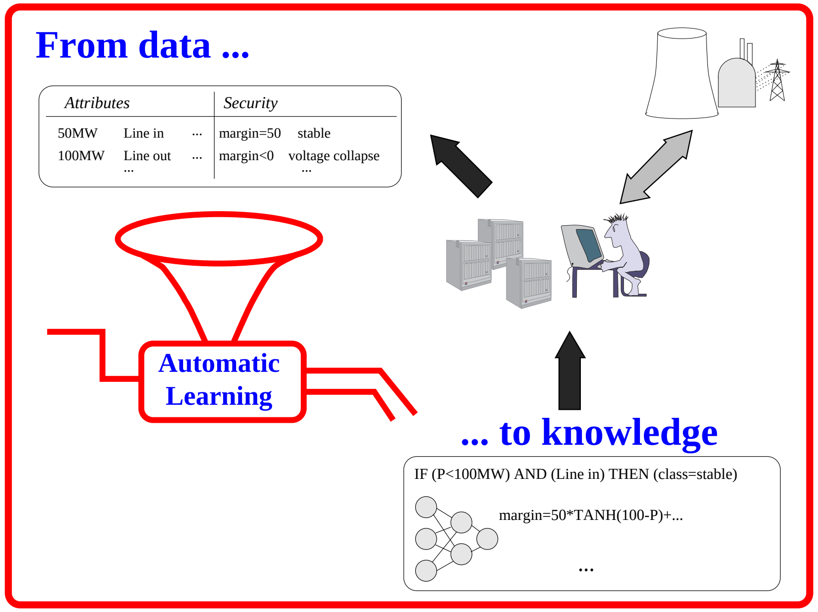
IEEE PES Winter Meeting 1998
Power System Stability Subcommittee Meeting

Artificial Intelligence Methods for Voltage Stability Assessment

Louis WEHENKEL
University of Liège - Belgium

I. (Quick) overview of the AI field in 1998
II. Automatic Learning framework for DSA
III. Applications to voltage stability/security
IV. Present status and research

Copies of the slides can be downloaded from the Web at `http://www.montefiore.ulg.ac.be/~lwh/`



I. (Quick) overview of the AI field in 1998

Two main complementary approaches :

- Model centered ⇒ Knowledge based (expert) systems
  Knowledge representation, reasoning mechanism, explanations,
  End-user interfaces and integration issues (e.g. with EMS)

- Data centered ⇒ Automatic learning based systems
  Machine learning (e.g. decision trees)
  Artificial neural networks
  Statistical pattern recognition, density estimation, regression

Hard vs Soft computing (neural nets, fuzzy syst., evolutionary comp.)

Recent progress (since 1985) :

- In automatic learning :
  Integration of various techniques (toolbox, hybrids ...)
  New methods
  Advances in theory (e.g. statistical learning theory)

- Use of probability methods :
  Uncertain reasoning (e.g. Bayesian belief networks)
  Automatic learning theory

- Fuzzy systems :
  Knowledge representation : imprecision and graduality
  Automatic learning methods (e.g. fuzzy trees, neuro-fuzzy...)

- Evolutionary computation (e.g. genetic algorithms...)

Summary

AI field :

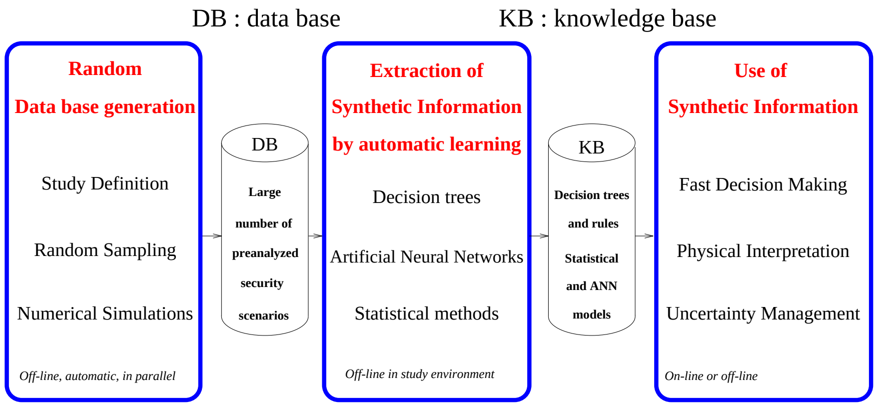
- Earlier work : centered on representing (human) knowledge and simulating (human) reasoning mechanisms
- Today : towards data (and computationally) intensive methods

⇒ Data mining : methodologies and tools to extract meaningful and useful *information from large amounts of* raw data

Relevance to the power system field :

- Many data sources : substations, SCADA, simulations...
- Many potential applications :
  Monitoring and forecasting
  Modeling and design (combination with analytical techniques)

II. AL framework for Dynamic Security Assessment



Applications : Dynamic performance analysis (modes, regions)
Design of operating and emergency control rules

Data base generation

Preliminary remarks

- Security information DB : several 1000 security scenarios
- Quality of the DB : determines quality of extracted knowledge
- Sound methodology is needed : specification and validation
- Scenarios should be uncorrelated : to apply AL tools

NB. DB specification is time consuming.

But, if done properly once, may serve several times.

⇒ Let the computer do the job for which it is best suited...

What is a security scenario ?

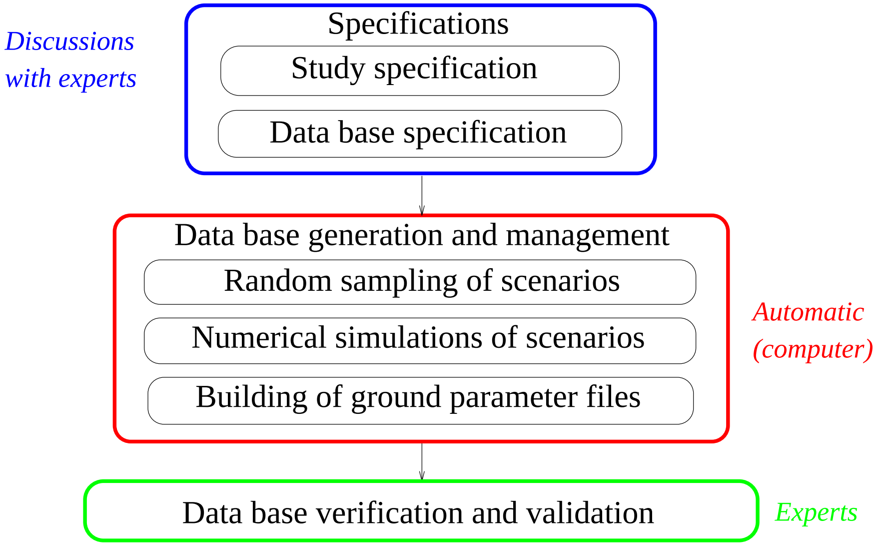
Three components

- Initial operating point (OP) :
  Equilibrium, defined by available equipments and their initial state
- External disturbances (ED) :
  Events which initiate dynamics (faults, load trends...)
- Dynamic modeling hypothesis (MH) :
  Assumptions on how the system is supposed to behave

NB.

1. All three may vary from one scenario to another (examples later)
2. How they vary depends on the objective of the security study

Overall data base generation process

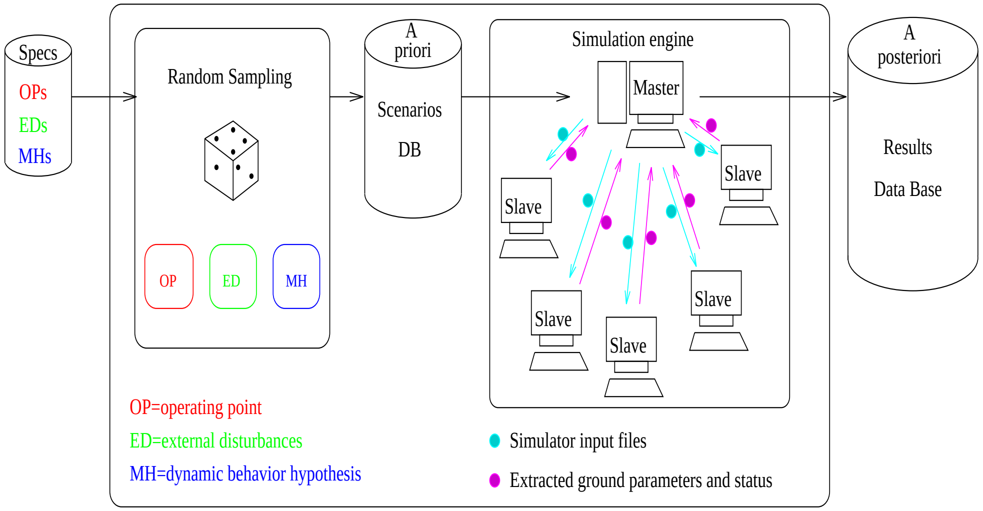


Specifications

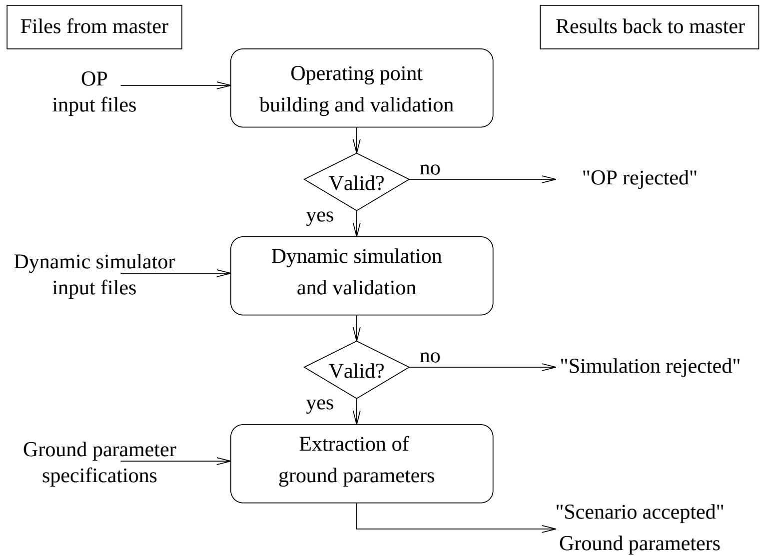
- Study scope
  Define objectives of the study and range of target conditions. Types of phenomena. Range of operating points and faults. Modeling assumptions.
- Data base per se
  - Random sampling specifications (variables and probability distributions)
  - Extracted ground parameters (attributes, security information)
  - Acceptability criteria and filtering
  - Number of scenarios to simulate

⇒ Many discussions with experts

Data base generation tool



Scenario simulation



Essentials of Automatic Learning

Some definitions

Supervised learning.

Given a set of examples (the learning set (LS)) of associated input/output pairs, derive a general rule representing the underlying input/output relationship, which may be used to explain the observed pairs and/or predict output values for any new unseen input.

Unsupervised learning

Discover similarities and/or correlations ⇒ later...

Toolbox of Automatic Learning Methods

Motivation : different AL methods provide different functionalities

- Interpretability ⇒ decision trees
- Accuracy ⇒ non-linear regression like ANNs
- Local reasoning ⇒ nearest neighbor techniques
- Identification of modes, regions ⇒ unsupervised learning

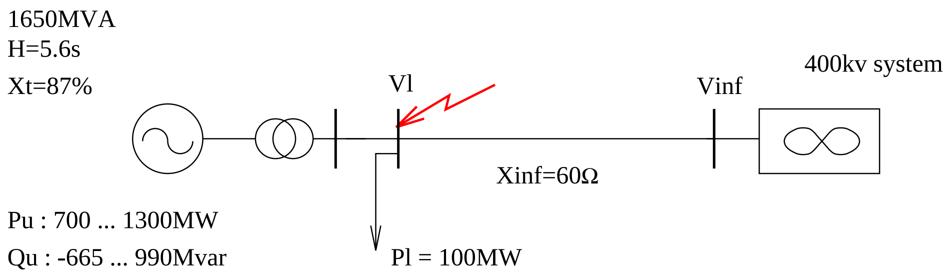
Hybrid techniques : combine advantages of different methods

- DT-ANN, DT-KNN
- Fuzzy decision trees

Example Security Problem

Transient stability assessment

NB. Toy problem...

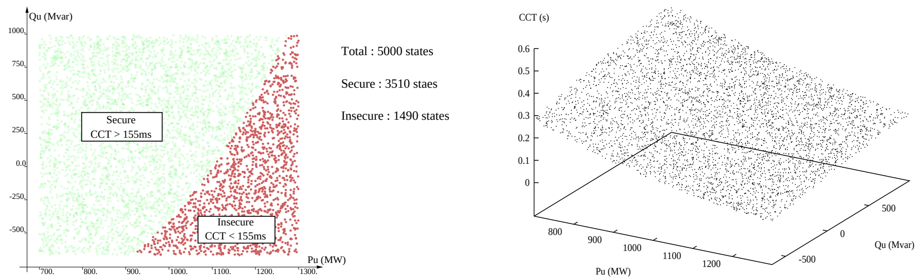


Inputs : Pu and Qu

Output : CCT or security Class (Secure iff CCT > 155ms)

Example Security Problem : Data Base

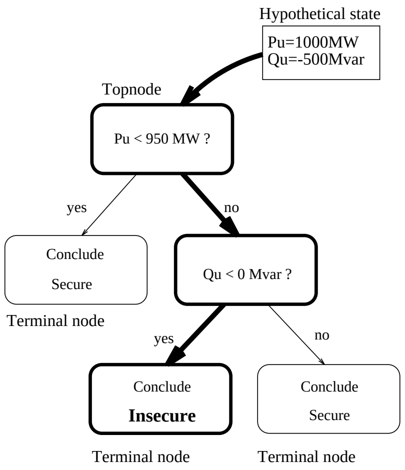
Data base : 5000 operating points (uniform distributions in P-Q space)
CCTs : by SBS dichotomy (simplified model)



Learning set (LS) : 3000 states
Test set (TS) : 2000 other states

Decision Tree Learning

What is a decision tree ?



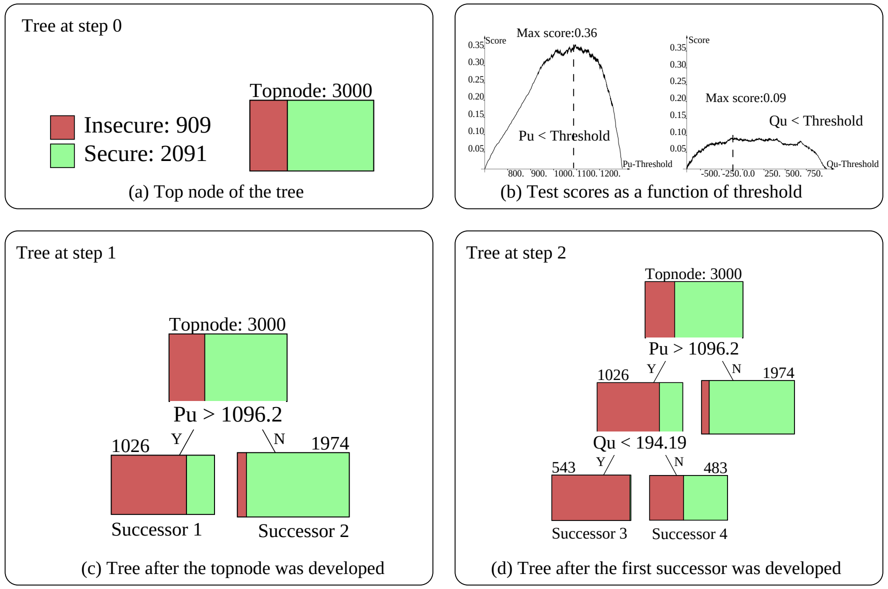
Equivalent If-Then rules :

Rule 1 : If (Pu < 950MW) then Conclude Secure

Rule 2 : If (Pu > 950MW) and (Qu < 0Mvar) then Conclude Insecure

Rule 3 : If (Pu > 950MW) and (Qu > 0Mvar) then Conclude Secure

How is it "learned" from a learning set ?



(a) Top node of the tree

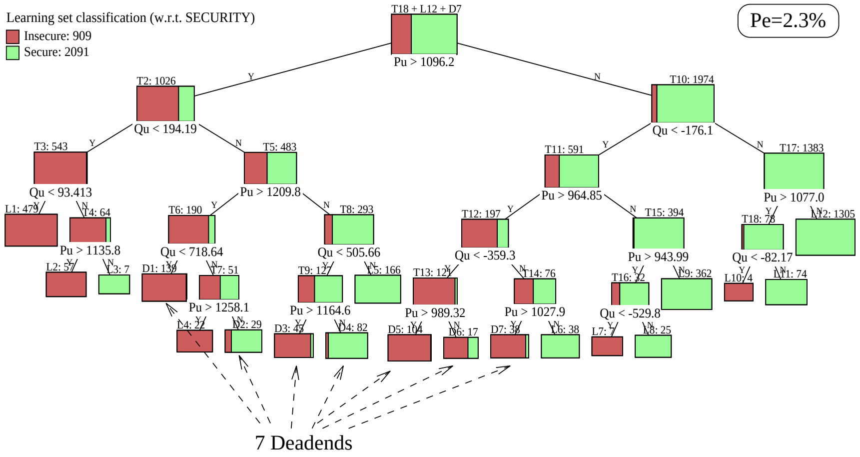
(b) Test scores as a function of threshold

(c) Tree after the topnode was developed

(d) Tree after the first successor was developed

Technicalities : optimal splitting and stopping to split $\Rightarrow$ later...

This is the end-result for our example problem



NB. Testing the tree : how many and which kind of errors

In practice :

Define security classes : number, thresholds

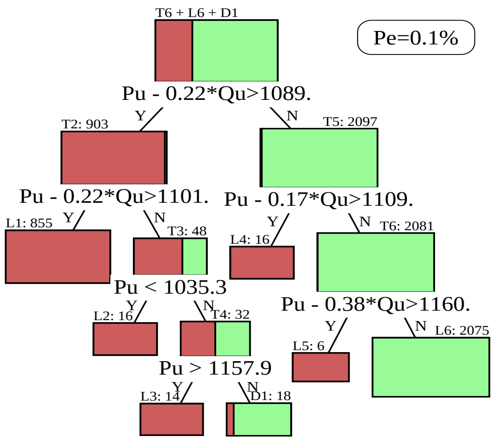
NB : classes can be biased to avoid dangerous errors...

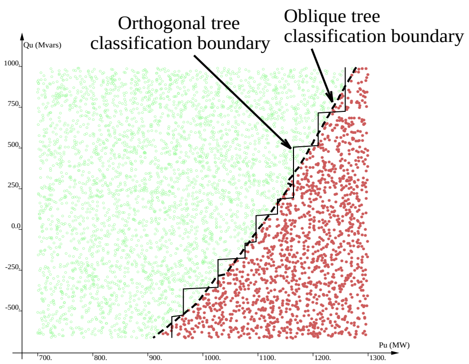
Propose many candidate attributes

Algorithm will select (most) appropriate ones automatically

Tree building $\Rightarrow$ interesting by-products (see demo)

Refinements : oblique trees, regression trees, fuzzy trees...





... simpler, more accurate : better

Salient features of decision trees

Interpretability ⇒ physical insight

Identify relevant attributes ⇒ reduce dimensionality

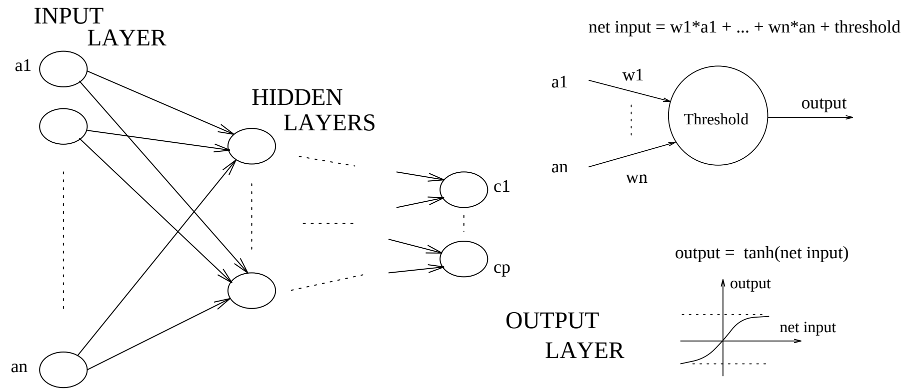
Computational efficiency ⇒ trial and error

Discrete and rather rough... (but improvements exist)

⇒ Heart of the AL tool box (more about it later...)

Multilayer perceptrons

What is a multilayer perceptron ?

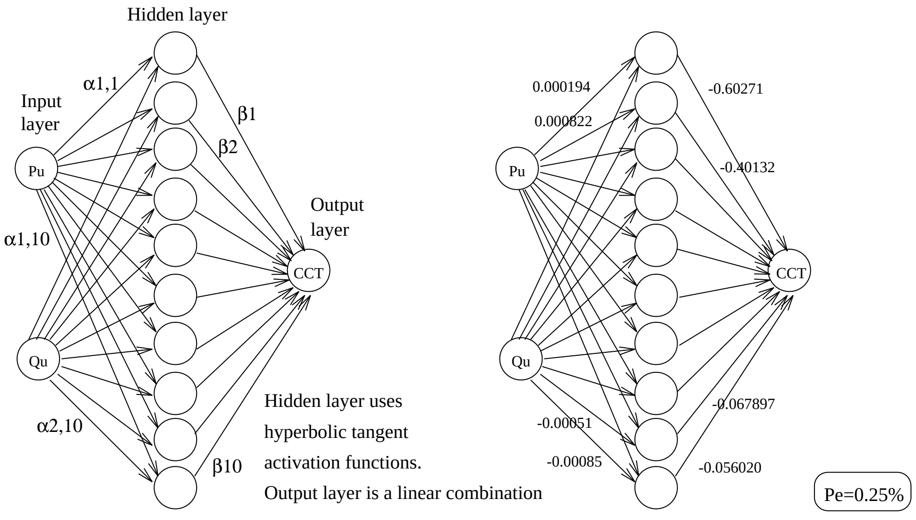


How is it "learned" ?

- Coding
  - Inputs : feature selection and normalization
  - Outputs : human choice... ⇒ security margins or classes
- Structure
  - Layers, neurons, connections
  - Rules of thumb + manual (or systematic) trial and error
- Tuning the parameters
  - For a given structure
  - Iterative optimization (many algorithms)

NB. Cross-validation to avoid overfitting problems

Illustration on our toy problem



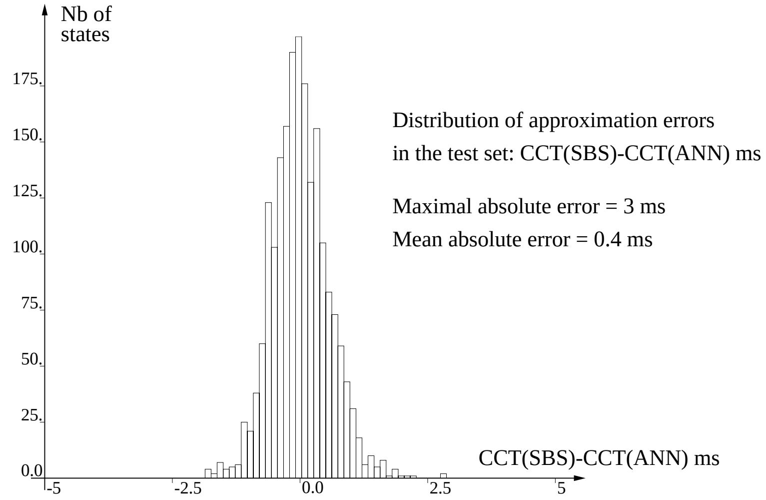
(a) Initial values of the weights are random (b) After training the weights are tuned to fit the problem

Parameter tuning (BFGS) yields the following after 46 iterations

$$
\begin{aligned}
\mathrm{CCT}_{\mathrm{MLP}} = \; & -0.602710 \tanh(0.000194Pu - 0.00034Qu - 0.93219) \\
& -0.401320 \tanh(0.000822Pu - 0.00020Qu - 0.76681) \\
& +0.318249 \tanh(0.000239Pu - 0.00050Qu - 0.29351) \\
& -0.287230 \tanh(0.002004Pu - 0.00034Qu - 1.20080) \\
& +0.184522 \tanh(0.000131Pu - 0.00057Qu - 0.03152) \\
& +0.177701 \tanh(0.001799Pu - 0.00011Qu - 2.08190) \\
& -0.150720 \tanh(0.001530Pu - 0.00056Qu - 1.68040) \\
& +0.142678 \tanh(0.002152Pu - 0.00046Qu - 1.72280) \\
& -0.067897 \tanh(0.001910Pu - 0.00051Qu - 1.71343) \\
& -0.056020 \tanh(0.000202Pu - 0.00085Qu - 0.39876)
\end{aligned}
$$

NB: a simpler structure could have worked as well...

Testing the MLP's generalization to unseen cases :



or $P_e = 0.25\%$ ....very accurate indeed!

Salient features of MLPs

- Able to infer security margins
- Very flexible and accurate in practice
- Black box (in large scale problems)
- May lead to overfitting if used "naively"
- Slow parameter tuning algorithms

⇒ hybrid DT-ANN setting (more about it later...)

Nearest neighbor techniques

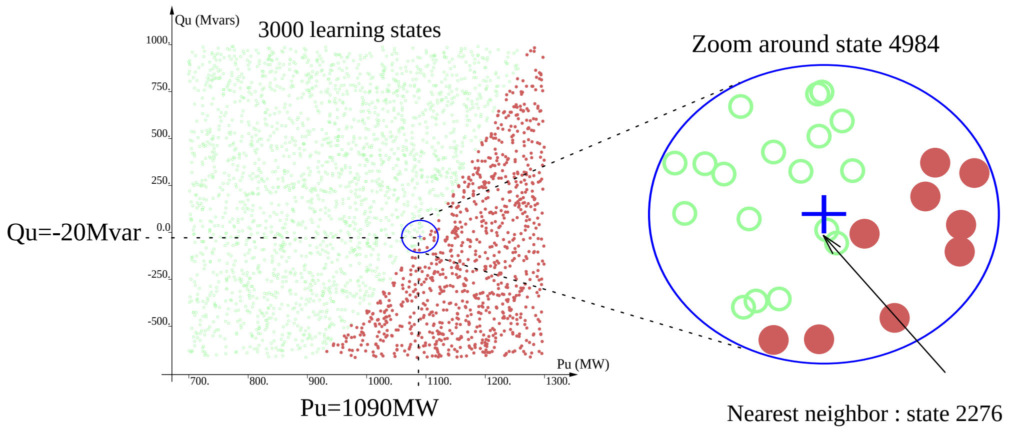
What is it ?

Define a distance (or similarity measure) in the input attribute space.

To predict output of an unseen state :

- First find the (few) most similar state(s) in the LS
- Extrapolate their output to the unseen state

Illustration on our toy problem



CCT(state 2276) = 0.157s (error = -0.001s) $P_e = 0.9\%$

Salient features of KNN

- Able to infer security margins as well as classes
- Provides case by case analysis (detection of outliers)
- No global view
- Very sensitive to irrelevant or redundant attributes
- Rather slow at use and excessively slow tuning (GAs)

$\Rightarrow$ hybrid DT-KNN setting (more about it in a moment...)

Refinements

Adapting K to the problem

Feature selection and distance tuning

Local distances

Efficient search techniques

...

Features of pure and hybrid supervised learning methods

	Method	Functionalities	Computational Off-line	Computational On-line
Pure	Crisp DTs	Good interpretability (global). Discrete. Good accuracy for simple "localized" problems. Low accuracy for complex, diffuse problems.	Very fast	Ultra fast
Pure	MLPs	Good accuracy. Low interpretability. Margins and sensitivities.	Very slow	Fast
Pure	kNN	Good interpretability (local). Conceptual simplicity.	Very slow	Very slow
Hybrid	Fuzzy DTs	Good interpretability (global). Symbolic and continuous. More accurate than crisp trees. Margins and sensitivities.	Slow	Very Fast
Hybrid	DT-ANN	Combine features of DTs & MLPs	Slow	Very Fast
Hybrid	DT-kNN	Combine features of DTs & kNNs	Slow	Slow

Unsupervised learning

- Discover similarities
  - Among states ⇒ clustering
  - Among variables ⇒ correlation analysis
- Various more or less sophisticated techniques exist
  - K-means ⇒ illustrated later
  - Hierarchical clustering ⇒ illustrated later
  - Kohonen feature maps ⇒ illustrated later

III. Applications of AL to Voltage Stability Assessment

General idea : exploit DB by AL to analyse system behavior in the context of a large number of diversified scenarios, and to extract decision rules or to "tune" parameters of some (detection or control) device.

NB. The AL approach may be applied to any kind of security assesment problem, as well as to other design problems based on simulations.
It was initially developed in the context of transient stability assessment, and is presently applied also to static security assessment.

MENU

- Overview of types of problems which may be tackled by AL
- Examples of actual applications (EDF system)

Practical application environments and possible uses of AL

- Generation transmission system planning
  - Screening large numbers (100,000) of different configurations
  - → Use of AL to extract synthetic information from simulations
  - → Combination with Monte-Carlo simulations (e.g. to reduce variance)
- Design of protection and control systems
  - → Assessment of existing special stability control systems
  - → Tuning of thresholds and delays
  - → Selection of triggering signals/measurements
  - → Design of new systems
  - NB. Temporal aspects are important

- Operation planning
  - → Design of synthetic security criteria
  - For operators or to include in operation planning software
- On-line operation
  - Use security criteria prepared off-line
  - → Adapt security to changing conditions
- Real-time monitoring and control
  - Use criteria and devices designed off-line
- Operator training
  - Exploit DB of interesting scenarios
  - Use knowledge extracted off-line to build scenarios
  - Give explanations to trainee

AL and analytical tools

- Analytical tools
  - Load-flow, SBS, direct, eigenvalues...
  - Used to build DBs
  - Provide detailed case by case analysis
- Automatic Learning
  - Extract synthetic information from DBs
  - May compare simplified tools (or modelings) with detailed ones
  - May formulate security constraints compatible with other tools (e.g. Unit Commitment)

⇒ They are essentially complementary

Examples : application to the EDF system

Problem statement

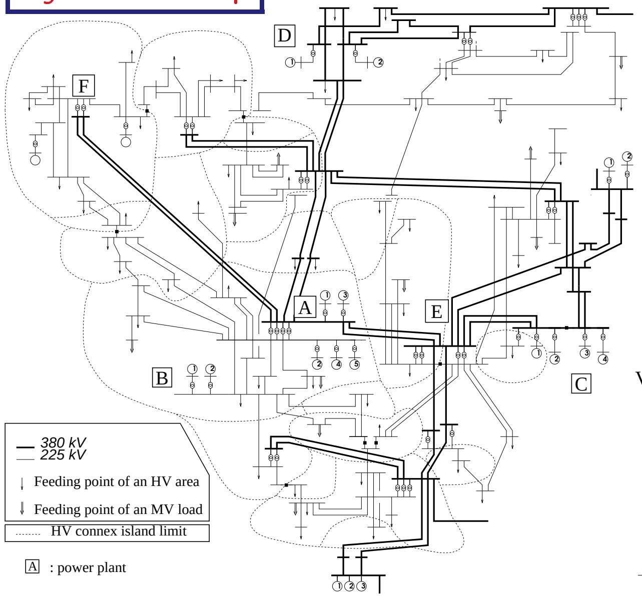
- Main phenomenon : risk of voltage collapse induced by load restoration through automatic OLTCs
- Simulation model : ASTRE
  (no fast "electromechanical" dynamics, detailed model otherwise)
- Generation of a large range of operating conditions of study region (ex. Western part and South-Eastern parts are "voltage weak")

Data base generation

- For each operating state, simulation of a list of potentially harmful contingencies (10 to 30), and computation of pre-disturbance and post-disturbance security margins
- Uncertainties are taken into account by randomizing parameters of the model used for simulation (e.g. load model and distribution among individual HV/MV transformers...)
- Data base stores attributes' values in the predisturbance state and just after the occurence of a disturbance (JAD) : can be used both for preventive and emergency modes

Several 100,000 simulations : - a few days of CPU time
- about 10 to 100MB of raw data.

System Map



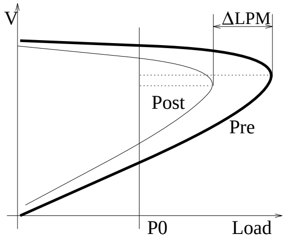
Study region load : 4700-7500MW

Topologies : N, N-1, N-2

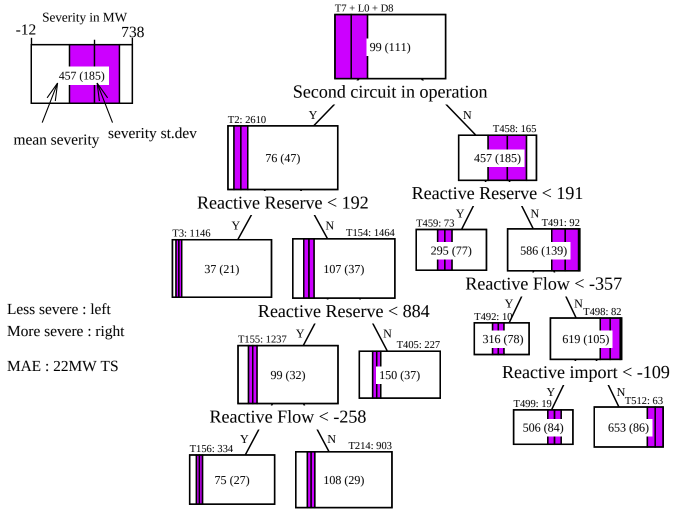
Model : 1200 buses, 450 OLTCs
CSVC, 70 machines

For a given contingency and OP :

ΔLPM : measure of severity

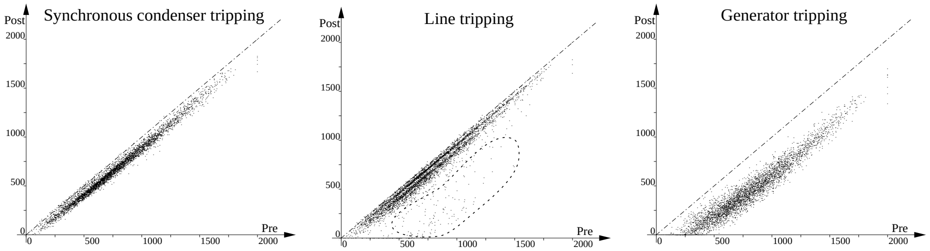


Severity regression tree : loss of a line circuit



Pre- vs post-contingency LPMs

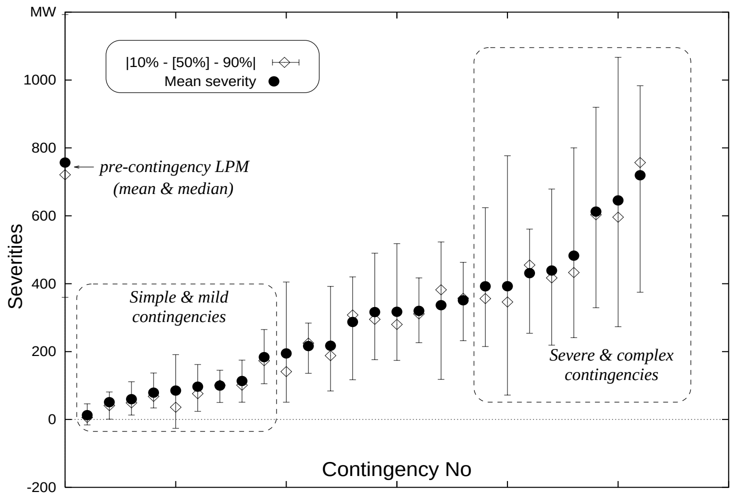
3 contingencies, 5000 OPs



Mean Δ LPM = 99 MW	Mean Δ LPM = 97 MW	Mean Δ LPM = 355 MW
Stand. Dev. 38MW	Stand. Dev. 105MW	Stand. Dev. 88MW
⇒ very simple	⇒ less simple	⇒ more severe

L. Wehenkel. Contingency severity assessment for voltage security using non-parametric regression techniques. *IEEE Trans. on Power Syst.*, PWRS-11(1):101–111, February 1996.

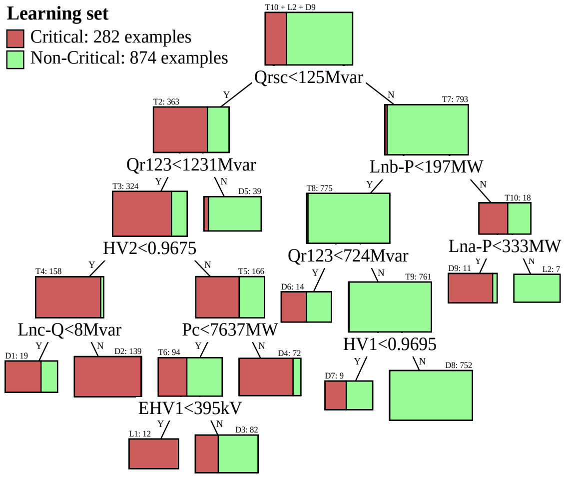
Severity ranges of 26 contingencies (5000 OPs)



Severity : Δ LPM (pre-cont. - post-cont. load-power-margin)

NB. Uncertainty of LPM ≈ 40MW

Emergency state detection : generator trip (JAD state)



Attributes are measured at t0+30s.

Qr* denotes a reactive reserve

HV* denotes a HV voltage (p.u.)

Ln* denotes a power flow

Pc denotes the regional load level

Contingency

Loss of a generator

Test results :

Number of test states : 1156
Pe = 8.5%
P(FA) = 3.8%
P(ND) = 4.7%
P(DE) = 0.2%

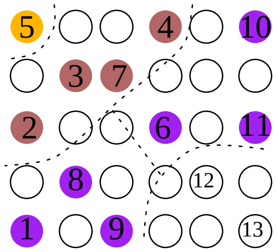
Variants : multi-contingency trees, other acquisition times

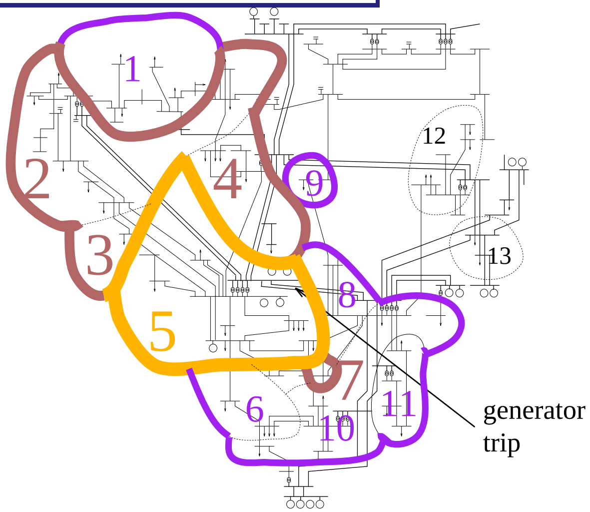
Voltage coherent zones

1,2... : coherent regions

"empty" prototypes

Feature map after learning





NB. Analysis carried out simultaneously on 100 different JAD states

IV. Present Status

Methodology in use at the R&D Division of EDF

Last spring, an operational study has been carried out by EDF to define operating guidelines for the South-Eastern part of their system. The so designed rules are presently in use.

Engineers from various departments of EDF start being aware of this methodology and some seem to be really interested...

Preliminary specification of overall software architecture for systematic use of the technique has been carried out. Industrial grade software development is projected for the near future.

New Research : Global Dynamic Security Assessment

Global : - all kinds of possible causes of system failure are studied
- consequences due to slow and fast dynamics are evaluated

- Aims :
  - Identify main system weaknesses, without prior hypothesis on the dynamics involved.
  - Identify distance to insecurity, taking into account probability of causes and severity of consequences.
- Applications :
  - Evaluate existing defense plans and their interactions in very disturbed modes
  - Identify structural weaknesses and means to improve them, by modifying existing defense plans or implementing new ones

Data base (overview)

NB. Ongoing work, since 1995

Data base of 1100 extreme scenarios on the EDF system (now 2000)

Each scenario is simulated during 40-50 minutes (very detailed model)

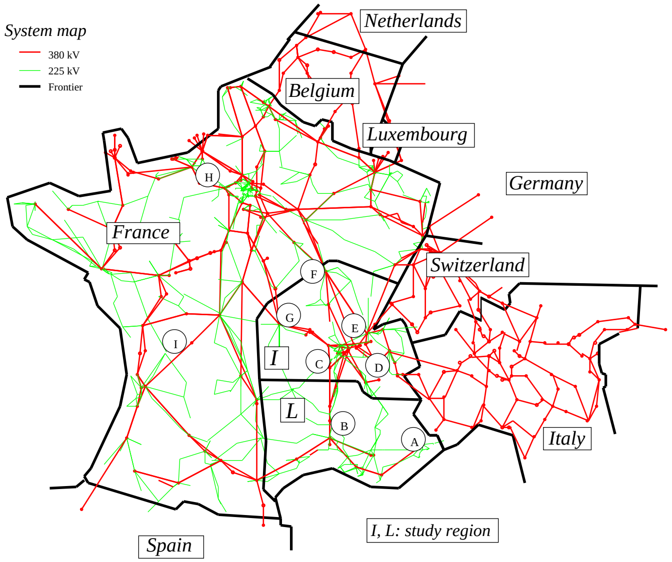
Attributes are temporal variables (curves)

800 attributes ⇒ 1GB data base (sic)

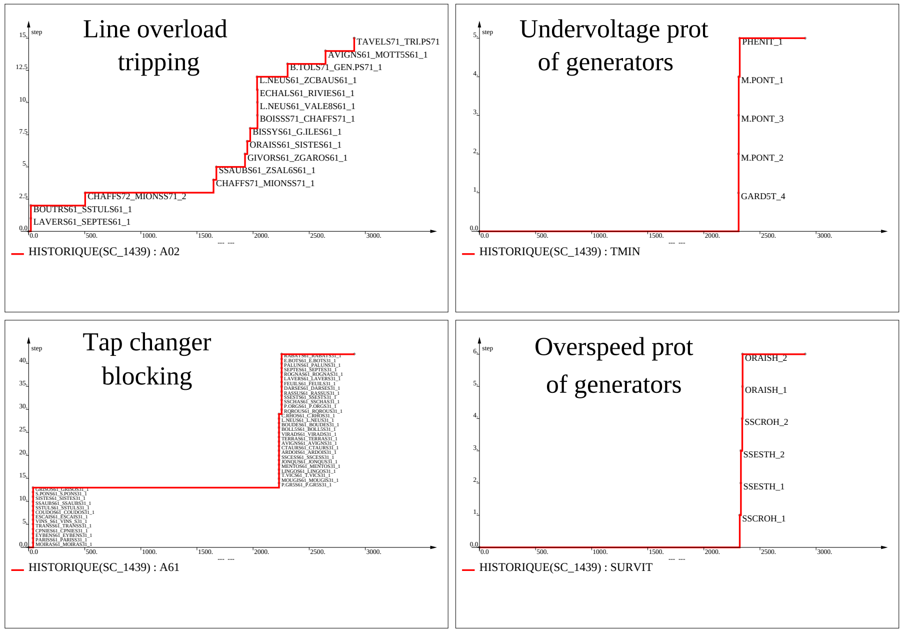
Various collapse phenomena :

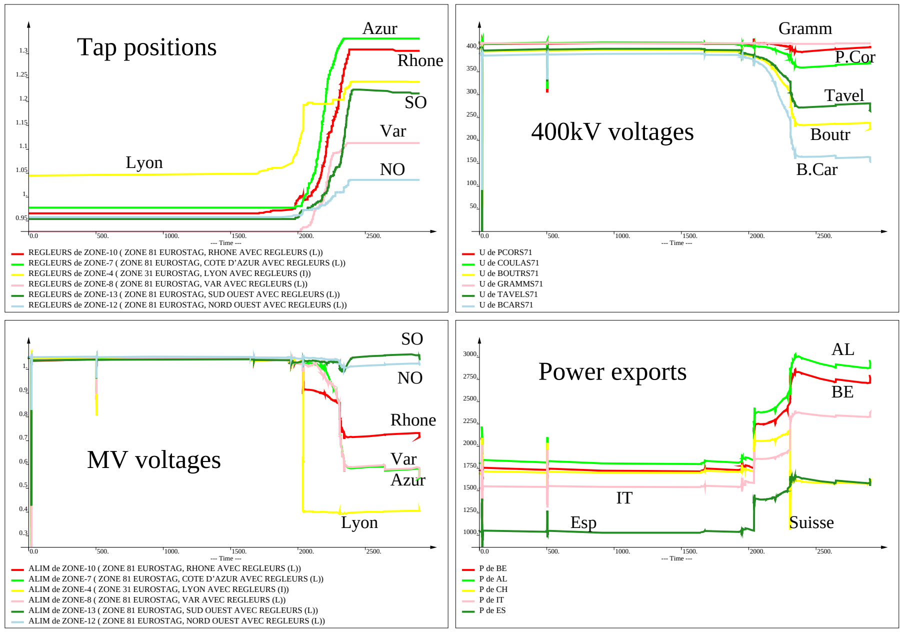
- Line overloads (cascades)
- Voltage collapse (local, regional)
- Loss of synchronism (plant and area modes)

EDF system



- (A) B.CARS71
- (B) TAVELS71
- (C) P.CORS71
- (D) G.ILES71
- (E) GEN.PS71
- (F) VIELMS71
- (G) BAYETS71
- (H) VAUPAS61
- (I) FLEACS61





First application : identify main failure modes

Attributes : characterize the scenarios in terms of consequences

- Number of lines and generators tripped
- Variation of active power generation and interface flows
- Amount of load lost in various regions
- Voltages at end of scenario in various places

Trial and error with K-means clustering algorithm, finally :

- 702 stable scenarios (150MW load lost in the mean),
- 77 local losses of synchronism (2000MW),
- 90 local losses of load without collapse (2000MW),
- 90 local losses of load with local voltage collapses (2000MW),
- 113 regional voltage collapses (7400MW),
- 33 wide area voltage collapses (17000MW),
- 17 regional losses of synchronism (9500MW)

Second application : coherency of voltages

EHV voltages (85 buses) and mean MV voltages of 13 load areas.

Voltage magnitudes at the end of the simulation.

Compute correlation coefficients of all pairs of variables (4753 correlations, estimated from the 1100 learning states).

Hiearchical grouping of variables : first the most correlated a.s.o.

Build dendrogram (graphical representation of the grouping tree) and analyse visually

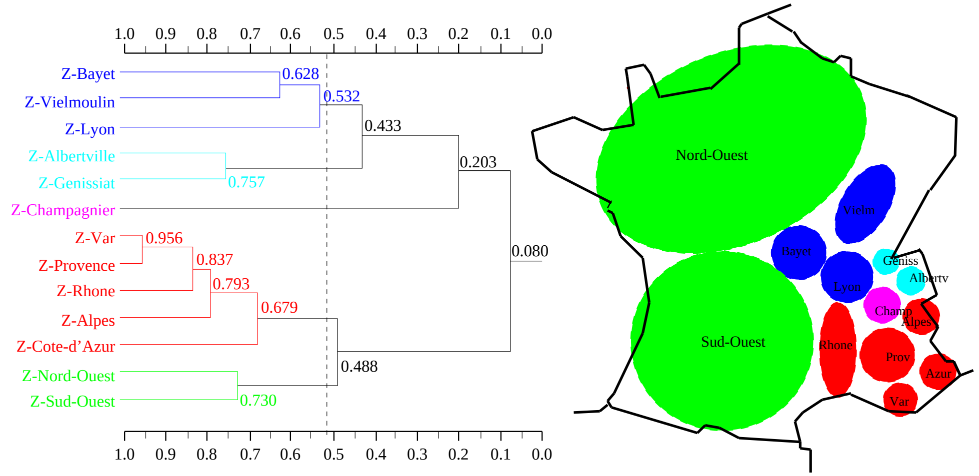
Find out zones of coherent behaviour :

MV ⇒ voltage collapse zones ⇒ where to act to mitigate

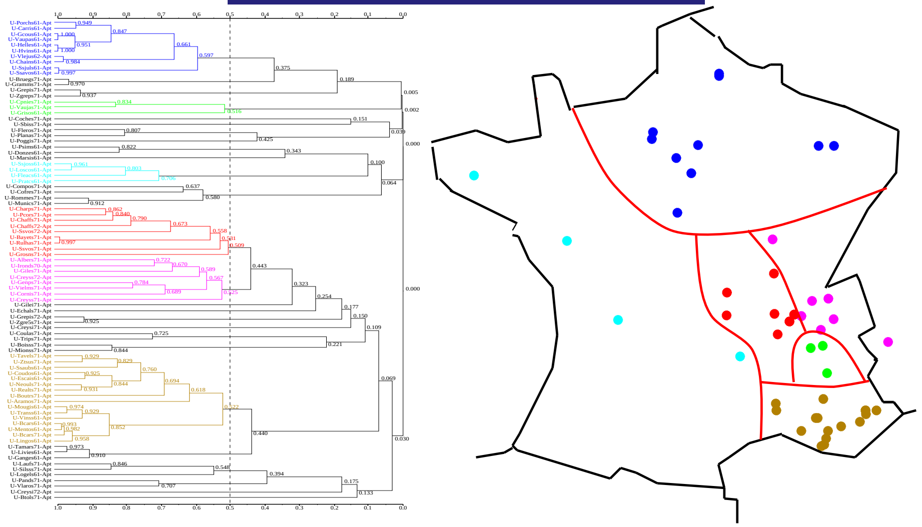
EHV ⇒ impact on EHV system ⇒ where to put triggering signals

MV voltages at end of simulation

Dendrogram (correlations on 1100 scenarios)



EHV voltages at some buses



Ongoing work

- Automatic learning : adapt decision tree induction to handle temporal data (ULg) : find out automatically a good compromize between anticipativity and selectivity of incipient voltage collapse detection.
- Study effectiveness of TCB (tap changer blocking) devices in South-Eastern part : compare scenarios with and without action of TCBs.
- Define measures of scenario severity (loss of load, of generation and transmission equipments, change in exports)
- Identify main classes of failure paths
- Evaluate distance to blackout on an actual situation

Conclusions

- Summary
  - Tool box of AL methods
  - DB generation methodology
  - Large variety of possible applications
- Status
  - Mature technology
  - Needs motivations to be used
  - Strong motivations exist and more are coming...

Next stage

- Management of uncertainties
  - Towards probabilistic security assessment
  - Data collection problem (statistics...)
- Temporal information
  - Improve AL methods
  - Parallel computations
- Software environments