Journal of Mines, Metals and Fuels, *71(12A): 30-39; 2023. DOI: 10.18311/jmmf/2023/43590*

Print ISSN : 0022-2755

Journal of Mines, Metals and Fuels

Contents available at: *www.informaticsjournals.com/index.php/jmmf*

Power System Transient Stability Analysis using Decision Tree Classifier- A Case Study on the IEEE 57-Bus System

Rituparna Mukherjee[1]*, Abhinandan De[2], Promit Kumar Saha[1], Susmita Dhar Mukherjee[1], Abhishek Dhar[1] and Saurabh Adhikari[1]

[1]Department of Electrical Engineering, Swami Vivekananda University, Kolkata – 700121, West Bengal, India; rituparnamukherjee@svu.ac.in

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

Abstract

This paper presents a novel method of "power system dynamic security assessment" using "decision tree (DT) classifier". The standard "pattern recognition framework", has been followed in the research work presented in this paper, in order to ensure that real-time implementation of the proposed framework is feasible. With the aim of recognizing the "degree of criticality" associated with various "pre-contingency operational circumstances," the "DTSC" was created and taught offline. The "Decision Tree Security Classifier (DTSC)" was successfully implemented in a simulated environment to recognize a power system's "unforeseen operating conditions" and predict their vulnerability to "post- contingency dynamic insecurity".

Keywords: *Classification, Decision Tree, Dynamic Security, Power System Transient Stability*

1.0 Introduction

Electrical power systems are complex networks designed to produce and supply electrical power reliably and economically to the consumers. In recent years, there has been increasing competition among the power utilities to deliver quality electrical power at affordable rates. De- regulation[1] in electrical power market has further intensified such competition and forced all the three major entities, namely the generation, transmission and distribution system operators to utilize their resources to the maximum possible extent. While this has led the power generators to push the operation of synchronous generators close to their stability limits, the transmission utilities have been compelled to exploit the network capacities to highest possible extent. Operating such overstressed power systems are technically challenging, as any major perturbation can lead to catastrophic consequences, including equipment failure, system collapses and complete black outs. These overstressed power systems have therefore raised serious concerns about operational reliability and have posed new challenges to "power system security". A power system network often experiences severe disturbances like equipment outages, such as outage of some of the generating units, transformers, and transmission lines etc., commonly termed as the "contingencies". Such contingencies often result due to unintended operation and mal-operation of the system protection devices, such as the relays. The relays are generally intended to protect major power equipment

*Author for correspondence

like alternators, transformers and transmission lines from a variety of plausible power system faults. When a fault occurs, the relay dedicated to protect a particular equipment is supposed to operate and isolate the faulty equipment selectively, from healthy part of the system. However, faulty operation of a relay such as a relay mal-tripping may lead to isolation of much larger section of a power system than it is actually necessary to isolate the faulty equipment. The consequences are the sudden loss generators, transformers and important transmission lines, which may challenge "power system security". A power system can be called operationally "secure" if there is little possibility of a "wide- scale system outage" or complete "black out" consequent to any major perturbations, which can result temporary suspension of system operation and interruption of power supply to consumers. It is imperative that operation of a power system must be "secure" under all conditions. The design of a power system should therefore be robust to absorb the consequences of major contingencies, without much impact on "system security". It is also important to follow certain operational practices, which are critical for maintaining "system security", even when some critical equipment is unavailable due to contingencies. "Power system security analysis" is therefore considered one among the most important studies in power system operation and research, which is meant to evaluate the resilience of a power system network against variety of contingencies which a power network may experience in day to day operation. The power system "contingencies", can therefore be viewed as the adverse events which can result undesirable circumstances and operating conditions, which are plausible, but not always predictable with high degree of certainty. "Power system security analysis" includes: "Static Security Analysis (SSA)"[2] and "Dynamic Security Analysis (DSA)"[3]. After a severe disturbance and contingency, power system usually undergoes a change of "state". It is desirable that a power system restores back to "normal" or "stable" state post such contingencies. SSA assumes that stable operation is restored post disturbance and the analysis mainly focuses on whether any kind of "limit violation" or any compromise with system's physical or security parameters occurred in order to reach post-contingency new steady state operating point[4]. In the event of a severe contingency, quick transition to new steady-state operating point is often infeasible and the system may continue to operate in a "quasi-stable state" for a considerably long duration of time[5]. Unlike in SSA, "Dynamic Security Analysis (DSA)"[6,7] involves study of the operating state transition post contingencies. Thus, the "quasi-stable operating state", referred earlier is of greater significance in DSA. There exist several methods for "dynamic security assessment" of power system. "Time Domain Simulation (TDS)" is considered a relatively accurate method for DSA for studying "large disturbances rotor angle stability" analysis, also known as "Transient Stability Analysis (TSA)"[3]. TDS requires representation a power system by a set of non-linear time domain equations to model the dynamic characteristic of every power system equipment. These equations are then solved by "numerical integration" methods in order to assess dynamic behavior of the system post contingency and TSA then analyses whether a disturbance may lead to loss of stability. The major hindrance in performing TSA is the heavy computational overhead, which makes the analysis both time and resource consuming and usually slow. This renders many of the existing DSA techniques unsuitable for real-time application[8]. "Direct method" of TSA, which utilizes "transient energy function" is a viable alternative approach to TDS for determining post contingency operating condition of a power system[9]. However, the "direct method" uses reduced order modeling of a "contingent system", and therefore, usually lacks the high levels of accuracy which TDS offers. It is worth mentioning that, the vulnerable "pre-contingency operating states" of a power system, which can result potential instability and system outages are often unique. As such, almost no exclusive method to reveal such vulnerable operating conditions, fast enough, to be usable in "real-time security assessment" hardly exists. It is, therefore imperative, that developing a powerful and robust "online security monitoring system" is of pivotal importance in order to assess the current "security level" of a power system and to make the power system operator aware of possible security issues. When a security issue is detected, it is also necessary to take appropriate preventive and control actions to avert any possible future system outage and to regain "system security".

"Power system security analysis" has been a major focus area of power system research for long. The review of existing literature reveals that, researchers[8,10] considered "Time Domain Simulation (TDS)" as one

of the most accurate methods for "Dynamic Security Analysis (DSA)" under large perturbations, which is more commonly termed as "Transient Stability Analysis (TSA)"[3]. The TDS method relies on developed mathematical model of a power system network in the form of nonlinear time-domain differential and/or algebraic equations. These equations can presumably represent the dynamic behaviour of generators, loads and other dynamic components present in the power system. Numerical integration is usually performed to solve these equations to obtain the dynamic behaviour of a power system under perturbed conditions. However, these numerical integrations are highly time and resource consuming, and therefore real-time application of TDS in TSA is mostly unsuccessful, as the analysis has to performed very fast, within short time-frame of few tens of milliseconds. The research work in[4] however revealed a novel method to quickly analyse "transient stability" using TDS.

The "direct method", which uses "transient energy function" [11,12] to determine stability of a power system at its new "post-contingency operating point", is an alternative to the TDS method and a workable way for TSA. Comparing the "direct technique" to the "numerical integrations" carried out in TDS, the former requires less computer power. However, because it uses "reduced order modelling" of the post- contingency system and a number of simplifying assumptions and hypotheses, the "direct technique" is likewise less accurate than TDS[13]. In order to get around some of the drawbacks of the old "energy function" method, a new approach put forward in[14] generalised the idea of "energy function" and expanded the standard "energy function" method to create a more expansive "Lyapunov Functions Family (LFF)". Traditionally, the "direct method" was viewed as being unfeasible for TSA in large-scale power system networks. The "direct method" was reportedly used in a recent research study's[15] real-time "dynamic security evaluation" of a very large-scale power system. The power system employed in the case study described in this research had 3000 synchronous generators and 14,500 system buses. The lack of any viable computational solution for quick and accurate real-time DSA prompted the scientific community working on power system security studies to adopt "Machine Learning (ML)" and "Pattern Recognition (PR)" techniques early on. In the latter half of the 1980s, several cutting-edge studies[16-18] attempted to map the relationship between a power system's "pre-contingency operational condition" and the "dynamic security state" following a contingency. Once these underlying correlations could be effectively identified, it was possible to anticipate the "dynamic stability state" for operating instances with unexpected contingencies with the least amount of computational work. The ML/PR based algorithms might even forecast the "pre-contingency operational conditions", which may have caused these "dynamic unsecure" conditions. A strategy to address the "power system transient-stability" problem online was developed in a trailblazing research paper in[16]. The authors suggested using "inductive inference" to create "rules" that connect system parameters with stability in power systems.

The large pool of above-mentioned research works reveal that applications of AI and ML can be effective to ease the computational burden involved in the analysis of "power system security" and therefore, they can be effective in the development of fast, real-time "Dynamic Security Assessment (DSA)" methods[19,20].

The "transient stability-based security evaluation" of power system networks in real-time contexts was the focus of this paper's innovative PR technique. In the research, an effective "Decision Tree based Security Classifier (DTSC)" was created to forecast and categorize the dynamic operational states of power systems into "safe" and "insecure" classes under a variety of operating scenarios and plausible situations. This study work greatly decreased the computational cost by utilizing the effective "Decision Tree (DT) based pattern categorization", which made the suggested method acceptable for real-time use. The "redundant" and "irrelevant" features were removed from the relevant system attributes (features) without significantly losing information. The report included an exemplary case study that illustrated the creation and application of the suggested DTSC for "dynamic security status categorization" in the IEEE 57-bus power system. The suggested method outperformed existing well-known classifiers based on "Support Vector Machine (SVM)", "Method of Least Squares (MLS)", "Learning Vector Quantization (LVQ)", and "Probabilistic Neural Network (PNN)" in terms of accuracy and development/implementation time. The findings were encouraging.

2.0 The Decision Tree Based Security Classifier (DTSC)

The creation of a "security classifier" is intended to categorize the "pre-contingency operating circumstances" of a power system by assessing its susceptibility to "transient instability" in the case of a significant contingency or equipment failure. With the aim of providing real-time "power system dynamic security status prediction and classification," a "Decision Tree Security Classifier," or "DTSC," has been created as a "Dynamic Security Assessment (DSA)-tool". The Supervisory Control and Data Acquisition (SCADA) system was used to acquire real-time power system operational data for the DTSC. The expected "post-contingency dynamic state" of the system—which is either "secure" or "insecure" is the DTSC's output. These security evaluations were conducted under a wide range of severe, but plausible situations. A power system's "pre-contingency operational states" in which there is "zero" possibility of any "critical line-faults" occurring are referred to as "secure" classes (faults which can cause potential instability). Those "pre-contingency operating states" that have at least one (or more) "critical line-faults" present and the potential for future instability are referred to as "insecure" classes. The number of "critical line- faults" that could exist under a given operating condition was used to determine the "index of criticality" of a "pre- contingency operating condition." With the aim of identifying the "degree of criticality" connected to various "pre-contingency operational situations," the "DTSC" was created and taught off-line. In a simulated setting, the "DTSC" was effectively used to identify "unforeseen operational situations" in a power system and forecast its susceptibility to "post-contingency dynamic insecurity." Dynamic Security State Classification by DTSC – a Case Study on IEEE 57-bus system.

An illustrative case study showing development and implementation of the proposed "Decision Tree Security Classifier (DTSC)" for "dynamic security state classification" in the IEEE 57-bus power system has been presented in this case study. The IEEE 57 Bus Test Case represents a portion of the American Electric Power System (in the Midwestern US) as it was in the early 1960's which contains of 57 buses, 7 generators and 42 loads. The schematic diagram shown in Figure 1.

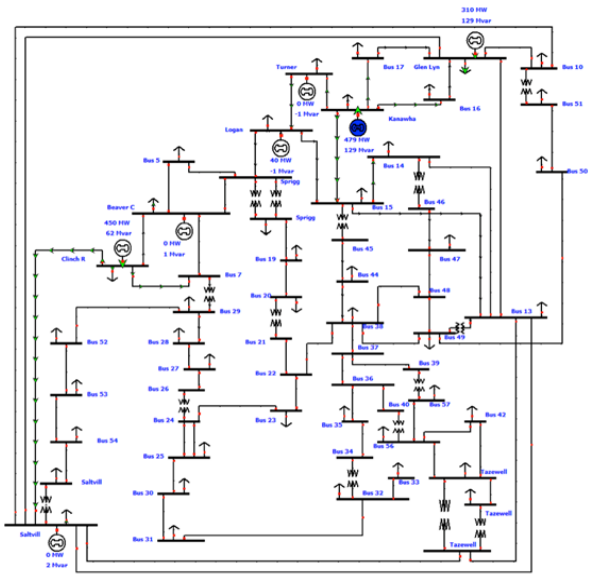

Figure 1. Schematic Diagram of IEEE 57 bus test system.

2.1 Offline Simulation of the IEEE 57 Bus Test System in MATLAB Power System Analysis Toolbox (PSAT)

A "dynamic model" of the IEEE 57-bus system was created in MATLAB based "Power System Analysis Toolbox (PSAT)" for the present study. The "power flow" and "Time Domain Simulation (TDS)" functions, which are available in the "Power System Analysis Toolbox (PSAT)", were used in this case study and the "TDS function" was suitably extended for the calculation of "transient stability".

All simulations were performed on a "desktop PC" running on "Intel Core i7 3.4 GHz CPU with 8GB of RAM". Data files containing power system model-data and contingency information were created to serve as input to the TDS program. The "time domain simulations" were initialized by the "power flow" results. Each "Time Domain Simulation (TDS)" was run over a chosen time-horizon of 200mS (10 cycles), unless the simulation got automatically terminated as a result of singularity arising due to plausible "transient instability". "Transient instability" happened in several cases following major disturbances, such as faults, when the faults were not cleared within tcr. Critical clearing time (tcr) of each line fault was determined by running TDS recurrently, by

varying "fault clearing time" values in the range of 80ms ~ 180ms in steps of 10ms. The computed values of tcr were later used to assess the "security state" of the IEEE 57-bus system.

2.2 Simulation of Pre-Contingency Operating Conditions for Training the DTSC

In the present research work, large numbers of diverse and well-spread "pre-contingency Operating Conditions (OCs)" were simulated by multiple power-flow simulations of the test system. Variable initial starting conditions, such as: diffident load-generation scenarios, changed network topologies arising out of generator, transformer and line outages and their combinations were considered while performing such multiple power-flow simulations. To simulate well-dispersed "pre-contingency OCs" following variations in operating conditions were simulated. Load variations in random sets of 6 buses were considered at a time. The loads were varied in 5 discrete steps of 0.5, 0.75, 1.0, 1.25 & 1.5 p.u. of the "base load" of these selected buses. This procedure was then recursively followed for next 6 randomly chosen buses, not common with any one of the previously selected buses. The process was repeated a total of 7 times to cover all the 42 load buses. In response to changes in the load, generation scenarios also altered, and these changes were reflected in the power-flow solutions. The aforementioned method resulted in 5×6=30 distinct yet plausible load-generation scenarios. The single-generator outage scenarios were mixed with each of the aforementioned 6 loading conditions. A total of 30×8=240 distinct load- generation-generator outage scenarios were simulated, with the IEEE 57 bus system's 7 number generators and "no generator outage" as an additional scenario. Multiple generator outages were not taken into consideration because doing so would greatly increase the number of operating situations that are significantly less credible in real-time operation, making it ineffective to use huge representations of such operating scenarios as training exemplars. Based on the same concept, single line-outage cases were seen as another form of variation in OC. 80 single line-outage scenarios and 100 load-generation patterns were combined to simulate the 80 lines in the test system plus the extra condition of "no line-outage." This led to 81×30=2430 combinations of load-generation-line outages that were mutually incompatible. In order to mimic a comprehensive view of the whole operational area of the IEEE 57-bus test system, 240+2430 = 2670 distinct yet credible initial steady- state OCs were generated.

2.3 Offline Building and Training of the Decision Tree Security Classifier

The Decision Tree Security Classifier (DTSC) was created using a "desktop PC" with an Intel Core i7 3.4 GHz CPU and 8 GB of RAM using the "Python, scikit-learn" framework. The Decision Tree classifier was created using the Classification and Regression Tree (CART) paradigm. The Operating Cases (OCs) produced earlier served as the training set for the DTSC. The goal of the DTSC was to divide the OCs into "secure" and "in-secure" categories. 1780 randomly picked OCs (about 2/3 of all OCs) were utilized to train the DTSC out of the 2670 OCs that were simulated. Remaining 890 cases (approximately 1/3rd of total OCs) were used later as test OCs. Table 1 depicts the distribution of training and test OCs for the DTSC. Both training and test data comprised of 59% secure OCs (shaded with green colour in Table 1) and 41% insecure OCs (shaded with red colour in Table 1).

2.4 Estimation of DTSC-Building and Training Time

With the top-15 highly correlated "feature variable" in as attributes/nodes, a "desktop PC" running on "Intel Core i7 3.4 GHz CPU with 8GB of RAM" accomplished DTSC building and training in just over 4.5 hours with only 1203 iteration. The DT-building and training time in such case exceeded 37 hours with average training cycle time of 49.15 Sec. Thus, DTSC building and training time dropped by more than 87% when using reduced number of "feature variables".

2.5 Training Accuracy of the Developed DTSC

The "training accuracy" of the "DTSC" was evaluated and is depicted in the form of "confusion matrix" of Table 2. The "training accuracy" was found to be encouraging

Table 1. Distribution of training and test data for the DTSC

Security Conditions				No. of credible pre-contingency operating conditions	
Security State	**No. of non-critical lines: A (tcr> 160 mS)**	**No. of moderately critical lines: B (80 > tcr > 160 mS)**	**No. of highly critical lines: C (tcr < 80 mS)**	**Training Samples**	**Test Samples**
Secure	A=80	B=0	C=0	0	0
	79 ≥ A ≥ 55	1 ≤ B ≤ 34	C=0	180	90
	55 ≥ A ≥ 34	34 ≤B ≤ 55	C=0	280	140
	0 ≤ A ≤ 34	B ≥ 55	C=0	570	285
Insecure	0 ≤A ≤ 79	B=(79-A)	C=1	450	225
	0 ≤A ≤77	B=(79-C-A)	2 ≤ C ≤3	220	110
	0 ≤A ≤71	B=(186-C-A)	C > 3	80	40
	Total:			1780	890

Table 2. Confusion Matrix of the "DTSC" for 1780 training cases

		Predicted as		
		Secure	Insecure	
Actual	Secure	**TP=** 1092	FP = 35	TP + FP = 1127
	Insecure	FN = 96	**TN=** 557	FN + TN = 653
		TP + FN= 1188	FP + TN= 592	N = 1780

for a large power network like the IEEE 57-bus system considered in this case-study.

In the training data-set, 96 "insecure OCs" out of 653 originally "insecure OC" were misclassified as "secure OCs". However, the rest 557 "insecure OCs" were correctly classified as "insecure OCs".

- On the contrary, 35 OCs out of 1127 originally "secure OCs" were misclassified as "insecure OCs", while the rest 1092 "secure OCs" were correctly identified as "secure OCs".

Where as

- "TP (True Positive)": when an OC is classified as "secure" when it is truly "secure".
- "FP (False Positive)": an OC is classified as "insecure" when it is truly "secure"

Table 3. Confusion matrix depicting performance of DTSC on890 unseen test OCs

		Predicted as		
		Secure	Insecure	
Actual	Secure	TP = 440	FP = 50	TP + FP =490
	Insecure	FN = 40	TN =360	FN + TN =400
		TP + FN= 480	FP + TN= 410	N = 890

Table 4. Classification performance of DTSC for the 3143training cases

Performance Metric	Ratio of Cases	% value
Classification Accuracy(CA)	800/890	89.9
Composite Misclassification Rate (CMR)	1-0.9	0.1
Secure Misclassification Rate (SMR)	50/490	0.102
Insecure Misclassification Rate (IMR)	40/400	0.1

- "TN (True Negative)": an OC is classified as "insecure" when it is truly "insecure"
- "FN (False Negative)": an OC is classified as "secure" when it is truly "insecure"
- N: Total number of OCs used = TP + FP + TN + FN

A number of metrics were developed and employed to evaluate the performance of the proposed "DTSC" as under using the terminologies explained: numbers of unseen test OCs. "Confusion matrix" in Table 3 depicts the security state classification results of the DTSC for the 890 unseen test OCs. The "DTSC" could capably classify

Table 5. Classification performance of DTSC for unseen test cases performance of DTSC for the 3143 training cases

Performance Metric	Ratio of Cases	% value
Classification Accuracy(CA)	1649/1780	92.64
Composite Misclassification Rate (CMR)	(1-0.926)	0.074
Secure Misclassification Rate (SMR)	35/1127	0.031
Insecure Misclassification Rate (IMR)	96/653	8.24

the unseen cases with only 60-instances of "insecure OC" misclassifications and 70-instances of "secure OC" misclassifications, which results "Secure Misclassification Rate (SMR)" of 10.2% and "Insecure Misclassification Rate (SMR)" of 10%. Table 4 depicts the performance of "DTSC" on 3143- training OCs in terms of the performance metrics defined in equation(1)–(4).

Classification performance of "DTSC" for unseen test operating conditions was evaluated in the way similar to what was done previously for the training cases. The performance metrics defined in equation (1) – (4) were used for a comprehensive assessment of the DTSC's classification efficacy. The results are presented in Table 5.

"Classification Accuracy (CA)" = $(TP + TN)/N$ (1)

"Composite Misclassification Rate (CMR)" = (1 – CA) (2)

"Secure Misclassification Rate (SMR)" $= FP/(TP + FP)$ (3)

"Insecure Misclassification Rate (IMR)" = $FN/(TN + FN)$ (4)

3.0 Performance of the DTSC in Classifying Unseen Test Operating Cases

After the DTSC was successfully built and trained, its "classification performance" was evaluated using 890 numbers of unseen test OCs. "Confusion matrix" in Table 3 depicts the security state classification results of the DTSC for the 890 unseen test OCs. The "DTSC" could capably classify the unseen cases with only 60-instances of "insecure OC" misclassifications and 70-instances of "secure OC" misclassifications, which results "Secure Misclassification Rate (SMR)" of 10.2% and "Insecure Misclassification Rate (SMR)" of 10%.

Classification performance of "DTSC" for unseen test operating conditions was evaluated in the way similar to what was done previously for the training cases. The performance metrics defined in equation (1) – (4) were used for a comprehensive assessment of the DTSC's classification efficacy. The results are presented in Table 5.

3.1 Comparison of Classification Performance of DTSC with Other Classifiers

The effectiveness of the DTSC classification algorithm was also evaluated in comparison to that of other well-known classification algorithms, including the "Support Vector Machine (SVM)", "Method of Least Squares (MLS)", "Learning Vector Quantization (LVQ)", and "Probabilistic Neural Network (PNN)". Tables 8 and 9 show the outcomes of the comparison. It is clear from the data shown in Table 6 that DTSC provided DSA results that were more accurate and trustworthy than those provided by KNNSC. Additionally, it was determined

Table 6. Comparison of performance of differentclassification methods

Classifier Performance Metrics

Classifier	CA (%)	CMR (%)	SMR (%)	IMR (%)
DT	89.9	10	10.2	10
KNN	81.04	18.96	21.16	15.79
SVM	79.9	20.1	28.2	17.1
MLS	76.3	23.7	32.3	18.6
LVQ	74.2	25.8	35.5	22.3
PNN	72.6	27.4	39.4	26.21

Table 7. Comparison of training and execution time ofdifferent classifiers

Classification Method	Classifier Training Time	Execution Time
DT	4.5 hour	180 ms
KNN	8.7 hour	221 ms
SVM	8.2 hour	372 ms
MLS	8.5 hour	585 ms
LVQ	9.1 hour	781 ms
PNN	9.3 hour	ms

that DTSC outperformed other examined classification methods like "SVM," "MLS," "LVQ," and "PNN" in terms of classification performance.

The results presented in Table 7 on the other hand reveal that the DTSC is computationally lighter and more efficient than "KNN", "SVM", "MLS", "LVQ" and "PNN" with shorter training and execution times.

4.0 Conclusion

The "Pattern-Recognition (PR)" methodology was used in this study to propose yet another innovative technique for "Dynamic Security Assessment (DSA)" of electrical power systems in real-time. To analyze and categorize the dynamic operational states of power systems into "safe" and "insecure" classes under a wide range of operating situations and plausible eventualities, an effective "Decision-Tree Security Classifier (DTSC)" was created. The computational cost of the proposed method was minimized through the use of effective Decision Tree (DT) based pattern categorization, which allowed it to be used in real-time. The "redundant" and "irrelevant" elements were eliminated without significantly compromising information by only screening the pertinent system attributes (features). An effective technique for identifying "critical qualities" that are important in the context of "dynamic security state prediction" was found to be "Gini-Index" for "feature screening." The creation and application of the suggested DTSC for real-time DSA have been demonstrated in this work using an illustrative case study on the IEEE 57-bus power system. It performed better than other common classification techniques including "SVM," "MLS," "LVQ," and "PNN," and required less time for both training and execution.

5.0 References

1. Woo CK, King M, Tishler A, Chow LCH. Costs of electricity deregulation. Energy. 2006; 31(6-7):747-68. https://doi.org/10.1016/j.energy.2005.03.002
2. Wehenkel L. Machine learning approaches to power system security assessment. IEEE Intell Syst. 1977; 12(5):60-72. https://doi.org/10.1109/64.621229
3. Kundur P. Power System Stability and Control, McGraw-Hill Education; 1994.
4. Zhang R, Xu Y, Dong ZY, Wong KP. Post- disturbance transient stability assessment of power systems by a self-adaptive intelligent system. IET Gener Transm Distrib. 2015; 9(3):296-305. https://doi.org/10.1049/iet-gtd.2014.0264
5. Laufenberg MJ, Pai MA. A new approach to dynamic security assessment using trajectory sensitivities. EEE Trans Power Syst. 1998; 13(3):953-8. https://doi.org/10.1109/59.709082
6. Dong ZY, Xu Y, Zhang P, Wong KP. Using IS to assess an electric power system's real-time stability. IEEE Intelligent Systems. 2013; 28(4):60-6. https://doi.org/10.1109/MIS.2011.41
7. Sun K, Likhate S, Vittal V, Kolluri VS, Mandal S. An online dynamic security assessment scheme using phasor measurements and decision trees. IEEE Transactions on Power Systems. 2007; 22(4):1935-43. https://doi.org/10.1109/TPWRS.2007.908476

8. James JQ, Hill DJ, Lam AYS, Gu J, Li VOK. Intelligent time-adaptive transient stability assessment system. IEEE Transactions on Power Systems. 2017; 33(1):1049-58. https://doi.org/10.1109/TPWRS.2017.2707501
9. Chang HD, Chu CC, Cauley G. Direct stability analysis of electric power systems using energy functions: Theory, applications, and perspective. Proc IEEE. 1995; 83(1):1497-529. https://doi.org/10.1109/5.481632
10. Morteza S, Wu NE, John SB. Transient stability assessment of large lossy power systems. IET Gener Transm Distrib. 2018; 12(8):1822-30. https://doi.org/10.1049/iet-gtd.2017.0864
11. Rahimi FA, Lauby MG, Wrubel JN, Lee KL. Evaluation of the transient energy function method for on-line dynamic security analysis. IEEE Trans Power Syst. 1993; 8(2):497-507. https://doi.org/10.1109/59.260834
12. Vu TL, Turitsyn K. Lyapunov functions family approach to transient stability assessment. IEEE Trans Power Syst. 2015; 31(2):1269-77. https://doi.org/10.1109/TPWRS.2015.2425885
13. Chiang H. D, Li H, and Tong J, On-Line Transient Stability Screening of a Practical 14,500-Bus Power system: Methodology and Evaluations, High Performance Computing in Power and Energy Systems, pp 335-358, 2013. https://doi.org/10.1007/978-3-642-32683-7_11
14. Ren LY, Tian F, Yan JF, Yu ZH, Su F, Wu T. Online application and fast solving method for critical clearing time of three-phase short circuit in power system. International journal of Smart grid and Clean Energy. 2013; 2(1). https://doi.org/10.12720/sgce.2.1.93-99
15. Wehenkel L, Van Cutsem T, Ribbens-Pavella M. An artificial intelligence framework for on-line transient stability assessment of power systems. IEEE Power Eng Rev. 1989; 9(5):77-8. https://doi.org/10.1109/MPER.1989.4310721
16. Fouad AA, Vekataraman S, Davis JA. An expert system for security trend analysis of a stability-limited power system. IEEE Trans Power Syst. 1991; 6(3):1077-84. https://doi.org/10.1109/59.119249
17. El Sharkawi MA. Vulnerability assessment and control of power system. IEEE/PES Transmission and Distribution Conference and Exhibition: Asian Pacific; 2005. p. 656-60.
18. Aghamohammadi MR, Mahdavizadeh F, Bagheri R. Power system dynamic security classification using Kohenen neural networks. IEEE/PES Power Systems Conference and Exposition Date of Conference; 2009. https://doi.org/10.1109/PSCE.2009.4840047 PMid:19339796
19. Rituparna M, Abhinandan D. Development of an ensemble decision tree-based power system dynamic security state predictor. IEEE Systems Journal. 2020; 14(3):3836-43. https://doi.org/10.1109/JSYST.2020.2978504
20. Rituparna M, Abhinandan D. Real-time dynamic security analysis of power systems using strategic PMU measurements and decision tree classification. Electr Eng; 2020,