Bilevel programming applied to power system vulnerability analysis under multiple contingencies

José M. Arroyo

E-mail: JoseManuel.Arroyo@uclm.es
Departamento de Ingeniería Eléctrica, Electrónica, Automática y Comunicaciones
Universidad de Castilla – La Mancha

Contents

- Introduction

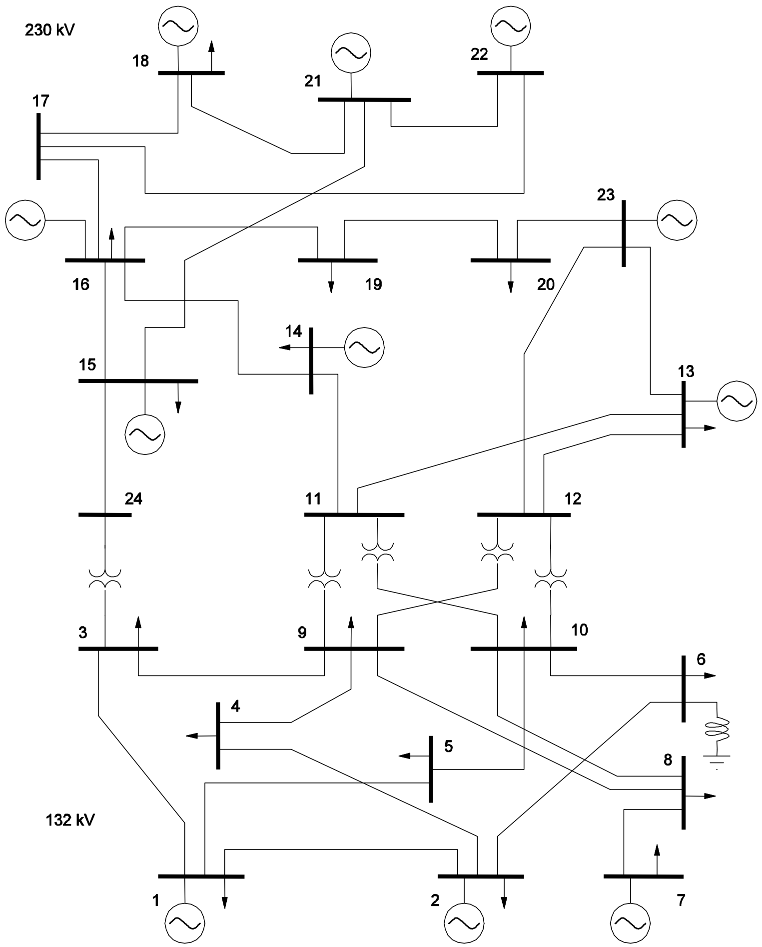
- Atacker-defender bilevel programming models

- Numerical results

Power system

- Physical components: wires, transformers, etc.
- Electrical companies
- Regulators
- Retailers
- Consumers
- Market
- Networks (transmission, distribution)

Power system



Power system

- Operation $\Rightarrow$ Mainly performed by private companies

- Operation monitoring $\Rightarrow$ Government

- Critical infrastructure subject to new risks

- Risks must be managed by both groups of entities

Power system

- Critical infrastructure:
  - Provision of vital services to society or government (security = high standard of life)
  - Closely related to social welfare
  - Availability taken for granted

Power system

- However, experience has shown it does fail:
  - Recent blackouts (North America, Italy, Greece, central Europe)
  - Recent malicious actions

Recent changes in power systems

- Liberalization ⇒ Power markets ⇒ ↑complexity of social network
  - Moved from a monopoly controlled by government to a competitive framework ⇒ New agents and rules
  - However, physical network unchanged

Recent changes in power systems

- Internationalization
- Different use with respect to the original design
- Use of information and communication technologies ⇒ Internet

Vulnerability of power systems

- Susceptibility of attack or damage

- Characteristic of the design, implementation or operation of the infrastructure that makes it susceptible of destruction by a threat

Power system
Factors that make it vulnerable

- Asocciated with generation and transmission assets $\Rightarrow$ Technical weakness

- Market $\Rightarrow$ Operators driven by economic issues

- Pervasive use of open communication networks (cyber-attacks)

Technical weaknesses

- Failure of critical components (ageing, overheating, etc.)
- Inadequate maintenance
- Incorrect tripping of line protections
- Incorrect tripping of generators

Technical weaknesses

- Insufficient load shedding
- Insufficient communication and cooperation among operators
- Insufficient monitoring by operators
- Incorrect action by operators

Types of outages in power systems

- Impact on electricity supply (electrical installations and/or market)
  - Unintentional outage ≡ Uncertain <u>random</u> event (with probability distribution)
  - Deliberate outage ≡ Uncertain <u>non-random</u> event ⇒ Maximization of damage

Traditional definition of risk

- Objective measure of risk:

$$\text{Risk} = \text{Probability} \times \text{Consequence}$$

- Useful for unintentional outages

- Subjective aspects must also be considered (there is risk when perceived by society)

New risk definitions

- Risk measure under deliberate outages:

Probability

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$$

Probability

$$\text{Risk} = \text{Capability} \times \text{Intention} \times \text{Vulnerability} \times \text{Consequence}$$

New risk definitions

- Difficulties in risk analysis:
  - Estimation of probabilities and consequences of unlikely but catastrophic events
  - Need for advances in Statistics

Traditional security assessment

- System designed to survive a set of “credible” contingencies which are selected according to:
  - Past events
  - Apparent occurrence probability
  - Consequences

Traditional security assessment

- N-1 criterion ≡ System survives the loss of any single component
- Considered components:
  - Generators
  - Power lines
  - Transformers
  - Compensation devices

Traditional security assessment

- Drawbacks of N-1 criterion:
  - Implementation depends on the country (number of credible contingencies)
  - Multiple contingencies are not considered
  - Failures of communication and information systems are not considered
  - Malicious intentionality is not considered

Contents

- Introduction
- Atacker-defender bilevel programming models
- Numerical results

Vulnerability analysis under deliberate outages

- Identification of critical system components under intentional attacks

- Useful for:
  - Network planner
  - Terrorist (regrettably!!)

Objective of the network planner

- Identification of the extended contingency set the system is most vulnerable
- Implementation of adequate surveillance and protection actions

Objective of the terrorist

- Identification of an interdiction scheme to:

  - Maximize the damage subject to limited destructive resources, or

  - Minimize the destructive resources to reach a pre-specified level of damage

Objective of the terrorist

- Interdictable system components:
  - Generators
  - Substations
  - Buses
  - Lines
  - Transformers

System operator

- After an attack, the system operator reacts:
  - Implementation of corrective actions (generation redispatch, redirection of line power flows, load shedding)
  - Objective $\Rightarrow$ Minimization of system damage

Measure of damage or vulnerability

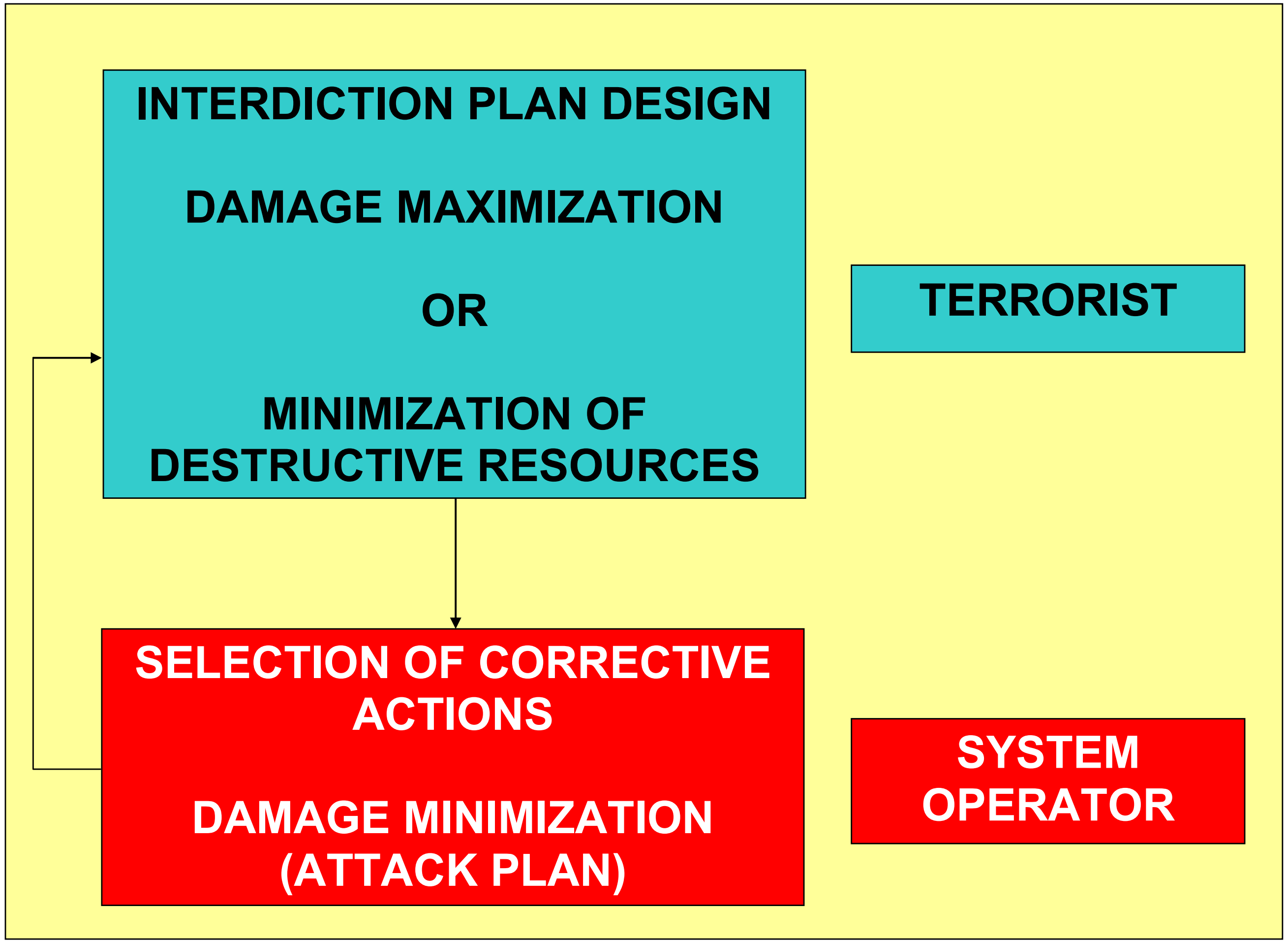
- System load shedding ⇒ Involuntary and non-remunerated disconnection of power demanded

- Other measures are possible ⇒ Load shedding in particular areas, economic cost of unserved energy, etc.

Attacker-defender bilevel model

- Two antagonistic agents operating sequentially
  - Terrorist $\Rightarrow$ Designs interdiction plan
  - System operator $\Rightarrow$ Reacts against the attack
- Each agent optimizes its own objective function over a jointly dependent set

Attacker-defender bilevel model



NETWORK PLANNER

IDENTIFICATION OF VULNERABLE COMPONENTS

Bilevel programming

- 2-player game of non-zero sum and perfect information
- Sequential, non cooperative, 1-round game
- Feasibility region implicitly characterized by 2 optimization problems which are solved in a pre-determined sequence

2 players

- Leader, upper-level agent or outer-level agent
  - Decision variables $x \in X$
  - Optimizes its objective function by selecting a strategy (variables x) that anticipates the reactions of the other player
  - The other player’s objective function is known

2 players

- Follower, lower-level agent or inner-level agent
  - Decision variables $y \in Y$
  - Reacts against the leader's strategy (variables x) by selecting its strategy (variables y) to optimize its objective function without considering the external consequencies of its actions

General bilevel formulation

$$\underset{x,y}{\text{Min}}\, F(x,y)$$

Subject to:

$$G(x,y) \le 0$$

$$y \in \arg\min_{y'} f(x,y')$$

Subject to:

$$g(x,y') \le 0$$

Mathematical characterization

- Optimization problem
- Even with linear constraints $\Rightarrow$ Non-convex problem $\Rightarrow$ Local optima
- Development of solution procedures $\Rightarrow$ Difficult task
- Existing methods of limited application

Solution approaches

- Under certain convexity and differentiability conditions $\Rightarrow$ Conversion to a standard mathematical program

  - KKT optimality conditions

  - Linear lower-level problem $\Rightarrow$ Dual problem + Strong duality theorem

  - Max-min problems $\Rightarrow$ Dual problem

Bilevel programming models for vulnerability analysis

- Two antagonistic agents acting sequentially:
  - Leader $\Rightarrow$ Terrorist
  - Follower $\Rightarrow$ System operator

Leader ≡ Terrorist

- Decision variables $x \in \{0,1\}$
  - $x = 0 \Leftrightarrow$ System component is destroyed/attacked
  - $x = 1 \Leftrightarrow$ System component is not destroyed/attacked

Follower ≡ System operator

- Decision variables ⇒ Network operation (simplified DC model):
  - Power flows
  - Nodal phase angles
  - Generation levels
  - Nodal load shedding

Bilevel programming models for vulnerability analysis

- Two models:
  - Minimum vulnerability model
  - Maximum vulnerability model

Minimum vulnerability model

$$\underset{\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub},b,v,\gamma,P^{Gen},P^{Line},S_c,\theta}{\text{Min}} \quad \text{Rec\_dest}\left(\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub}\right)$$

Subject to:

$$\text{Feasibility of }\left(\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub},b,v\right)$$

$$\gamma \geq \underline{\gamma}$$

Terrorist

$$\gamma = \min_{P^{Gen},P^{Line},S_c,\theta} \sum_{c} S_c$$

System operator

Subject to:

$$\text{Feasibility of }\left(P^{Gen},P^{Line},S_c,\theta\right)$$

Maximum vulnerability model

$$\max_{\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub},b,v} \gamma$$

Subject to:

$$\text{Feasibility of }\left(\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub},b,v\right)$$

$$\text{Rec\_dest}\left(\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub}\right)\leq M$$

$$\gamma = \min_{P^{Gen},P^{Line},S_c,\theta} \sum_c S_c$$

Subject to:

$$\text{Feasibility of }\left(P^{Gen},P^{Line},S_c,\theta\right)$$

Terrorist

System operator

Terrorist's constraints

$$\delta_g^{Gen} \in \{0,1\}, \quad \forall g \Rightarrow \text{Generator attack}$$

$$\delta_\ell^{Line} \in \{0,1\}, \quad \forall \ell \Rightarrow \text{Line attack}$$

$$\delta_i^{Bus} \in \{0,1\}, \quad \forall i \Rightarrow \text{Bus attack}$$

$$\delta_s^{Sub} \in \{0,1\}, \quad \forall s \Rightarrow \text{Substation attack}$$

$$v_\ell \in \{0,1\}, \qquad \forall \ell \Rightarrow \text{Line operation}$$

$$b_g \in \{0,1\}, \qquad \forall g \Rightarrow \text{Generator operation}$$

Terrorist's constraints

$$v_\ell = \left(1-\delta_\ell^{Line}\right)\left(1-\delta_{o(\ell)}^{Bus}\right)\left(1-\delta_{d(\ell)}^{Bus}\right)\prod_{s \mid \ell \in L_s^{Sub}}\left(1-\delta_s^{Sub}\right)$$

$$\prod_{\ell' \mid \ell' \in L_\ell^{Par}}\left(1-\delta_{\ell'}^{Line}\right), \qquad \forall \ell$$

$$b_g = \left(1-\delta_{i(g)}^{Bus}\right)\left(1-\delta_g^{Gen}\right), \qquad \forall g$$

Terrorist's constraints Destructive resources

$$\text{Rec\_dest}\left(\delta^{\text{Gen}}, \delta^{\text{Line}}, \delta^{\text{Bus}}, \delta^{\text{Sub}}\right) = \sum_{g} M_g^{\text{Gen}} \delta_g^{\text{Gen}} + \sum_{\ell} M_\ell^{\text{Line}} \delta_\ell^{\text{Line}} + \sum_{i} M_i^{\text{Bus}} \delta_i^{\text{Bus}} + \sum_{s} M_s^{\text{Sub}} \delta_s^{\text{Sub}}$$

System operator's constraints: OPF(v,b)

Line power flows

$$P_\ell^{Line} = \frac{v_\ell}{x_\ell}\left(\theta_{o(\ell)} - \theta_{d(\ell)}\right) : \mu_\ell, \qquad \forall \ell$$

Power balances

$$\sum_{g \in G_i} P_g^{Gen} + \sum_{c \in C_i} S_c - \sum_{\ell | o(\ell)=i} P_\ell^{Line} + \sum_{\ell | d(\ell)=i} P_\ell^{Line} = \sum_{c \in C_i} d_c : \lambda_i, \quad \forall i$$

$$-\overline{P}_\ell^{Line} \leq P_\ell^{Line} \leq \overline{P}_\ell^{Line} : \left(\phi_\ell, \varphi_\ell\right), \qquad \forall \ell$$

Line capacities

System operator's constraints: OPF(v,b)

$$-\overline{\theta} \le \theta_i \le \overline{\theta} : (\chi_i, \varepsilon_i), \qquad \forall i$$

Angle limits

$$0 \le P_g^{Gen} \le b_g \overline{P}_g^{Gen} : \gamma_g, \qquad \forall g$$

Generation limits

$$0 \le S_c \le d_c : \alpha_c, \qquad \forall c$$

Load shedding limits

Problem characterization

- Bilevel programming problem
- Non-linear (products of variables)
- Mixed-integer
- Large scale
- Solution based on duality theory

Follower's dual constraints

$$\lambda_{i(g)} + \gamma_g \le 0 \qquad \forall g$$

$$\lambda_{i(c)} + \alpha_c \le 1 \qquad \forall c$$

$$-\lambda_{o(\ell)} + \lambda_{d(\ell)} + \mu_\ell + \phi_\ell + \varphi_\ell = 0 \qquad \forall \ell$$

$$-\sum_{\ell | o(\ell)=i} \frac{v_\ell \mu_\ell}{x_\ell} + \sum_{\ell | d(\ell)=i} \frac{v_\ell \mu_\ell}{x_\ell} + \chi_i + \varepsilon_i = 0, \qquad \forall i$$

$$\chi_i \ge 0, \quad \forall i \qquad \varepsilon_i \le 0, \quad \forall i \qquad \gamma_g \le 0, \quad \forall g$$

$$\phi_\ell \ge 0, \quad \forall \ell \qquad \varphi_\ell \le 0, \quad \forall \ell \qquad \alpha_c \le 0, \quad \forall c$$

Strong duality theorem

$$\sum_{c} S_c = \sum_{\ell} (\varphi_\ell - \phi_\ell)\overline{P}_\ell^{Line} + \sum_{c} \left(\alpha_c + \lambda_{i(c)}\right) d_c$$

$$+ \sum_{g} \gamma_g b_g \overline{P}_g^{Gen} + \sum_{i} (\varepsilon_i - \chi_i)\overline{\theta}$$

Conversion to a single level: MINLP

- Optimize terrorist's objective function
- Subject to:
  - Terrorist's non-linear constraints
  - SO's non-linear primal constraints
  - SO's non-linear dual constraints
  - SO's non-linear strong duality equality

Linearization of product of 0/1 variables

$$z = \prod_{i=1}^{n} x_i , \; x_i \in \{0,1\}$$

- MILP model:

$$z \geq 0$$

$$z \leq x_i , \quad i = 1,\ldots,n$$

$$z \geq \sum_{i=1}^{n} x_i - n + 1$$

$$x_i \in \{0,1\}$$

Linearization of constraints Leader

$$v_\ell \leq \left(1 - \delta_\ell^{Line}\right), \qquad \forall \ell$$

$$v_\ell \leq \left(1 - \delta_{\ell'}^{Line}\right), \qquad \forall \ell, \forall \ell' \in L_\ell^{Par}$$

$$v_\ell \leq \left(1 - \delta_{o(\ell)}^{Bus}\right), \qquad \forall \ell$$

$$v_\ell \leq \left(1 - \delta_{d(\ell)}^{Bus}\right), \qquad \forall \ell$$

$$v_\ell \leq \left(1 - \delta_s^{Sub}\right), \qquad \forall s, \forall \ell \in L_s^{Sub}$$

Linearization of constraints Leader

$$v_{\ell} \geq \left(1-\delta_{\ell}^{\text{Line}}\right)+\left(1-\delta_{o(\ell)}^{\text{Bus}}\right)+\left(1-\delta_{d(\ell)}^{\text{Bus}}\right)+\sum_{s \mid \ell \in L_s^{\text{Sub}}}\left(1-\delta_s^{\text{Sub}}\right)$$

$$+\sum_{\ell' \in L_{\ell}^{\text{Par}}}\left(1-\delta_{\ell'}^{\text{Line}}\right)-3+\text{card}\left(L_{\ell}^{\text{Par}}\right)+\text{card}\left(\left\{s : \ell \in L_s^{\text{Sub}}\right\}\right)$$

$$+1, \qquad \forall \ell$$

$$v_{\ell} \geq 0, \qquad \forall \ell$$

Linearization of constraints Leader

$$b_g \leq \left(1 - \delta_{i(g)}^{Bus}\right), \qquad \forall g$$

$$b_g \leq \left(1 - \delta_{g}^{Gen}\right), \qquad \forall g$$

$$b_g \geq 0, \qquad \forall g$$

$$b_g \geq \left(1 - \delta_{i(g)}^{Bus}\right) + \left(1 - \delta_{g}^{Gen}\right) - 1, \qquad \forall g$$

Linearization of product of 0/1 variable and continuous variable

$$z = xp, \quad x \in \{0,1\}, \quad p \in \left[p^{min}, p^{max}\right]$$

- MILP model:

$$z = p - r$$

$$x \in \{0,1\}$$

$$xp^{min} \le z \le xp^{max}$$

$$(1 - x)p^{min} \le r \le (1 - x)p^{max}$$

Linearization of constraints
Follower

$$P_\ell^{\text{Line}} = \frac{1}{x_\ell}\left[\theta_{o(\ell)} - \tilde{\theta}_{o\ell} - \left(\theta_{d(\ell)} - \tilde{\theta}_{d\ell}\right)\right], \qquad \forall \ell$$

$$-v_\ell \overline{\theta} \le \theta_{o(\ell)} - \tilde{\theta}_{o\ell} \le v_\ell \overline{\theta}, \qquad \forall \ell$$

$$-v_\ell \overline{\theta} \le \theta_{d(\ell)} - \tilde{\theta}_{d\ell} \le v_\ell \overline{\theta}, \qquad \forall \ell$$

$$-(1 - v_\ell) v_\ell \overline{\theta} \le \tilde{\theta}_{o\ell} \le (1 - v_\ell)\overline{\theta}, \qquad \forall \ell$$

$$-(1 - v_\ell) v_\ell \overline{\theta} \le \tilde{\theta}_{d\ell} \le (1 - v_\ell)\overline{\theta}, \qquad \forall \ell$$

Linearization of constraints Follower

$$-\sum_{\ell|o(\ell)=i} \frac{(\mu_\ell - \tilde{\mu}_\ell)}{x_\ell} + \sum_{\ell|d(\ell)=i} \frac{(\mu_\ell - \tilde{\mu}_\ell)}{x_\ell} + \chi_i + \varepsilon_i = 0, \qquad \forall i$$

$$-v_\ell \overline{\mu}_\ell \le \mu_\ell - \tilde{\mu}_\ell \le v_\ell \overline{\mu}_\ell, \qquad \forall \ell$$

$$-v_\ell (1 - \overline{\mu}_\ell) \le \tilde{\mu}_\ell \le v_\ell (1 - \overline{\mu}_\ell), \qquad \forall \ell$$

Linearization of constraints Follower

$$\sum_{c} S_c = \sum_{\ell} (\varphi_\ell - \phi_\ell)\overline{P}_\ell^{Line} + \sum_{c} \left(\alpha_c + \lambda_{i(c)}\right) d_c$$

$$+ \sum_{g} \left(\gamma_g - \tilde{\gamma}_g\right) \overline{P}_g^{Gen} + \sum_{i} (\varepsilon_i - \chi_i)\overline{\theta}$$

$$-b_g \overline{\gamma}_g \le \gamma_g - \tilde{\gamma}_g \le 0, \qquad \forall g$$

$$-\left(1 - b_g\right)\overline{\gamma}_g \le \tilde{\gamma}_g \le 0, \qquad \forall g$$

Resulting MILP problem

- Optimize terrorist's objective function
- Subject to:
    - ❑ Terrorist's linear constraints
    - ❑ SO's linear primal constraints
    - ❑ SO's linear dual constraints
    - ❑ SO's linear strong duality equality

Contents

- Introduction
- Atacker-defender bilevel programming models
- Numerical results

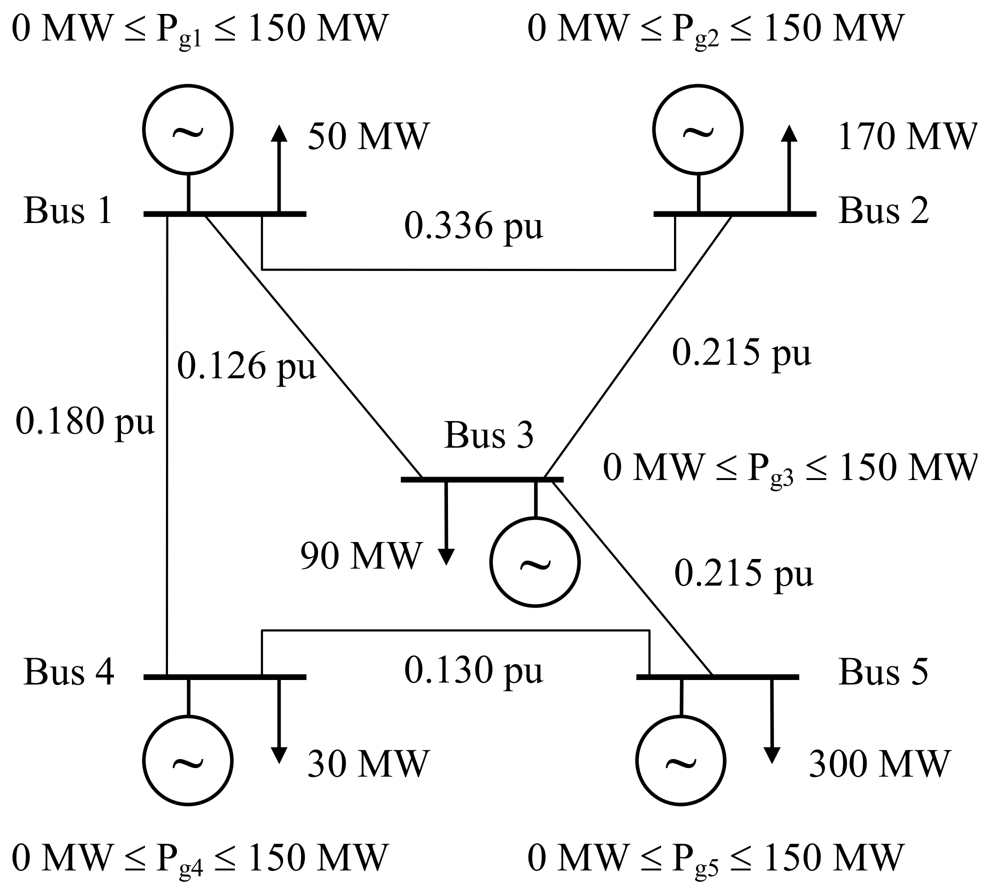
Minimum vulnerability model

- 5-bus example and One-Area IEEE RTS
- Scenario of peak demand
- Only destruction of lines
- Results parameterized as a function of the minimum level of system load shed $\underline{\gamma}$

Minimum vulnerability model

- GAMS and CPLEX 9.0
- Dell PowerEdge 6600, 2 processors, 1.6 GHz, 2 GB of RAM
- Computing time for optimality $\leq$ 10 seconds

5-bus example



5-bus example

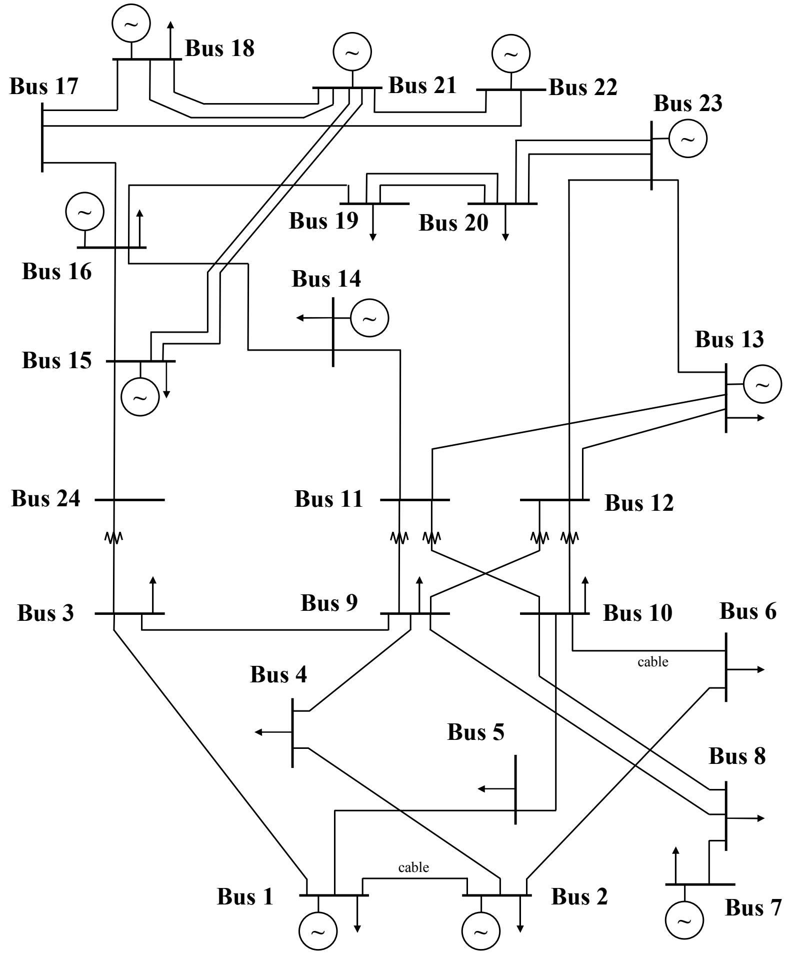
# destroyed lines	System load shed (MW)	Worst combination of destroyed lines
1	50	3-5 4-5
2	150	3-5, 4-5
3	150	1-2, 3-5, 4-5 1-3, 3-5, 4-5 1-4, 3-5, 4-5 2-3, 3-5, 4-5
4	170	1-2, 2-3, 3-5, 4-5
5	170	1-2, 1-3, 2-3, 3-5, 4-5 1-2, 1-4, 2-3, 3-5, 4-5
6	170	1-2, 1-3, 1-4, 2-3, 3-5, 4-5

5-bus example

Range of $\underline{\gamma}$ (MW)	Destroyed lines
$0 < \underline{\gamma} \leq 50$	3-5
$50 < \underline{\gamma} \leq 150$	3-5, 4-5
$150 < \underline{\gamma} \leq 170$	1-2, 2-3, 3-5, 4-5

IEEE RTS

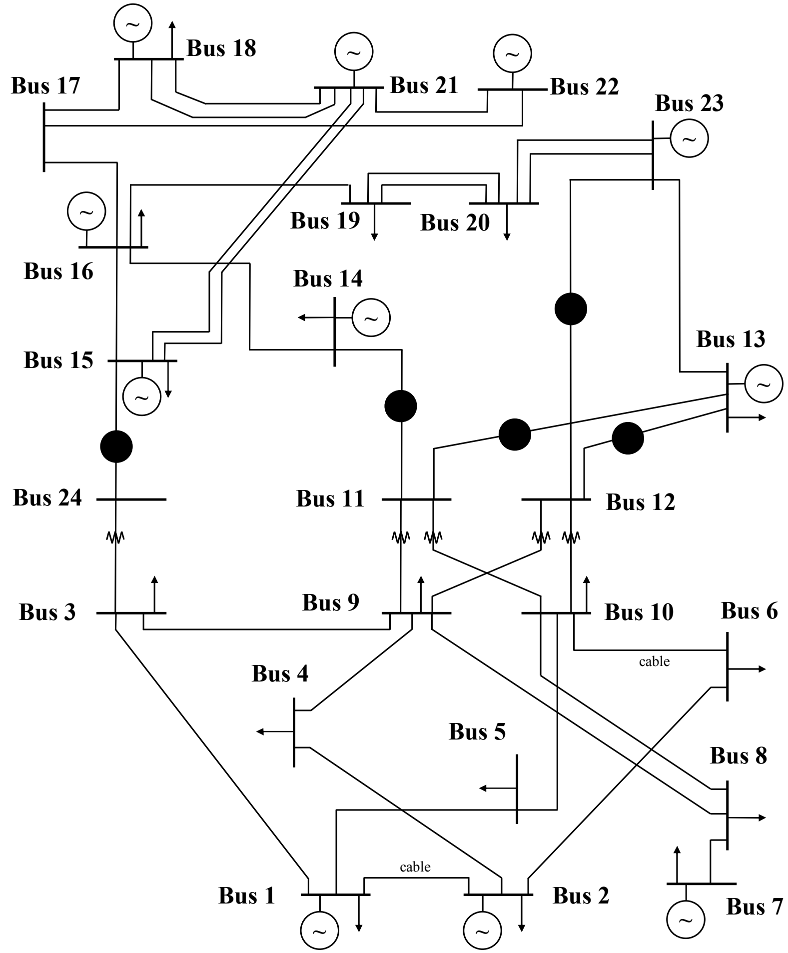
- 24 buses
- 38 lines
- 32 generators
- 17 loads
- Peak demand scenario (2850 MW)
- All lines destroyed ⇒ 1607 MW shed



IEEE RTS

$\underline{\gamma}$ (MW)	Destroyed lines	Load shed (MW)
200	16-19, 20-23A, 20-23B	309
400	3-24, 9-12, 11-13, 14-16	442
600	11-13, 11-14, 12-13, 12-23, 15-24	648
800	11-13, 12-13, 12-23, 14-16, 15-24	842
1000	7-8, 11-13, 12-13, 12-23, 14-16, 15-24	1017

IEEE RTS


Bus 18
Bus 17
Bus 21
Bus 22
Bus 23
Bus 19
Bus 20
Bus 16
Bus 14
Bus 15
Bus 13
Bus 24
Bus 11
Bus 12
Bus 3
Bus 9
Bus 10
Bus 6
cable
Bus 4
Bus 5
Bus 8
cable
Bus 1
Bus 2
Bus 7

IEEE RTS

Bus	P_g(MW)	P_d(MW)	S_c(MW)	Bus	P_g(MW)	P_d(MW)	S_c(MW)
1	192	108	0	13	265	265	0
2	192	97	0	14	0	194	0
3	0	180	180	15	215	317	0
4	0	74	0	16	54	100	0
5	0	71	71	17	0	0	0
6	0	136	136	18	100	333	0
7	300	125	0	19	0	181	0
8	0	171	86	20	0	128	0
9	0	175	175	21	224	0	0
10	0	195	0	22	0	0	0
11	0	0	0	23	600	0	0
12	0	0	0	24	0	0	0

Maximum vulnerability model

- One-Area IEEE RTS and Two-Area IEEE RTS
- Maximum demand scenario
- Results parameterized as a function of M

Maximum vulnerability model

- Destruction of a line or several parallel lines $\Rightarrow$ 1 person
- Destruction of a transformer $\Rightarrow$ 2 persons
- Destruction of a bus or substation $\Rightarrow$ 3 persons
- Destruction of a generator or an underground cable $\Rightarrow$ Impossible

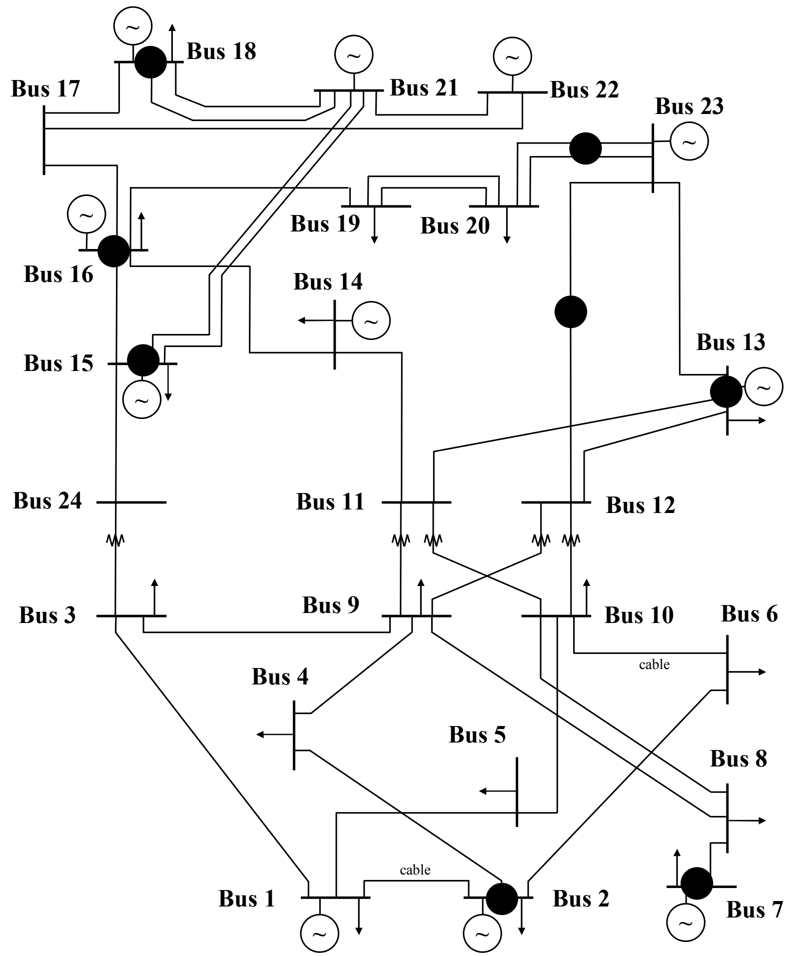
Maximum vulnerability model

- GAMS and CPLEX 8.1
- Pentium IV, 2.66 GHz, 512 MB of RAM
- Computing time for optimality $\leq$ 180 seconds

One-Area IEEE RTS

M	Load shed (MW)	CPU time (s)	M	Load shed (MW)	CPU time (s)
0	0	0.08	16	2378	2.34
2	309	1.56	18	2533	2.08
4	842	3.91	20	2658	1.23
6	1373	1.77	22	2753	1.02
8	1638	2.30	24	2850	0.31
10	1853	4.78	26	2850	0.30
12	2011	3.86	28	2850	0.36
14	2241	1.39			

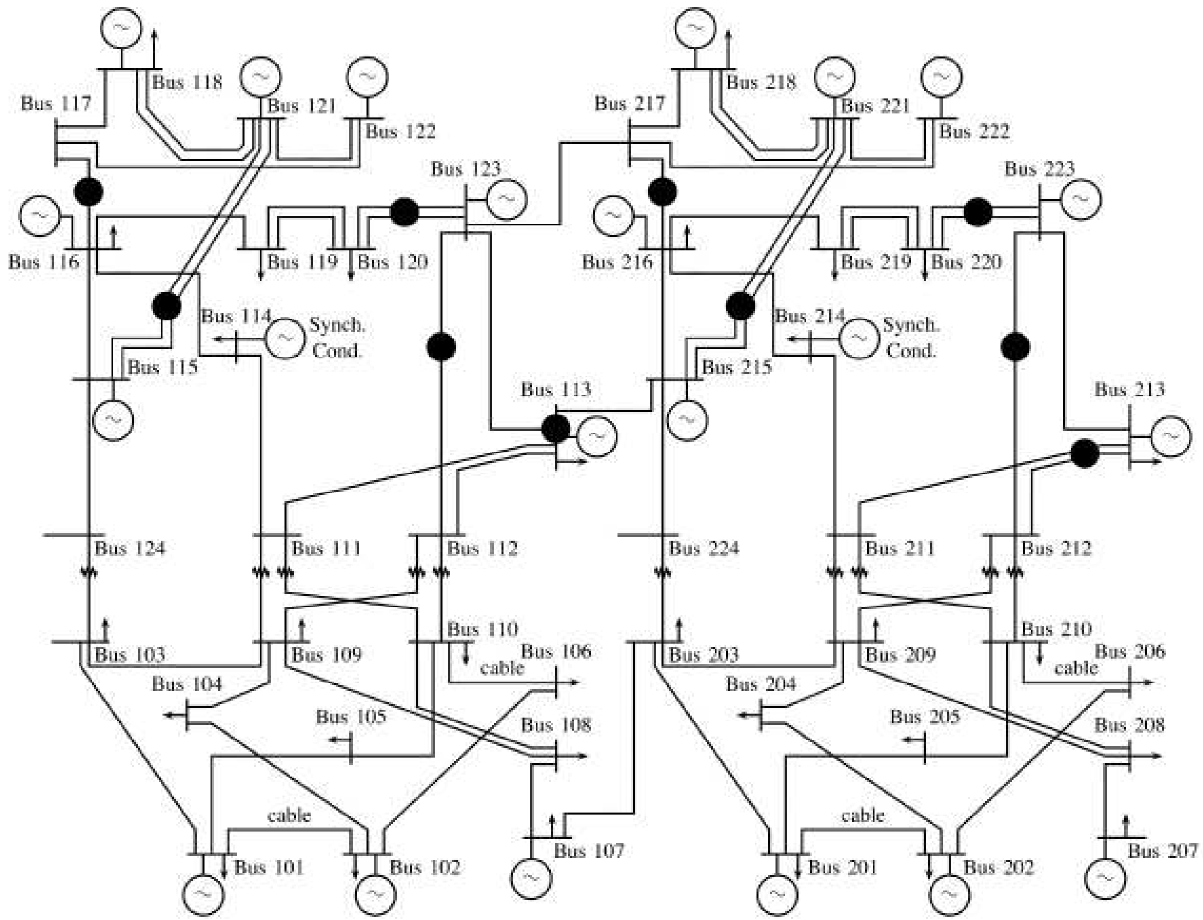
One-Area IEEE RTS. M = 20



Two-Area IEEE RTS

M	Load shed (MW)	CPU time (s)	M	Load shed (MW)	CPU time (s)
0	0	0.14	28	4497	54.28
4	842	26.56	32	4807	67.84
8	1684	132.78	36	5036	106.58
12	2661	102.46	40	5316	28.59
16	3169	147.05	44	5575	4.09
20	3649	170.69	46	5700	3.22
24	4067	170.08			

Two-Area IEEE RTS. M = 12



Future and ongoing work

- More precise power flow model (AC)
- Alternative corrective actions (disconnection of generators and/or lines)
- Analysis of power vs. energy shed
- Use of game theory

References

- A. V. Gheorghe, M. Masera, M. Weijnen, L. de Vries. “Critical Infrastructures at Risk. Securing the European Electric Power System”. Springer. Dordrecht, The Netherlands. 2006.

- IEEE/CIGRÉ Joint Task Force on Stability Terms and Definitions. “Definitions and classification of power system stability”. IEEE Trans. Power Syst. Vol. 19, no. 3, pp. 1387–1402, Aug. 2004.

References

- J. Salmerón, K. Wood, R. Baldick. "Analysis of Electric Grid Security under Terrorist Threat". IEEE Transactions on Power Systems, vol. 19, no. 2, pp. 905-912, May 2004.

- J. M. Arroyo, F. D. Galiana. "On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem". IEEE Transactions on Power Systems, vol. 20, no. 2, pp. 789-797, May 2005.

References

- A. L. Motto, J. M. Arroyo, F. D. Galiana. “A Mixed-Integer LP Procedure for the Analysis of Electric Grid Security under Disruptive Threat”. IEEE Transactions on Power Systems, vol. 20, no. 3, pp. 1357-1365, August 2005.

- M. Carrión, J. M. Arroyo, N. Alguacil. “Vulnerability-Constrained Transmission Expansion Planning: A Stochastic Programming Approach”. IEEE Transactions on Power Systems, vol. 22, no. 4, pp. 1436-1445, November 2007.

Thanks for your attention!

GSEE:
http://www.uclm.es/area/gsee