A rare event approach to build security analysis tools when $N-k$ ($k>1$) analyses are needed (as they are in large scale power systems)

Florence Fonteneau-Belmudes, *Student Member, IEEE,* Damien Ernst, *Member, IEEE,* and Louis Wehenkel, *Member, IEEE*

***Abstract*— We consider the problem of performing $N-k$ security analyses in large scale power systems. In such a context, the number of potentially dangerous $N-k$ contingencies may become rapidly very large when k grows, and so running a security analysis for each one of them is often intractable. We assume in this paper that the number of dangerous $N-k$ contingencies is very small with respect to the number of non-dangerous ones. Under this assumption, we suggest to use importance sampling techniques for identifying rare events in combinatorial search spaces. With such techniques, it is possible to identify dangerous contingencies by running security analyses for only a small number of events. A procedure relying on these techniques is proposed in this work for steady-state security analyses. This procedure has been evaluated on the IEEE 118 bus test system. The results show that it is indeed able to efficiently identify among a large set of contingencies some of the rare ones which are dangerous.**

I. Introduction

The usual approach for planning and operation of electric power transmission systems is based on the generally recognized $N-1$ criterion. This criterion was originally designed for small to middle size power systems, scaled to one country and sometimes its neighborhood. In such transmission systems, what is defined as an incident is for example the loss of one generation unit or the tripping of one transmission line. These events are rare enough so that it is a priori very unlikely that two of them occur at the same time. For example, if the probability of one transmission line being unavailable is around 10^{-4} and if we consider a $1\,000$ line system (assuming that all the lines of this system have the same reliability properties), the probability that one single line of the transmission network is unavailable at a given moment is equal to 0.0905 and the probability that two lines are disconnected at the same time is equal to 0.0045.

However, the continual increase in complexity in power systems, and especially the growing number of new interconnections may raise the question of whether this $N-1$ criterion is still sufficient or even relevant. For example, when considering the interconnected European transmission system, it is very likely that there is at least one transmission line disconnected for maintenance operations in the entire European network. In terms of probabilities, if we consider a large network of $20\,000$ transmission lines and if each transmission line is assumed to have a probability 10^{-4} to be unavailable, the probability that one of the lines of the whole network is unavailable at a given moment is equal to 0.2707. This value is high enough to consider that the $N-1$ criterion is no longer conservative enough and that $N-2$ contingencies also have to be studied in order to make sure that it is possible to mitigate them while serving the electricity demand and respecting the operational constraints of the transmission network.

The authors are with the Department of Electrical Engineering and Computer Science of the University of Liège, Belgium. E-mails: {belmudes,ernst,wehenkel}@montefiore.ulg.ac.be

The Transmission System Operators (TSOs) of each interconnected country therefore need to be able to perform $N-2$, $N-3$ or even deeper security analyses in order to operate safely the transmission system they are responsible for.

When running $N-k$ ($k>1$) security analyses, a severe computational problem arises. Indeed, when k starts growing, the size of the set of potentially dangerous events for $N-k$ analyses becomes rapidly huge and analyzing individually every event to find the dangerous ones becomes computationally irrelevant. As way of example, the size of the event space for a 1000 line electric network grows from approximately 10^6 to 10^{12} when k goes from 2 to 4.

Within these extremely large sets of events, we assume in this paper that the $N-k$ events that can indeed threaten the security of the system are *rare*. Under this assumption, the problem of finding $N-k$ dangerous events becomes equivalent to the problem of finding rare-events in combinatorial search spaces. This equivalence suggests that importance sampling techniques, which have been vastly successful for solving combinatorial problems, could also be used for efficiently identifying dangerous contingencies.

In this paper, we develop and validate an approach based on these importance sampling techniques for the fast identification of dangerous contingencies within the context of steady-state security analysis.

The rest of this paper is organized as follows. The background for identifying rare events in combinatorial search spaces with iterative sampling methods is described in Section II. The approach for applying these techniques to $N-k$ static security analyses is presented in Section III. This approach is illustrated on the IEEE 118 bus test system in Section IV, in which some simulation results are reported. Section V discusses this method with respect to existing work and conclusions are drawn in Section VI.

II. Iterative sampling methods for identifying rare events in combinatorial search spaces

In the literature many iterative sampling methods have been proposed for searching solutions to combinatorial or non-convex optimization problems, such as genetic algorithms, distribution estimation methods, Markov-Chain Monte Carlo methods, and also the so-called cross-entropy method (see [10], [12], [2] and [15]).

A common feature of these methods, from an algorithmic point of view, is to combine random sampling with an iterative process allowing to "learn" the best sampling scheme for the problem under consideration. Many of these algorithms work in the following generic way:

- define some initial sampling distribution over the considered search space;
- at each iteration:
  - generate a subset of potential solutions over the search space by using the current sampling distribution;
  - evaluate the objective function for each configuration in the current sample;
  - use the pairs (configuration, objective function) in the current sample so as to determine a new sampling distribution better targeting the interesting solutions of the problem;
- halt the iterative process when the computational resources have been exhausted, or when the current sample is sufficiently pure in terms of objective function distribution, or when the variation of some sample statistics has not changed significantly since a certain number of iterations.

In this paper, we want to exploit such iterative sampling based methods for rare combinatorial event simulations, i.e. in order to identify elements of a very small subset of "interesting" configurations among a very large number of candidate ones located in an originally unstructured discrete search space. To this end, we first define an objective function over the original discrete space which is maximal only for the sought interesting solutions. Then we embed this discrete search space in a continuous metric space where the objective function varies in a sufficiently progressive way and on which we may apply naturally linear operators such as averaging and interpolation, and we use the iterative sampling based optimization approach together with averaging/interpolation operators over the embedding space so as to generate a sequence of sampling distributions defined over this space which progressively targets elements corresponding to interesting configurations of the original problem. One main component of this approach, needed to allow the computation of the objective function over the embedding space, consists of a reverse mapping (pre-image computation) of the embedding so as to associate to each point of the embedding space an element of the original discrete space over which the objective function is defined.

In our simulations reported below, we use as iterative sampling method the cross-entropy method [15]. This method works as follows:

- Define a hypothesis space of candidate sampling densities p_λ defined over $\mathbb{R}^n$ and indexed by a parameter vector λ.
- Set λ to its initial value λ_0 (typically λ_0 will be chosen so as to let the distribution p_{λ_0} cover the complete space $\mathbb{R}^n$).
- At each iteration i, draw a sample S_i of size s of configurations according to the current distribution defined by the current value λ_i (s is a parameter of the algorithm) and evaluate the value of the objective function for each one of these configurations.
- Keep the subset S_i' of S_i corresponding to the $m < s$ best solutions (m is another parameter of the algorithm).
- Use the sample S_i' to determine a new value λ_{i+1}. In the cross-entropy method, one uses at this step the maximum likelihood principle, i.e. one choses the value λ_{i+1} such that the likelihood of the sample S_{i+1}' is maximal.

In the next section, we describe the precise setting that we propose in order to apply this approach to the identification of dangerous $N-k$ events in power systems. These comprise the choice of an objective function measuring correctly the *severity* of an event, the metrization and pre-image computations associated to the embedding of the $N-k$ events in a continuous space, and the choices associated to the application of the cross-entropy method per se (space of sampling distributions, as well as the parameters s and m).

III. Static security, $N-k$ and iterative sampling

In this section, we describe a method for applying the generic iterative sampling approach explained previously to the identification of dangerous $N-k$ contingencies in the context of static security. Simulations results generated on the IEEE 118 bus system are reported later in Section IV. The remainder of this section is structured as follows. First, we start by defining the event space and the notion of dangerous and non-dangerous events. Afterwards, we elaborate on the choice of the objective function, the representation of the events in a (low-dimensional) continuous space and the pre-image computation. Finally, a fully specified algorithm for searching for dangerous events is given.

A. The (rare) dangerous events

The event space $\mathcal{X}$ (here the set of potentially dangerous contingencies) is made of the events that correspond to the loss of k distinct transmission lines. An element of this space is represented by the k-tuple $(l_1, l_2, \ldots, l_k)$ where every l_i refers to a line.[1] A dangerous event of this space is set to be an event for which there exists no post-fault steady-state equilibrium point of the system. In our simulations, the system is said to have no post-fault equilibrium point if the power flow diverges or does not converge after a specified number of iterations. When the loss of k transmission lines splits the power system into several subsystems, a power flow should in principle be run for every area of the system and the stability

[1] Notice that in this paper we do not consider "mixed" $N-k$ events (i.e., contingencies which correspond to the loss of various types of power system elements) so as to simplify the metrization of the event space (see later).

or instability diagnosis should be based on the analysis of these separate runs. Since it adds difficulty to the problem (e.g., if the system is splitted into two areas such that one is very small with respect to the other and if only the smaller has no steady-state operating point, then, should the system be considered as being stable or unstable?), we have preferred to remove from the set of events those which increase the degree of connexity of the system.

B. The objective function

The objective function $O(x)$ is a real-valued function defined over the space of events which takes its maximum values when x is a dangerous event. This function is used at every iteration of the algorithm for selecting among the several events drawn from a sampling density, those which correspond to the largest value of $O(x)$. These are used to define, based on the maximum likelihood principle, the next sampling density. As the iterations go on, the algorithm should generate sampling densities which give more weight to the dangerous events. In the classical so-called cross-entropy framework, the function $O(x)$ is given. In our problem, one has the flexibility to choose among the set of real-valued function defined on $\mathcal{X}$, one which leads to good performances. Picking up a good function $O(x)$ may be challenging. In the context of steady state security, we propose as pragmatic approach to define this function to associate to an event x a value that reflects *how close* $-$ according to a metric based on some power engineering concepts $-$ the system is from instability. This can be achieved by exploiting several criteria such as the reactive power reserve still available on the generators, the distance between the current loading condition and the maximum loading condition or other severity indices published in the power system literature. In this work, we chose to relate the value $O(x)$ to the number of iterations that are needed by a power flow to converge when the event x occurs. Indeed, it is likely that the closer an event is from instability, the more the power flow has to iterate to converge. Note that, according to some simulations carried out on the benchmark IEEE 118 bus system, the number of iterations to convergence and the distance between the current loading condition and the maximum loading condition tend to be correlated. This is illustrated on Figure 1 depicting the relationship between the global system load and the number of iterations needed by the power flow computation. When, for an event x, the power flow diverges or does not converge after the maximum number of iterations has been reached, the value of $O(x)$ is set equal to this maximum number of iteration plus one. This ensures that $O(x)$ takes its maximum value on the dangerous events.

C. Metrization and pre-image computation

For iterative sampling methods to work well, the event space should be metrized in a way that the objective function on the continuous metrized space should vary sufficiently progressively.

To explain the strategy we have chosen to metrize the event space, we will first reason as if only $N-1$ contingencies were considered. In such a case, one approach for metrization

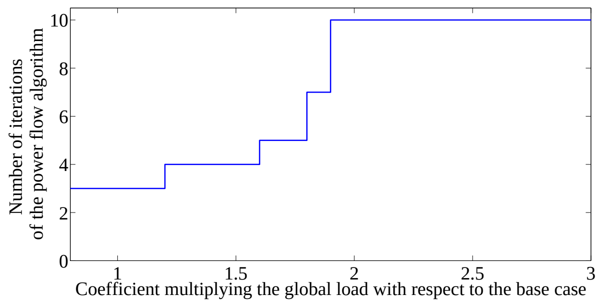
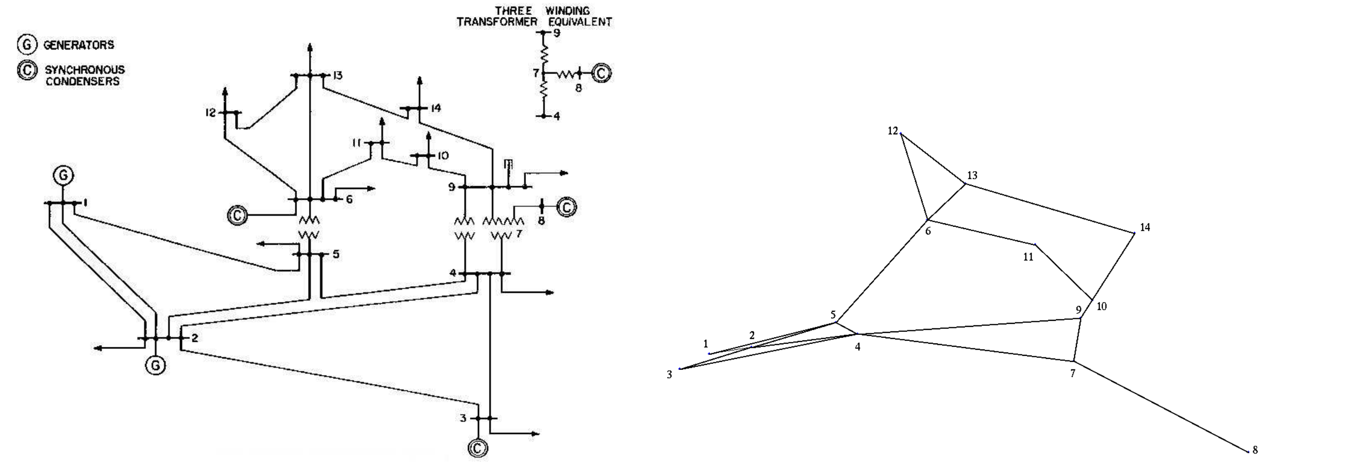


Fig. 1. Evolution of the number iterations to convergence of the power flow algorithm when the load increases monotonically. The test system is the IEEE 118 bus system.

and pre-image computation could be to use the plane ($\mathbb{R}^2$) as metrized space, to plot the geographical map of the power system on this plane and to associate to every event of the metrized space the line which stands the closest to it (pre-image computation). The distance between an event in the plane and a line could for example be defined as the area of the triangle formed by the event and the two end buses of the line. By assuming that the closer two lines are from an element of $\mathbb{R}^2$, the more likely it is that their loss has similar effects on the steady-state properties of the post-fault system, this strategy may indeed lead to an objective function that varies progressively on the continuous metrized event space.

Unfortunately, one main drawback of this strategy is that this assumption may often be false since, among others, the geographical distance between two nodes may often be very poorly correlated with their electrical distance. To circumvent this problem, while still having the possibility to define the pre-image computation procedure based on the location of the buses in a two-dimensional space, we have chosen to represent these buses differently on the plane. Indeed, rather than to position the buses according to their geographical location, they are represented in a way such that the distance between every pair of nodes is correlated to their electrical distance. Technically, this has been achieved as follows. First, we compute for every two buses of the electrical network the reduced admittance between them (computed by reducing the admittance matrix to these two buses) and take the modulus of the inverse of this value to represent their electrical distance. Second, we place the buses on a plane such that the Euclidean distance between any two bus locations in this plane represents well their electrical distance. For this purpose, we have chosen to use multidimensional scaling (MDS) algorithms (see, e.g., [5]), and in particular the Torgerson algorithm. MDS algorithms have been specifically developed to map objects between which measures of distances are given into points in a low-dimensional Euclidean space such that their distances computed in this space are close to the given distances. For the sake of illustration, Figure 2b represents on a plane the position of the buses of the IEEE 14 bus test system computed by such an approach. The figure also shows the lines connecting these buses. The one-line diagram of this test system, as it is usually found in the literature, is given on Figure 2a. Obviously, the positions of the buses on this latter



(a) The "classical" one-line diagram

(b) One-line diagram that positions buses according to their electrical distances

Fig. 2. Representation of two one-line diagrams of the IEEE 14 bus test system. Figure (a) gives the classical one-line diagram, as published in the literature. The second diagram positions the nodes according to their electrical distances by using a multi-dimensional scaling (MDS) algorithm.

diagram do not give a good image of their electrical distances. For example, nodes 1, 2, 4 and 5 are much closer from an electric point of view than they appear on the original one-line diagram. Also, it is worth noticing that node 8 which is connected to nodes 4 and 9 through a three windings transformer appears quite remote on the one-line diagram drawn on Figure 2b while it is not the case on the other. This was expected since the windings of a transformer generally have a reactance whose value is in the range of the reactance value of a few tens of kilometers long transmission line.

We discuss now the case when $N-k$ events with $k>1$ are considered. First, we consider $\mathbb{R}^{2k}$ as metrized space rather than $\mathbb{R}^2$, as it was the case with $N-1$ contingencies. The computation of the pre-image $(l_1, l_2, \ldots, l_k)$ of an event in the metrized space is done as follows. To identify the component l_1, we take the first two components of the $2k$-dimensional event vector in the metrized space and exploit these two coordinates to identify a line as if we were dealing with an $N-1$ event. By taking the second two components of the $2 \times k$-dimensional event vector, we identify l_2 using the same procedure, and then similarly (l_3, …, l_k). The rationale behind this approach lies on the assumption that if two events $(l_1, l_2, \ldots, l_k)$ and $(l'_1, l'_2, \ldots, l'_k)$ are such that if for any i, l_i is close to l'_i, then these events will have similar effects on the steady-state properties of the post-fault system.

Finally, note that the pre-image computation just described may lead to some k-tuples $(l_1, l_2, \ldots, l_k)$ which do not belong to $\mathcal{X}$ since nothing does guarantee that the k-tuple is made of distinct lines or that the k-tuple does not correspond to an event which splits the network in several areas (see Subsection III-A). To address this problem, we have slightly modified the pre-image computation procedure as follows. First, we consider that the elements of a k-tuple are identified sequentially. At every step j, we check after having identified l_j whether there exists in $\mathcal{X}$ a k-tuple whose first j elements are (l_1, l_2, …, l_j). If it is not the case, we choose as l_j the second closest line to the point extracted from the metrized event. There is again a similar checking on this new l_j and the procedure repeats if necessary.

In the following, we denote by $PreImage : \mathbb{R}^{2\times k} \rightarrow \mathcal{X}$ the function that computes the pre-image of an element of the metrized space.

D. A fully specified algorithm

Figure 3 gives the tabular version of an iterative sampling based algorithms for identifying rare events. This algorithm uses n-dimensional Gaussian laws as sampling distributions (referred to by $Gauss_{\mathbb{R}^n}(\cdot, \lambda_i)$ in the algorithm) and is a particular instance of the cross-entropy based approach for identifying rare events described in Section II.

The algorithm takes as input an objective function $O(\cdot)$, its maximum value $max\_objective$ and the pre-image function. It outputs a set of events which maximize this function.

The parameters $\lambda_0 = [\mu_0, \sigma_0]^n$ of the initial sampling distribution (μ and σ refer to the mean and the standard deviation of the distribution, respectively) are usually chosen such that the initial sampling distribution covers well the entire event space. In our simulations, these will be chosen such that (i) μ_0 corresponds to the geometrical center of the subspace of the metrized event space in which all the buses and lines of the electric system are located (ii) the ith component of σ_0 is equal to half the size of this subspace alongside its ith dimension.

At each iteration i, a sample of s elements is drawn according to $Gauss_{\mathbb{R}^n}(\cdot, \lambda_i)$. Usually, in cross-entropy algorithms, the value of s is chosen an order of magnitude larger than the number of elements parameterizing the sampling distributions. In our simulations, n is equal to 12 and s is chosen equal to 200. The pre-image function is first applied to every element of the sample to identify to which events they correspond. Afterwards, the different values that the objective function takes over these events are computed. These values are first exploited to identify which events x are such that $O(x) = max\_objective$. If such events are found, they are

Problem definition: An objective function $O : \mathcal{X} \rightarrow \mathbb{R}$, the maximum value ($max\_objective$) of $O(\cdot)$, a pre-image function $PreImage : \mathbb{R}^n \rightarrow \mathcal{X}$.
Algorithm parameters: The parameters $\lambda_0 = [\mu_0, \sigma_0]^n$ of the initial n-dimensional Gaussian sampling distribution, the size s of the sample drawn at each iteration, the number m of best solutions chosen at each iteration.
Output: A set $\mathcal{X}_{\max}$ such that every element of this set maximizes $O(\cdot)$.
Algorithm:
Step 1. Set i equal to 0.
Step 2. Set S_i, SO_i and S'_i to empty sets.
Step 3. Draw independently s elements according to the pdf $Gauss_{\mathbb{R}^n}(\cdot, \lambda_i)$ and store them in S_i.
Step 4. For every element $y \in S_i$, compute $x = PreImage(y)$, compute $o = O(x)$, add the pair (y, o) to SO_i and, if $o = max\_objective$, add x to $\mathcal{X}_{\max}$.
Step 5. Identify in SO_i the m pairs which have the largest value of o and set their y values in S'_i.
Step 6. Set $\mu_{i+1}[j] = \frac{\sum_{y \in S'_i} y[j]}{m}$ and $\sigma_{i+1}[j] = \sqrt{\frac{\sum_{y \in S'_i} (y[j] - \mu_{i+1}[j])^2}{m}}$ for $j = 1, \ldots, n$ and set $\lambda_{i+1} = [\mu_{i+1}, \sigma_{i+1}]$.
Step 7. If stopping conditions are reached, output $\mathcal{X}_{\max}$ and stop. Otherwise, $i \leftarrow i + 1$ and go to **Step 2.**

Fig. 3. An algorithm for identifying the elements that maximize a function $O : \mathcal{X} \rightarrow \mathbb{R}$ by iterative sampling when $\mathbb{R}^n$ is chosen as metrized space.

stored. Afterwards, the events which lead to the m best values of the objective function are used to compute the next sampling distribution. The parameter m is usually chosen 10 to 20 times smaller than s. In our simulations, m is equal to 10.

Different stopping conditions can be thought of for this algorithm (see Section II). In our simulations, we will mostly for illustrative purposes either stop the algorithm as soon as one element that maximizes $O(\cdot)$ has been found or when a specific number of iterations has been reached.

IV. Results on the IEEE 118 bus test system for $N-3$ security analysis

In this section, we evaluate the proposed methodology on the IEEE 118 bus test system, which has been vastly used as benchmark test system in the literature. $N-3$ contingencies are considered.

To assess our approach, we first screened all the possible $N-3$ contingencies and identified the dangerous ones. This analysis has shown that there exist 895 649 $N-3$ contingencies that do not split the network into several subsystems. Among them, 187 contingencies are dangerous, that is contingencies for which the power flow diverges or does not converge after a maximal number of iterations. The ratio between the dangerous contingencies and all possible contingencies is thus around $2.09.10^{-4}$, and so we can indeed consider that identifying such dangerous contingencies can be parented to a rare-event problem.

To illustrate the efficiency of our methodology, we have studied the speed at which it can identify one single dangerous contingency. This speed has then been compared with the one corresponding to a classical Monte-Carlo sampling of the event space. For the cross-entropy based method, we ran the algorithm 100 times with different initial random seeds and stored the number of events after which the first dangerous one was found. For the Monte-Carlo sampling method, we took 100 series of 100 random permutations of the 895 649 $N-3$ contingencies and computed for each of these permutations the number of contingencies to screen before encountering the first dangerous one. The results of these simulations are collected in the histograms reported in Figure 4, where the horizontal axis represents the number of screened contingencies and where each vertical bar represents the number of runs out of hundred which found the first dangerous contingency within the corresponding range of numbers of runs.

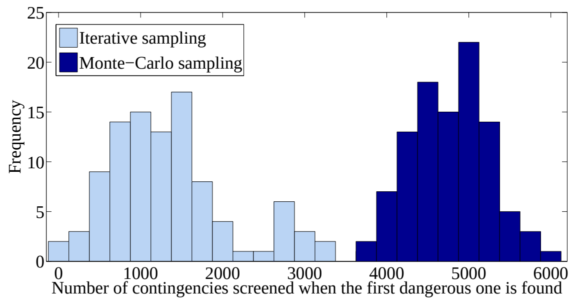


Fig. 4. Comparison of the number of contingencies to screen before identifying the first dangerous one with the iterative sampling algorithm and the Monte-Carlo sampling method.

We observe that the number of contingencies screened before identifying the first dangerous one is centered around 1 403 with a standard deviation 941 for the cross-entropy based algorithm, and centered around 4 770 with a standard deviation 484 for the Monte-Carlo method. The average number of contingencies screened when the first dangerous one is found is about 4 times smaller for the method we propose in this work, which means that our iterative sampling method is significantly more efficient than the classic Monte-Carlo method, as regards the search of one dangerous contingency. This result is explained by the fact that our approach can at every iteration $i > 1$ exploit the information contained in the previously drawn sample to compute a new sampling distribution which is more likely to give more weight to events

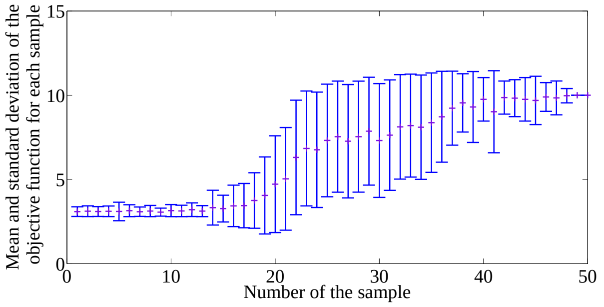


Fig. 5. Evolution of the range of values that the objective function takes on the 200 element samples generated by our importance sampling approach for identifying dangerous events for a typical run.

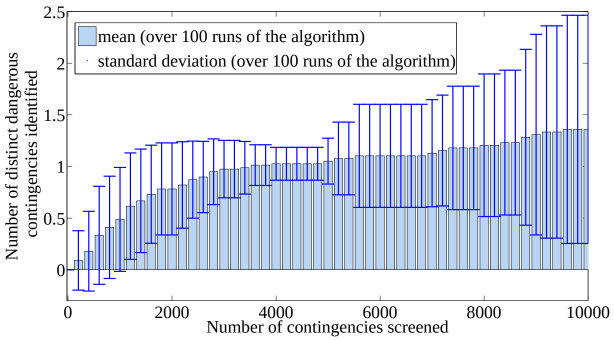


Fig. 6. Total number of dangerous contingencies identified versus number of contingencies screened.

leading to high values of $O(\cdot)$. This is illustrated on Figure 5 which shows the average values taken by the objective function on the successive samples drawn, for a typical run of the algorithm. In this figure, the horizontal axis represents the iteration number of the algorithm while each vertical bar represents the average plus/minus the standard deviation of the objective function in the sample of size 200 at a given iteration.

While Figure 4 gives information on the speed at which our approach can identify one single dangerous contingency, it does not tell anything about its ability to identify rapidly several dangerous contingencies. To study this, we have plotted on Figure 6, the average and the standard deviation (computed over 100 runs of the algorithms) of the number of different dangerous contingencies identified by the algorithm as a function of the number of contingencies it has screened. As one observes, this average number gets quite rapidly close to one but does not increase rapidly afterwards. This is due to the fact that once the first dangerous contingency has been identified by the algorithm, the sampling distributions built in the successive iterations are likely to give more and more weight to this specific contingency. We have however observed that for a few runs of the algorithm, this was not necessary the case. These runs were identifying a larger number of contingencies, between 3 and 6. This explains why the variance plotted on the figure grows to rather large values.

V. Related work

The cross-entropy based importance sampling approach proposed in this paper for efficiently identifying rare dangerous events was first used within the context of power systems in [4]. In this latter paper, the space of "events" was made of load/generation patterns and the cross-entropy algorithm was applied without any metrization of the event space.

As regards the identification of dangerous events or the computation of reliability indices, it has long been recognized by power system engineers that crude Monte-Carlo simulations may be computationally inefficient. Numerous techniques were proposed to address this problem. For example, References [1], [13] propose to combine, in the context of distribution systems, Monte-Carlo simulations with some analytical approaches. Paper [11] proposes to exploit artificial neural networks based on the learning vector quantization algorithm to make Monte-Carlo techniques more computationally efficient for loss of load probability calculations. Importance sampling as well as other variance reduction techniques have also been recurrently proposed in the power system literature as an enhancement of Monte-Carlo methods (see, e.g., [13], [3], [14], [8]).

In order to identify probability distributions targeting dangerous $N-k$ contingencies, the method proposed in this paper only requires to run a security analysis for a relatively small set of events. Viewed in this light, it can be parented to the significant body of work related to contingency filtering and contingency screening in power systems (see, e.g., [9], [6], [7]). Most of the approaches for contingency filtering however rely on deterministic algorithms while the one proposed in this paper is a stochastic one. The importance sampling distributions computed over the course of the cross-entropy algorithm algorithm could possibly also be used as classifiers for dangerous and non-dangerous events: indeed, they should ideally associate a low probability to non dangerous events and a high probability to dangerous ones. To this extent, the approach proposed has some similarities with the many works where classifiers for assessing the degree of severity of power system scenarios are built (see, e.g., [7], [17], [16]).

VI. Conclusions and future work

In this paper, we have proposed an approach for identifying rapidly among large sets of $N-k$ events, some of the assumed few that could endanger the steady-state security of a power system. The approach relies on importance sampling techniques, a proper measure of the severity of an event and a metrization of the contingency space. Simulations carried out on the IEEE 118 bus system have shown that the approach is able to find dangerous events significantly faster than pure Monte-Carlo approaches.

From a technical point of view, this work suggests several research directions. At first, the procedure proposed for metrizing the event space was specific to events corresponding to the loss of k lines. Therefore, we believe it would be interesting to develop flexible metrization procedures that could be applied to compare events of various nature and, in particular, to compare $N-k$ events corresponding to the simultaneous loss of different types of power system elements (e.g., one generator, some loads and a line). Secondly, while our approach was able to identify rapidly some dangerous events, it would be relevant to study whether it could be modified to identify all the dangerous events or at least a significant fraction of them. Thirdly, investigating how the approach could be adapted to deal with other stability issues than steady-state ones (e.g., angle stability, voltage stability) would certainly be another interesting topic of research.

Due to the increasing penetration of renewable energies, the generation patterns that need to be considered when analyzing the stability of a power system may become very numerous and running even only a $N-1$ security analysis for every of them may become impossible. This suggests that developing a methodology for identifying the dangerous production patterns without having to analyze them one by one would be desirable. We believe that such a methodology could be developed by extending the approach proposed in this paper.

Acknowledgments

Florence Fonteneau-Belmudes thanks the FRIA (Belgian Fund for Research in Industry and Agriculture) for supporting her research.

Damien Ernst is a Research Associate of the Belgian FNRS (French acronym for National Fund of Scientific Research) from which he acknowledges the financial support.

This paper presents research results of the Belgian Network DYSCO, funded by the Interuniversity Attraction Poles Programme, initiated by the Belgian State, Science Policy Office. The scientific responsibility rests with its authors.

References

[1] R.N. Allan and M.G. Da Silva. Evaluation of reliability indices and outage costs in distribution systems. *IEEE Transactions on Power Systems*, 10(1):413–419, 1995.

[2] C. Andrieu, N. de Freitas, A. Doucet, and M.I. Jordan. An introduction to MCMC for machine learning. *Machine Learning*, 50:5–43, 2003.

[3] K. Bae and J.S. Thorp. An importance sampling application: 179 bus WSCC system under voltage based hidden failures and misoperations. In *Proceedings of the Thirsty-First Annual Hawaii International Conference on System Sciences*, page 39. IEEE Computer Society, 1998.

[4] F. Belmudes, D. Ernst, and L. Wehenkel. Cross-entropy based rare-event simulation for the identification of dangerous events in power systems. In *Proceedings of the 10th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS-08)*, Rincon, Puerto Rico, 2008. (8 pages).

[5] I. Borg and P. Groenen. *Modern Mutlidimensional Scaling: Theory and Applications*. Springer New York, 2005.

[6] F. Capitanescu, M. Glavic, D. Ernst, and L. Wehenkel. Contingency filtering techniques for preventive security constrained optimal power flow. *IEEE Transactions on Power Systems*, 22(4):1690–1697, 2007.

[7] K.W. Chan, R.W. Dunn, A.R. Daniels, J.A. Padget, A.O. Ekwue, P.H. Buxton, and M.J. Rawlins. On-line dynamic-security contingency screening and ranking. *IEE Proceedings- Generation, Transmission and Distribution*, 144(2):132–138, 1997.

[8] Q. Chen. *The Probability, Identification and Prevention of Rare-Events in Power Systems*. PhD thesis, Iowa State University, 2004.

[9] D. Ernst, D. Ruiz-Vega, M. Pavella, P. Hirsch, and D. Sobajic. A unified approach to transient stability contingency filtering, ranking and assessment. *IEEE Transactions on Power Systems*, 16(3):435–444, 2001.

[10] D.E. Goldberg. *Genetic Algorithms in Search, Optimization and Machine Learning*. Addison-Wesley, 1989.

[11] X. Luo, C. Singh, and A.D. Patton. Power system reliability evaluation using learning vector quantization and Monte-Carlo simulations. *Electrical Power Systems Research*, 66(2), 2003.

[12] H. Muehlenbein, T. Mahnig, and A. Ochoa Rodriguez. Schemata, distributions and graphical models in evolutionary optimization. *Journal of Heuristics*, 5:215–247, 1999.

[13] M.V.F. Pereira, M.E.P. Maceira, G.C. Oliveira, and L.M.V.G. Pinto. Combining analytical models and Monte-Carlo techniques in probabilistic power system analysis. *IEEE Transactions on Power Systems*, 7:265–272, 1992.

[14] J.H. Pickels and I.H. Russel. Importance sampling for power system security assessment. In *Proceedings of the Third International PMAPS Conference*, pages 47–52, 1991.

[15] R.Y. Rubinstein and D.P. Kroese. *The Cross-Entropy Method. A Unified Approach to Combinatorial Optimization, Monte-Carlo Simulation, and Machine Learning*. Information Science and Statistics. Springer, 2004.

[16] L. Wehenkel, C. Lebrevelec, M. Trotignon, and J. Batut. Probabilistic design of power-system special stability controls. *Control Engineering Practice*, 7(2):183–194, 1999.

[17] L. Wehenkel, T. Van Cutsem, and M. Ribbens-Pavella. An artificial intelligence framework for on-line transient stability assessment of power systems. *IEEE Transactions on Power Systems*, PWRS-4:789–800, 1989.

VII. BIOGRAPHIES

Florence Fonteneau-Belmudes (M'07) received her M.Sc. from SUPELEC (France) in 2007. She is now a Ph.D. student in the Systems and Modeling Research Unit of the University of Liège. Her main research interests are in the field of power system analysis and control.

Damien Ernst (M'98) received the M.Sc. and Ph.D. degrees from the University of Liège in 1998 and 2003, respectively. He is currently a Research Associate of the FNRS (Belgian National Fund of Scientific Research) and he is affiliated with the Systems and Modeling Research Unit of the University of Liège. Damien Ernst spent the period 2003-2006 with the University of Liège as a Postdoctoral Researcher of the FNRS and held during this period positions as visiting researcher at CMU, MIT and ETH. He spent the academic year 2006-2007 working at SUPELEC (France) as professor. His main research interests are in the field of power system dynamics, optimal control, reinforcement learning and design of dynamic treatment regimes.

Louis Wehenkel (M'93) graduated as an Electrical Engineer (electronics) in 1986 and received the Ph.D. degree in 1990, both at the University of Liège, where he is full Professor of Electrical Engineering and Computer Science. His research interests lie in the fields of stochastic methods for systems and modeling, machine learning and data mining, with applications in power systems planning, operation and control and bioinformatics.