulty in adequate system design due to uncertainty in generation plans Uncertainty in dispatch
Market driven transactions	Unpredictable power flows and system usage leading to congestion and/or poor dynamic behavior New forms of stability problems such as voltage and small signal stability
Increased dependence on communication and computer systems	Software/hardware failures may leave large portions of system unobservable to operators, leading to inappropriate, or lack of, control actions during disturbances
Limited integrated system planning	Insufficient/improper generation and transmission resources
Trend toward interconnection	Exposure to cascading disturbances brought on by events in neighboring systems. New forms of stability problems such as small signal stability
New technologies such as advanced control systems, wind power, biomass, fuel cells, etc.	Lack of operating experience with technologies which may have unique dynamic characteristics Unpredictable behaviors during disturbances
Aging and downsized workforces	Lack of experienced personnel that may lead to the instability to deal appropriately with emergency conditions

During the times of regulated and vertically integrated power systems, systems tended to be more secure for a number of reasons. First, as the grids were designed, built, and operated by the government, integrated planning ensured that generation and transmission facilities kept pace with the load growth, thereby limiting overloading and equipment failures that could lead to system disturbances. Maintenance programs were also, in general, rigorous. From an operations perspective, forecasting system conditions was simpler because there were fewer generation and transmission owners and they were operating in a carefully planned and cooperative manner. As a result, systems, which were exposed to fewer potential disturbances, were more robust in their responses to disturbances that did occur, and were more predictable in their patterns of operation.

However, the evolution of the electric power industry toward open markets over the last decade has introduced a number of factors that have increased the possible sources for system disturbances, reduced the robustness of systems, and reduced the predictability ofoperation. Some of these factors are described in Table 1 [1].

Contingencies may be external or internal events (for instance, faults subsequent to lightning versus operator-initiated switching sequences) and may consist of small/slow or large/fast disturbances (for example, random behavior of the demand pattern versus generator or line tripping). Usually, numerical simulation of the contingency scenario is used to assess the effect of a contingency on a power system in a given state. However, the

non-linear nature of the physical phenomena and the growing complexity of real-life power systems make security assessment difficult. For example, monitoring a power system every day calls for fast sensitivity analysis to identify the salient parameters driving the phenomena, and suggestions on how to act on the system so as to increase its level of security.

Reliability of a power system refers to the probability of its satisfactory operation over the long run. It denotes the ability to supply adequate electric service on a nearly continuous basis, with few interruptions over an extended time period [2]. Power system stability is the ability of an electric power system, for a given initial operating condition, to regain a state of operating equilibrium after being subjected to a physical disturbance, with most system variables bounded so that practically the entire system remains intact.

Reliability is the overall objective in power system design and operation. To be reliable, the power system must be secure most of the time. To be secure, the system must be stable but must also be secure against other contingencies that would not be classified as stability problems e.g., damage to equipment such as an explosive failure of a cable, fall of transmission towers due to ice loading or sabotage. As well, a system may be stable following a contingency, yet insecure due to post-fault system conditions resulting in equipment overloads or voltage violations.

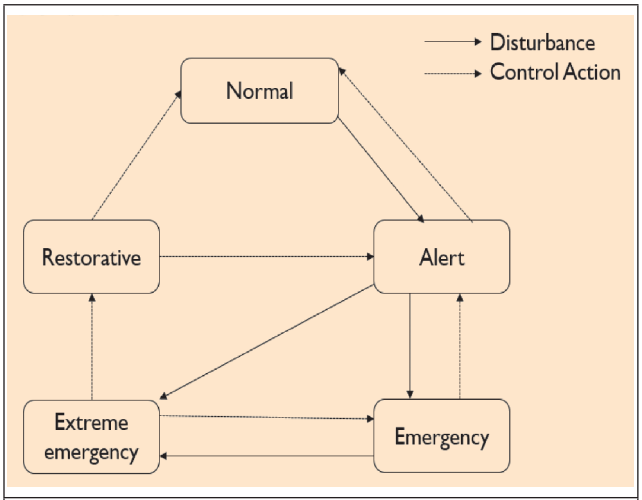

FIG. 1 POWER SYSTEM OPERATIONAL STATES

Figure 1 depicts the operational states of a power system and the ways in which transition can occur from one state to another. The operation of a power system is usually in a normal state. Voltages and the frequency of the system are within the normal range and no equipment is overloaded in this state. The system can also maintain stability during disturbances considered in the power system planning. The security of the power system is described by Thermal, voltage and stability limits. The system can also withstand any single contingency without violating any of the limits. The system transits into the emergency state if a disturbance occurs when the system is in the alert state. Many system variables are out of normal range or equipment loading exceeds short-term ratings in this state. The system is still complete. Emergency control actions, more powerful than the control actions related to alert state, can restore the system to alert state. The emergency control actions include fault clearing, excitation control, fast valving, generation tripping, generation run back-up, HVDC modulation, load curtailment, blocking of on-load tap changer of distribution system transformers and rescheduling of line flows at critical lines. The extreme emergency state is a result of the occurrence of an extreme disturbance or action of incorrect of ineffective emergency control actions. The power system is in a state where cascading outages and shutdown of a major part of power system might happen. The system is in unstable state. The control actions needed in this state must be really powerful. Usually load shedding of the most unimportant loads and separation of the system into small independent parts are required.

Every small change in load is a disturbance that causes a change in system conditions. However, system security is assessed for larger changes that cause major changes in system conditions. These changes are mainly caused by contingencies. Most commonly contingencies result in relay operations that are designed to protect the system from faults or abnormal conditions. Typical relay operations result in the loss of a line, transformer, generator, or major load.

Various components in a power system respond to changes that occur and may reach an equilibrium condition that is acceptable according to some criteria. Mathematical analysis of these responses and the new equilibrium condition is called security analysis.

3.0 ON-LINE POWER SYSTEM SECURITY ANALYSIS

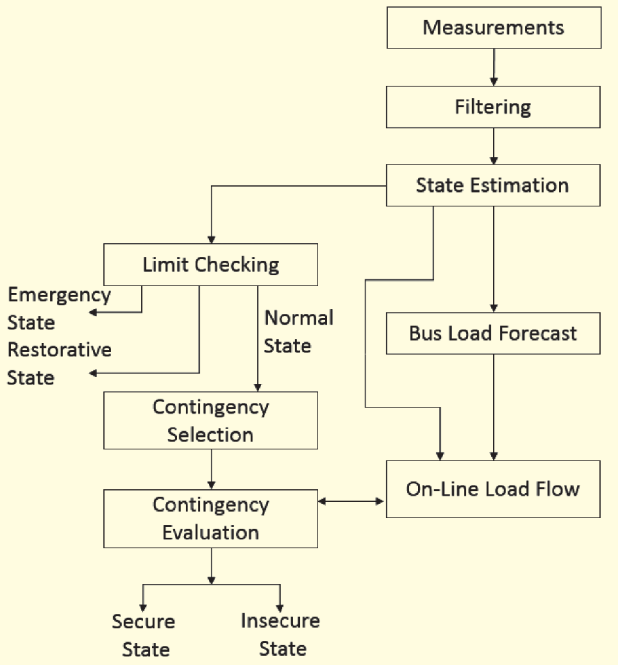

FIG. 2 ON-LINE POWER SYSTEM SECURITY ASSESSMENT

The major components of On-Line Security Analysis are shown in Figure 2-3. The monitoring component starts with the real-time measurements of physical quantities such as line power flows, line current flows, power injections, and bus voltage magnitudes. The measurement data are transferred from various locations to the control center. The data received is then filtered through a simple check of reasonability and consistency. The remaining data are first systematically processed to determine the network topology. Then the available data are further processed to obtain an estimate of the system state variables (bus voltage magnitudes and phase angles for normal steady-state). State estimation is a mathematical procedure for computing the "best" estimate of the state variables of the power system based on the available data, which are in general corrupted with errors.

A set of contingencies is needed to assess whether a normal operating state is secure or not. A set of important and plausible disturbances is created. Security assessment currently involves primarily steady-state load flow analysis. Stability constraints are expressed in terms of the limits on line flows and bus voltages. Therefore, to assess the system response to contingencies, a contingency evaluation is carried out using the on-line load flows. The on-line load flow uses the actual load flow model from the state estimation solution together with a system representation of the unmonitored network and neighboring systems, i.e., an external network model. Because the contingencies are future events, a bus load forecast is needed. Certain implementations of the state estimator render the external model observable by strategic placement of pseudo-measurements. Then the state estimate is performed on the entire model in one step.

4.0 TYPES OF SECURITY ASSESSMENT

If the analysis evaluates only the expected post disturbance equilibrium condition (steady-state operating point), then it is called Static Security Assessment (SSA). Static or steady state security is the ability of the system to supply load without violating operating conditions following a contingency. Conventionally, SSA is performed by analytically modeling the network and solving the algebraic load flow equations repeatedly for all prescribed outages, one at a time.

If the analysis is used for determining whether the system oscillations, following a fault, result in loss of synchronization among the system generators, then it is called Transient Security Assessment (TSA). It pertains to the rotor angle stability of the system. Transient energy is the excess energy possessed by the system at the instant of fault clearing that must be absorbed by the network for stability to be maintained. Critical energy indicates the maximum capacity of system to absorb the accumulated energy during disturbance. The Transient Energy Function (TEF) based method is adopted to determine the transient security level of a power system.

Dynamic Security Assessment (DSA) has been formally defined by the IEEE, Power Engineering Society (PES) working group on DSA as an evaluation of the ability of a certain power system to withstand a defined set of contingencies and to survive the transition to an acceptable steady state condition. In other words, it is the ability of the system to withstand all the contingencies, maintaining synchronism for a long duration after the system is found to be transiently secure.

SSA can be used quickly to determine if a system is insecure by simply looking at the static outcome of each contingency. However, to know whether the system is fully secured, DSA must be performed. It determines if the associated dynamics of each contingency are acceptable.

Security Assessment approaches can be classified either as deterministic or probabilistic. Deterministic methods provide very simple rules to make decisions. These methods, however are expensive and hence researchers are looking at techniques which indicate whether the system is secure which are also economically viable.

5.0 DYNAMIC SECURITY ASSESSMENT

Mathematically, a dynamic security problem can be expressed as a large set of Differential Algebraic Equations (DAEs), which are difficult to be solved analytically. Conventional methods for DSA are mainly based on Time Domain Simulation (TDS) techniques. In TDS techniques, the system dynamic trajectories are simulated by solving the DAEs using step-by-step integrations. The major advantages of TDS include [3]:

- Provide essential information about relevant parameters of system dynamic evolution with time
- Consider any power system modeling and stability scenario
- Reach the required accuracy, provided that the modeling of a power system is correctly designed and its parameters accurately known.

However there are also a couple of shortcomings of adopting this method:

- This is a computation intensive method as it may require to solve several thousands of differential and algebraic equations for a simulation time of 10-20 seconds while deployed in a power station. Besides the number of contingencies to be considered will also be huge.
- The TDS can only provide the system dynamic trajectories and offer very limited information about system security characteristics. Hence, for dynamic security assessment (DSA) aspect, it can only give a binary answer about secure or insecure; for dynamic security control (DSC) aspect, the computation process is usually not transparent and interpretable.

This method, being very time consuming, is generally used only in off-line applications. The process consists of conducting TDS on forecasted operating conditions and disturbances and heuristically finding a secure operating condition in a trial-and-error way. In on-line operating phase, the analysis results are used by operators in a look-up pattern.

The algorithm for the proposed scheme is shown in Figure 3. The proposed scheme is developed in three stages:

1. Firstly, operating conditions for the next 24 hours is forecasted. All the single line to ground faults are simulated at those operating conditions and stored in a database. This is called the Dynamic Security Database.
2. Using this database as the learning and the testing set, we build a Decision Tree. The Decision tree is used to identify the Critical Attributes (CAs) from the system parameters that characterize the system dynamic performance and evaluate the thresholds that result in insecurity. These CAs are the measurements which need to be made using the PMU or SCADA.
3. Around an hour before the online deployment, the Decision Tree is updated with the

projected operating conditions, available after performing short term load forecasting and running the TDS on these new OCs. The real-time measurements available through the Phasor Measurement Units (PMUs) or Supervisory Control and Data Acquisition (SCADA) units are then fed to the DT and the security level is found out.

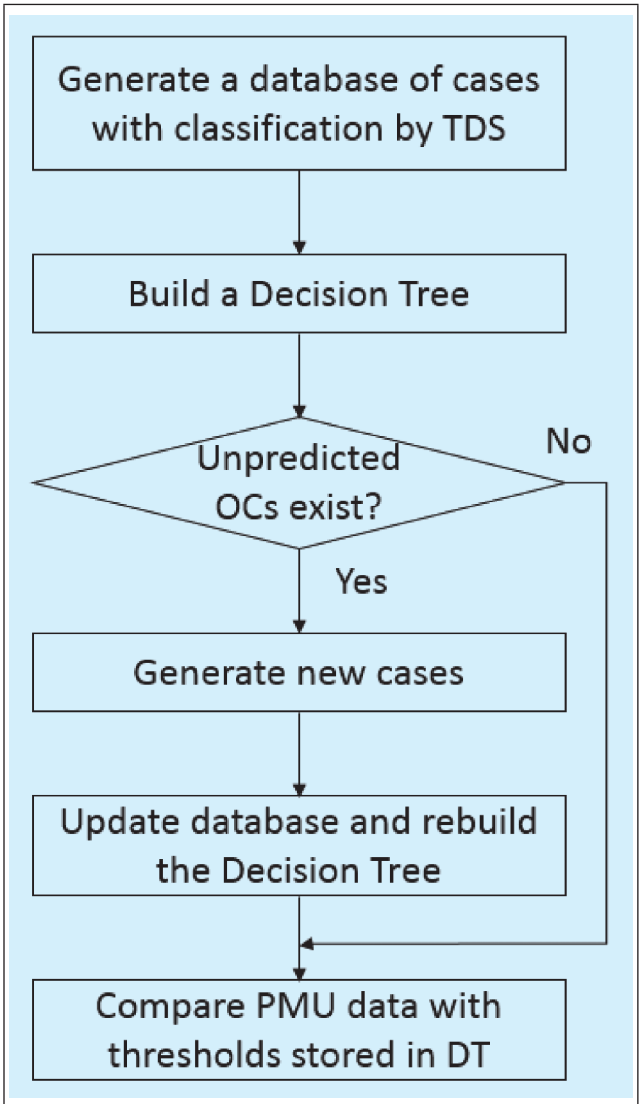

FIG. 3 FLOW CHART FOR THE PROPOSED METHOD OF DSA

The implementation of proposed DSA algorithm was done in MATLAB, using the packages MatPower and MatDyn, and the experimental performances for the algorithm were conducted on the WSCC 9 bus system, under increased loading conditions in order to exhibit instances of instability caused by faults. The one-line diagram of the WSCC 9 bus system is shown in Figure 4.

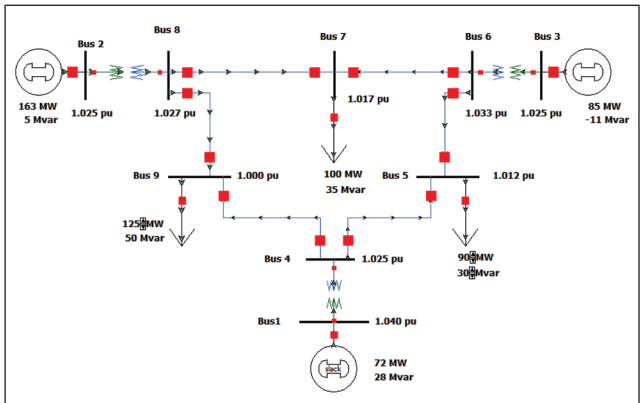

FIG. 4 ON-LINE POWER SYSTEM SECURITY ASSESSMENT

6. CASE STUDY

The trees are constructed using a test set of 30 operating points obtained by varying the system's active load and generation from 50% to 200%, in steps of 5%, of base case and distributing among all buses in proportion to their respective base value. For each operating condition, the performance of the system during the (N-1) line to ground faults is evaluated. With the data generated, the Dynamic Security Database is built. The database is used for the decision tree building and verification and then deployed on on-line where we get real-time system information from the Measurement Units (either the PMU or SCADA) and using these measurements, classify the current operating state as secure or insecure using the Decision Tree.

The Classification Accuracy (CA) and the misclassification of a class (MC) are used as the performance measures for the decision tree.

$$CA\ (\%) = \frac{No.of\ samples\ classified\ correctly}{Total\ number\ of\ samples\ in\ data\ set} \times 100$$

$$MC_S\ (\%) = \frac{No.of\ misclassification\ in\ class\ "secure"}{Total\ number\ of\ samples\ belonging\ to\ class\ "secure"}$$

$$MC_I\ (\%) = \frac{No.of\ misclassification\ in\ class\ "insecure"}{Total\ number\ of\ samples\ belonging\ to\ class\ "insecure"}$$

The details about the cases considered and the splitting of the cases into Learning Set and the Testing set is shown in Table 2. We split the total of cases into a Learning Set, to be used for the creation of the DT and a Testing Set, to test the performance of the DT generated. We split

the total set in the ratio 3:1, i.e 75% of the total cases are taken as Learning Set and the 25% of the cases are taken as the Testing Set.

TABLE 2
DATA FOR BUILDING THE DT FOR DSA

	Learning Set	Testing Set	Total
Cases belonging to class "secure"	91	31	122
Cases belonging to class "insecure"	227	75	302
Total Operating Cases	318	106	424

The resulting Decision Tree is shown in Figure 5. The Decision uses the Phase Angles and the voltages of each bus as well as the real and reactive power flows in each of the transmission lines as the attributes for the decision tree.

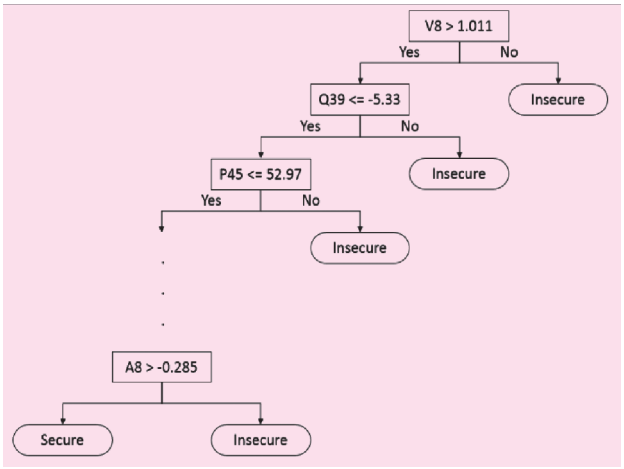

FIG 5. DECISION TREE FOR DYNAMIC SECURITY ASSESSMENT

TABLE 3
PERFORMANCE OF THE DT

	Occur-rences	Number of cases to be classified	Per-centage
Classification Accuracy	82	106	77.36
Misclassification in class "secure"	11	31	35.38
Misclassification in class "insecure"	13	75	17.33

The classification results obtained are shown in Table 3. It can be observed from these results that the usage of Decision Tree to determine the security status of the system is fairly accurate. The security classification problem aims to minimize the misclassification in class "insecure", as they indicate the wrong classification of insecure states, leading to a severe blackout. Thus the Decision tree model capable of predicting the security status of the system accurately and quickly is found suitable for on-line implementation. The real-time measurement of only selected features are used for the classification. Such an application will allow the operator to monitor the status of the system security from time to time, and take appropriate control actions, whenever needed.

7. CONCLUSION

Power system dynamic security analysis is an essential task for protecting power system against credible contingencies. Conventional methods for dynamic security assessment are mainly based on time-domain simulation techniques, which usually suffer from excessively high computational burden and inability to provide useful information about system dynamic security characteristics and guideline for control.

Using the decision trees, this research developed a series of alternative and more efficient algorithms and tools for real-time and information-rich DSA. The proposed method is able to infer stability control rules (for either single- or multi-contingency) from a strategically trained DT. The rules can be readily incorporated into a standard OPF model for on-line preventive control.

The proposed methods for DSA can be applied to other general classification and regression problems in power engineering. In particular, the proposed ensemble learning and decision-making rules for multiple ELMs are able to identify potentially inaccurate ensemble output, hence can be extended to predict confidence interval, which can then be applied to wind power forecasting and electricity price forecasting problems.

REFERENCES

[1] Morison K, Wang, L,Kundur P, "Power system security assessment," *Power and Energy Magazine, IEEE* , vol.2, no.5, pp.30,39, Sept.-Oct. 2004

[2] Kundur P, Paserba, J, Ajjarapu V, Andersson, G.; Bose, A.; Canizares, C.; Hatziargyriou, N.; Hill, D.; Stankovic, A.; Taylor, C.; Van Cutsem, T.; Vittal, V., "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," Power Systems, IEEE Transactions on , vol.19, no.3, pp.1387-1401, Aug. 2004

[3] Pavella, Mania, Damien Ernst, and Daniel Ruiz-Vega. *Transient stability of power systems: a unified approach to assessment and control*. Vol. 581. Springer, 2000.

[4] Balu N, Bertram T, Bose A, Brandwajn, V, Cauley G, Curtice David, Fouad A, Fink L, Lauby M G, Wollenberg B F, Wrubel, Joseph N "On-line power system security analysis," *Proceedings of the IEEE* , vol.80, no.2, pp.262-282, Feb 1992

[5] Kundur, Prabha *Power system stability and control*. Eds. Neal J Balu, and Mark G Lauby. Vol. 7. New York: McGraw-hill, 1994.

[6] K Sun, S Likhate, V Vittal, V Kolluri, and S Mandal, "An online dynamic security assessment scheme using phasor measurements and decision trees," *IEEE Trans. Power Syst*., vol.22, no.4, pp. 1935-1943, Nov. 2007.

[7] Wu, Xindong, "Top 10 algorithms in data mining." *Knowledge and Information Systems* 14.1 (2008): 1-37.

[8] R Diao, K Sun, V Vittal, R O Keefe, M Richardson, N Bhatt, D Stradford, and S Sarawgi, "Decision tree-based online voltage security assessment using PMU measurements,"IEEE Trans. Power Syst., vol. 24, no. 2, pp. 832–839, May 2009.

[9] R Banfield, L Hall, K Bowyer, and W Kegelmeyer, "A comparison of decision tree ensemble creation techniques," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 1, pp. 173–180, Jan. 2007.

[10] L Wehenkel, T Van Cutsem, and M Ribbens-Pavella, "An artificial in-telligence framework for online transient stability assessment of power systems,"IEEE Trans. Power Syst., vol. 4, no. 2, pp. 789–800, May 1989.

[11] M He, J Zhang, and V Vittal, "A data mining framework for on-line dynamic security assessment: Decision trees, boosting, complexity analysis," inProc. 2012 IEEE PES Innovative Smart Grid Technolo-gies (ISGT), Washington, DC, USA, Jan. 2012, pp. 1–8.