Methodology for a Security/Dependability Adaptive Protection Scheme Based on Data Mining

Emanuel E. Bernabeu, *Member, IEEE*, James S. Thorp, *Life Fellow, IEEE*, and Virgilio Centeno, *Senior Member, IEEE*

***Abstract*—Recent blackouts offer testimonies of the crucial role played by protection relays in a reliable power system. It is argued that embracing the paradigm shift of adaptive protection is a fundamental step toward a reliable power grid. The purpose of this paper is to present a methodology to implement a security/dependability adaptive protection scheme. The advocated methodology aims to reduce the likelihood of manifestation of hidden failures and potential cascading events by adjusting the security/dependability balance of protection systems. The proposed methodology is based on wide-area measurements obtained with the aid of phasor measurement units. A data-mining algorithm, known as decision trees, is used to classify the power system state and to predict the optimal security/dependability bias of a critical protection scheme. The methodology is tested on a detailed 4000-bus system.**

***Index Terms*—Adaptive protection, decision trees (DTs), hidden failures, phasor measurement units (PMUs).**

I. Introduction

THE POWER industry is currently in the process of reinventing itself. The unbundling of the traditional monopolistic structure that gave birth to a deregulated electricity market, the mass tendency toward a greener use of energy, the new emphasis on distributed generation and alternative renewable resources, and new emerging technologies have revolutionized the century-old industry.

Recent blackouts [1]–[3] offer testimonies of the crucial role played by protection relays in a reliable power system. Reliability in power system protection comprehends two aspects: dependability and security. Dependability is the measure of the certainty that the relays will operate correctly for all of the faults for which they are designed to operate [4]. Security is defined as the measure of the certainty that the relays will not operate incorrectly for any fault. In general, enhancing security implies an intrinsic loss of dependability and vice-versa. Protection engineers try to achieve an optimal balance between these two conflicting concepts; this is why power systems protection is often recognized as an art. Traditionally, protection systems have been biased toward dependability. System topology and good stability margins justified such design. It is argued that due to the manner in which the system has evolved, this philosophy needs to be reviewed and that, under stressed system conditions, a favorable bias toward security is beneficial.

Manuscript received October 19, 2010; revised April 04, 2011; accepted June 03, 2011. Date of publication October 26, 2011; date of current version December 23, 2011. Paper no. TPWRD-00801-2010.

E. E. Bernabeu is with Dominion Virginia Power, Protection, Richmond, VA 23220 USA.

J. S. Thorp and V. Centeno are with the Electrical and Computer Engineering Department, Virginia Polytechnic Institute and State University, Blacksburg, VA 24061-0202 USA (e-mail: virgilio@vt.edu).

Digital Object Identifier 10.1109/TPWRD.2011.2168831

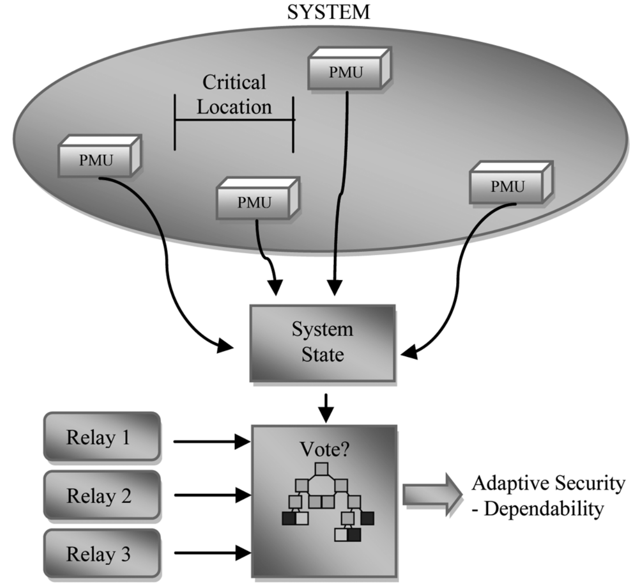


Fig. 1. Security/dependability adaptive protection schematic.

The methodology proposed in this paper aims to reduce the likelihood of manifestation of hidden failures and potential cascading events by adjusting the security/dependability balance of protective relays to suit prevailing system conditions. When the power system is in a "safe" state, a bias toward dependability is desired. Under these conditions, not clearing a fault with primary protection has a greater impact on the system than a relay misoperation due to a lack of security. However, when the power system is in a "stressed" state, unnecessary line trips can greatly exacerbate the severity of the outage, contribute to the geographical propagation of the disturbance, and may even lead to a cascading event and subsequent blackout. Under these states, it is desirable to alter the reliability balance in favor of security.

A conceptual overview of the advocated adaptive protection scheme is shown in Fig. 1. The voting scheme consists of a set of three independent and redundant relays. Wide-area measurements are obtained with the aid of PMUs. The underlying hypothesis is that phasor measurements at strategic buses provide enough information to discriminate the need for a bias toward security. These measurements are used to infer the state of the power system which is then classified as either "stressed" or "safe." If the system is found to be stressed, the proper course of action is to enable the voting scheme and, therefore, bias the protection system toward security. On the other hand, if the system is found to be safe, the voting scheme will be disabled and only

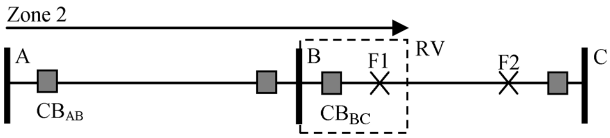


Fig. 2. Example of a hidden failure in a distance relay.

one relay will perform the protective function (i.e., a favorable bias toward dependability).

The advocated methodology is based on data mining, specifically, on decision trees (DTs). DTs can extract information of large data sets and intuitively represent the gained knowledge through a series of if-else sentences. This nonparametric statistical analysis is highly suited to power systems due to the complex nonlinear behavior of the system.

In Section II, the notion of hidden failures in protective relays is defined. DTs are briefly described in Section III. The proposed methodology for an adaptive security/dependability protection scheme is presented in Section IV. Simulation results are presented in Section V. Conclusions and final remarks are presented in Section VI.

II. Hidden Failures and Critical Locations

A hidden failure is defined as a permanent defect on a relay system that will cause the incorrect removal of a circuit element as a direct consequence of another event [5]. As conveyed by the definition, hidden failures remain dormant until a particular event causes its manifestation and associated relay misoperation.

The modes of hidden failures are a function of the relay type (i.e., different protection schemes are prone to different hidden failures). The analysis of the different modes is highly correlated with the logic diagram of the protective scheme. A detailed description of the different modes of hidden failures for each relay type can be found in [6].

The region of vulnerability is defined as a physical region in the network so that any fault within that region will trigger the hidden failure and produce an unwanted operation [5]. The length of the region of vulnerability is a function of the relay type, the relay settings, and the topology of the system.

As an example, consider the one-line diagram of two adjacent transmission lines shown in Fig. 2. Assume that an impedance relay is located at bus A and that its Zone-2 timer has a defect. The aftermath is a lack of coordination between breakers $\mathrm{CB_{AB}}$ and $\mathrm{CB_{BC}}$. Therefore, a fault F1 within the reach of Zone 2 of relay A will caused the trip of breaker $\mathrm{CB_{AB}}$ and the incorrect removal of the line between bus A and bus B.

In Fig. 2, the region of vulnerability is denoted by a dashed rectangle. It needs to be emphasized that any fault outside the reach of the region of vulnerability will not awake the hidden failure. Therefore, the fault labelled F2 would leave the defect on the timer hidden.

Overall, the probability of a protective relay having a hidden failure is relatively small. Manufacturers perform extensive quality control tests to ensure a low rate of misoperations. The threat that hidden failures pose is due to the intrinsic high risk associated with them. Risk is defined as the product of the probability of a hidden failure times its impact or consequence. Typically, hidden failures are prone to manifest themselves under stressed system conditions [6] and, therefore, their consequence tends to be rather noteworthy. In general, faults and other switching events tend to increase the likelihood of hidden failures. Prevailing systems conditions, such as overloaded lines, voltage dips, and overloaded generators also boost the probability of hidden failures.

An analysis of NERC outages reports indicates that hidden failures are involved in more than 70% of cascading outages. The "Great Northeast Blackout" of 1965 [7] represents a quintessential example of the threat posed by hidden failures. The blackout was initiated by a hidden failure in a distance relay. The relay had been set for a typical load in 1963. However, line loading steadily increased in the next two years until it reached the outdated relay setting which tripped and initiated a cascading event that left 30 million people without power.

A significant research effort has been employed in developing technology to detect hidden failures and prevent them from causing unwanted operations. However, hidden failures in protection relays are low probability events so it is difficult to economically justify deploying systems to protect every relay from hidden failures. Attention and resources must be concentrated on areas in which the severity of an unwanted disconnection due to a hidden failure is relatively high. These areas are defined as the critical locations of the power system. The methodology presented in this paper is independent of the selected critical location but a thorough description of the possible systematic procedure can be found in [8].

III. Data Mining: DTs

Data mining is defined as the process of discovering patterns in data [9]. A DT is a form of inductive learning. Given a data set, the objective is to build a model that captures the mechanism that gave rise to the data (i.e., we are not trying to model the data itself but the underlying mechanism that gave rise to the data); this fact allows the model to transcend the particular data set used to grow the DT and to make inferences on new data.

DTs are grown through a systematic process known as recursive binary partitioning; a "divide-and-conquer" approach where successive questions with yes/no answers are asked in order to partition the sample space. The objective is to recursively partition the sample space L in order to extract the knowledge exhibited in data regularity patterns.

The process begins with a "root" node that encloses the learning sample L; the data set that summarizes past experiences. The learning sample L is composed by a set of measurement vectors $X = \{x_1, x_2, \ldots, x_m\}$. Each column of a measurement vector x_i is known as an attribute. Attributes can be of two types: 1) categorical or 2) numerical. Categorical attributes take a finite set of values and do not have an intrinsic order. Numerical attributes take values in the real line and, therefore, have a natural order. As a supervised learning method, the class of each vector must be known prior to the data-mining process. Therefore, each measurement vector x_i must be classified by the modeler into a set of mutually exclusive classes $C = \{C_1, C_2, \ldots, C_J\}$. To summarize, the learning sample L is a matrix with m rows (the number of measurement vectors) and $n + 1$ columns (the number of attributes on each measurement vector plus the class assigned to each vector).

The DT algorithm intents to partition the space into disjoint subsets in order to increase the "purity" of such subsets. In our context, purity is understood as a measurement of class homogeneity. Homogeneous nodes that include only one class C_j achieve maximum purity, whereas heterogeneous nodes with an equal proportion of classes $C_0, \ldots, C_J$ have minimum purity.

A partition is said to be optimal when it maximizes the purity, or equivalently, minimizes the impurity of the descendent nodes. In order to compare potential splitting attributes and threshold values, a "goodness of split" criterion needs to be defined. In this research, the Gini impurity index is used.

In this paper, the Classification and Regression Trees (CARTs) algorithm is used to grow DTs [10]. The CARTs algorithm initially grows a tree as large as possible. A node is considered to be terminal if it has achieved zero impurity (maximum class homogeneity, only a unique class remains) or if the total number of measurement vectors x_i at such a node is less than some predetermined value $n_{\min}$. A sequence of smaller size subtrees $\{T_1 > T_2 > \ldots > T_{\text{root}}\}$ is then generated through minimal cost-complexity pruning. Cost-complexity is understood as a function that measures the tradeoff between error rates and tree sizes. For a fixed complexity (tree size), the objective is to find the subtree T_k with the lowest misclassification rate (i.e., the tree T_k that minimizes the cost-complexity function). Finally, an optimal sized tree is selected based on V-fold cross validation, an estimator of the misclassification rate.

A thorough description of CART's methodology and a Matlab implementation of the algorithm can be found in [8].

IV. Methodology for a Security/Dependability Adaptive Protection Scheme

Conventional relays react in a predetermined and fixed manner and are typically biased toward dependability. Experience shows that such rigid relay settings may become unreliable under abnormal stressed conditions.

Adaptive relaying can be defined as the ability of relays to change their settings, operation, or logic to adapt to prevailing system conditions [11]. The methodology proposed in this paper aims to reduce the likelihood of hidden failures and potential cascading events by adjusting the security/dependability balance of protective relays to suit prevailing system conditions. When the power system is in a "safe" state, a bias toward dependability is desired. Under these conditions, not clearing a fault with primary protection has a greater impact on the system than a relay misoperation due to a lack of security. However, when the power system is in a "stressed" state, unnecessary line trips can greatly exacerbate the severity of the outage, contribute to the geographical propagation of the disturbance, and may even lead to a cascading event and subsequent blackout. Under these states, it is desirable to alter the reliability balance in favor of security.

The voting scheme consists of a set of three independent and redundant relays. The scheme can be categorized as an open-loop discrete-event control (i.e., the voting function is armed when a threshold is exceeded). Wide-area measurements are obtained with the aid of PMUs. These measurements are used to infer the state of the power system which is then classified as either "stressed" or "safe." If the system is found to be stressed, the proper course of action is to enable the voting scheme and, therefore, bias the protection system toward security. On the other hand, if the system is found to be safe, the voting scheme will be disabled and only one relay takes on the protective function (i.e., a favorable bias toward dependability). It should be emphasized that the advocated scheme alters the functionality of a group of relays without directly modifying relay settings.

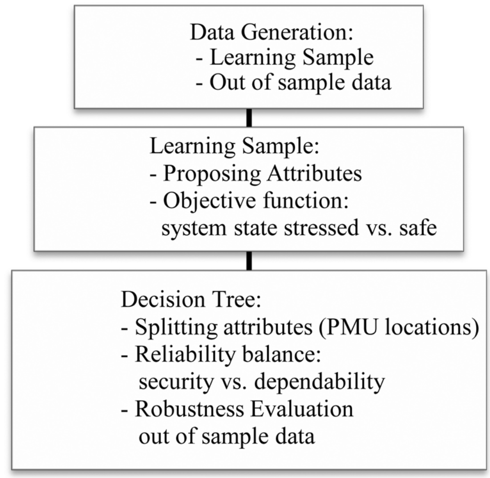


Fig. 3. Methodology flowchart.

The methodology to implement the proposed security/dependability adaptive voting scheme is concerned with the following:

- determining PMU placement;
- defining an objective function to classify the system state into "stressed" or "safe";
- identifying which measurements are more adept at classifying the system state;
- defining the decision logic to alter the security/dependability bias of the adaptive protection scheme.

A flowchart of the proposed methodology is shown in Fig. 3. Simulation results and studies performed by the participating utility show that the most beneficial site for the adaptive scheme is at the three parallel lines connecting Vincent and Midway (see Fig. 11).

The modeler's main task is to develop a learning sample to train the DT. Since DTs is a supervised learning algorithm, an objective function to classify the system state into "safe" or "stressed" needs to be defined. The classification is based on the ability of the system to withstand the manifestation of hidden failures at the critical location. The modeler also needs to propose attributes to be used in the mining process. The procedure is described in Section IV-A.

Finally, the advocated data-mining method, DTs, tackles two problems at the same time. First, and foremost, it provides an intuitive and simple model to predict the appropriate reliability balance of the adaptive protective scheme based on wide-area

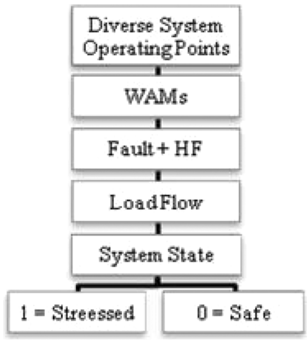


Fig. 4. Flow diagram: developing the learning sample L.

measurements. Second, splitting attributes determine the locations where PMU are needed; the methodology proposed in this paper is itself an application-oriented PMU placement algorithm.

The DT is trained offline by using CART's algorithm and it is utilized online with real-time data. A vector with attributes measured by PMUs is dropped down the tree, and the final decision to alter the security/dependability balance is made upon reaching a terminal node. The DT should be updated whenever significant changes are made to the system model.

A. Developing the Learning Sample L

The flow diagram of the proposed procedure to build the learning sample L is shown in Fig. 4. First, diverse operating points are generated through a combination of load scaling and load-flow solutions.

Consider the four major control areas in California: Pacific Gas and Electric (PG&E), Southern California Edison (SCE), San Diego Gas and Electric (SDG&E), and Los Angeles Department of Water and Power (LADW&P). The idea is to systematically scale the system load by subsequently increasing and decreasing the load at each area. A combinatory of load scaling using two areas at the same time is also performed; for example, the load at PG&E may be increased by 3% while the load at SCE is decreased by 10%.

It is argued that the proposed load scaling process induces enough variation in voltage phasors across the 500-kV network to mine patterns in the data. It is likely that the sample generated will include typical system states and some unrealistic ones. However, "unrealistic" conditions also provide valuable information since it is precisely those atypical and unexpected conditions of the ones that tend to jeopardize the system. If available, historical information of daily load curves can further enhance the learning sample. Ultimately, the main objective is to induce as much variation in the operating points as possible.

It is assumed that PMUs are located at all 500-kV buses. A set of complex phasor voltages at every bus fully specifies the system state (assuming that the topology of the system is perfectly known). In general, several attributes can be included as potential predictors: voltage magnitudes, angle differences, MVar flows, current magnitudes, etc. Voltage magnitudes throughout the system tend to sit around 1 p.u. and, therefore, obscure the mining process; in general, the square of voltage magnitudes is a better predictor since bus voltages close to the normal value of 1 p.u. remain unchanged while deviation from it are magnified. Results show that an outstanding predicting attribute can be obtained by decomposing the current flowing through a transmission line into its real and imaginary parts.

For each operating point, a fault and a hidden failure are assumed to occur at the predetermined critical location. Since DTs is a supervised learning method, an objective function is defined to classify the system state prior to the contingencies into two classes: "safe" or "stressed." The goal is to determine whether the manifestation of a hidden failure has a severe impact on the system or not. If the system prevailing conditions are such that it can withstand the materialization of a hidden failure at the critical location, then a favorable bias toward dependability is desired since the consequence of not tripping a fault due to lack dependability is far worse than overtripping due to a lack of security. On the other hand, if the system is stressed and the unnecessary removal of a critical line can potentially jeopardize the power system, then a bias toward security is preferred. It should be emphasized that the classification of the system state into "safe" and "stressed" is done with respect to the selected critical location (i.e., it is not a general statement regarding the system state).

The exact form of the objective function is a matter of engineering judgment and empirical evidence. For the purpose of this paper, extreme contingencies were contemplated. A natural criterion, due to the inherent high severity of the contingency, is to check the convergence of the load-flow problem. Cases in which the load flow fails to converge are classified as "stressed." If a solution is achieved, then the system state is labelled as "safe." Note that the classification refers to the system prevailing conditions prior to the contingencies and it is determined by evaluating the operating point, or lack of it, after the events.

To conclude, the algorithm to develop the learning sample can be summarized by the following steps.

- Diverse system operating conditions are obtained through a systematic load scaling process.
- At each system state, several measurements are taken at all 500-kV buses in the system. Proposed attributes: voltage phasor angles and real and imaginary currents.
- For each operating point, a fault within the region of vulnerability of a protective relay with a hidden failure is assumed to occur. A load-flow solution is attempted. If it converges, the system state prior to the contingencies is said to be "safe" and it is classified as a zero; otherwise, it is said to be "stressed" and it is classified as a one.

V. Simulation Results

In the advocated methodology, decision trees are trained offline to be used as an online application. An accurate model of the power system is therefore crucial for optimal performance of DTs. In general, load characteristics, generation dispatched, amounts of imported power, peak load, topology, and scheduled maintenance vary from season to season. The proposed methodology is tested using two seasonal models of the power system of California: heavy winter and heavy summer. The decision tree logic should be updated whenever significant changes are made to the system model.

TABLE I
LEARNING SAMPLE: HEAVY WINTER MODEL

	Class	θ_{GATES}	θ_{DIABLO}	…	Ir_{1106}	Ii_{1106}
x_1	1	-3.91	2.57	…	5.40	1.78
x_2	0	-2.52	4.14	…	3.97	1.83
x_3	1	-3.95	2.52	…	5.14	1.69
x_4	1	-3.68	2.84	…	4.92	1.72
…	…	…	…	…	…	…
x_{4150}	0	-3.00	3.61	…	4.36	1.77

Regularity patterns in the data are mined using CART's algorithm to grow DTs; a commercial implementation of CART by Salford Systems can be found in [12].

A. Heavy Winter Model

To demonstrate the methodology, it is assumed that two out of the three parallel lines at the critical location have defective protective relays (i.e., hidden failures). Analogously, this scenario could be conceived as having scheduled maintenance on one of the transmission lines and a single hidden failure. Under such circumstance, a status input variable should be included in the learning sample.

The learning sample is developed using the procedure described in Section IV. Loading conditions were systematically modified to generate 4150 different system operating points; out of those 4150 system states, 2514 cases were classified as one and 1636 as zero. Cases classified as one represent "stressed" system conditions and, under such circumstances, a favorable bias toward security is desired (i.e., the voting scheme should be armed). Cases classified as zero identify "safe" system states and, therefore, a bias toward dependability is preferred; the voting scheme should be disarmed and a single relay performs the protective function.

To infer the system state, it is assumed that PMUs are placed at all 500-kV buses in the system. The learning sample consists of 132 attributes: voltage angles and the rectangular decomposition into real and imaginary of the current flowing through 500-kV transmission lines; angles are measured in degrees and currents in per unit. Table I depicts the learning sample L; it has 4510 measurement vectors (rows) and 132 attributes (columns). Further attributes were initially considered. However, optimal results were obtained with the attributes proposed in Table I.

Based on the learning sample L, a sequence of minimal cost-complexity subtrees is grown by the DT algorithm. A plot of the estimated misclassification rate for each subtree is shown in Fig. 5. The estimator used is known as V-fold cross-validation and is thoroughly discussed in [8]. The selection of a right sized tree is made based on classification accuracy and tree complexity. In general, a parsimonious principle is invoked: simple models are preferred over complex ones. In the case of DTs, simplicity is associated with tree size, which is measured as the total number of terminal nodes. For our particular application, parsimony has a practical interpretation: fewer nodes imply fewer PMU units deployed which, in turn, reduces investment costs.

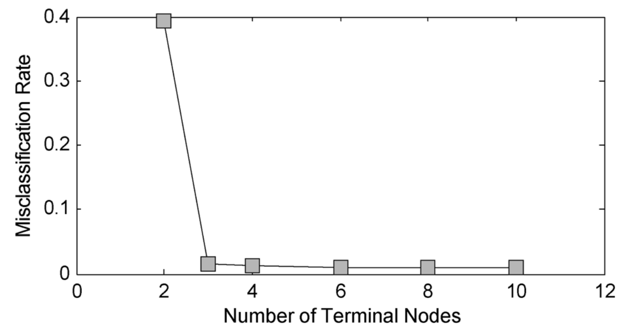


Fig. 5. Cross-validation estimate of the misclassification rate: heavy winter.

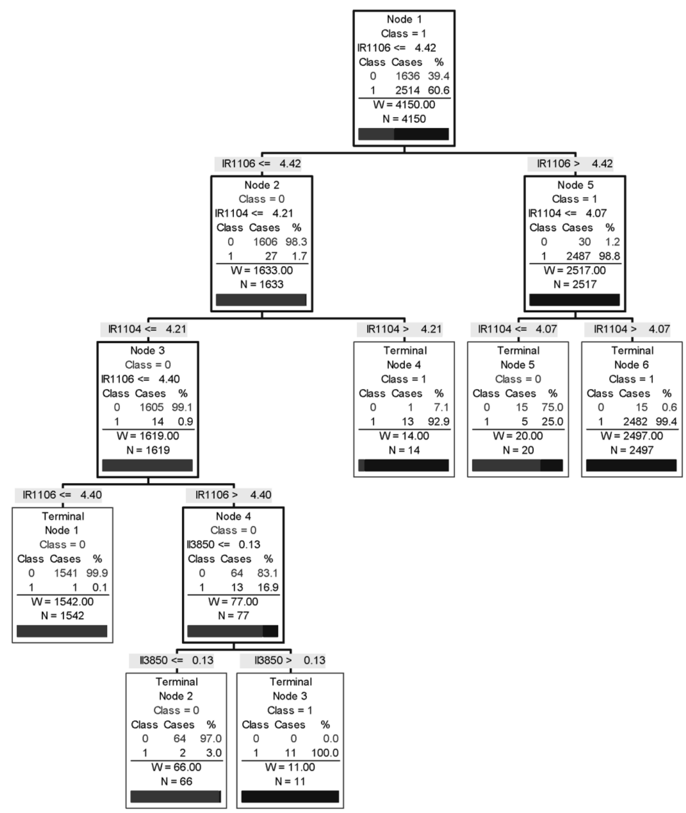


Fig. 6. DT: heavy winter model.

The chosen DT is shown in Fig. 6. The tree has six terminal nodes and an estimated misclassification rate of approximately 1%.

1) Partitioning the Sample Space: As stated in Section III, the goal of the data-mining algorithm is to extract rules or knowledge from regularity patterns exhibited by the data. DTs recursively partition the sample space with hyperplanes to uncover knowledge. In order to illustrate the underlying idea, consider the plot shown in Fig. 7. The figure depicts a plot of all the contemplated attributes in the learning sample. Black dots in the plot represent measurements taken under a "safe" system state (class labeled as zero). Under these circumstances, a bias towards dependability is desired. PMU measurements taken under "stressed" conditions are colored in gray (class labeled as one); on those situations a biased toward security is beneficial. In order to develop decision rules to adjust the

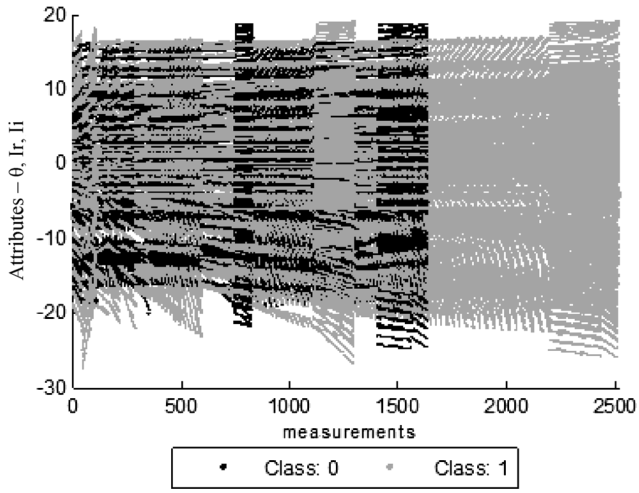


Fig. 7. Plot of all attributes in the learning sample L.

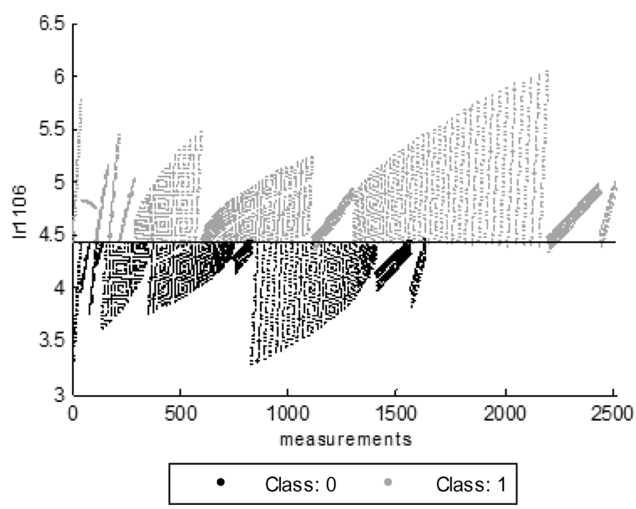


Fig. 8. First partition of the sample space.

security/dependability balance of the protection scheme, the goal is to discriminate between black dots (class 0) and gray dots (class 1) in the figure by subsequently partitioning the learning sample with planes.

Fig. 8 shows a 2-D plot of the first split in the tree; is Ir1106 $\leq$ 4.4249. The attribute Ir1106 represents the real current flowing through line 1106 in the model; a 500-kV transmission line connected between Tesla and Los Banos. The increase in homogeneity achieved by the first split is outstanding. If a unique PMU where to be used to adjust the security/dependability balance, it would have an error rate of approximately 4%. It can be observed in the figure that several black dots lie above the splitting line and some gray dots below the line. Subsequent partitions in the following branches of the tree are able to further reduce the misclassification rate to about 1%.

2) Out-of-Sample Testing: Heavy Winter: In order to test the performance of the DT with out-of-sample data, further test cases can be created by simulating circuit element outages. The objective is to induce additional system operating points to assess the robustness of the tree to topology changes. The out-of-sample data consists of 660 system operating conditions obtained by simulating outages in generators delivering more than 200 MW, loads larger than 200 MW, and in 230- and 500-kV transmission lines.

TABLE II
OUT-OF-SAMPLE TESTING: HEAVY WINTER

		Classified class 0	Classified class 1
Generator Outage	True class: 0	30	5
	True class: 1	0	45
Load Outage	True class: 0	117	1
	True class: 1	0	50
230 kV Lines	True class: 0	132	0
	True class: 1	0	132
500 kV Lines	True class: 0	62	6
	True class: 1	2	78

Each of these outages was simulated under diverse loading conditions. The results of the test are summarized in Table II. Out of the 660 cases, 14 cases were misclassified by the DT; an error rate of approximately 2%. Out of those 14 cases, only 2 "stressed" states were misclassified as class zero. These results show an outstanding performance of the DT. As stated previously, if the system undergoes significant departures from the model assumptions, a new DT should be trained. The proposed out-of-sample test only attempts to assess tree robustness under small departures.

B. Heavy Summer Model

The prevailing system condition in the heavy summer model is more stressed than in heavy winter. The power-consumed doubles and therefore transmission-line loading increases significantly. In order to demonstrate the methodology, a single hidden failure at the critical location is considered. The learning sample is developed by using the procedure described in Section IV. Loading conditions were systematically modified to generate 11 367 different system operating points; out of those 11 367 system states, 5363 cases were classified as one and 6004 as zero. Cases classified as one represent "stressed" system conditions and under such circumstances, a favorable bias toward security is desired (i.e., the voting scheme is armed). Cases classified as zero identify "safe" system states and a bias toward dependability is preferred (i.e., the voting scheme is disarmed and a single relay performs the protective function).

Following the same procedure as in the heavy winter model, in order to infer the system state, it is assumed that PMUs are placed at every 500-kV bus in the system. The learning sample consists of 132 attributes: voltage angles and the rectangular decomposition into real and imaginary current flowing through 500-kV transmission lines; angles are measured in degrees and currents are in per unit. The learning sample L has 11 367 measurement vectors (rows) and 132 attributes (columns).

Fig. 9 shows a plot of the estimated misclassification rate for each subtree. The tree shown in Fig. 10 is selected as the final DT since it attains the best balance between classification accuracy

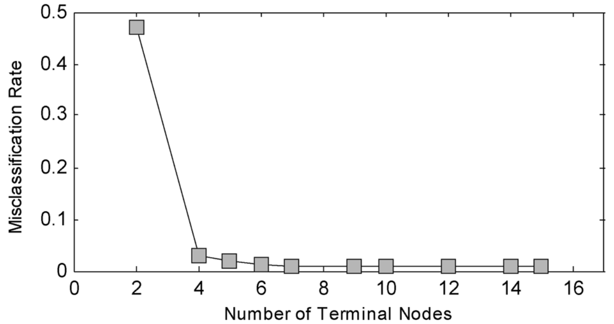


Fig. 9. Misclassification rate for the sequence of subtrees: heavy summer.

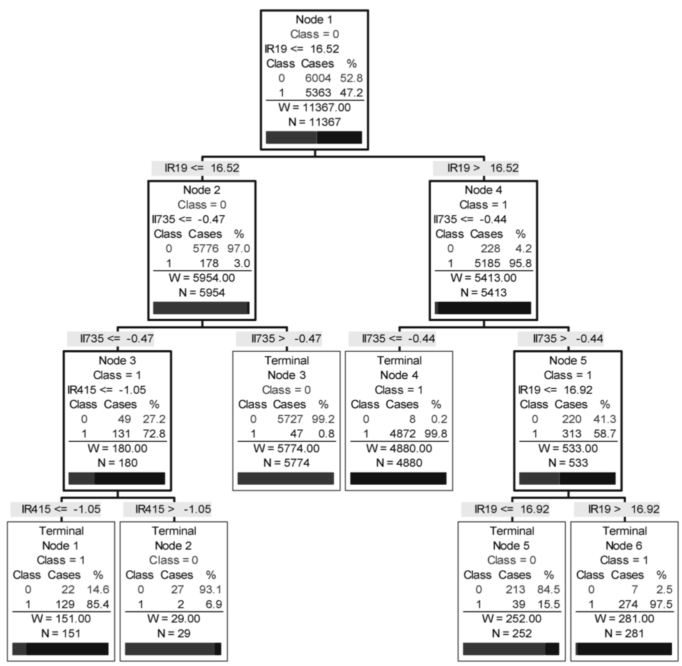


Fig. 10. Heavy summer DT.

and tree complexity. The tree has six terminal nodes and an estimated misclassification rate of approximately 1%.

1) Out-of-Sample Testing: Heavy Summer: In order to test the robustness of the DT to small departures, test cases, not included in the learning sample, are created by simulating outages. As stated previously, the objective is to assess robustness against topology changes. The out-of-sample data consists of 1138 system operating conditions obtained by simulating outages in generators, loads, and transmission lines.

Each of these outages was simulated under diverse loading conditions. The results of the test are summarized in Table III. Out of the 1137 cases, 49 cases were misclassified by the DT; an error rate of approximately 4.3%. The tree has adequate performance when subjected to topology changes.

C. PMU Placement

The overall PMU placement, contemplating the DTs grown using both seasonal models, heavy winter and heavy summer, is shown in Fig. 11. The PMU placement is determined by the splitting attributes in the DT.

TABLE III
OUT-OF-SAMPLE TESTING: HEAVY SUMMER

		Classified class 0	Classified class 1
Generator Outage	True class: 0	107	2
	True class: 1	6	112
Load Outage	True class: 0	154	0
	True class: 1	7	37
230 kV Lines	True class: 0	278	0
	True class: 1	25	284
500 kV Lines	True class: 0	62	6
	True class: 1	3	54

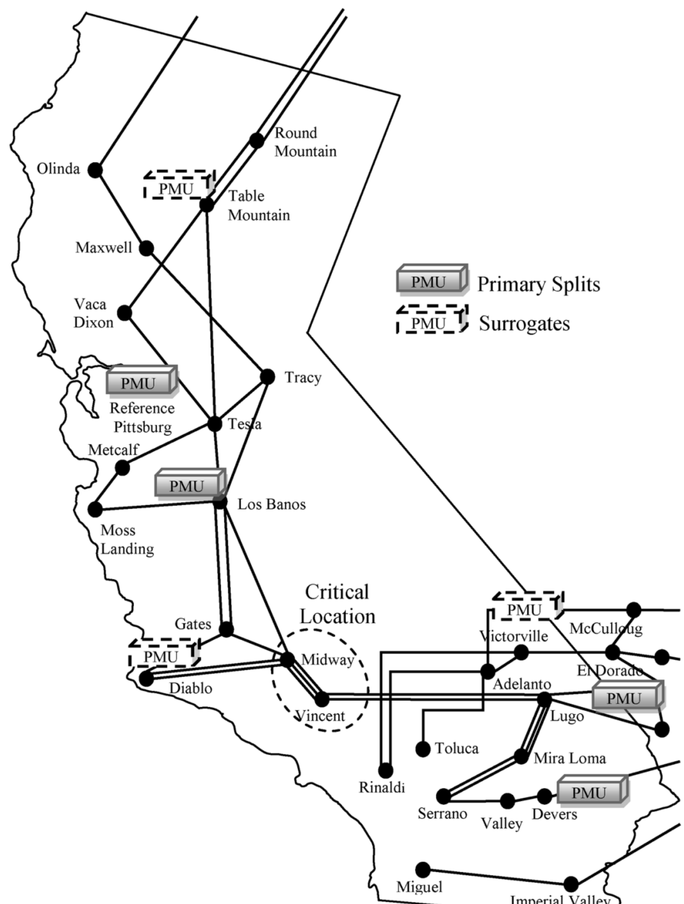


Fig. 11. PMU placement contemplating seasonal DTs.

VI. CONCLUSION

The methodology proposed in this paper aims to reduce the likelihood of hidden failures and potential cascading events by adjusting the security/dependability balance of protection systems. Aided with wide-area measurements, the scheme tailors the security/dependability balance to suit prevailing system conditions. When the power system is in a "safe" state, a bias toward dependability is desired. Under such conditions, not clearing a fault with primary protection has a greater impact on the system than a relay misoperation due to lack of security. However, when the power system is in a "stressed" state, unnecessary line trips can greatly exacerbate the severity of the outage, contribute to the geographical propagation of the disturbance, and may even lead to cascading events and subsequent blackouts. Under such states, it is desirable to alter the reliability balance in favor of security. The advocated scheme alters the functionality of a group of relays without directly modifying relay settings.

The main hypothesis in this paper is that few, strategically placed, PMU measurements are sufficient to recognize the need to alter the security/dependability balance of the adaptive protection scheme. Simulation results on a highly detailed 4000-bus model of California confirm the premise. Patterns associated with different system states can be uncovered with the aid of wide-area measurements and data-mining algorithms. The proposed method, DTs, has proved to be highly adept to the task of mining knowledge in nonlinear systems. Simulation results show that the proposed adaptive scheme has a misclassification rate of 1%. As a further advantage, DTs provide an intuitive description of the uncovered knowledge. The systematic procedure used by DTs to make induction inferences resembles the thinking process of engineers.

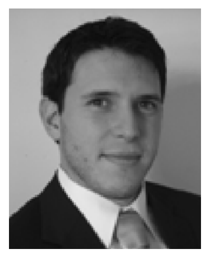
The proposed adaptive protection scheme is susceptible to two types of errors as follows.

1) Type I: Fail to vote when a bias toward security would be desirable. This circumstance characterizes the current protection practice, that is, a single protective relay typically biased toward dependability. Therefore, this error, though potentially extremely harmful, does not go in detriment of any existing practice.
2) Type II: Vote when a bias toward dependability would be preferred. A customary practice to increase security is to implement a voting scheme in which three relays continuously vote, regardless of prevailing conditions. Therefore, under this type of error, the scheme again reduces to current practices.

To conclude, the scheme presents a "win-win" situation. When it correctly predicts the appropriate security/dependability balance, which it does, according to simulations, approximately 99% of the time, it reduces the likelihood of the manifestation of a hidden failure under stressed conditions, potentially preventing a cascading sequence of events. When it errors, no harm is done since it responds in the same manner as ordinary protection relays. The proposed scheme is an improvement over current practices.

REFERENCES

[1] NYISO, "Blackout August 14, 2003 Final Rep." 2005.
[2] UCTE, "Final report of the Investigation Committee on the 28 September 2003 blackout in Italy," 2004.
[3] UCTE, "Final report: System disturbance on 4 November 2006," 2006.
[4] S. H. Horowitz and A. G. Phadke, *Power System Relaying*, 2nd ed. Taunton, U.K.: Research Studies Press, 1995.
[5] S. Tamronglak, "Analysis of power system disturbances due to relay hidden failures," Ph.D. dissertation, Dept. Elect. Comput. Eng., Virginia Polytech. Inst. State Univ., Blacksburg, VA, 1994.
[6] D. Elizondo, "Hidden failures in protection systems and its impact on power system wide area disturbances," M.S. dissertation, Dept. Elect. Comput. Eng., Virginia Polytech. Inst. State Univ., Blacksburg, VA, 2000.
[7] Federal Power Comm., "Northeast Power Failure: Nov. 9 and 10, 1965," 1965.
[8] E. Bernabeu, "Methodology for a security-dependability adaptive protection scheme based on data mining," Ph.D. dissertation, Dept. Elect. Comput. Eng., Virginia Polytech. Inst. State Univ., Blacksburg, VA, 2009.
[9] I. H. Witten and E. Frank, *Data Mining: Practical Machine Learning Tools and Techniques*, 2nd ed. San Mateo, CA: Morgan Kaufmann, 2005.
[10] *Classification and Regression Trees*. Belmont, CA: Wadsworth, 1984.
[11] S. H. Horowitz, A. G. Phadke, and J. S. Thorpe, "Adaptive transmission system relaying," *IEEE Trans. Power Del.*, vol. 3, no. 4, pp. 1436–1445, Oct. 1988.
[12] Salford Systems, CART. 2008. [Online]. Available: www.salford-systems.com



Emanuel E. Bernabeu (M'11) received the B.S. degree in electrical and electronics engineering from Universidad Catolica de Cordoba, Cordoba, Argentina, in 2004, and the M.S. degree in electrical engineering, the M.S. degree in applied economics, and the Ph.D. degree in electrical engineering from the Virginia Polytechnic Institute and State University, Blacksburg, in 2009.

Currently, he is a System Protection Engineer with Dominion Virginia Power, Richmond, VA, where he has been since 2010.

James S. Thorp (LF'02) was the Hugh P. and Ethel C. Kelley Professor of Electrical and Computer Engineering and Department Head of the Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, from 2004 to 2009.

He was the Charles N. Mellowes Professor in Engineering with Cornell University, Ithaca, NY, from 1994 to 2004. He was the Director of the Cornell School of Electrical and Computer Engineering from 1994 to 2001, a Faculty Intern with American Electric Power Service Corporation in 1976–1977, and an Overseas Fellow with Churchill College, Cambridge University, Cambridge, U.K., in 1988.

Prof. Thorp was an Alfred P. Sloan Foundation National Scholar and was elected a Member of the National Academy of Engineering in 1996. He received the 2001 Power Engineering Society Career Service Award, the 2006 IEEE Outstanding Power Engineering Educator Award, and shared the 2007 Benjamin Franklin Medal with Prof. A. G. Phadke.

Virgilio Centeno (M'92–SM'06) received the M.S. and Ph.D. degrees in electrical engineering from Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, in 1988 and 1995, respectively.

He was a Project Engineer with Macrodyne, Inc., Clifton Park, NY, involved in the development of phasor measurement units from 1991 to 1997. He joined the faculty of Virginia Tech as a Visiting Professor in 1997 and became an Assistant Professor in 2001 and an Associate Professor in 2006. His research interest is wide-area measurement and its applications.