A rare-event approach for analyzing power system reliability

Florence Belmudes, Damien Ernst, Louis Wehenkel

Department of Electrical Engineering and Computer Science
University of Liège

Benelux Meeting, March 18, 2008

Outline

Introduction

Typically, security and reliability studies cover the events having a rather high probability of occurrence.
However, is this approach still appropriate ?

Goal of this research

- *identify in a "computationally feasible way" the events that could endanger power system security*
- *compute reliability indices*

Proposed approach

Reformulation of the problem of reliability assessment of a power system as a rare-event simulation problem.

Cross-entropy (CE) method for rare-event simulation

- X a random variable taking its value in some space $\mathcal{X}$ with a probability density function (pdf) $f(\cdot)$
- $S(\cdot)$ a real-valued function defined on $\mathcal{X}$
- γ a real number

We need to estimate the probability of occurrence l of an event $\{S(X) \geq \gamma\}$.

Crude Monte Carlo estimator: computationally irrelevant (sample size of 10^{10} required to estimate $l \simeq 10^{-6}$)

Importance sampling: the ideal importance sampling function depends on parameter l.

Cross-entropy (CE) method for rare-event simulation

Main idea of the CE method: find a pdf $g(\cdot)$ which distance to the ideal sampling distribution is minimal.
Convenient measure of distance (Kullback-Leibler divergence):

$$\mathcal{D}(g^*, g) = E_{X \sim g^*(\cdot)} \left[\ln \frac{g^*(X)}{g(X)} \right] \tag{1}$$

Problem to solve:

$$\arg\min_{g \in \mathcal{G}} \mathcal{D}(g^*, g) \tag{2}$$

It is equivalent to solve:

$$\arg\max_{g \in \mathcal{G}} E_{X \sim f(\cdot)} \left[I_{\{S(X) \geq \gamma\}} \ln g(X) \right] \tag{3}$$

Cross-entropy (CE) method for rare-event simulation

If l is not too small, CE based algorithms for rare-event simulation estimate a good solution of (3) by solving its stochastic counterpart:

$$\arg\max_{g \in \mathcal{G}} \sum_{j=1}^{M} I_{\{S(X_j) \geq \gamma\}} \ln g(X_j) \tag{4}$$

When l is too small, the number of samples necessary to obtain a "good" stochastic counterpart (4) of (3) is prohibitively high. $\Rightarrow$ **iterative algorithms** are to be used to solve this stochastic counterpart

Cross-entropy (CE) method for power system analysis

Identification of dangerous events

- events are seen as pairs “operating conditions-disturbance”
- screening each plausible pair by the stability evaluation tool is generally not possible
- let $S(x) = 1$ if the event x drives the system to unacceptable conditions and 0 otherwise. Running the CE method on the rare-event problem $\{S(x) \geqslant 1\}$ outputs a pdf which concentrates on the dangerous events.

Cross-entropy (CE) method for power system analysis

Computation of reliability indices

- reliability index: probability that the system may be driven to unacceptable conditions
- the computation of the reliability index is equivalent to the resolution of the rare-event problem $\{S(x) \geqslant 1\}$.

Key factors for the successful application of the framework

- quality of the models of the power system
- choice of the function $S(x)$: the CE based algorithm behaves better when, instead of taking binary values, the function $S(x)$ is an image of the severity of the event x.
- choice of the initial probability distribution f: this pdf has to give a good coverage of the event space.

Experiment for static voltage security

IEEE 30 bus system was chosen to experiment the framework.
Problem considered: static voltage security (loadability)

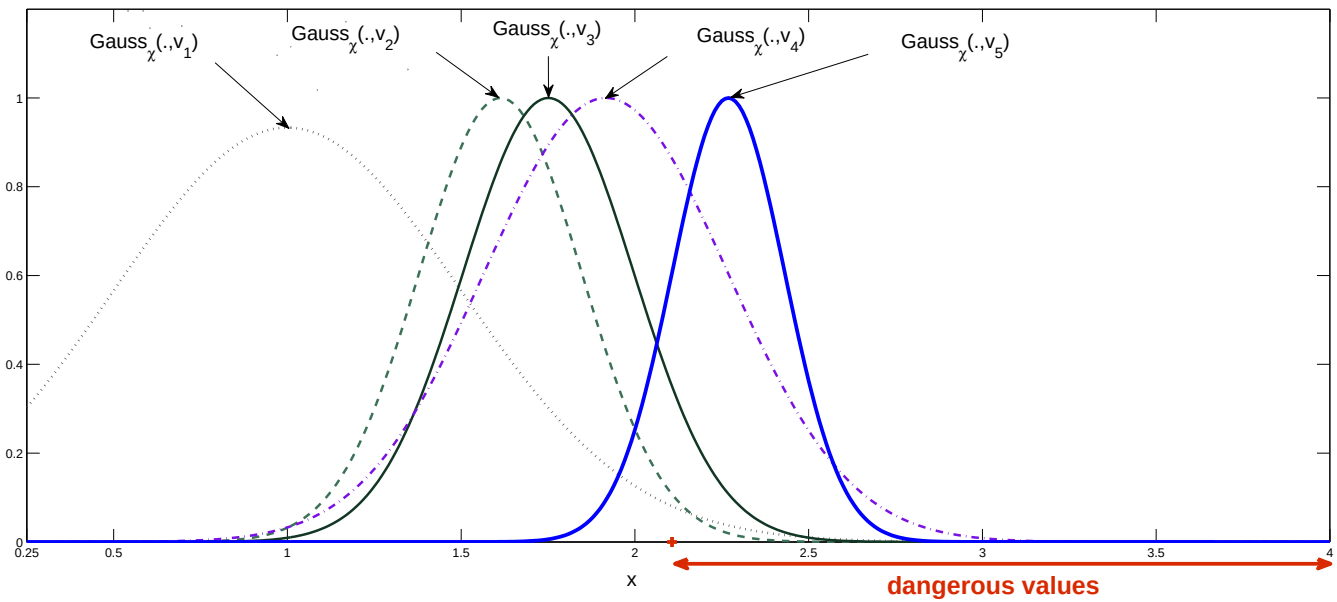
Parameters

- an event is defined as a homothetic increase/decrease of the load with respect to the base case (coefficient $x \in [0,25;4]$).
- an event (value of x) is considered acceptable if the corresponding demand level can be served while respecting voltage constraints, an Optimal Power Flow being run to find out if the event is feasible.
- the value of the severity function for an event x is chosen equal to the number of iterations of the OPF to convergence. If convergence does not occur, $S(x)$ is set to an arbitrary high value (1000).

Experiment for static voltage security

Results

When choosing the initial pdf $f(\cdot) = Gauss_{[0.25;4]}(\cdot, [1, 0.5])$, we obtain the sequence of pdfs drawn here:



The pdf evolves to give strong preference to the dangerous events.

Conclusion

- We have proposed a new framework for identifying dangerous events and computing reliability indices in a power system.
- The approach was illustrated on a problem of static voltage security. Even if preliminary, the results were encouraging.

Future work

- *application of this framework to more realistic "large scale" reliability problems*
- *identification of the type of severity function that would lead to the best results*