An Online Dynamic Security Assessment Scheme Using Phasor Measurements and Decision Trees

Kai Sun, *Member, IEEE*, Siddharth Likhate, *Student Member, IEEE*, Vijay Vittal, *Fellow, IEEE*, V. Sharma Kolluri, *Senior Member, IEEE*, and Sujit Mandal, *Member, IEEE*

***Abstract*—This paper describes an online dynamic security assessment scheme for large-scale interconnected power systems using phasor measurements and decision trees. The scheme builds and periodically updates decision trees offline to decide critical attributes as security indicators. Decision trees provide online security assessment and preventive control guidelines based on real-time measurements of the indicators from phasor measurement units. The scheme uses a new classification method involving each whole path of a decision tree instead of only classification results at terminal nodes to provide more reliable security assessment results for changes in system conditions. The approaches developed are tested on a 2100-bus, 2600-line, 240-generator operational model of the Entergy system. The test results demonstrate that the proposed scheme is able to identify key security indicators and give reliable and accurate online dynamic security predictions.**

***Index Terms*—Decision trees, online dynamic security assessment, phasor measurements, preventive control, transient stability.**

NOMENCLATURE

A_X_Y	Voltage phase angle of bus X minus that of bus Y.
CA	Critical attribute.
$c(i\|j)$	Cost for misclassifying a class j case as class i.
CR_i^{ts}	DT correctness rate for classifying class i cases.
CSR	Critical splitting rule.
DT	Decision tree.
FB	Faulted bus.
OC	Operating condition.
PMU	Phasor measurement unit.
P_X_Y	MW-flow from bus X to bus Y.
R^{ts}	DT misclassification cost.
ΔR^{ts}	Standard error estimate for R^{ts}.
S	Insecurity score for a path.
S_M	Upper limit of S. $S > S_M$ means an insecure path.

I. INTRODUCTION

WIDE AREA measurements (WAMS) using synchronized phasor measurement units (PMUs) are being extensively adopted across the North American interconnection to monitor power systems. PMU-based measurements are extensively used in the WECC for a wide range of applications including situational awareness for operational decision making. A number of novel applications that utilize measurements from PMUs to determine small signal oscillatory modes, model parameter identification, and post scenario system analysis have also been developed [1]–[10]. With the initiation of the Eastern Interconnection Phasor Project (EIPP) [11], [12] new opportunities have arisen to incorporate measurements from PMUs in real time analysis to evaluate system dynamic performance. Recent efforts involving the use of PMU measurements for voltage stability analysis and monitoring power system dynamic behavior have been developed [13]–[18].

This paper presents an approach to online dynamic security assessment using PMU measurements. The technique is developed using the operational model of the Entergy system. Entergy is one of the companies involved in the EIPP effort. Its operational model includes 2100-buses, 2600-lines, and 240-generators. Based on the load forecast and information regarding component availability, Entergy has the capability to provide an accurate representation of the online system for a 24-h horizon. This includes the network power flow database and the associated dynamic data and modeling specification needed to conduct detailed time-domain (T-D) simulations. The proposed scheme is developed in three stages.

1) For the 24-h horizon online system data, a series of operating conditions representing the projected variation in daily load together with the unit commitment-based generation pattern are obtained using power flows. Exhaustive T-D simulations for "$n-1$" contingencies and probable "$n-k$" contingencies are conducted on the generated cases and stored in a database.
2) A decision tree (DT) is then trained using the database obtained. The DT is used to identify critical attributes (CAs) from system parameters that characterize the system dynamic performance and evaluate their thresholds that result in insecurity.
3) These CAs serve as the measurements to be made using PMUs. For contingencies analyzed, the real time measurements are compared to their thresholds stored in the DT to determine related paths and terminal nodes. An insecurity score is calculated for each path. If any score exceeds a preset limit and the associated contingencies have high

Manuscript received May 22, 2007; revised July 12, 2007. This work was supported by the National Science Foundation under Grant NSF EEC-9908690 at the Power System Engineering Research Center. Paper no. TPWRS-00354-2007.

K. Sun, S. Likhate, and V. Vittal are with the Department of Electrical Engineering, Arizona State University, Tempe, AZ 85287 USA (e-mail: ksun@epri.com; siddharth.likhate@asu.edu; vijay.vittal@asu.edu).

V. S. Kolluri and S. Mandal are with Entergy Services, Inc., New Orleans, LA 70403 USA (e-mail: vkollur@entergy.com; smandal@entergy.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRS.2007.908476

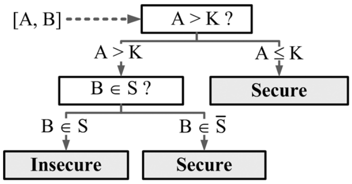


Fig. 1. Simple 5-node DT example.

probabilities of occurrence, appropriate preventive control can be designed and armed.

The subject of online dynamic security assessment by machine learning techniques has been addressed in [19]–[27]. In these previous attempts, DTs have been generated offline to identify CAs that accurately characterize system security. Potential insecurity is then identified by simply observing these CAs using traditional SCADA-based data which is not necessarily synchronized across the system. The application of wide-area-based PMU measurements allows the synchronized monitoring of the CAs and their variation with changing system conditions. Most previous efforts make security predictions based on the security classes assigned to the terminal nodes. This is based on the assumption that the attributes and their thresholds decided by training data are always valid and accurate. However, if some unpredictable system conditions occur, the training data, and the CAs or thresholds may lack validity. As a result, the terminal nodes, which are sensitive to CAs and their thresholds, will also be unreliable. The scheme proposed in this paper can give more reliable security predictions based not only on the terminal nodes but all nodes of the related paths of the DTs.

The rest of this paper is organized as follows. Section II introduces the DT technique used in this scheme; Section III describes the details of the scheme proposed; Entergy's online case is analyzed in Section IV to show the scheme's performance; finally, conclusions are provided in Section V.

II. Decision Trees

The DTs developed in the proposed scheme are all classification trees of the classification and regression trees (CART) methodology introduced by Breiman *et al.* [28]. As shown in Fig. 1, a DT can predict the classification (e.g., "secure" or "insecure") of an object. The object is represented by a vector comprising of the values of a group of critical attributes (CAs, e.g., A and B in Fig. 1). The classification process consists of dropping the vector of CAs down the DT starting at the root node until a terminal node is reached along a path, the class assigned to which is the classification result. At each inner (nonterminal) node, a question (i.e., a splitting rule) concerning a CA is asked to decide which child node the vector should drop into. For numerical variable A, the question compares it with a threshold; for categorical variable B, the question checks whether it belongs to a specified set.

A DT is built from a learning set and a test set. Each of their elements (i.e., cases) consists of a classification and a vector comprising of the values of a group of CA candidates (called "predictors"). The building process initially grows a maximal (i.e., large enough) tree by recursively splitting a set of learning cases (i.e., a parent node) into two purer subsets (i.e., two new child nodes). To achieve each split, all possible splitting rules related to predictors are scored by how well different classes of cases in the parent node are separated. Here, the score is calculated by the GINI rule [28]. The splitting rule with the highest score is selected and called a "critical splitting rule" (CSR). The other splitting rules are called "competitors". Some splitting rules that can completely mimic the action of the CSR are called "surrogates". A competitor with the same improvement score as that of the CSR can generate an equivalently good split and a surrogate can generate exactly the same split as the CSR. The maximal tree is then pruned to generate a series of smaller DTs. The test set is used to test their performance. A commonly used index is the misclassification cost, which is calculated using

$$R^{ts} = \frac{1}{N^{ts}} \sum_{i,j} c(i|j) \cdot N_{ij}^{ts} \tag{1}$$

where N^{ts} is the number of test cases, $c(i|j)$ is the cost of misclassifying a class j case as a class i case. N_{ij}^{ts} is the number of the class j cases whose predicted class is i. To avoid missing insecure cases in online security assessment, the cost of misclassifying an insecure case as "secure" is often larger than that of misclassifying a secure case. The correctness rate for classifying class i cases is denoted by CR_i^{ts}

$$\mathrm{CR}_i^{ts} = N_{ii}^{ts} / N_i^{ts} \times 100\% \tag{2}$$

where N_i^{ts} is the number of class i test cases. For a sufficient number of test cases, a smaller R^{ts} generally corresponds to a better DT. If statistical errors are considered, the standard error estimate for R^{ts} (denoted by ΔR^{ts}) is calculated by

$$\Delta R^{ts} = \left[R^{ts}(1 - R^{ts}) / N^{ts} \right]^{1/2}. \tag{3}$$

Two DTs whose cost difference is smaller than the standard error estimate of either one have almost equal performance. Finally, from the series of DTs generated, the best DT could be selected based on either of the following criteria: the DT with the minimal R^{ts} (denoted by R_m^{ts}) or the smallest-sized DT whose cost is within $R_m^{ts} \pm \Delta R_m^{ts}$. The approach used in this paper selects the DT with the minimal R^{ts}.

III. Proposed Scheme

A flowchart describing the DT-based online security assessment scheme is given in Fig. 2. Details of the scheme are introduced and then some related issues are discussed.

A. DT-Based Online Security Assessment Scheme

The scheme consists of three stages:

1) Offline DT Building: This stage is executed offline to generate a database of cases and build a DT for a 24-h horizon. Initially, N_{OC} prospective operating conditions (OCs) in the next 24 h are obtained from short-term load forecast and unit commitment programs to sufficiently reflect prospective power flow profiles and network topologies. N_C contingencies based on types, locations, fault duration, etc., are either assumed widely in the power system or selected by the operator from a history of critical contingencies and the OCs represented by the cases analyzed. For each OC, detailed T-D simulations of all the N_C

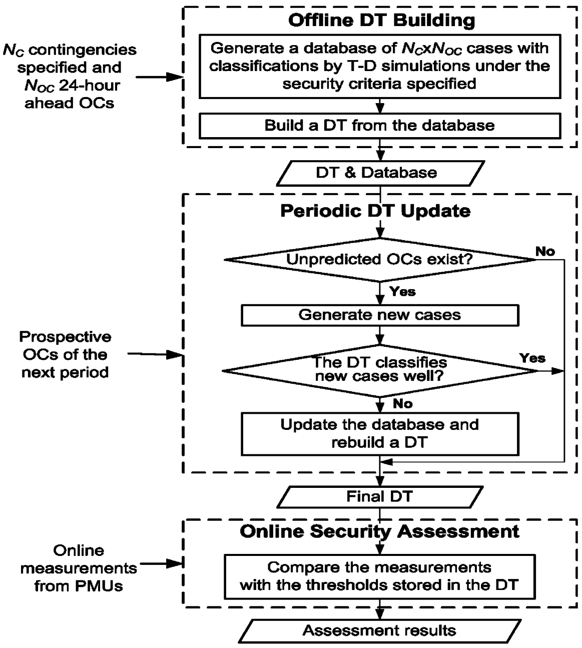

Offline DT Building
N_C contingencies specified and N_{OC} 24-hour ahead OCs
Generate a database of N_CxN_{OC} cases with classifications by T-D simulations under the security criteria specified
Build a DT from the database
DT & Database
Periodic DT Update
Unpredicted OCs exist?
No
Yes
Generate new cases
Prospective OCs of the next period
The DT classifies new cases well?
Yes
No
Update the database and rebuild a DT
Final DT
Online Security Assessment
Online measurements from PMUs
Compare the measurements with the thresholds stored in the DT
Assessment results

Fig. 2. DT-based online security assessment scheme.

contingencies are executed. Specified security criteria dealing with transient stability, transient voltage dip, transient frequencies, and damping ratios are then checked to determine the security classification for each case. The classifications may be binary, i.e., "secure" (if no criterion is violated) and "insecure" (otherwise) or multiple, e.g., "transient instability," "insufficient damping," "voltage insecurity," and "frequency insecurity" with different priorities assigned to criteria. Thus, the class of an insecure case is determined by the criterion with the highest priority. Finally, a database of $N_C \times N_{\mathrm{OC}}$ cases each including a security classification and a vector of predictor values is generated and further divided into a learning set and a test set.

Then, a group of predictors is selected from either fault-dependent variables, e.g., the fault type and location, or fault-independent variables, e.g., bus voltage angles, MW transfers across lines or interfaces, outputs of generators, etc. Some predictors critical to the system's security are screened out as CAs to form CSRs of the DT. Fault-independent CSRs are particularly of interest because they define the insecure regions in the space of the fault-independent CAs, where the current OC can be located. To exactly determine the location of the OC, it is generally necessary to obtain accurately synchronized values of fault-independent CAs. A number of PMUs have been installed in many power systems and provide accurately synchronized measurements of frequently changing parameters typically including the voltages of the buses where they are installed and the currents and power flows of the branches connected to the bus. If impedances of the branches are constant, then voltage angles of the other ends of the branches can also be acquired. Thus, the synchronized measurements from PMUs are good candidates for fault-independent predictors. In addition, predictors can be selected from the parameters monitored by the SCADA system if they change infrequently, e.g., outputs of generators. In this case the measurements obtained may not be synchronized.

Then, classification tree algorithms build a DT from the learning and test sets. CAs and CSRs are decided from all predictors and are stored in each inner node. The DT built could be two-class ("insecure" or "secure") or contain $K+1$ classes if K insecure classes are concerned. If storage space allows, even K two-class DTs could be built at the same time, each of which focuses on one type of insecurity.

2) Periodic OC Prediction and DT Updating: The time horizon is divided into periods of equal length (typically, several minutes to tens of minutes), depending on the speed of computers used. The DT update is executed for each period to predict the performance of the DT for the upcoming period and rebuild a new DT if necessary.

Prospective OCs in the next period can be predicted using a short-term load forecast and the associated unit commitment rules. If the prospective OCs are close to any of the N_{OC} OCs already considered, the DT will remain unchanged until the next period. If new OCs appear the DT may not perform well. Thus, the N_C contingencies will be simulated again at the new OCs to generate new cases, which are used to test the existing DT. If its performance is still satisfactory the DT remains frozen until the next period in the time horizon. Otherwise, the new cases together with the old are used to build a new DT.

The speed of building a DT from scratch is illustrated as follows. For the case studied in the next section, 280 "$n-1$" contingencies are considered for 56 OCs of the operational representation of the Entergy system. Thus, 15 680 simulations are needed. Using a PC with a single Pentium 4 3.4-GHz CPU, each simulation takes 5~10 s and the 280 simulations for each OC are completed within 50 min. Since all simulations are independent, they can be executed on a system with multiple parallel CPUs to accelerate the computation time. Finally, CART's growing and pruning processes are extremely fast (a few seconds) such that an iterative DT building procedure may be designed to quickly generate a better DT from the simulation results. Comparatively, updating an existing DT takes much less time since it just executes simulations for new OCs and then builds a new DT from the updated database. When parallel processors are used, it is possible to finish the DT update within several minutes or even faster. The scheme continuously updates the DT to avoid missing any significant OC change in terms of the power flow pattern or the network topology.

3) Online Security Assessment: In real time, the control center obtains synchronized measurements of fault-independent CAs to perform dynamic security assessment for either one or a group of contingencies. To consider a general case, assume that $N_C' \ (1 \leq N_C' \leq N_C)$ contingencies are considered. The following procedure can predict security and give guidelines for preventive control.

i) Deciding a sub tree only for the N_C' contingencies: Prune all branches of the DT that do not correspond to the fault-dependent CAs already known (if any) to produce a more compact tree (denoted by DT') dealing with only the N_C' contingencies. Specially, when $N_C' = N_C$, no branch is removed.

ii) Dynamic security assessment: Unlike the traditional DT classification methods, which are based only on the classification result given by a terminal node, the scheme proposed in this paper employs a paths-based method, which scores insecurity for each associated path and then gives a classification result based on the path's insecurity score. The new method can give more reliable assessment results against perturbations of OCs. The synchronized measurements of fault-independent CAs are dropped down DT to determine all associated paths as well as terminal nodes. An overall insecurity score S is calculated for each path by (4)

$$S=\sum_{j=1}^{K}\left(\lambda_j\cdot\sum_{i=1}^{L}\omega_i\cdot p_{ij}\right)\Bigg/\left(\sum_{i=1}^{L}\omega_i\cdot\sum_{j=1}^{K}\lambda_j\right). \quad (4)$$

The calculation may be based on all the cases in the database, only the learning set, or only the test set. K is the number of insecure classes and L is the node number of the path. p_{ij} is the percentage of the cases of the jth insecure class in node i, and ω_i and λ_j are respectively the weights assigned to the node i and the jth insecure class. The scores of all paths count in ω_1, the weight of the root node. Hence, it is reasonable to always let $\omega_1 = 0$. Numerically, S reflects a weighted average percentage of insecure cases in each node of the path. The weight λ_j can be increased if the jth insecure class is of more concern with regard to system performance. Weight ω_i shows how much node i of the path can contribute to security assessment. The following situations arise.

1) If the probability of occurrence of an unpredicted OC in the next period can be negligible, or in other words, the database is sufficient, then all CSRs can reliably result in a credible classification result at the terminal node. Thus, the terminal node should be assigned a dominant weight ω_L to make good use of its classification result. In fact, the methods based only on terminal nodes are just special cases of the new method and always let $\omega_2 \sim \omega_{L-1} = 0$, and $\omega_L = 1$ to completely trust the classification result of the terminal node.
2) Otherwise, thresholds of some fault-independent CAs may become unsuitable for an unpredicted OC or fault-dependent CSRs may become incorrect. As a result, the classification result at each terminal node is not credible for unpredicted cases. However, a path as a whole is comparatively fixed because even if few CSRs become invalid, other CSRs can still work. To set proper $\omega_2 \sim \omega_L$, either of the following approaches could be considered.
   - Set a uniform weight ω_i for the ith node of every path and consider increasing the weights of the nodes closer to the root to increase reliability of the DT.
   - Simply let ω_i $(i > 1)$ be the number of the learning cases in node i due to the consideration that the nodes with more cases are more important.

   An upper limit S_M is then set for all scores. Any score exceeding S_M means an insecure path. If no scores exceed S_M, the system will credibly maintain security after any of the N'_C contingencies and even some similar contingencies; otherwise, preventive control is needed. In fact, when a DT has been built, the new method endows it with self-adaptability under nondeterministic conditions by using $\omega_2 \sim \omega_L$ and S_M to reasonably emphasize a portion (e.g., a sub-tree containing the root node) in it. The choice of optimal values of $\omega_2 \sim \omega_L$ and S_M will be dealt with in future studies. Basically, a higher accuracy for insecure cases comes with a lower S_M and the nodes closer to the root need higher weights when perturbations of OCs increase. In Section IV-C, $\omega_2 \sim \omega_L$ are set by the second approach above and S_M is simply selected at an apparent boundary between low and high insecurity scores.

iii) Preventive control: Preventive control needs to be designed for each path with a score higher than S_M. For the path, the criticality of an insecure class j can be estimated by

$$c_j=\lambda_j\cdot\sum_{i=1}^{L}\omega_i\cdot p_{ij}. \quad (5)$$

Without loss of generality, the preventive control for only the insecure class maximizing c_j is discussed. In the path, the nodes with big values of $\omega_i p_{ij}$ are important factors causing the high insecurity score, so the CSRs at their parent nodes also indicate reasonable directions for preventive control. For example, if a node maximizing $\omega_i p_{ij}$ satisfies "measurement $X > 0$" (i.e., the CSR at its parent node), "X" will be a key CA and the preventive control measure making $X < 0$ will most probably succeed. However, to design an approach directly adjusting a key CA like X towards the desired direction does not necessarily improve security since a new OC may be created after preventive control. Only when this OC is still credibly covered by the database, the key CA will continue acting as a good security indicator. An approach to consider is to control the system towards an OC known by the database. Further simulations for the OC caused by preventive control will be necessary to verify the impact of the control.

B. Building a Better DT by Adjusting Penalties of Predictors

Both fault independent and dependent CAs are used in the DT. Sometimes, the former are preferable since they are measurable and partially controllable. For the purpose of security analysis, it may be important to separate or order their use, e.g., using the latter before the former to first identify insecure areas of the system, or alternatively, using the former before the latter to identify insecure regions in the measurement space and design preventive control. Either approach can be used by assigning appropriate penalties between 0 and 1 to fault independent or dependent predictors to reduce their improvement scores. A penalty of 0 and 1 respectively means "no limitation on using" and "not using" the predictor. The higher the penalty a predictor has, the later it is used in the DT. Based on this reasoning, the following procedure is used to build a good DT using fault-dependent CSRs after fault-independent ones by adjusting the penalties of fault-dependent predictors.

Procedure-1:

1) Assign each fault-dependent predictor a penalty $p = p_{\min}$.
2) Generate a series of DTs by CART's growing and pruning processes and select the best DT. The "best DT" is selected based on either of the two criteria mentioned in Section II. For each of its paths with fault-dependent CSRs, treat the child nodes that the fault-dependent CSR closest to the

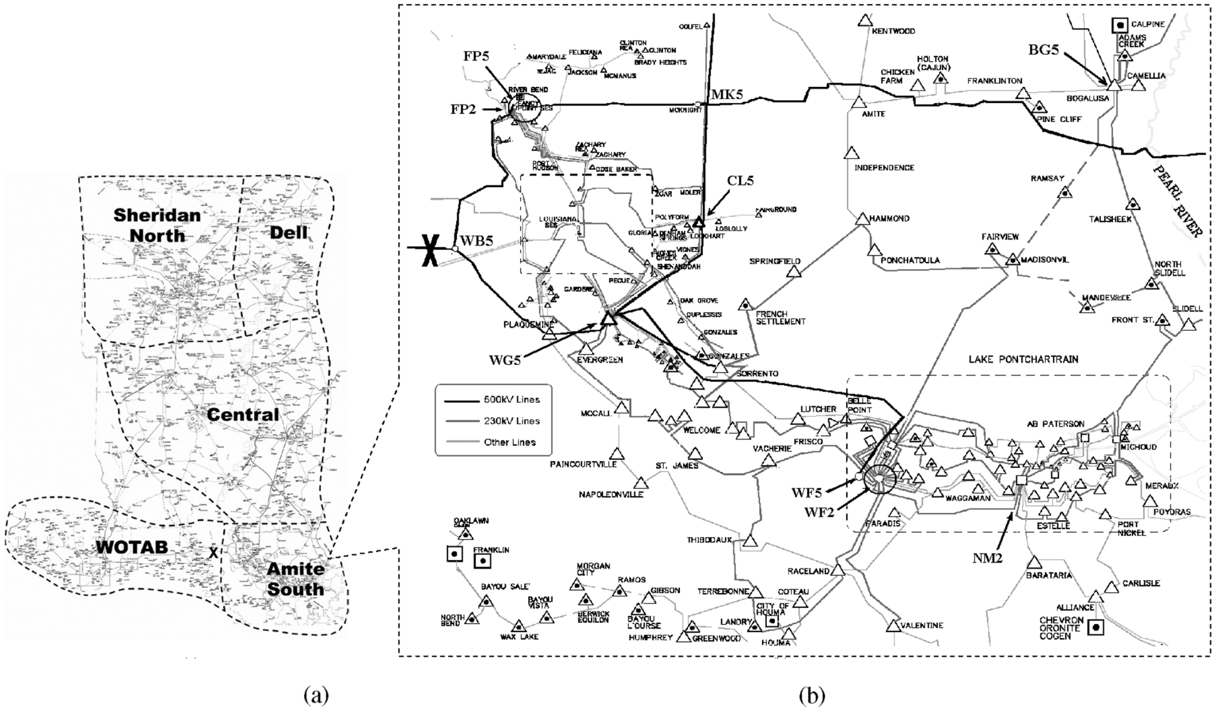


Fig. 3. Operating zones in (a) the Entergy system and (b) the Amite South area.

root node produces as terminal nodes, i.e., prune all nodes succeeding them. Thus, a DT using fault-dependent CSRs at only the last splits is generated and stored.

3) Let $p = p + \Delta p$ if $p > p_{\max}$, give the best DT from all DTs stored and end the procedure; otherwise, go to 2).

Heuristic seeking techniques could be applied to find a good measure of penalty more quickly. Similar procedures could be designed to generate a DT meeting other requirements.

Another approach to build DTs is to only select predictors from critical variables, e.g., plant generation outputs of critical plants, power flows of critical interfaces or transmission lines, and phase angle differences between critical buses. In this case, CART's DT building algorithm cannot guarantee building an optimal DT. At each step of DT growing, i.e., splitting a node, the algorithm simply seeks the CSR best separating cases of different classes only for this node but does not make any prediction on how the split caused by the CSR will affect the trend of future DT growing. Simulations have shown that replacing a CSR by a slightly inferior competitor totally changes the nature of future DT growing. In fact, finding an optimal DT based on certain predictors is a complicated problem, which results in an exponentially explosive search space in terms of numerous predictor combinations. However, the following *Procedure-2* can quickly find a better DT by recursively executing CART's DT building algorithm.

Procedure-2:

1) Select a group of reasonable predictors and build a DT. Let $i = 1$.
2) For the CSRs of all nodes at the ith level starting from the root node, check their nonsurrogate competitors.
3) If a CSR at a node has a good nonsurrogate competitor whose improvement score is larger than γ times (e.g., $\gamma = 0.9$) of its score, then assign its associated predictor the minimum penalty making the new DT use the competitor instead of the old CSR at that node. The value of the "minimum penalty" is easily determined by simple tests. Then, go to step 5).
4) If no such good nonsurrogate competitor exists at the ith level, go to step 6).
5) If the new DT built in step 3) is better than the old DT, replace the old DT by the new DT and go to step 2).
6) If no inner node is below the ith level, then end the procedure; otherwise, let $i = i + 1$ and go to step 2).

In the procedure, each DT is built by either CART's algorithm or a modified algorithm like *Procedure-1* to meet the requirements specified.

IV. Case Study

The scheme proposed in this paper is tested on the Entergy system operational model with about 240-generators, 2000-buses and 2100-lines. Based on past operating practices at Entergy, the Entergy network shown in Fig. 3(a) is divided into five operating areas. Separate DTs are required for each of these areas. The network topology, the system conditions for peak and minimum load, and the dynamic data are considered on a day-ahead basis for a 24-h period for July 19, 2006. A credible stressed condition with a 500-kV transmission line (connecting the WOTAB area and the Amite South area) from Wells to Webre being out of service, as indicated by "X" in Fig. 3(a) and (b), was analyzed. Using this as a starting point and knowing the daily variation in load pattern, power flow solutions are obtained at 56 OCs derived from different load assumptions based on the unit commitment data. The DTs could be rebuilt every 24 h and updated at the beginning of every short period (several minutes to an hour) or when a significant topology change occurs or the operator envisions a change to be analyzed.

In the analysis shown in this paper, the results for the DT generated for the Amite South area [shown in detail in Fig. 3(b)] are shown. This critical area with 54-generators, around 400-buses and about 430-lines includes the city of New Orleans which is a major load center. T-D simulations using Powertech Lab's TSAT software [29] are conducted for all the 56 OCs by considering, all "$n-1$" three-phase faults followed with line clearing on all 230-kV buses and above only in this area to generate a database of cases. Other contingencies, e.g., "$n-k$," based on operator experience may also be included in the database if necessary. By respectively considering future location of PMUs and existing PMUs, two groups of predictors are selected. From each group DTs are built on a day-ahead basis using the CART software developed by Salford Systems [30] for evaluating transient insecurity conditions and low damping problems. It is found that the DTs especially those built based on future PMU locations reach very high prediction accuracies for prospective OCs on July 19, 2006. For the purpose of verifying their prediction reliability against OC perturbations, they are then tested on the OCs observed on July 26 (a week apart) with the same "$n-1$" faults.

A. Database of Cases

Based on the peak-load (26600 MW) and minimum-load (17 819 MW) power flow profiles for July 19, 2006, 56 typical OCs ($N_{\mathrm{OC}} = 56$) are obtained. The following "$n-1$" contingencies in the Amite South area were analyzed for each OC.

1) Three-phase faults at both ends of all 500-kV lines with a clearing time of five cycles.
2) Three-phase faults at both ends of all 230-kV lines with a clearing time of six cycles.

As a result, there are totally 280 (N_C) contingencies and $280 \times 56 = 15680$ cases for the 56 OCs. Each case is simulated in TSAT and the following two security criteria are respectively checked for transient instability and low damping problems.

1) Transient stability criterion: after the contingency is cleared the system's transient stability margin is greater than 5% and the duration for any bus voltage going out of the range $0.70 \sim 1.20$ pu is less than 20 cycles. Here, the stability margin is estimated by TSAT's power swing-based algorithm [29].
2) Low damping criterion: Entergy requires the damping ratio to be $>3\%$. This criterion is applied to the interarea oscillation modes of generator rotor angles (the frequency range is $0.25 \sim 1.0$ Hz and amplitudes $> 5^{\circ}$).

Overall, 355 (2.3%) cases violate the transient stability criterion and 2501 (16.0%) cases violate the low damping criterion.

B. DT Performance

Entergy has placed nine PMUs to monitor critical interfaces and to obtain a good visibility of the system. The Amite South area has three PMUs at buses "WF2" and "FP2" [encircled in Fig. 3(b)]. The PMUs measure bus voltages and currents of the lines indicated as follows.

1) Bus "WF2" looking at line to bus "NM2."
2) Bus "WF2" looking at bus "WF5."
3) Bus "FP2" looking at bus "FP5."

Thus, voltage phase angles of the above five buses and MW-flows of the three branches can be obtained by the three PMUs. In order to seek better security indicators and locations of PMUs, it is assumed that candidate PMUs are also installed at the other 500-kV buses in the area and monitor flows on 13 branches. Thus, a total of 16 branches and 13 buses are measured. Consider the following two groups of predictors.

Group-1 (from candidate PMUs).

1) The name of the faulted bus (denoted by FB).
2) MW-flows of the 16 branches (each denoted by P_X_Y, i.e., the MW-flow from bus X to bus Y).
3) Angle differences between voltage phase angles of 13 buses (each denoted by A_X_Y, i.e., the voltage phase angle of bus X minus that of bus Y).

Group-2 (from existing PMUs): Respectively replace the above 16 branches and 13 buses by the three branches and five buses currently being monitored using PMUs.

For each group of predictors (e.g., *Group-i*), two 2-class of DTs, denoted by $\mathrm{DT}_i^{\mathrm{ts}}$ and $\mathrm{DT}_i^{\mathrm{ss}}$ respectively, were built for insecurities in terms of the transient stability criterion and low damping criteria. Each DT classifies the cases violating the corresponding criterion as "insecure" (I) and regards the remaining cases as "secure" (S). Randomly select 20% of the cases to form the test set and let the remaining cases form the learning set. To ensure an acceptable balance between CR_I^{ts} and CR_S^{ts} and also a higher weight on misclassifying the I cases, $c(I|S)/c(S|I)$, respectively, equals 40 and 7.5 for DT_i^{ts} and DT_i^{ss}. Performance parameters of the four DTs are given in Table I. $\mathrm{DT}_1^{\mathrm{ss}}$ and $\mathrm{DT}_2^{\mathrm{ss}}$ are built using FB only at the last splits by *Procedure-2* embedded with *Procedure-1* at its first step. $\gamma = 0.9$, $p_{\min} = 0$, $p_{\max} = 1$, and $\Delta p = 0.025$. Fig. 4 illustrates how the penalty p affects the resulting DT the first time *Procedure-1* is executed during the $\mathrm{DT}_1^{\mathrm{ss}}$ building process. The dashed lines depict $R^{ts} \pm \Delta R^{ts}$; 41 DTs using FB at the last splits are built. Their misclassification costs (R^{ts}) and correctness rates (CR_I^{ts} and CR_S^{ts}) are evaluated. The DT with $p = 0.975$ minimizes R^{ts} and has $R^{ts} \pm \Delta R^{ts} = 0.115 \pm 0.006$,

TABLE I
PERFORMANCE PARAMETERS OF DTS

DTs	Size	$R^{ts} \pm \Delta R^{ts}$	CR_I^{ts}(%)	CR_S^{ts}(%)
$\mathrm{DT}^{\mathrm{ss}}_1$	31	0.100±0.005	97.9	91.0
$\mathrm{DT}^{\mathrm{ss}}_2$	31	0.113±0.006	96.7	91.1
$\mathrm{DT}^{\mathrm{ss}}_A$	25	0.115±0.006	96.7	90.9
$\mathrm{DT}^{\mathrm{ts}}_1$	17	0.070±0.005	97.3	95.5
$\mathrm{DT}^{\mathrm{ts}}_2$	17	0.072±0.005	97.3	95.3

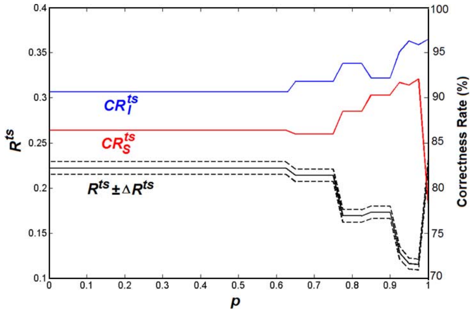


Fig. 4. Example of *Procedure-I*.

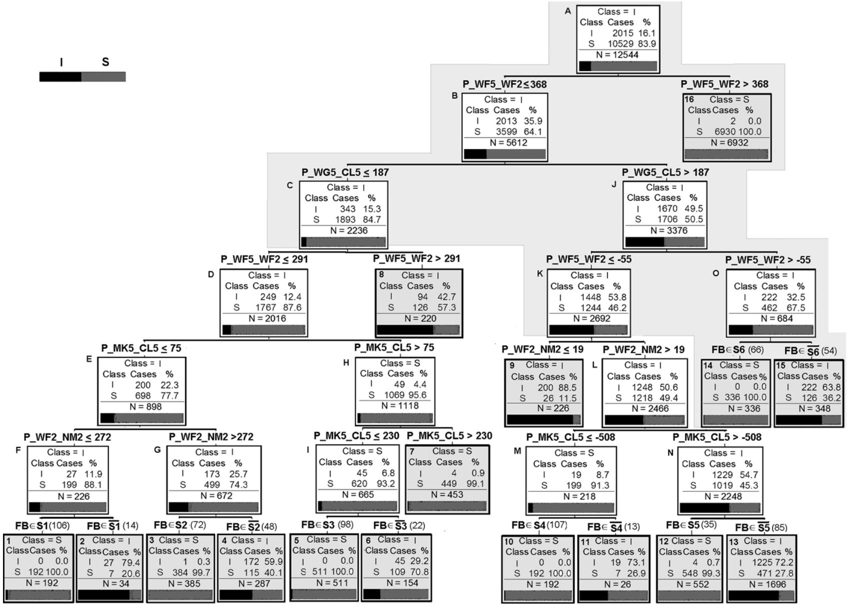
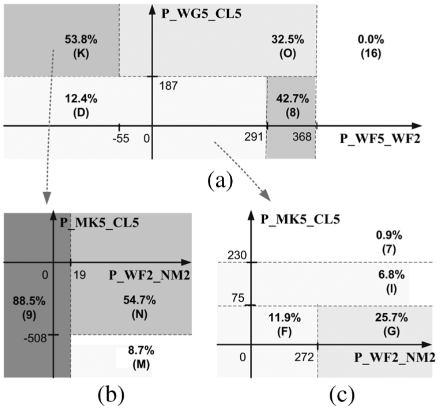

I S
A Class = I; I 2015 16.1; S 10529 83.9; N = 12544
P_WF5_WF2≤368
P_WF5_WF2 > 368
B Class = I; I 2013 35.9; S 3599 64.1; N = 5612
16 Class = S; I 2 0.0; S 6930 100.0; N = 6932
P_WG5_CL5 ≤ 187
P_WG5_CL5 > 187
C Class = I; I 343 15.3; S 1893 84.7; N = 2236
J Class = I; I 1670 49.5; S 1706 50.5; N = 3376
P_WF5_WF2 ≤ 291
P_WF5_WF2 > 291
D Class = I; I 249 12.4; S 1767 87.6; N = 2016
8 Class = I; I 94 42.7; S 126 57.3; N = 220
P_WF5_WF2 ≤ -55
P_WF5_WF2 > -55
K Class = I; I 1448 53.8; S 1244 46.2; N = 2692
O Class = I; I 222 32.5; S 462 67.5; N = 684
P_MK5_CL5 ≤ 75
P_MK5_CL5 > 75
E Class = I; I 200 22.3; S 698 77.7; N = 898
H Class = S; I 49 4.4; S 1069 95.6; N = 1118
P_WF2_NM2 ≤ 19
P_WF2_NM2 > 19
9 Class = I; I 200 88.5; S 26 11.5; N = 226
L Class = I; I 1248 50.6; S 1218 49.4; N = 2466
FB∈S6 (66)
FB∈$\overline{S6}$ (54)
14 Class = S; I 0 0.0; S 336 100.0; N = 336
15 Class = I; I 222 63.8; S 126 36.2; N = 348
P_WF2_NM2 ≤ 272
P_WF2_NM2 >272
F Class = I; I 27 11.9; S 199 88.1; N = 226
G Class = I; I 173 25.7; S 499 74.3; N = 672
P_MK5_CL5 ≤ 230
P_MK5_CL5 > 230
I Class = S; I 45 6.8; S 620 93.2; N = 665
7 Class = S; I 4 0.9; S 449 99.1; N = 453
P_MK5_CL5 ≤ -508
P_MK5_CL5 > -508
M Class = S; I 19 8.7; S 199 91.3; N = 218
N Class = I; I 1229 54.7; S 1019 45.3; N = 2248
FB∈S1(106)
FB∈$\overline{S1}$ (14)
FB∈S2 (72)
FB∈$\overline{S2}$(48)
FB∈S3 (98)
FB∈$\overline{S3}$ (22)
FB∈S4(107)
FB∈$\overline{S4}$(13)
FB∈S5(35)
FB∈$\overline{S5}$(85)
1 Class = S; I 0 0.0; S 192 100.0; N = 192
2 Class = I; I 27 79.4; S 7 20.6; N = 34
3 Class = S; I 1 0.3; S 384 99.7; N = 385
4 Class = I; I 172 59.9; S 115 40.1; N = 287
5 Class = S; I 0 0.0; S 511 100.0; N = 511
6 Class = I; I 45 29.2; S 109 70.8; N = 154
10 Class = S; I 0 0.0; S 192 100.0; N = 192
11 Class = I; I 19 73.1; S 7 26.9; N = 26
12 Class = S; I 4 0.7; S 548 99.3; N = 552
13 Class = I; I 1225 72.2; S 471 27.8; N = 1696
Class Cases %

Fig. 5. $\mathrm{DT}_1^{\mathrm{ss}}$.



(a)

(b)

(c)

Fig. 6. Nomograms from $\mathrm{DT}_1^{\mathrm{ss}}$.

$\mathrm{CR}_I^{ts} = 95.9\%$ and $\mathrm{CR}_S^{ts} = 92.1\%$. $\mathrm{DT}_1^{\mathrm{ss}}$ is finally generated as shown in Fig. 5, where "A"∼"O" are the serial numbers of the inner nodes, "1"∼"16" are the serial numbers of the terminal nodes, and "S1"∼"S6" are FB sets. The size of each FB set is given in parentheses, and all the class histograms, case numbers, and accuracy percentages are provided for the learning cases. $\mathrm{DT}_1^{\mathrm{ss}}$ has four fault-independent CAs: P_WF5_WF2(=P_WG5_WF5), P_WF2_NM2, P_WG5_CL5, and P_MK5_CL5, which belong to a key power transmission path critical to the low damping problem in the system: buses "NM2" → "WF2" → "WF5" → "WG5" → "CL5" → "MK5." From $\mathrm{DT}_1^{\mathrm{ss}}$, the space of the four fault-independent CAs, can be partitioned into ten regions each corresponding to a node that cannot be further split by a fault-independent CSR. For the convenience of analysis, Fig. 6 uses three 2-D nomograms to depict the space and its regions. In each region, the percentage of insecure cases and the serial number of the corresponding node are indicated. Fig. 6(b) and (c), respectively, continues to partition the regions K and D of Fig. 6(a) into smaller regions corresponding to their child nodes. By means of the nomograms like Fig. 6 together with the FB sets given by the terminal nodes of the DT, the security of an OC can be obtained if its location in the space is determined by synchronized phasor measurements. Compared with $\mathrm{DT}_1^{\mathrm{ss}}$, $\mathrm{DT}_2^{\mathrm{ss}}$ only uses P_WF5_WF2 and P_WF2_NM2 (from existing PMUs) as fault-independent CAs.

$\mathrm{DT}_1^{\mathrm{ts}}$ and $\mathrm{DT}_2^{\mathrm{ts}}$ are built without the limitation on using FB as a predictor. The fault-independent CAs of $\mathrm{DT}_1^{\mathrm{ts}}$ are P_WF5_WF2, P_WF2_NM2, and P_WG5_CL5, which also belong to the key power transmission path mentioned above. $\mathrm{DT}_2^{\mathrm{ts}}$ has the exactly same structure as $\mathrm{DT}_1^{\mathrm{ts}}$ except that P_WG5_CL5 is replaced by P_WF2_NM2.

The above four DTs only use MW-flows as fault-independent CAs due to the fact that the MW-flows on that key transmission path are most critical to system security after contingencies occur in the Amite South area. However, that is not a general case. Another DT, denoted by $\mathrm{DT}_{\mathrm{A}}^{\mathrm{ss}}$, is built for the low damping criteria from *Group-1* as shown in Fig. 7. The fault-independent CAs it picks up are A_WG5_FP5, A_CL5_WB5, A_WG5_BG5, A_FP5_WF2, and A_MK5_FP5, which are differences between the voltage phase angles of some key buses as shown in Fig. 3(b). The performance of $\mathrm{DT}_{\mathrm{A}}^{\mathrm{ss}}$, as given in Table I, is worse than that of $\mathrm{DT}_1^{\mathrm{ss}}$.

It needs to be pointed out that irrespective of whether phase angles are involved in the final DT, accurately synchronized values of fault-independent CAs are necessary to precisely determine the current OCs location relative to the insecure regions as shown by the nomograms in Fig. 6. Unlike PMUs, the SCADA system or state estimators cannot synchronously measure all the fault independent CAs, so they may not accurately determine the locus and location of the OC. Especially when some fault independent CAs change sharply to make the OC approach the boundary of an insecure region, that may not be detected in a timely manner by the SCADA system and state estimators.

In terms of R^{ts} and ΔR^{ts}, $\mathrm{DT}_1^{\mathrm{ts}}$ and $\mathrm{DT}_2^{\mathrm{ts}}$ perform equally well. $\mathrm{DT}_1^{\mathrm{ss}}$ is better than $\mathrm{DT}_2^{\mathrm{ss}}$. If necessary, a new PMU could be installed at bus "CL5" to provide measurements of P_MK5_CL5 and P_WG5_CL5. The above performance

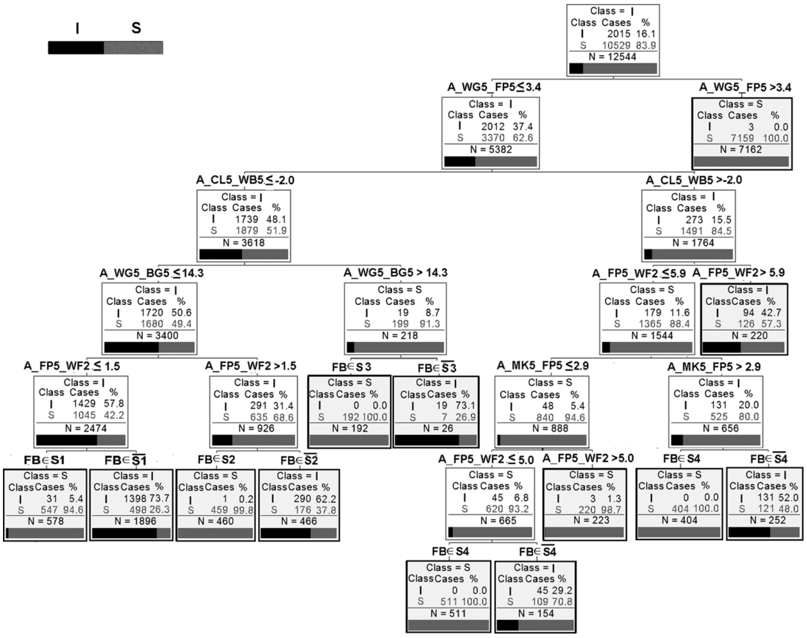


Fig. 7. $\mathrm{DT}_{\mathrm{A}}^{\mathrm{ss}}$.

indices are estimated from the test set and are only based on the classification results of the terminal nodes. If the real time OCs considered are captured by the database used in building the DTs, the DTs will give accurate security predictions as indicated by the indices. Otherwise, the paths-based method will give more reliable and self-adaptable results as shown by the following test, where only $\mathrm{DT}_1^{\mathrm{ss}}$ is considered.

C. Reliability Tests on Two Classification Methods

To compare the traditional (terminal nodes-based only) and new (paths-based) classification methods, $\mathrm{DT}_1^{\mathrm{ss}}$ is tested on the contingency cases for July 26, 2006. 24 OCs are generated based on the peak-load (24078 MW) and minimum-load (16100 MW) conditions with the 500-kV line from Wells to Webre out of service. Compared with the network data on July 19, 2006, 15 lines change in/out status and the generation distribution among generators is also changed. In this area, the same "$n-1$" contingencies are considered to generate $278 \times 24 = 6672$ "$n-1$" cases. Quite a few cases are found with damping ratios slightly higher than 3.0%. Considering the estimation errors of the Prony analysis method used by TSAT, the cases with damping ratios <3.3% are all regarded as I cases. As a result, there are 942 (14.1%) I cases and 5730 (85.9%) S cases. The traditional method correctly classifies 92.8% I cases and 77.7% S cases.

Let ω_i $(i > 1)$ be the number of the learning cases at node i. Calculate the insecurity score S of each path based on the learning set. The scores are given in Table II, and the case percentages and the classification results at the terminal nodes are also given. From the table, the paths to terminal nodes 9, 10, 11, 12, 13, and 15 have high scores. Let S_M equal 40% to consider the cases entering the six terminal nodes as "insecure." The last column gives the numbers of the I and S cases of July 26, 2006 that enter each terminal node of $\mathrm{DT}_1^{\mathrm{ss}}$. The new method correctly classifies 99.3% I cases and 82.4% S cases. Both of the accuracies are much higher than those of the traditional method.

TABLE II
INSECURITY SCORES OF PATHS AND TEST RESULTS FOR 7/26/2006

Path	Terminal Node Cases (%)	Terminal Node Class	S (%)	7/26/2006 Cases (S / **I**)
A-B-C-D-E-F-**1**	1.5	S	25.3	0 / 0
A-B-C-D-E-F-**2**	0.3	I	25.9	0 / 0
A-B-C-D-E-G-**3**	3.1	S	25.2	0 / 0
A-B-C-D-E-G-**4**	2.3	I	26.9	0 / 0
A-B-C-D-H-I-**5**	4.4	S	22.2	216 / **2**
A-B-C-D-H-I-**6**	1.2	I	23.3	58 / **2**
A-B-C-D-H-**7**	3.6	S	23.2	556 / 0
A-B-C-**8**	1.8	I	30.4	555 / **1**
A-B-J-K-**9**	1.8	I	**44.8**	57 / **221**
A-B-J-K-L-M-**10**	1.5	S	**44.0**	0 / 0
A-B-J-K-L-M-**11**	0.2	I	**44.6**	0 / 0
A-B-J-K-L-N-**12**	4.4	S	**44.9**	344 / **64**
A-B-J-K-L-N-**13**	13.5	I	**48.8**	610 / **650**
A-B-J-O-**14**	2.7	S	39.0	0 / 0
A-B-J-O-**15**	2.8	I	**41.2**	0 / 0
A-**16**	55.3	S	0.0	3334 / **2**

The results show that the new, paths-based method exhibits a better reliability against perturbations of OCs than the traditional method. From Fig. 5, the new method equivalently regards nodes C, K, 14, 15, and 16 as terminal nodes such that the nine-node sub-tree indicated by the shadowed area is picked up to make security classifications. Node weights of each path as well as the limit S_M could be adjusted according to the degree of perturbations of OCs such that a proper sub-tree of the DT is adaptively selected.

V. CONCLUSION

This paper proposes an online security assessment scheme based on PMUs and DTs. The scheme was applied to an important operational area of the Entergy system. Off line simulations show that the proposed approach can build DTs with high prediction accuracies to reliably identify stability problems for prospective OCs and provide guidelines for preventive control. The scheme also identifies critical security indicators, which could be candidates for new PMU locations. A new paths-based

DT classification method is also proposed and compared with the traditional terminal nodes-based method to regulate the DTs prediction reliability for changes in OCs. This new method focuses on the development of self-adaptive rules to make better use of available DTs and introduces a shift from "Black-Box" DTs to "White-Box" DTs, or rule-based DT classification systems. The DTs built in this paper can reach prediction accuracies of about 97% for insecure cases. This research is a first step towards the goal that in the future, more practical versions of the scheme proposed can achieve a high, accuracy (e.g., 99% or even 99.9%) acceptable by electricity industry. To realize that goal, several issues will have to be carefully analyzed. One aspect that we are currently investigating is the impact of the use of a larger number of OCs to increase the number of insecure cases used in DT training.

REFERENCES

[1] J. F. Hauer, "Validation of phasor calculations in the macrodyne PMU for California-Oregon transmission project tests of March 1993," *IEEE Trans. Power Del.*, vol. 11, no. 4, pp. 1224–1231, Jul. 1996.

[2] N. Zhou, J. W. Pierre, and J. F. Hauer, "Initial results in power system identification from injected probing signals using a subspace method," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1296–1302, Nov. 2006.

[3] J. F. Hauer, N. B. Bhatt, and K. Shah *et al.*, "Performance of 'WAMS East' in providing dynamic information for the North East blackout of August 14, 2003," in *Proc. IEEE Power Eng. Soc. General Meeting*, Jun. 2004, vol. 2, pp. 1685–1690.

[4] Z. Huang, R. T. Guttromson, and J. F. Hauer, "Large-scale hybrid dynamic simulation employing field measurements," in *Proc. IEEE Power Eng. Soc. General Meeting*, Jun. 2004, vol. 2, pp. 1570–1576.

[5] B. Bhargava, "Synchronized phasor measurement system project at Southern California Edison Co," in *Proc. IEEE Power Eng. Soc. General Meeting*, Jul. 1999, vol. 1, pp. 16–22.

[6] J. W. Ballance, B. Bhargava, and G. D. Rodriguez, "Monitoring power system dynamics using phasor measurement technology for power system dynamic security assessment," presented at the IEEE Power Tech. Conf., Bologna, Italy, Jun. 2003.

[7] J. H. Chow, A. Chakrabortty, and M. Arcak *et al.*, "Synchronized phasor data based energy function analysis of power transfer paths," presented at the IEEE Power Eng. Soc. General Meeting, Jun. 2006.

[8] I. Kamwa, J. Beland, G. Trudel, and R. Grondin *et al.*, "Wide-area monitoring and control at Hydro-Quebec: Past, present and future," presented at the IEEE Power Eng. Soc. General Meeting, Jun. 2006.

[9] M. La Scala, M. De Benedictis, S. Bruno, and A. Grobovoy *et al.*, "Development of applications in WAMS and WACS: An international cooperation experience," presented at the IEEE Power Eng. Soc. General Meeting, Jun. 2006.

[10] H. Li, X. Xie, and L. Tong *et al.*, "Implement of on-line transient stability control pre-decision in wide-area measurement system in jiangsu power network," presented at the IEEE/PES Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005.

[11] J. Y. Cai, Z. Huang, and J. Hauer *et al.*, "Current status and experience of WAMS implementation in North America," presented at the IEEE/PES Asia and Pacific Transmission and Distribution Conf. Exhibition, Dalian, China, Aug. 2005.

[12] M. Donnelly, M. Ingram, and J. R. Carroll, "Eastern interconnection phasor project," presented at the 39th Annu. Hawaii Int. Conf. System Sciences, Jan. 2006.

[13] B. Milosevic and M. Begovic, "Voltage-stability protection and control using a wide-area network of phasor measurements," *IEEE Trans. Power Syst.*, vol. 18, no. 1, pp. 121–127, Feb. 2003.

[14] A. R. Khatib, R. F. Nuqui, M. R. Ingram, and A. G. Phadke, "Real-time estimation of security from voltage collapse using synchronized phasor measurements," in *Proc. IEEE Power Eng. Soc. General Meeting*, 2004, vol. 1, pp. 582–588.

[15] R. Burnett, M. Butts, and T. Cease *et al.*, "Synchronized phasor measurements of a power system event," *IEEE Trans. Power Syst.*, vol. 9, no. 8, pp. 1643–1650, Aug. 1994.

[16] Z. Zhong, C. Xu, and B. J. Billian *et al.*, "Power system frequency monitoring network (FNET) implementation," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1914–1921, Nov. 2005.

[17] J. Rasmussen and P. Jorgensen, "Synchronized phasor measurements of a power system event in eastern Denmark," *IEEE Trans. Power Syst.*, vol. 21, no. 1, pp. 278–284, Feb. 2006.

[18] N. Kakimoto, M. Sugumi, T. Makino, and K. Tomiyama, "Monitoring of interarea oscillation mode by synchronized phasor measurement," *IEEE Trans. Power Syst.*, vol. 21, no. 1, pp. 260–268, Feb. 2006.

[19] L. Wehenkel, T. Custsem, and M. Pavella, "An artificial intelligence framework for on-line transient stability assessment of power systems," *IEEE Trans. Power Syst.*, vol. 4, no. 2, pp. 789–800, May 1989.

[20] L. Wehenkel, T. Custsem, and M. Pavella, "Inductive inference applied to on-line transient stability assessment of electric power systems," *Automatica*, vol. 25, pp. 445–451, May 1989.

[21] L. Wehenkel and M. Pavella, "Decision trees and transient stability of electric power systems," *Automatica*, vol. 27, pp. 115–134, Jan. 1991.

[22] L. Wehenkel, M. Pavella, and E. Euxibie *et al.*, "Decision tree based transient stability method a case study," *IEEE Trans. Power Syst.*, vol. 9, no. 1, pp. 459–469, Feb. 1994.

[23] E. S. Karapidakis and N. D. Hatziargyriou, "Online preventive dynamic security of isolated power systems using decision trees," *IEEE Trans. Power Syst.*, vol. 17, no. 2, pp. 297–304, May 2002.

[24] K. Morison, L. Wang, and P. Kundur, "Power system security assessment," *IEEE Power Energy Mag.*, vol. 2, pp. 30–39, Sep.–Oct. 2004.

[25] K. Morison, "On-line dynamic security assessment using intelligent systems," presented at the IEEE Power Eng. Soc. General Meeting, Jun. 2006.

[26] S. Rovnyak, S. Kretsinger, J. Thorp, and D. Brown, "Decision trees for real-time transient stability prediction," *IEEE Trans. Power Syst.*, vol. 9, no. 3, pp. 1417–1426, Aug. 1994.

[27] S. Rovnyak, C. Taylor, and Y. Sheng, "Decision trees using apparent resistance to detect impending loss of synchronism," *IEEE Trans. Power Syst.*, vol. 15, no. 4, pp. 1157–1162, Oct. 2000.

[28] L. Breiman, J. Friedman, R. A. Olshen, and C. J. Stone, Classification and Regression Trees. Belmont, CA, Wadsworth, 1984.

[29] TSAT Transient Security Assessment Tool. [Online]. Available: http://www.dsapowertools.com/downloads/TSAT_Brochure.pdf

[30] CART Tree-Structured Non-Parametric Data Analysis. [Online]. Available: http://www.salfordsystems.com/cart.php

Kai Sun (M'06) received the B.S. degree in automation and the Ph.D. degree in control science and engineering from Tsinghua University, Beijing, China, in 1999 and 2004, respectively.

He was a Postdoctoral Research Associate at Arizona State University, Tempe, from 2005 to 2007. He is currently a Project Manager at EPRI.

Siddharth Likhate (S'05) received the B.S. degree in electrical engineering from Sardar Patel College of Engineering, Mumbai University, India, in 2005. He is currently pursuing the M.S. degree in electrical engineering at Arizona State University, Tempe.

Vijay Vittal (S'78–F'97) received the B.E. degree in electrical engineering from the B.M.S. College of Engineering, Bangalore, India, in 1977, the M.Tech. degree from the Indian Institute of Technology, Kanpur, in 1979, and the Ph.D. degree from Iowa State University, Ames, in 1982.

Dr. Vittal is a member of the National Academy of Engineering.

V. Sharma Kolluri (SM'86) received the M.S.E.E. degree from West Virginia University, Morgantown, and the M.B.A. degree from the University of Dayton, Dayton, OH.

He was with AEP Service Corporation, Columbus, OH, from 1977 to 1984. In 1984, he joined Entergy Services, Inc., New Orleans, LA, where he is currently the Manager of Transmission Planning. His main areas of interest are power system planning and operations, voltage and dynamic stability, and reactive power planning.

Sujit Mandal (M'99) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT), Kanpur, and the M.S. degree in electrical engineering from Kansas State University, Manhattan, in 1997 and 1999, respectively.

He was a Consultant at Power Technologies, Inc., Schenectady, NY, from 1999 to 2000. Presently, he is with Technical System Planning, Entergy Services, Inc., New Orleans, LA.