

# TRANSMISSION NETWORK EXPANSION PLANNING UNDER DELIBERATE OUTAGES

Natalia Alguacil, Miguel Carrión, José Manuel Arroyo  
Universidad de Castilla – La Mancha  
Ciudad Real, Spain

Natalia.Alguacil@uclm.es, Miguel.Carrion@uclm.es, JoseManuel.Arroyo@uclm.es

**Abstract** – The reasons why the transmission network is a potentially attractive target for deliberate outages are twofold: i) its crucial importance as a critical infrastructure for the society welfare, and ii) its high level of vulnerability due to the current operation close to the static and dynamic limits. This new context where destructive agents come into play has been recognized by several agencies in Europe and North America, and various initiatives have been launched worldwide in order to assess and mitigate the vulnerability of transmission.

Within this framework, this paper proposes the reinforcement and expansion of the transmission network as a way of mitigating the impact of increasingly plausible deliberate outages. The network planner selects the new lines to be built accounting not only for economic issues, as traditionally done, but also for the vulnerability of the transmission network against a set of credible intentional outages. The resulting vulnerability- and economic-constrained transmission expansion planning problem is formulated as a mixed-integer linear program.

A number of case studies numerically illustrate the tradeoff between economic- and vulnerability-related issues and its impact on the expansion plans. In addition, we compare the results with those achieved by a traditional expansion planning model based on cost minimization.

**Keywords:** *Deliberate outages, mixed-integer linear programming, transmission network expansion planning, vulnerability*

## 1 INTRODUCTION

Due to economic, environmental and political reasons, in many countries the transmission network has not been expanded according to the increase in electricity consumption. As a consequence, the transmission network is being operated close to its static and dynamic limits, thus increasing its vulnerability. This higher level of vulnerability and the crucial importance of transmission infrastructure make the transmission network a potentially attractive target for intentional attacks. This issue has raised the concern of governments, utilities and researchers, and several initiatives have been launched worldwide in order to assess and mitigate the vulnerability of transmission [1].

One way of mitigating the impact of increasingly plausible deliberate outages is the reinforcement and expansion of the transmission network. The traditional transmission expansion planning problem consists in determining the optimal timing, location and sizing of transmission facilities to be installed in an existing net-

work so that investment and operation costs are minimized over the planning horizon. Other decisions, such as the modification of the network topology or the interconnection of isolated systems, may also be considered part of this problem. The transmission expansion problem arises in both centralized and competitive frameworks. Hereinafter, we consider that a central entity, namely the network planner, is responsible for expansion decisions of the entire transmission network.

Different methodologies have been applied to solve the classical transmission expansion planning problem such as linear programming [2], mixed-integer linear programming [3], dynamic programming [4], decomposition techniques [5], heuristic approaches [6], and game theory [7]. A detailed bibliographical review of the transmission expansion problem can be found in [8].

In the new context where destructive agents come into play, transmission expansion planning should be driven not only by economic reasons but also by vulnerability issues. Carrión et al. [9] have recently presented a vulnerability-constrained transmission expansion planning approach in which the vulnerability aspects were emphasized.

This paper extends the work in [9] by analyzing the tradeoff between economic- and vulnerability-related issues and its impact on the expansion plans. Here, the network planner has two conflicting objectives: (i) the reduction of the vulnerability of the network against deliberate outages, and (ii) the minimization of the investment cost.

The proposed vulnerability- and economic-constrained expansion model is formulated as a mixed-integer nonlinear programming problem comprising products of binary variables and continuous variables. Such nonlinearities can be equivalently expressed as linear equalities and inequalities by using results from binary algebra [10]. Thus, the resulting mixed-integer linear programming problem can be efficiently solved using commercial branch-and-cut software.

The remainder of the paper is organized as follows. Section 2 describes the decision framework in which the proposed vulnerability- and economic-constrained transmission expansion planning problem is embedded. Section 3 presents the mathematical formulation of the problem. Section 4 provides numerical results to illustrate the performance of the proposed approach. Finally, in Section 5 relevant conclusions are drawn.

## 2 DECISION FRAMEWORK

A planning horizon of one year is considered, thus yielding a static transmission expansion planning model. As it is commonly assumed in static transmission expansion planning [8], during this target year generation sites are known and a single load scenario is modeled, typically corresponding to the highest load demand forecast for the considered time span.

During the one-year horizon the vulnerability- and economic-constrained transmission expansion problem involves two types of decisions: (i) expansion decisions made by the network planner, and (ii) operation decisions made by the system operator. At the beginning of the planning horizon the network planner decides how to expand the transmission network. In this paper expansion plans consist in building new lines from a candidate set. These expansion decisions are made under the uncertainty associated with intentional attacks. In addition, if a deliberate outage occurs, we assume that the system operator reacts so that the damage is minimized. Thus, operation decisions such as power generation and load shedding, and the resulting power flows depend on the attack plan.

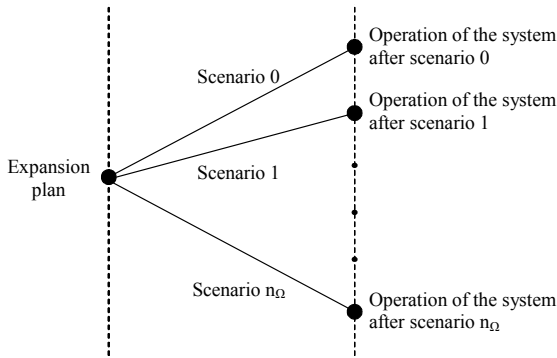


Figure 1: Decision framework.

Intentional attacks to the transmission network can be classified as nonrandom uncertain events [9]. They are uncertain because they are unknown a priori. Furthermore, they are nonrandom because they cannot be modeled using a known probability distribution based on past observations. The uncertainty of attack plans is characterized through a set of scenarios  $\Omega$ , where each scenario  $\omega$  represents a credible attack plan resulting in a particular level of damage. The level of damage is measured in terms of the total load shed. Although any network component is a potential target for destructive agents, for the sake of clarity and conciseness, this paper only considers intentional outages of transmission lines. The set of scenarios  $\Omega$  is made up of vectors  $v(\omega)$  of 0s and 1s as follows:

$$v(\omega) = \{v_1(\omega), \dots, v_{n_L}(\omega)\}; \quad \omega = 0, \dots, n_\Omega \quad (1)$$

where  $n_L$  is the number of lines in the original transmission network,  $n_\Omega$  is the number of attack plans consid-

ered as scenarios, and  $v_\ell(\omega)$  is a constant equal to 0 if line  $\ell$  is destroyed in scenario  $\omega$ , being 1 otherwise. A scenario  $\omega = 0$  with no attacks is included in  $\Omega$  when the estimated demand requires transmission expansion. The decision framework of the proposed transmission expansion planning problem is depicted in Fig. 1.

Attack plans are selected as scenarios depending on the level of damage caused. The scenario generation procedure is based on the solution of the so-called terrorist threat problem [11]. The terrorist threat problem is a static vulnerability analysis of the transmission network considering intentional outages. The objective of this problem is to determine the attack plan causing the largest disruption in the network given limited destructive resources. Fig. 2 shows the flowchart of the scenario generation procedure.

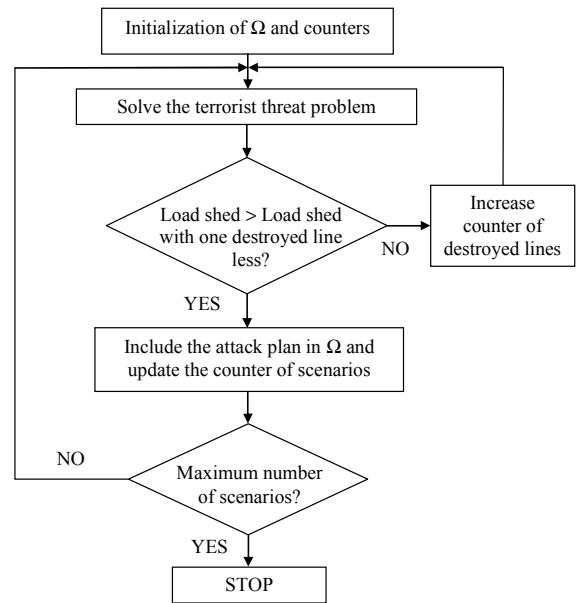


Figure 2: Scenario generation procedure.

Each attack plan selected as a scenario ( $\omega = 1, \dots, n_\Omega$ ) is associated with a weight or degree of importance in order to represent its perceived relative likelihood. These weights are based on the level of load shed and on the number of network components that are destroyed in the corresponding scenario, and are calculated as follows:

$$\pi(\omega) = \frac{\Delta P_T^D(\omega)}{I(\omega)}; \quad \omega = 1, \dots, n_\Omega \quad (2)$$

$$\sum_{\omega'=1}^{n_\Omega} \frac{\Delta P_T^D(\omega')}{I(\omega')}$$

where  $\pi(\omega)$  is the weight of scenario  $\omega$ ,  $\Delta P_T^D(\omega)$  is the system load shed in the original network associated with scenario  $\omega$ , and  $I(\omega)$  is the number of destroyed lines in scenario  $\omega$ . With (2) we model the tradeoff faced by the destructive agents between the level of damage achieved

and the effort required to reach that level of destruction. The destructive effort might be a function of the terrorist resources, i.e., number of agents, cost of explosives, etc., and here has been modeled by the number of destroyed lines.

A detailed description of the scenario generation procedure can be found in [9]. Notwithstanding, it should be emphasized that the scenario generation process is external to the proposed tool. Therefore, alternative ways of generating scenarios, such as those including subjective aspects through Bayesian networks [12], can be used.

Under this uncertainty characterization, the vulnerability of the transmission network against intentional attacks is defined in terms of the weighted load shed over the considered set of attack plans.

### 3 FORMULATION

The mathematical formulation of the vulnerability- and economic-constrained transmission expansion problem is stated below:

$$\text{Minimize } \sum_{\omega=1}^{n_{\Omega}} \pi(\omega) \left[ \sum_{n \in N} \Delta P_n^D(\omega) \right] + \beta \sum_{\ell \in L^C} C_{\ell}^L s_{\ell} \quad (3)$$

Subject to:

$$\sum_{\ell \in L^C} C_{\ell}^L s_{\ell} \leq C_T^L \quad (4)$$

$$\sum_{g \in G_n} P_g^G(\omega) - \sum_{\ell | O(\ell)=n} P_{\ell}^L(\omega) + \sum_{\ell | R(\ell)=n} P_{\ell}^L(\omega) = P_n^D - \Delta P_n^D(\omega); \quad \omega = 0, \dots, n_{\Omega}, \forall n \in N \quad (5)$$

$$P_{\ell}^L(\omega) = \frac{1}{x_{\ell}} [\delta_{O(\ell)}(\omega) - \delta_{R(\ell)}(\omega)] v_{\ell}(\omega); \quad \omega = 0, \dots, n_{\Omega}, \forall \ell \in L^O \quad (6)$$

$$P_{\ell}^L(\omega) = \frac{1}{x_{\ell}} [\delta_{O(\ell)}(\omega) - \delta_{R(\ell)}(\omega)] s_{\ell}; \quad \omega = 0, \dots, n_{\Omega}, \forall \ell \in L^C \quad (7)$$

$$-\bar{P}_{\ell}^L \leq P_{\ell}^L(\omega) \leq \bar{P}_{\ell}^L; \quad \omega = 0, \dots, n_{\Omega}, \forall \ell \in \{L^O \cup L^C\} \quad (8)$$

$$0 \leq P_g^G(\omega) \leq \bar{P}_g^G; \quad \omega = 0, \dots, n_{\Omega}, \forall g \in G \quad (9)$$

$$\underline{\delta} \leq \delta_n(\omega) \leq \bar{\delta}; \quad \omega = 0, \dots, n_{\Omega}, \forall n \in N \quad (10)$$

$$\Delta P_n^D(\omega) = 0; \quad \omega = 0, \forall n \in N \quad (11)$$

$$0 \leq \Delta P_n^D(\omega) \leq P_n^D; \quad \omega = 1, \dots, n_{\Omega}, \forall n \in N \quad (12)$$

$$s_{\ell} \in \{0, 1\}; \quad \forall \ell \in L^C \quad (13)$$

where  $N$  is the set of node indices;  $\Delta P_n^D(\omega)$  is the load shed in node  $n$  and scenario  $\omega$ ;  $\beta$  is a weighting factor for the investment cost;  $L^C$  is the set of indices of candidate lines;  $C_{\ell}^L$  is the investment cost of candidate line

$\ell$ ;  $s_{\ell}$  is a binary variable that is equal to 1 if candidate line  $\ell$  is built, being 0 otherwise;  $C_T^L$  is the expansion planning budget;  $G_n$  is the set of indices of generators connected to node  $n$ ;  $P_g^G(\omega)$  is the power output of generator  $g$  in scenario  $\omega$ ;  $P_{\ell}^L(\omega)$  is the power flow in line  $\ell$  and scenario  $\omega$ ;  $O(\ell)$  and  $R(\ell)$  are the sending and receiving nodes of line  $\ell$ , respectively;  $P_n^D$  is the demand in node  $n$ ;  $x_{\ell}$  is the reactance of line  $\ell$ ;  $\delta_n(\omega)$  is the phase angle in node  $n$  and scenario  $\omega$ ;  $L^O$  is the set of indices of lines in the original transmission network;  $\bar{P}_{\ell}^L$  is the power flow capacity of line  $\ell$ ;  $\bar{P}_g^G$  is the capacity of generator  $g$ ;  $G$  is the set of generator indices; and  $\underline{\delta}$  and  $\bar{\delta}$  are the lower and upper bounds for the nodal phase angles, respectively.

The objective function (3) comprises two terms. The first term represents the vulnerability of the transmission network against intentional attacks, which is calculated as the sum over all attack plans of the system load shed associated with each attack plan multiplied by its degree of importance. The investment cost is expressed by the second term. The weighting parameter  $\beta$  models the tradeoff between vulnerability- and economic-related goals and thus depends on the preferences of the network planner. The scope of this paper, which constitutes the main difference with respect to [9], is to help the network planner to determine appropriate values for  $\beta$ . The multiobjective function (3) differs from that in classical transmission expansion approaches where the goal is to minimize the investment and operation costs. In contrast, the proposed objective function incorporates the fundamental concern of the network planner within the context of this paper, i.e., the reduction in the vulnerability level against deliberate outages. Investment costs have also been accounted for in (4), in which an upper economic bound is set on expansion plans.

Constraints (5) enforce the power balance at every node and in every scenario. Using a dc load flow model, constraints (6) represent the power flows in the original network for each scenario as a function of the nodal phase angles. Note that for the lines destroyed in scenario  $\omega$ , i.e.,  $v_{\ell}(\omega) = 0$ , the corresponding power flows are 0. Analogously, constraints (7) express the line flows in the candidate lines for each scenario in terms of the nodal phase angles and the expansion variables  $s_{\ell}$ . Note that if the candidate line  $\ell \in L^C$  is not built, i.e.,  $s_{\ell} = 0$ , constraints (7) set the associated line flow to 0.

Constraints (8) provide the bounds for the line flows of the original and prospective lines for each scenario. Constraints (9)-(10) set the limits of generation and nodal phase angles, respectively, in each scenario. Likewise, constraints (11)-(12) bound the nodal load shed in each scenario. Note that the system load shed for scenario  $\omega = 0$  is set to 0 by constraints (11), i.e., the

network is expanded to at least meet the forecasted demand. Finally, the integrality of variables  $s_\ell$  is expressed in (13).

Problem (3)-(13) is a mixed-integer nonlinear programming problem. Nonlinear expressions (7) involving the product of binary variables  $s_\ell$  and continuous variables  $\delta_n(\omega)$  are subsequently transformed into linear expressions using some well-known integer algebra results [10]. Thus, the resulting vulnerability- and economic-constrained transmission expansion problem becomes a mixed-integer linear programming problem that can be efficiently solved by commercial branch-and-cut software.

#### 4 NUMERICAL RESULTS

The proposed model has been applied to Garver's 6-node test system [2] and to a case study based on the IEEE 24-node Reliability Test System (RTS) [13]. In order to analyze the tradeoff faced by the network planner, different values of the weighting parameter  $\beta$  and a range of expansion budgets have been tested. In all of the simulations  $\underline{\delta}$  and  $\bar{\delta}$  have been set to  $-\pi/2$  rad and  $\pi/2$  rad, respectively. The model has been implemented on a Sun Fire X4600 M2 with 4 processors at 2.60 GHz and 32 GB of RAM memory using CPLEX 10.2 under GAMS [14].

##### 4.1 Garver's system

Garver's example is a network with 6 nodes and 6 installed lines. The topology of this system, the nodal demands and the upper generation bounds are shown in Fig. 3. The data of every corridor are listed in Table 1 (obtained from [3]). The maximum number of lines (prospective plus installed) per corridor is 3, i.e., the number of candidate lines is 39. The maximum load shed in this network is obtained after destroying at least 5 lines and is equal to 640 MW, representing 84.2% of the total demand (760 MW).

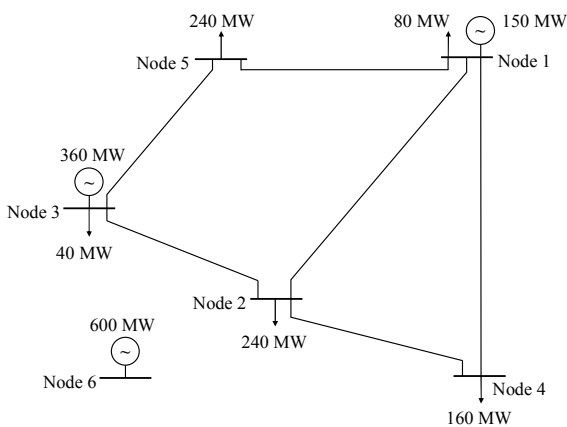


Figure 3: Garver's system.

After applying the procedure presented in Section 2, 4 attack plans have been considered as scenarios (Table 2). In the worst scenario all existing lines are destroyed

except for line 2-4. The load shed associated with this scenario is 640 MW, which is the maximum load shed attainable by the destructive agents. The scenario set  $\Omega$  also includes a scenario 0 with no attacks because the original system with isolated Node 6 is unable to supply the demand in the remaining nodes.

If the network is expanded following the traditional investment cost minimization approach without considering deliberate outages and without allowing load shedding, the resulting expansion plan consists in building 3 lines in corridor 4-6 and reinforcing corridor 3-5 with 1 new line. The total investment cost of this economic-driven solution is \$110; however, the level of vulnerability under the set of considered attack plans is equal to 115.1 MW. Finally, in order to require no load shed under any scenario the network planner should build 8 new lines: 1 line in corridors 1-5 and 2-6, and 2 lines in corridors 2-3, 3-5 and 4-6. The total cost incurred by this expansion plan is \$190.

Corridor	$x_\ell$ (pu)	$C_\ell^L$ (\$)	$\bar{P}_\ell^L$ (MW)
1-2	0.40	40	100
1-3	0.38	38	100
1-4	0.60	60	80
1-5	0.20	20	100
1-6	0.68	68	70
2-3	0.20	20	100
2-4	0.40	40	100
2-5	0.31	31	100
2-6	0.30	30	100
3-4	0.59	59	82
3-5	0.20	20	100
3-6	0.48	48	100
4-5	0.63	63	75
4-6	0.30	30	100
5-6	0.61	61	78

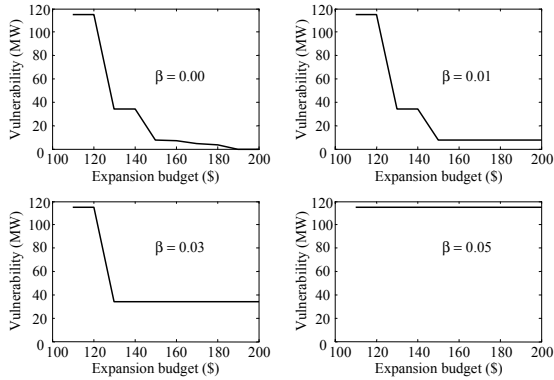
Table 1: Garver's system: Corridor data.

$\omega$	Destroyed Lines	$\Delta P_T^D(\omega)$ (MW)	$\pi(\omega)$
1	2-3	470	0.3474
2	3-5	470	0.3474
3	2-3, 3-5	570	0.2106
4	1-2, 1-4, 1-5, 2-3, 3-5	640	0.0946

Table 2: Garver's system: Attack plans.

Fig. 4 represents the variation of the vulnerability with the expansion budget for different values of  $\beta$ . Note that for each  $\beta$  the reduction of vulnerability stops at a certain value regardless of the expansion budget. This limit on the vulnerability reduction increases with the value of  $\beta$ , reaching a maximum for  $\beta = 0.05$  with which the expansion plan is identical to that achieved by the traditional approach and the vulnerability is 115.1 MW for all budgets. In other words, high values of  $\beta$  charac-

terize a transmission planner mainly concerned by economic issues and therefore, the investment costs are low at the expense of high levels of vulnerability. In contrast, low values of  $\beta$  imply lower levels of vulnerability with higher investment costs.



**Figure 4:** Garver's system: Vulnerability versus expansion budget.

$\beta$	Investment Cost (\$)	Vulnerability (MW)	Expansion Plan
0.00	170	4.6	2-3 (2), 2-6, 3-5 (2), 4-6 (2)
0.01	150	7.6	2-3, 3-5 (2), 4-6 (3)
0.03	130	34.2	2-6(3), 3-5 (2)
0.05	110	115.1	3-5, 4-6 (3)

**Table 3:** Garver's system: Results for a \$170 expansion budget.

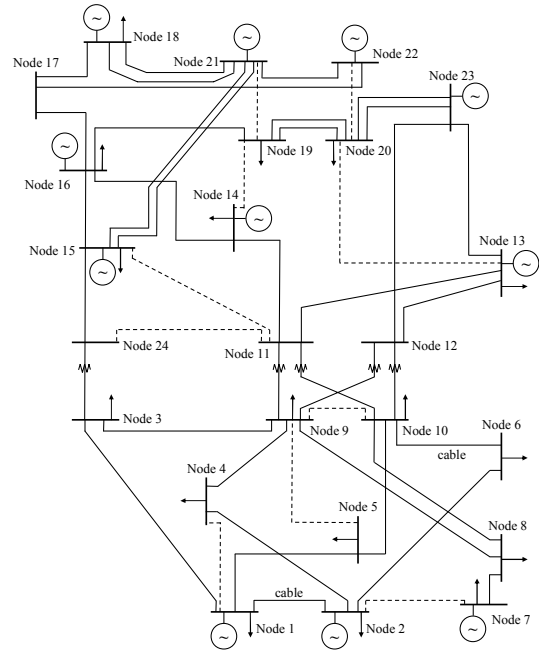
Finally, Table 3 lists the investment cost, the level of vulnerability, and the corresponding expansion plan for an expansion budget of \$170 and different values of  $\beta$  ranging between 0.00 and 0.05. The figures in brackets in the last column represent the number of parallel lines built in the corresponding corridor. As stated above, high values of  $\beta$  yield low investment costs, whereas low values of  $\beta$  imply lower levels of vulnerability with higher investment costs. As an example, with  $\beta = 0.00$  the level of vulnerability experiences a 96.0% reduction with respect to the original network ( $\beta = 0.05$ ) by building 1 line in corridor 2-6, and 2 lines in corridors 2-3, 3-5 and 4-6. The total investment cost incurred by this expansion plan is \$170.

The average computing time required to attain the optimal solutions to all simulations was 0.71 seconds.

#### 4.2 IEEE RTS-Based System

This system comprises 24 nodes, 34 corridors with 38 lines, 32 generators, and 17 loads. The load profile analyzed corresponds to a winter weekday at 18:00. It is assumed that circuits sharing the same tower are simultaneously destroyed when the tower is attacked. Therefore, for the sake of simplicity, parallel lines in the original network have been transformed into equivalent single lines. A set of 10 new corridors has been considered with 3 prospective lines per corridor. Candidate

corridors are represented in Fig. 5 by dashed lines and their parameters are listed in Table 4.



**Figure 5:** IEEE Reliability Test System.

Corridor	$x_\ell$ (pu)	$C_\ell^L$ ( $10^6$ \$)	$\bar{P}_\ell^L$ (MW)
1-4	0.015	7.72	175
2-7	0.021	10.82	175
5-9	0.018	9.27	175
9-10	0.016	8.24	175
11-15	0.022	11.13	500
11-24	0.011	5.66	500
13-20	0.011	5.66	500
14-19	0.017	8.76	500
19-21	0.014	7.21	500
20-22	0.014	7.21	500

**Table 4:** IEEE RTS: Parameters of the candidate corridors.

The methodology proposed in [11] has been used to determine the vulnerability of the test system with respect to the number of destroyed lines. As a result, at least two lines have to be destroyed in order to cause load shedding. Therefore, the attack plans considered as scenarios consist of a minimum of two outages. Moreover, the maximum load shed in this network is obtained after destroying at least 13 lines and is equal to 1607 MW, representing 56% of the total demand (2850 MW).

In this case the scenario set  $\Omega$  comprises 100 attack plans and does not include scenario 0. The worst scenario in  $\Omega$  includes 6 lines simultaneously down (11-13, 12-13, 12-23, 15-21, 16-17 and 20-23). The load shed associated with this scenario is 1198 MW, representing 74.5% of the maximum load shed attainable by the destructive agents.

Unlike Garver's 6-node example, the IEEE Reliability Test System is able to supply the estimated load

profile with its existing lines. Thus, the optimal solution to the traditional economic-driven expansion problem requires no investment. However, under the set of attack plans considered, the level of vulnerability of the original test system is equal to 626.39 MW.

The minimum level of vulnerability is 26.08 MW and is achieved by investing \$107.75 million through the construction of 13 candidate lines: 1 line in corridors 1-4, 2-7, 5-9, 11-24, 13-20 and 20-22; 2 lines in corridors 11-15 and 14-19; and 3 lines in corridor 19-21. It should be noted that the construction of all candidate lines yields the same level of vulnerability but with an investment cost of \$245.04 million.

Fig. 6 represents the variation of the vulnerability with the expansion budget for different values of  $\beta$ . Note that investing over \$50 million does not significantly reduce the level of vulnerability for most values of  $\beta$ .

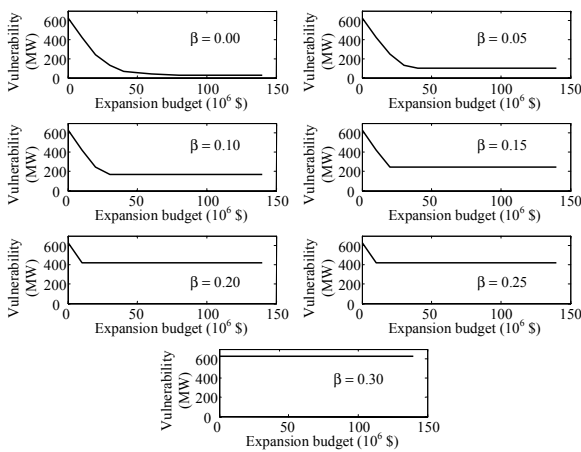


Figure 6: IEEE RTS: Vulnerability versus expansion budget.

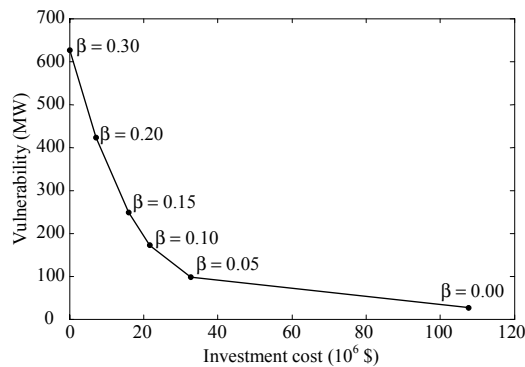


Figure 7: IEEE RTS: Efficient frontier for a \$110-million budget.

Fig. 7 shows the efficient frontier for a \$110-million budget, i.e., the level of vulnerability versus the investment cost for different values of  $\beta$ . This plot is interesting for the network planner since it provides relevant information on the tradeoff between investment cost minimization and actual mitigation of the vulnerability. For a network planner interested exclusively in vulnerability mitigation ( $\beta = 0.00$ ), the level of vulnerability is 26.08 MW with an investment cost of \$107.75 million.

On the other hand, for a network planner concerned solely on investment cost minimization ( $\beta = 0.30$ ) the level of vulnerability is 626.39 MW with an investment cost of \$0.

$C_T^L$ ( $10^6$ \$)	Investment Cost ( $10^6$ \$)	Vulnerability (MW)	Expansion Plan
0	0.00	626.39	-
10	7.21	422.29	19-21
20	18.53	241.16	11-24, 13-20, 19-21
30	27.29	130.00	11-24, 13-20, 14-19, 19-21
40	39.97	67.21	11-15, 13-20, 14-19, 19-21 (2)
50	47.18	54.13	11-15, 13-20, 14-19, 19-21 (2), 20-22
60	58.50	39.31	11-15, 11-24, 13-20 (2), 14-19, 19-21 (2), 20-22
70	63.66	33.94	2-7, 11-15, 11-24, 13-20, 14-19, 19-21 (2), 20-22
80	79.63	29.81	2-7, 11-15, 11-24, 13-20, 14-19 (2), 19-21 (3), 20-22
90	89.72	27.96	1-4, 2-7, 11-15 (2), 11-24, 13-20, 14-19, 19-21 (3), 20-22
100	98.48	26.30	1-4, 2-7, 11-15 (2), 11-24, 13-20, 14-19 (2), 19-21 (3), 20-22
110	107.75	26.08	1-4, 2-7, 5-9, 11-15 (2), 11-24, 13-20, 14-19 (2), 19-21 (3), 20-22
120	118.57	26.08	1-4, 2-7 (2), 5-9, 11-15 (2), 11-24, 13-20, 14-19 (2), 19-21 (3), 20-22

Table 5: IEEE RTS: Results for  $\beta = 0.00$ .

Finally, Table 5 lists the investment cost, the level of vulnerability, and the corresponding expansion plan for  $\beta = 0.00$  and expansion budgets up to \$120 million. With a \$20-million budget the level of vulnerability experiences a 61.5% reduction with respect to the original network by building lines 11-24, 13-20 and 19-21. The total investment cost incurred by this expansion plan is \$18.53 million. If the budget is increased up to \$110 million the vulnerability drops down to the aforementioned minimum level of 26.08 MW, i.e., a 95.8% reduction with respect to the level of vulnerability of the original network. Expansion budgets greater than \$110 million allow the network planner to build more lines

but the level of vulnerability of the system is not further reduced.

As can be seen in Table 5, expansion plans mainly correspond to lines belonging to the upper part of the network. This can be explained by the fact that the test system is divided into two areas: the upper area with excess of generation (nodes 11 through 24) and the lower area with deficit of generation (nodes 1 through 10). As a result of the vulnerability analysis performed on this system, most attack plans involve lines in the upper area, and therefore the expansion plans determined by the proposed approach are mainly located in this area.

The average computing time required to achieve the optimal solutions to all simulations was 9.1 minutes. However, it should be emphasized that computational issues are not a primary concern in this kind of planning problems.

## 5 CONCLUSION

This paper has presented a methodology to expand and reinforce the transmission network accounting for both economic issues and the impact of increasingly plausible deliberate outages. In order to model the uncertainty associated with intentional outages, a set of scenarios has been generated based on a recently reported method for vulnerability analysis. The proposed model has been formulated as a mixed-integer nonlinear mathematical problem. Nonlinearities have been subsequently expressed as linear equivalents using some well-known integer algebra results. The resulting mixed-integer linear formulation has been successfully tested through the use of commercially available software. As illustrated by the numerical results, the proposed approach provides the network planner with relevant information on expansion plans while taking into account the tradeoff between vulnerability mitigation and investment cost reduction. Research is currently underway to account for other sources of uncertainty such as demand fluctuation, reliability of network components, and those associated with competition in power markets. Another interesting avenue of research is to include risk constraints in the problem formulation to limit the load shed in the worst scenarios.

## ACKNOWLEDGEMENT

The authors acknowledge the support from the Ministry of Education and Science of Spain under CICYT Projects DPI2006-01501 and DPI2006-08001, and from the Junta de Comunidades de Castilla – La Mancha under Project PBI-05-053.

## REFERENCES

[1] A. V. Gheorghe, M. Masera, M. Weijnen and L. de Vries, "Critical Infrastructures at Risk. Securing the European Electric Power System", Dordrecht, Springer, 2006, ISBN 1-4020-4306-6

- [2] R. Villasana, L. L. Garver and S. J. Salon, "Transmission Network Planning Using Linear Programming", IEEE Transactions on Power Apparatus and Systems, vol. PAS-104, no. 2, pp 349-356, February 1985
- [3] N. Alguacil, A. L. Motto and A. J. Conejo, "Transmission Expansion Planning: A Mixed-Integer LP Approach", IEEE Transactions on Power Systems, vol. 18, no. 3, pp 1070-1077, August 2003
- [4] Y. P. Dusonchet and A. H. El-Abiad, "Transmission Planning Using Discrete Dynamic Optimization", IEEE Transactions on Power Apparatus and Systems, vol. PAS-92, no. 4, pp 1358-1371, July 1973
- [5] R. Romero and A. Monticelli, "A Hierarchical Decomposition Approach for Transmission Network Expansion Planning", IEEE Transactions on Power Systems, vol. 9, no. 1, pp 373-380, February 1994
- [6] G. C. Oliveira, A. P. C. Costa and S. Binato, "Large Scale Transmission Network Planning Using Optimization and Heuristic Techniques", IEEE Transactions on Power Systems, vol. 10, no. 4, pp 1828-1834, November 1995
- [7] J. Contreras and F. F. Wu, "A Kernel-Oriented Algorithm for Transmission Expansion Planning", IEEE Transactions on Power Systems, vol. 15, no. 4, pp 1434-1440, November 2000
- [8] G. Latorre, R. D. Cruz, J. M. Areiza and A. Villegas, "Classification of Publications and Models on Transmission Expansion Planning", IEEE Transactions on Power Systems, vol. 18, no. 2, pp 938-946, May 2003
- [9] M. Carrión, J. M. Arroyo and 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
- [10] C. A. Floudas, "Nonlinear and Mixed-Integer Optimization: Fundamentals and Applications", New York, Oxford University Press, 1995, ISBN 0-19-510056-3, pp 245-247
- [11] A. L. Motto, J. M. Arroyo and 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
- [12] C. Tranchita, N. Hadjsaid and A. Torres, "Ranking Contingency Resulting from Terrorism by Utilization of Bayesian Networks", 13th IEEE MELECON Proceedings, pp 964-967, May 2006
- [13] Reliability Test System Task Force, "The IEEE Reliability Test System-1996", IEEE Transactions on Power Systems, vol. 14, no. 3, pp 1010-1020, August 1999
- [14] A. Brooke, D. Kendrick, A. Meeraus and R. Raman, "GAMS/CPLEX 10.2 The Solver Manual", Washington, GAMS Development Corporation, 2007