Ensemble Methods of Classification for Power Systems Security Assessment

Zhukov, A., Tomin, N., Kurbatsky, V., Sidorov, D., Panasetsky, D., & Foley, A. (2017). Ensemble Methods of Classification for Power Systems Security Assessment. Applied Computing and Informatics, 1-27. DOI: 10.1016/j.aci.2017.09.007

Published in:
Applied Computing and Informatics

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Ensemble Methods of Classification for Power Systems Security Assessment☆

A. Zhukov[a], N. Tomin[a], V. Kurbatsky[a], D. Sidorov[a,*], D. Panasetsky[a], A.Foley[b]

[a] *Energy Systems Institute of Russian Academy of Sciences, Irkutsk, Russia*
[b] *Queen's University Belfast, Belfast, United Kingdom*

Abstract

One of the most promising approaches for complex technical systems analysis employs ensemble methods of classification. Ensemble methods enable a reliable decision rules construction for feature space classification in the presence of many possible states of the system. In this paper the novel techniques based on decision trees are used to evaluate power system reliability. In this work a hybrid approach based on random forests models and boosting model is proposed. Such techniques can be applied to predict the interaction of increasing renewable power, storage devices and intelligent switching of smart loads from intelligent domestic appliances, storage heaters and air-conditioning units and electric vehicles with grid to enhance decision making. This ensemble classification method was tested on the modified 118-bus IEEE power system to examine whether the power system is secured under steady-state operating conditions.

Keywords: power system, ensemble methods, boosting, classification, heuristics, random forests, security assessment.

2010 MSC: 90C59, 68T05

*Corresponding author

Email addresses: zhukovalex13@gmail.com (A. Zhukov), tomin@isem.irk.ru (N. Tomin), kurbatsky@isem.irk.ru (V. Kurbatsky), dsidorov@isem.irk.ru (D. Sidorov), panasetsky@gmail.com (D. Panasetsky), a.foley@qub.ac.uk (A.Foley)

1. Introduction

Assessment of security of bulk electric power systems is expected to become an issue in modern power engineering due to the continued growth in renewable energy generation and the future decentralization and electrification of heating, transport and smart domestic loads in the future smart grid. Trends towards liberalization and the need to expand electricity transmission due to increasing energy demand and generation expansion will result in power grid operating electrical networks at critical conditions, close to admissible security limits [1, 2, 3, 4, 5, 6, 7, 8].

In such conditions unforeseen excess disturbances, weak connections, hidden defects of the relay protection system and automated devices, human factors as well as a great amount of other factors can cause a drop in the system security or even the catastrophic accidents.

An analys of methods for the assessment of security and voltage stability of electric power system shows that the existing traditional approaches cannot be effectively applied online and real time conditions because of their computation complexity. For example, load flow calculation for the assessment of the aftermath of a system component fault, which underlie the classical approach to the assessment of security in electric power systems does not seem to be fully implemented due to complex modeling of the corresponding protections.

Most energy management systems (EMS), for example Siemens, ABB, AREVA etc., use one or more security assessment predictors such as sensitivity matrix, security indicators, distribution factors, fast decoupled load flows etc to reduce the computational effort of the security assessment. These analytical techniques are also usually time consuming and therefore are not always suitable for real-time applications. Moreover, these methods can suffer from the problem of misclassification or/and false alarm, for example in the cases of the "bad data" problem, cyber attackes, serious system topology changes etc. Despite the EMSs wide development, the decision making and onus is usually still with the expertise of the grid operators. However, as the number of market participants,

renewable power sources, storage devices and smart loads increase in the power system both at the transmission (and distribution) level the decision making will become ever more complex [9, 10].

One of the effective solutions to this problem is the use of a combination of traditional approaches on the basis of security indices and machine learning algorithms, such as artificial neural networks (ANNs), support vector machine (SVM) and decision trees (DTs) [11, 12, 13, 14, 10]. The main idea here lies in an intelligent model learning to independently determine the current value of an assumed indicator on the basis of input data, thus identifying the current state of power system. As studies by Wehenkel [15] and Diao [16] show such a modified approach makes it possible to neutralize the drawbacks of traditional algorithmic approaches owing to the original properties of the machine learning technologies [17].

Among machine learning algorithms, some DT algorithms [18], especially those of the "white box" nature, have gained increasing interest because not only do they provide the results of security assessment but they also reveal the principles learned by DTs for security assessment. These principles provide useful decision-making information required to make remedial action against recognized insecure conditions. Moreover, ensemble methods based on DT, such as random forest, boosting-based models, enable reliable decision rules for feature space classification in the presence of many possible states of the power system. This research employs the ensemble methods based on DTs. The calculations involved modifications of bagging models (Random Forest, Bagged CART) and boosting models (Stochastic Gradient Boosting, AdaBoost).

The paper is organized in 6 sections. Section 1 introduces. Section 2 presents the problem statement of security assessment. Section 3 introduces the applications of ensemble DT-based learning for the security assessment in power systems. In Section 4, database preparation with due considerations to power systems with high penetration of wind power generation and other distributed generation (DG) is described. Then, the feasibility of the ensemble DT-based approach is demonstrated in Section 6 using an IEEE 118 test power system.

The concluding remarks are provided in Section 6.

2. Problem Statement

Security is the ability of an electric power system to withstand sudden disturbances without unforeseen effects on the consumers. It is provided by the control capabilities of power systems. During operation the required level of security can be achieved by preventive control actions (before a disturbance) and emergency control actions (after disturbance). Control in the pre-emergency condition is mainly responsibility of the Operator in dispatch control. Naturally there can be situations where decision-making by the dispatch personnel can be insufficient to avoid dangerous situations. The complexity of the problem lies in the fact that most dangerous (pre-emergency) states of electric power system which lead to large-scale blackouts are unique and there is no single algorithm (for solving) to effectively reveal such conditions at the time. The problem gets complicated by the fact that the security limit of electric power system constantly changes. Therefore fast methods for real time security monitoring are required to analyze the current level of security and accurately trace the limit and detect the most vulnerable regions in a power system.

The key idea of the "pre-emergency" control concept is that the voltage instability following an emergency disturbance which accompanies many system emergencies does not develop as fast as the dynamic instability of the power system [6]. Thus, when a phase of slow emergency development occurs, the balance between generation and consumption is maintained for a long time making it possible to detect potentially dangerous states, which appear after the disturbance in order to make the appropriate preventive control actions [1].

To monitor if a power system is within its limit, primary measurement tools such as are SCADA systems and post processing by a state estimator as used [19]. The ENTSO-E [1] network code on operational security requires each trans-

[1] the European Network of Transmission System Operators

mission system operator (TSO) to classify its system according to the system operating states [20]. Figure 1 shows the different operating states of a power system as identified by Liacco [21] and adopted in this work. Kundur et al [22] describes power system stability concisely, details a precise method of classification and explains the real world impications to security and reliability.

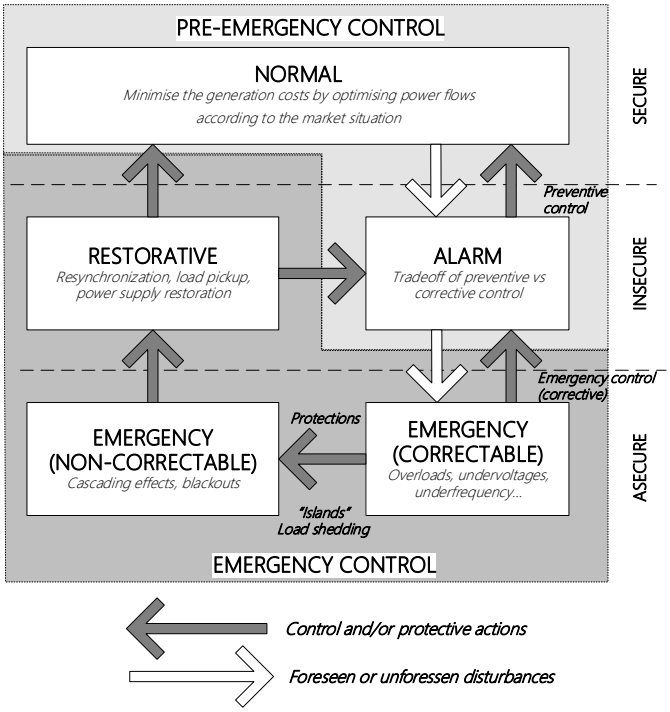

Figure 1: Operating states and transitions

3. Ensemble Learning for the Security Assessment in Power Systems

3.1. Ensembles methods of classifications

A great many studies show that the effective solution to this problem can be found on the basis of machine learning methods which normally include

artificial neural networks, decision trees, ensemble (committee) models, etc. These studies are summarised and discussed in Zhou et al [23].

The ability to solve the problem is related to the capability of the method to fast detect images, patterns (i.e. typical samples) and learning/generalization, which is important to identify instability boundaries at high speed.

One of the advanced approaches to analyse complex technical systems is ensemble methods of classification. This method makes it possible to form reliable decision rules of classification for a set of potential system states. In this approach the key idea is to build a universal classifier of power system states, which is capable of tracing dangerous pre-emergency conditions and predicting emergency situations based on certain system security indices. In this case the detection of dangerous operation patterns is not effective without considering probable disturbance/faults, whose calculation lead to a considerable increase in the computational complexity and a potential decrease in the accuracy for basic algorithms. This leads to need to find a way to improve the accuracy of the classifier of power system states. One of such methods is the creation of ensembles of the classification models and their training.

One of the first most general theory of algorithmic ensembles was proposed in the algebraic approach by Zhuravlev [24]. According to Zhuravlev [24] the composition of N basic algorithms $h_t = C(a_t(x))$, $t = 1, \ldots, N$ is taken to mean a superposition of algorithmic operators $a_t : X \to \mathbb{R}$, of a correction operation $\mathbf{F} : \mathbb{R}^N \to \mathbb{R}$ and decision rule $\mathcal{C} : \mathbb{R} \to Y$ such as $H(x) = \mathcal{C}\left(\mathbf{F}(a_1(x), \ldots, a_N(x))\right)$, where $x \in X$, X is a space of objects, Y is a set of answers, and $\mathbb{R}$ is a space of estimates.

Later Valiant and Kearns [25] were the first question whether or not a weak learning algorithm can be strengthened to an arbitrary accurate learning algorithm. This process was called boosting. Schapire [26] developed the first provable polynomial-time boosting algorithm. It was intended to convert weak models into strong model by constructing an ensemble of classifiers. The main idea of the boosting algorithm is a step-by-step enhancement of the algorithm ensemble. One of the popular implementations of this idea is Schapire's Ad-

aBoost algorithm, which involves an ensemble of decision trees [27].

Another approach to the classification and regression problems using the ensembles was suggested by Breiman [28]. This approach is an extension of the bagging idea. According to this idea, a collective decision can be obtained by using an elementary committee method which classifies an object according to a decision of most of the algorithms. Unlike the boosting method bagging is based on parallel learning of base classifiers. One of the progressive bagging-based approaches is the method called Random Forest [29]. Later there appeared the most effective modifications of both Random forests and boosting algorithms such as Extremely Randomized Trees [30], Oblique Random Forests [31] and Stochastic Gradient Boosting [32].

In the studies on security assessment there are many approaches oriented to the construction of models on the basis of decision trees. These studies are described by Panasetsky et al [1]. These models use both off-line (periodically updated) and on-line methods. Single trees are easily interpretable, yet do not always result in the required accuracy when approximating complex target relationships. Therefore, it is considered reasonable to use compositions.

3.2. Applications in power system security assessment

Several applications involving ensemble DTs have been addressed in real-time transient stability prediction and assessment, voltage security monitoring and estimation, loss of synchronism detection and timing of controlled separation in power systems [15, 16, 18, 33]. A recent approach has combined DT with another data mining tool for prediction performance improvement in the field of dynamic security controls [34]. Vittal et al [16] presented an online voltage security assessment scheme using PMUs and periodically updated DTs. The proposed tree-based model are trained offline using detailed voltage security analysis conducted and updated every hour by including newly predicted system conditions for robustness improvement. Sadeghi at al [13] proposed the AdaBoost algorithm as a new approach in security assessment by classifying pre-fault data of power system. The main benefits of using AdaBoost are a

higher accuracy compared to other machine learning approaches and the ability to display effects of different features in the security assessment problem.

Liu et al [35] proposed a random forest-based approach for online power system security assessment. The results are showed high accuracy in the presence of variance and uncertainties due to wind power generation and other dispersed generation units. The performance of this approach was demonstrated on the operational model of western Danish power system with the scale of around 200 lines and 400 buses. Kamwa et al [36] demonstrated the effectiveness of the random forest-based approach in a PMU predictive assessment of catastrophic power system events. To demonstrate the greatest generalization capability of the methodology, a single Random Forest is shown to have a 99.9% reliability on a large data set containing a mix of 90% instances from the Hydro-Quebec grid and 10% instances from a nine-area test system.

3.3. The problem of confirmation bias

Optimizing a machine learning-based model for security assesment often requires experimentation and tuning. Often, researchers compare their own favorite algorithm, for which they are presumably expert, with a set of competing methods, which they discover while doing the comparative study. For this reason, the compared algorithms often represent the state of the art only for the favorite method, and under such conditions highly biased conclusions may be reached. The analysis of many studies showed that we could not suggest that one particular kind of predictive model would be more appropriate than others [37].

Since the best security model depends on the problem and the data, the engineer must search a very large set of feasible options to find the best model. In operational dispatch management, however, the time is strictly limited. Strict time constraints do not permit much time for experimentation. Researchers tend to deal with this problem by settling for sub-optimal models, arguing that obtained models need only be good enough, or defending use of one technique

above all others. As power grids grow more complex, realizations of power system parameters more quickly changing, these tactics become ineffective.

The key to overcoming these challenges is to use automated modeling techniques. To find the best security assesment model, we need to be able to search across techniques and to tune parameters within techniques. Potentially, this can mean a massive number of model train-and-test cycles to run; we can use heuristics to limit the scope of techniques to be evaluated based on characteristics of the response measure and the predictors.

Therefore, we started from the premise that almost every method (model) may be useful within some restricted context, and summarize the respective strengths and limitations of the various methods so as to highlight their complementary possibilities. Therefore, the power system security assessment tool was developed based on the multi-model machine learning-based approach. In the paper, we propose an automated security assesment technique in order to predict alarm states in power systems based on the caret package in open source R.

4. An Automated Ensemble DT-based Technique for Security Assessment

Ensemble methods enable a reliable decision rules for feature space classification in the presence of many possible states of the system to be build. In this paper, an automated technique based on ensemble DTs learning is proposed for online power system security assessment (Fig. 2).

4.1. Test pattern

Specifically, ensemble DT models are first trained off-line using the cross-validation. For each candidate tuning parameter combination, an ensemble DT model is fit to each resampled data set and is used to predict the corresponding held out samples. The resampling performance is estimated by aggregating the results of each hold-out sample set. Resampling methods try to inject variation into the system to approximate the model's performance on future samples.

These performance estimates are used to evaluate, which combination(s) of the tuning parameters are appropriate. Once the final tuning values are assigned, the final model is refit using the entire training set. The "optimal" model from each ensemble DT technique is selected to be the candidate model with the largest accuracy or the lowest misclassification cost.

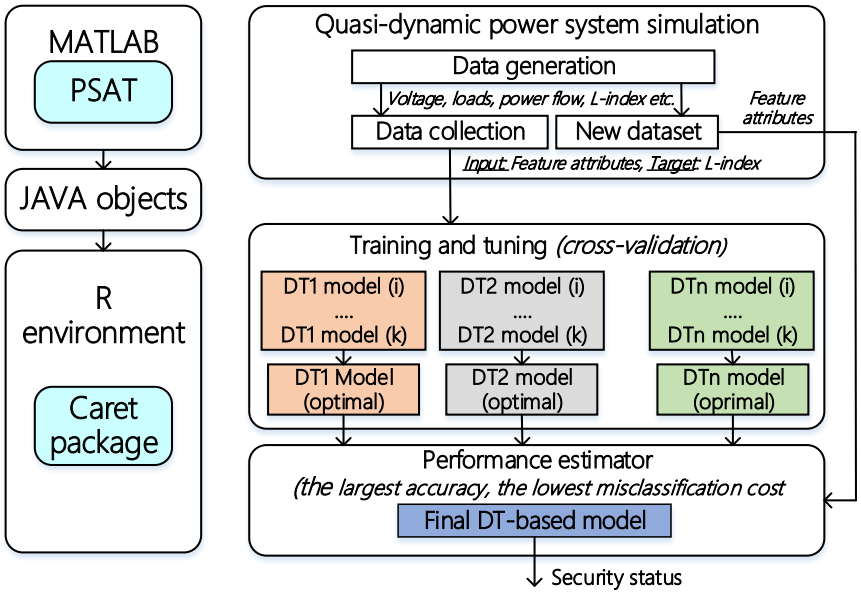

Figure 2: The basic method of the proposed idea.

The primary principle of the approach lies in the ensemble DT method of classification to automatically make a sufficiently accurate assessment of the power system conditions according to the criterion secure/insecure based on the significant classification attributes of a power system state, for example active and reactive power flows, bus voltage, etc. A great amount of such attributes are obtained from randomly generated data samples consisting of a set of really possible states of the electric power system. Depending on the ensemble method applied each decision rule will be trained by its subsampling according to the

bagging and boosting principles. The final decision on the classification of any power system state is made by the generalized classifier according to different principles of simple majority voting, weighted voting or by choosing the most competent decision rule.

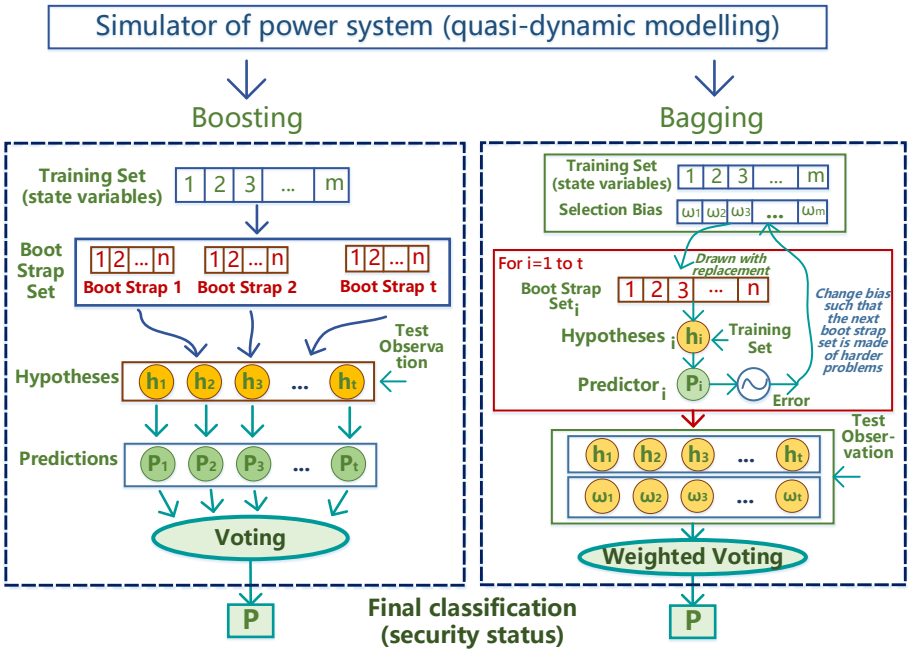

Figure 3: A general scheme of the assessment of potential power system security, using compositional models.

4.2. The Use of L-index in the Problem of Security Assessment

In this study L-index is used because it is one of the effective indices from this group, as a target indicator of system stability when training an ensemble DT model. The L-index is proposed by Kessel and Glavitsch in [38] as an indicator of impeding voltage stability. Starting from the subsequent analysis of a power line equivalent model, a voltage stability index based on the solution to power flow equations is developed. The L-index is a quantitative measure for the

estimation of the distance of the actual state of the system to the stability limit. The L-index describes the stability of the entire system with the expression:

$$L = \max_{j \in \alpha_L} (L_j) \tag{1}$$

where α_L is a set of load nodes. L_j is a local indicator that determines the buses which can be sources of collapse. The L-index varies in a range between 0 (no load) and 1 (voltage collapse) and is used to provide meaningful voltage instability information during the dynamic disturbances in the system.

Kessel and Glavitsch reformulate the local indicator L_j in terms of the power as:

$$L = \left| 1 + \frac{\dot{U}_{0j}}{\dot{U}_j} \right| = \left| \frac{\dot{S}_j^+}{\dot{Y}_{jj}^{+*} U_j^2} \right| = \frac{S_j^+}{Y_{jj}^+ U_j^2}. \tag{2}$$

where Y_{jj}^+ is transformed admittance, U_j is voltage of the load bus j, S_j^+ is transformed complex power, which can be calculated as

$$\dot{S}_J^+ = \dot{S}_j + \left(\sum_{j \in \alpha_L,\, i \neq j} \frac{\dot{Z}_{ji}^* \dot{S}_i}{\dot{Z}_{jj}^* \dot{U}_i} \right) \dot{U}_j,$$

and $\dot{Z}_{ji}^*$, $\dot{Z}_{jj}^*$ are the off-diagonal elements and leading elements of impedance matrix.

Evaluating the L-index as given by (2) each pattern is labeled as belonging to one of the four classes shown in Table 1.

Security Index	Class Category/System State
$0 < L - index \leq 0.3$	Normal state
$0.3 < L - index \leq 0.6$	Alarm state
$0.6 < L - index \leq 0.8$	Emergency correctable state
$L - index > 0.8$	Emergency non-correctable state

Table 1: Class labels for power security analysis.

The obtained labeling of L-index is based on modelling of many test power systems schemes with expert evualation different obtained states as normal,

dangerous and emergency conditions. The criteria for the system states are briefly described as follows:

- Normal state implies that all parameters of the power system are maintained within specified normal operation limits.
- Alarm state implies that some of the system parameters exceed the specified normal limits (for example, bus voltage can exceed 5%, but remain within 10%). Depending on the operation rules, actions can take place to bring the system to the normal state.
- Emergency correctable state implies the system is still intact. However, some system constraints are violated. The system can be restored to the normal state (or at least to the alarm state), if suitable corrective actions are taken.
- Emergency non-correctable state implies that the current situation cannot be corrected and will lead to major emergency. Control actions, like load shedding or controlled system separation are used for saving as much of the system as possible from a widespread blackout.

The performance indices can communicate contingency severity and thus the power system security degree by means of indicative colors [39]. These need to be carefully selected in order to deliver a suggestive message; if remedial actions are needed, for example. As illustrated in Fig.4, a smoothly changing color scale is suitable for that purpose. In this way, the reporting is simple but indicative, suggesting the alarm level and the expected magnitude of remedial actions for improvement of the condition. In the case where the values of the indices exceed the specified limits on security and the high probability of emergency situations that correspond to these values, respective preventive or emergency control measures can be formed.

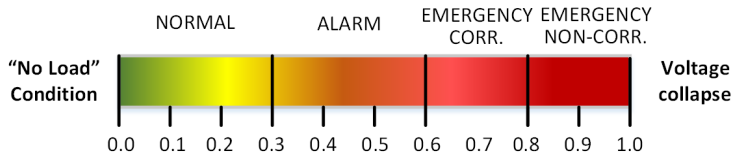

Figure 4: Visualization of power system security degree based on the L-index

5. Case study

The feasibility of this approach in a proof-of-concept has been demonstrated on the IEEE 118 power system consisting of more than 118 buses, 54 generators, and 186 transmission lines[2]. The base load of this system is about 4242 MW and 1438 MVar. An open-source environment R [40] with **caret** package [41] is used as the computing environment for the proposed models' design and testing.

5.1. Data base generation

In the analysis a list of potential power system states for the model learning is formed using quasi-dynamic modeling with a special program in the MATLAB environment (Power System Analysis Toolkit) [42]. The load model was represented by static characteristics depending on voltage. When critical values of voltage are achieved the load is automatically transferred to shunts. The method of a proportional increase in load at all nodes of the test system was optimized for the security analysis in such a way that the initial condition for each emergency disturbance is a stable condition closest to it, from those calculated. Thus, at each stage of an increase in the test scheme load the emergency events (primary disturbances) are randomly modeled by the $N-1$ reliability principle. The disturbances included losses of generation and connection of a large consumer at specified nodes. As a result, the database including a set of various pre-emergency and emergency states of the test scheme is built.

The database contains not only the data as predictor values, but also the target values. A set of the obtained system states was used to calculate the

[2]URL: `http://icseg.iti.illinois.edu/ieee-118-bus-system/`

values of global L-index, and on the basis of local indices L_j. As result, we computed the attribute values and pre-classified based on the L-index the obtained states as "normal", "alarm", "emergency correctable" and "emergency non-correctable". These characteristics were applied as class marks for training and testing the models.

5.2. Estimating Performance For Classification

In this analysis proper performance measurement metrics for classification problems are used. The following metrics are used:

- The overall accuracy of a model indicates how well the model predicts the actual data.
- The Kappa statistic k, takes into account the expected error rate:

$$k = \frac{O - E}{1 - E} \tag{3}$$

where O is the observed accuracy and E is the expected accuracy under chance agreement.

5.3. Ensemble DT Training and Performance

All 3000 cases in the created database were treated equally and 1000 cases (33%) are randomly selected to form a test set. The remaining 2000 ones (66%)were used to form the learning set. Namely, the following DT-based techniques were tested: boosting models - Stochastic Gradient Boosting (SGB), AdaBoost (AB) and bagging models - Random Forest (RF)[3], and Bagged CART [4]. DT models were trained using the cross-validation. For comparison purposes with other learning techniques, such as Extreme Learning Machine (MLP), Support Vector Machine (SVM), were also trained and tested using the same approach.

[3]Random Forest by Randomization (Extremely Randomized Trees)

[4]Conventional Breiman's non-parametric decision tree learning technique

As already discussed, the "optimal" model from each technique is selected to be the candidate model with the largest accuracy. If more than one tuning parameter is "optimal" then the function will try to choose the combination that corresponds to the least complex model. For example, for the Random Forest, *mtry* was estimated to be 124 and $numRandomCuts = 1$ appears to be optimal (Fig. 5).

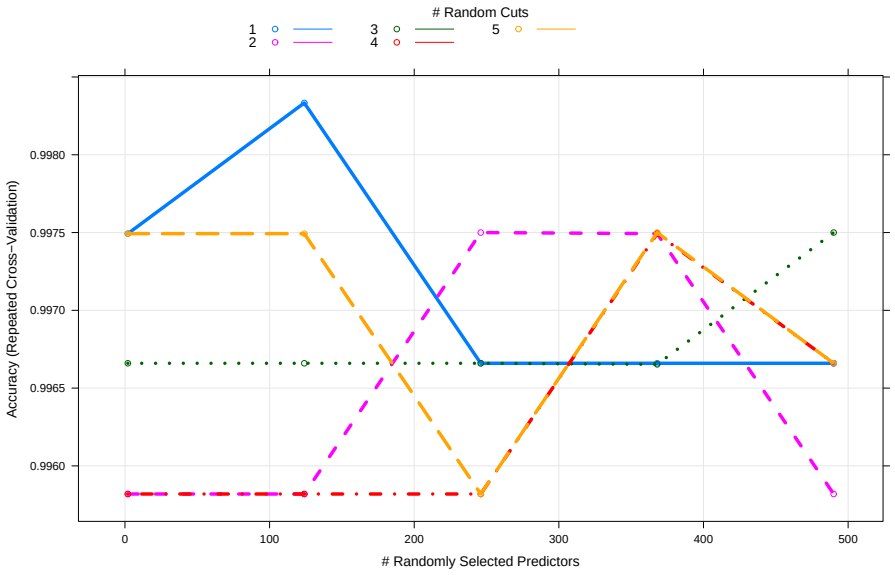

Figure 5: The relationship between the number of Random Forest technique components and the resampled estimate of the area under the cross-validation.

Table 2 shows comparison of accuracy achieved by the classification learning techniques. From Table 2, the comparison indicates that ensemble models produce more accuracy than the simple ones. For this case study, Random Forest and AdaBoost models are the "best" performance techniques to detect dangerous states in the IEEE 118 test system.

Compared with single DT, an ensemble DT model has the advantage that it gives each variable the chance to appear in a different context with different covariates, so as to better reflect its potential effect on the response. The importance of variables in ensemble modeling is computed to assess the contribution

Metrics	Ensemble Methods				Single Methods		
	RF	BCART	AB	SGB	SVM	MLP	Kohonen
Accuracy	99.91	99.74	99.88	99.58	99.83	91.03	96.91
Kappa	99.85	99.56	99.81	99.26	99.70	84.34	94.52

Table 2: Classification accuracy comparison.

of the variables to grow the ensemble model and the relevance of each variable over all DTs in the ensemble model [35]. Figure 6 shows the relative variable importance.

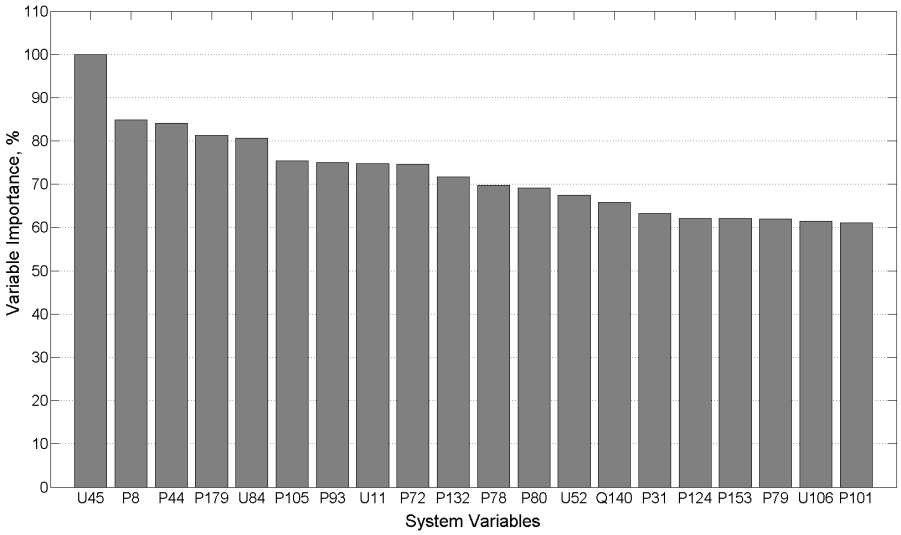

Figure 6: Relative variable importance obtained by computing of mean gini index decrease (where U - voltage of the load bus, P - active power flow, Q - reactive power flow).

5.4. Ensemble DT Performance in the Case of "Corrupted" Data

For comparison purposes the following computational experiements were carried out to compare the traditional and intelligent approaches. By analogy with the previous case study, the steady-states database were generated using quasi-dynamic modeling. All 3000 cases in the created database are treated equally and 1000 cases (33%) were randomly selected to form a test set. However,

the data of a test set were distorted such as 1% of the data was replaced by uniformly distributed random values lying within the limits of the changes of each particular system variables. Such distortions can be caused by a number of reasons, including the presence of "bad data" in telemetry information, cyberattacks, etc. Based on a learning set, approximations of the L-index were constructed using several machine learning methods, including ensemble DT models. Machine learning models were trained using cross-validation. After the trained models were tested using a "corrupted" test set to determine the value of the L-index. For clarity, the problem of regression recovery was solved.

As can be seen from Fig. 7, the traditional algorithmic approach based on the direct calculation of the L-index (according the original approach of Kessel and Glavitsch proposed in [38]) leads to a significant distortion of the assesment. At the same time, as shown in Table 3, all tested intelligent methods show high accuracy. The Random Forest method shows the best result.

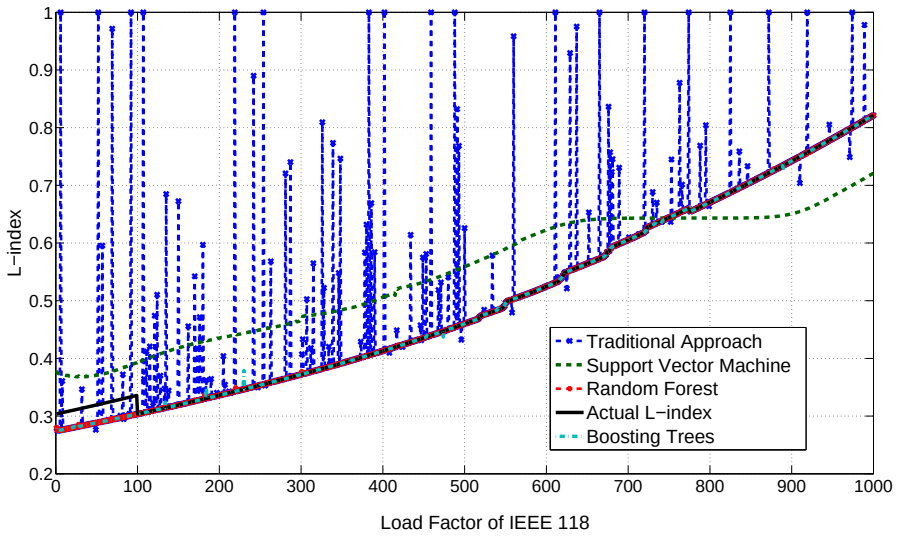

Figure 7: Comparison results of testing different approaches to IEEE 118 security assessment using "corrupted" test set.

The feasibility of dealing with missing data was also tested. Taking into

Table 3: Accuracy of different approaches to IEEE 118 security assessment using "corrupted" test set.

Method	RMSE	Parameters
Random Forest	0.0003	mtry=27
Gradient Boosting	0.0008	n.trees = 150, interaction.depth = 18, shrinkage = 0.1, n.minobsinnode = 10
Support Vector Machine	0.0856	sigma = 0.2751288, C = 0.25
Traditional method	0.0935	

consideration SCADA malfunctions the corrupted patterns were used to train ensemble classification trees. The results showed that the test error rate did not changed even with 50% gaps (Table 4).

% of gaps	time in sec.	test error, %
10	0.0123	0.93
30	0.0411	0.93
50	0.0514	0.93

Table 4: Filling the gaps in data.

These test results clearly show faster, better fitting and more efficient results if the test system model is adapted and updated periodically with new cases rather than using offline cases as used in Beiraghi and Ranjbar [43] and Diao et al [16]. The database can be periodically updated by the new cases together with the existing cases. Finally, a stronger ensemble model can be created immediately with strengthened information of the updated database. This theoretically means that not alone is less computational time required to identify a feasible solution but a better optimal solution is also achieved anabling the TSO to respond better to power system instability.

6. Conclusion

The ensemble classification methods were tested on the modified IEEE 118 power system showing that proposed technique can be employed to examine whether the power system is secured under steady-state operating conditions. The experimental studies showed that the ensemble methods can identify key system parameters as security indicators with high accuracy and, if required, the obtained security tree-based model can produce an alarm for triggering emergency control system. Hypothetically, this outlier identification ensemble method is able to improve the accuracy of power system security assessment to even 100%.

However, even in the case of retraining, the complete training of the ensemble DT model is associated with additional time, which excludes the retraining in real time. The next stage of this work will involve development of an on-line ensemble DT method, which updates the existing model, using new data without its total restructuring.

A potential security ensemble a DT based system can operate in two modes for control the power system states: (1) automatic control (closed loop) which automatically produces the optimal control actions (for example, control the reactive power sources) when interacting with local automation (automatic undervoltage protection, multi-agent automation, etc.) without checking the operator's actions and (2) advisor dispatcher (open loop) which generates control actions that can then be implemented by the dispatcher (for example, change the protective relay settings by decreasing the settings with respect to time, increasing sensitivity of startup signals of the emergency control functions through the selection of an appropriate group of settings, etc.). Overall this ensemble DT based system approach shows potential real world opportunities to enhance and optimize TSO power system stability capabilities. Such an approach will be invaluable in a future power system with increasing numbers of market participants, renewable power sources, storage devices and smart loads both at the transmission (and distribution) level.

Acknowledgements

This work is partly supported by the International science and technology cooperation program of China and Russia, project 2015DFR70850 and by the National Natural Science Foundation of China Grant No. 61673398.

References

[1] D. Panasetsky, N. Tomin, N. Voropai, V. Kurbatsky, A. Zhukov, D. Sidorov, Development of software for modelling decentralized intelligent systems for security monitoring and control in power systems, in: 2015 IEEE Eindhoven PowerTech, 2015, pp. 1–6. doi:10.1109/PTC.2015.7232553.

[2] M. M. Almenta, D. J. Morrow, R. J. Best, B. Fox, A. M. Foley, An analysis of wind curtailment and constraint at a nodal level, IEEE Transactions on Sustainable Energy 8 (2) (2017) 488–495. doi:10.1109/TSTE.2016.2607799.

[3] M. M. Almenta, D. Morrow, R. Best, B. Fox, A. Foley, Domestic fridge-freezer load aggregation to support ancillary services, Renewable Energy 87 (2016) 954–964.

[4] S. Wang, D. Yu, J. Yu, W. Zhang, A. Foley, K. Li, Optimal generation scheduling of interconnected wind-coal intensive power systems, IET Generation, Transmission & Distribution 10 (13) (2016) 3276–3287.

[5] P. Higgins, K. Li, J. Devlin, A. Foley, The significance of interconnector counter-trading in a security constrained electricity market, Energy Policy 87 (2015) 110 – 124. doi:https://doi.org/10.1016/j.enpol.2015.08.023.
URL http://www.sciencedirect.com/science/article/pii/S0301421515300689

[6] S. Wang, N. Chen, D. Yu, A. Foley, L. Zhu, K. Li, J. Yu, Flexible fault ride through strategy for wind farm clusters in power systems with high

wind power penetration, Energy Conversion and Management 93 (2015) 239 – 248. doi:https://doi.org/10.1016/j.enconman.2015.01.022.
URL http://www.sciencedirect.com/science/article/pii/S0196890415000266

[7] A. Foley, B. Tyther, P. Calnan, B. . Gallachir, Impacts of electric vehicle charging under electricity market operations, Applied Energy 101 (2013) 93 – 102, sustainable Development of Energy, Water and Environment Systems. doi:https://doi.org/10.1016/j.apenergy.2012.06.052.
URL http://www.sciencedirect.com/science/article/pii/S0306261912004977

[8] Y. Li, Z. Wen, Y. Cao, Y. Tan, D. Sidorov, D. Panasetsky, A combined forecasting approach with model self-adjustment for renewable generations and energy loads in smart community, Energy 129 (2017) 216 – 227. doi:https://doi.org/10.1016/j.energy.2017.04.032.
URL http://www.sciencedirect.com/science/article/pii/S0360544217305972

[9] J. B. A. London, S. A. R. Piereti, R. A. S. Benedito, N. G. Bretas, Redundancy and observability analysis of conventional and pmu measurements, IEEE Transactions on Power Systems 24 (3) (2009) 1629–1630. doi:10.1109/TPWRS.2009.2021195.

[10] P. Gopakumar, M. J. B. Reddy, D. K. Mohanta, Transmission line fault detection and localisation methodology using pmu measurements, IET Generation, Transmission Distribution 9 (11) (2015) 1033–1042. doi:10.1049/iet-gtd.2014.0788.

[11] L. Wehenkel, The title of the work, Ph.D. thesis, Machine Learning Approaches to Power System Security Assessment, University of Liege (7 1995).

[12] R. Diao, K. Sun, V. Vittal, R. J. O'Keefe, M. R. Richardson, N. Bhatt, D. Stradford, S. K. Sarawgi, Decision tree-based online voltage security

assessment using pmu measurements, IEEE Transactions on Power Systems 24 (2) (2009) 832–839. doi:10.1109/TPWRS.2009.2016528.

[13] M. Sadeghi, M. A. Sadeghi, S. Nourizadeh, A. M. Ranjbar, S. Azizi, Power system security assessment using adaboost algorithm, in: Proceedings of the North American Power Symposium (NAPS 2009), Starkville, Mississipp, Citeseer, 2009.

[14] S. Kalyani, K. S. Swarup, Design of pattern recognition system for static security assessment and classification, Pattern Analysis and Applications 15 (3) (2012) 299–311. doi:10.1007/s10044-011-0218-x.
URL http://dx.doi.org/10.1007/s10044-011-0218-x

[15] L. Wehenkel, Machine learning approaches to power-system security assessment, IEEE Expert 12 (5) (1997) 60–72. doi:10.1109/64.621229.
URL http://dx.doi.org/10.1109/64.621229

[16] R. Diao, K. Sun, V. Vittal, R. OKeefe, M. Richardson, N. Bhatt, D. Stradford, S. Sarawgi, Decision tree-based online voltage security assessment using PMU measurements, IEEE Transactions on Power Systems 24 (2) (2009) 832–839. doi:10.1109/tpwrs.2009.2016528.
URL http://dx.doi.org/10.1109/tpwrs.2009.2016528

[17] D. K. Bhattacharyya, J. K. Kalita, Network Anomaly Detection: A Machine Learning Perspective, Chapman & Hall/CRC, 2013.

[18] K. Sun, S. Likhate, V. Vittal, V. S. Kolluri, S. Mandal, An online dynamic security assessment scheme using phasor measurements and decision trees, IEEE Transactions on Power Systems 22 (4) (2007) 1935–1943. doi:10.1109/tpwrs.2007.908476.
URL http://dx.doi.org/10.1109/tpwrs.2007.908476

[19] K. Morison, L. Wang, P. Kundur, Power system security assessment, IEEE Power and Energy Magazine 2 (5) (2004) 30–39.

[20] Entso-e. network code on operational security. 24 september 2013 [ ], : http://networkcodes.entsoe.eu/operational-codes/operational-security/.

[21] T. E. D. Liacco, Power/energy: System security: The computer's role: Several security-related functions can be aided by the digital computer, and linked together by a software scheme, IEEE Spectrum 15 (6) (1978) 43–50. doi:10.1109/MSPEC.1978.6367726.

[22] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. V. Cutsem, V. Vittal, Definition and classification of power system stability ieee/cigre joint task force on stability terms and definitions, IEEE Transactions on Power Systems 19 (3) (2004) 1387–1401. doi:10.1109/TPWRS.2004.825981.

[23] Y. Zhou, J. Wu, Z. Yu, L. Ji, L. Hao, A hierarchical method for transient stability prediction of power systems using the confidence of a svm-based ensemble classifier, Energies 9 (10).

[24] Y. I. Zhuravlev, On the algebraic approach to solving the problems of recognition and classification, Problemy kibernetiki 33 (1978) 5–68.

[25] M. Kearns, L. Valiant, Cryptographic limitations on learning boolean formulae and finite automata, J. ACM 41 (1) (1994) 67–95. doi:10.1145/174644.174647.
URL http://doi.acm.org/10.1145/174644.174647

[26] R. E. Schapire, The Boosting Approach to Machine Learning: An Overview, Springer New York, New York, NY, 2003, pp. 149–171. doi:10.1007/978-0-387-21579-2_9.
URL http://dx.doi.org/10.1007/978-0-387-21579-2_9

[27] Y. Freund, R. E. Schapire, Experiments with a new boosting algorithm, in: L. Saitta (Ed.), Proceedings of the Thirteenth International Conference on Machine Learning (ICML 1996), Morgan Kaufmann, 1996, pp. 148–156.

URL http://www.biostat.wisc.edu/~kbroman/teaching/statgen/2004/refs/freund.pdf

[28] L. Breiman, Random forests, Machine Learning 45 (1) (2001) 5–32. doi:10.1023/A:1010933404324.
URL http://dx.doi.org/10.1023/A:1010933404324

[29] A. Saffari, C. Leistner, J. Santner, M. Godec, H. Bischof, On-line random forests, in: Computer Vision Workshops (ICCV Workshops), 2009 IEEE 12th International Conference on, IEEE, 2009, pp. 1393–1400.

[30] P. Geurts, D. Ernst, L. Wehenkel, Extremely randomized trees, Machine Learning 63 (1) (2006) 3–42. doi:10.1007/s10994-006-6226-1.
URL http://dx.doi.org/10.1007/s10994-006-6226-1

[31] B. H. Menze, B. M. Kelm, D. N. Splitthoff, U. Koethe, F. A. Hamprecht, On oblique random forests, in: Proceedings of the 2011 European Conference on Machine Learning and Knowledge Discovery in Databases - Volume Part II, ECML PKDD'11, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 453–469.
URL http://dl.acm.org/citation.cfm?id=2034117.2034147

[32] J. H. Friedman, Stochastic gradient boosting, Comput. Stat. Data Anal. 38 (4) (2002) 367–378. doi:10.1016/S0167-9473(01)00065-2.
URL http://dx.doi.org/10.1016/S0167-9473(01)00065-2

[33] C. T. S. Rovnyak, Y. Shengl, Decision trees using apparent resistance to detect impending loss of synchronism, IEEE Trans. Power Del. 15 (4) (2000) 1157–1162. doi:10.1109/61.891496.
URL https://doi.org/10.1109/61.891496

[34] E. Voumvoulakis, N. Hatziargyriou, Decision trees-aided self-organized maps for corrective dynamic security, IEEE Transactions on Power Systems 23 (2) (2008) 622–630. doi:10.1109/tpwrs.2008.920194.
URL http://dx.doi.org/10.1109/tpwrs.2008.920194

[35] Z. C. Ch. Liu, C. L. Bak, P. Lund, Dynamic security assessment of western danish power system based on ensemble decision trees, in: Proceedings of the 12th IET Inter. Conf. on Developments in Power System Protection (DPSP 2014), DPSP 2014, Copenhagen, 2014, pp. 1–6.
URL https://doi.org/10.1049/cp.2014.0150

[36] I. Kamwa, S. R. Samantaray, G. Joos, Catastrophe predictors from ensemble decision-tree learning of wide-area severity indices, IEEE Transactions on Smart Grid 1 (2) (2010) 144–158. doi:10.1109/tsg.2010.2052935.
URL http://dx.doi.org/10.1109/tsg.2010.2052935

[37] M. Kuhn, Building predictive models in r using the caret package, Journal of Statistical Software 28 (5) (2008) 1–26.

[38] P. Kessel, H. Glavitsch, Estimating the voltage stability of a power system, IEEE Transactions on Power Delivery 1 (3) (1986) 346–354. doi:10.1109/tpwrd.1986.4308013.
URL http://dx.doi.org/10.1109/tpwrd.1986.4308013

[39] U. Kerin, C. Heyde, R. Krebs, E. Lerch, Real-time dynamic security assessment of power grids, The European Physical Journal Special Topics 223 (12) (2014) 2503–2516. doi:10.1140/epjst/e2014-02272-1.
URL https://doi.org/10.1140/epjst/e2014-02272-1

[40] L. Leemis, Learning Base R, Lightning Source, 2016.
URL http://www.amazon.com/Learning-Base-Lawrence-Mark-Leemis/dp/0982917481

[41] M. K. C. from Jed Wing, S. Weston, A. Williams, C. Keefer, A. Engelhardt, caret: Classification and Regression Training, r package version 5.15-044 (2012).
URL http://CRAN.R-project.org/package=caret

[42] F. Milano, An open source power system analysis toolbox, IEEE Trans-

actions on Power Systems 20 (3) (2005) 1199–1206. doi:10.1109/TPWRS.2005.851911.

[43] M. Beiraghi, A. Ranjbar, Online voltage security assessment based on wide-area measurements, IEEE Trans. on Power Delivery 28 (2) (2013) 989–997. doi:10.1109/TPWRD.2013.2247426.
URL https://doi.org/10.1109/TPWRD.2013.2247426