Optimal protection of complex networks exposed to a terrorist hazard: a multi-objective evolutionary approach

D E Salazar A1, C M Rocco S2*, and E Zio3
1Universidad de Las Palmas de Gran Canaria, Spain
2Universidad Central de Venezuela, Caracas, Venezuela
3Politecnico di Milano, Milano, Italy

The manuscript was received on 12 October 2007 and was accepted after revision for publication on 2 May 2008.

DOI: 10.1243/1748006XJRR133

Abstract: The present paper proposes an approach for prioritizing the protection of a network system exposed to a terrorist attack. The approach is based on a multi-objective optimization (MO) formulation for finding Pareto optimal solutions with respect to two indicators measuring the damage that the attack may cause: the time to reach all network destination nodes (TTRAD) and the average number of persons affected (ANPA). The MO is tackled by means of a multi-objective evolutionary algorithm (MOEA) that combines the basic concepts of dominance with the general characteristics of evolutionary algorithms. Within this optimization scheme, the goodness of each alternative protection scheme is quantified by a combination of cellular automata (CA) and Monte Carlo (MC) simulation. Numerical examples illustrate how the approach is capable of identifying effective protection schemes.

Keywords: critical infrastructures, network systems, security, cellular automata, Monte Carlo simulation, multi-objective optimization, multi-objective evolutionary algorithm

1 INTRODUCTION

Critical infrastructures, such as water supply networks [1, 2] or electricity networks [3–5], are 'understood as vital for economic performance and social welfare' (reference [6], p. 859). Hence, the protection of critical infrastructures is a top priority for current societies. Correspondingly, many efforts have been devoted in recent years towards a new understanding of ways to analyse the safety and security of critical infrastructures and of how to protect them against random failures, natural disasters, and/or intentional attacks [7–12].

The present paper focuses on malevolent attacks to complex network infrastructures. On the one hand, such attacks may be directed to damaging the infrastructure itself by impacting its components. On the other hand, an antagonist could use the infrastructure for propagating a hazard to the population and the environment (e.g. a contaminant, a poison, or a virus injected for transmission into a water supply network). Propagation modelling is therefore a quite relevant task for providing the necessary information to devise effective countermeasures to the attacks.

Within this realm, the present paper presents the development of a methodology for the protection of complex networks. The decision-making problem of optimally allocating protection against propagating attacks is tackled within a multiple-objective framework which makes use of a multiple-objective evolutionary algorithm (MOEA) search combined with a cellular automata (CA) and Monte Carlo (MC) simulation propagation modelling technique.

The remainder of the article is organized as follows. The next section introduces the decision-making problem; section 3 presents the basic concepts of the techniques employed; section 4 presents an example of application of the methodology; finally, conclusions are given in section 5.
2 THE DECISION-MAKING PROBLEM

One of the challenges that security officers and policy makers face regarding terrorist attacks is the fact of having to deal with ‘a malevolent intelligence directed toward maximum social disruption’ [13]. In any security consideration one must then consider that the attacker would choose the target that maximizes the amount of harm delivered. Correspondingly, the assessment of the vulnerabilities of a network system should adopt first the ‘How can I make something go wrong?’ perspective in order to identify all the possible scenarios [14–16]. Then, the second step would be to ask ‘How can I maximize the havoc?’

As mentioned in section 1, the paper is concerned with intentional attacks to network infrastructures aimed at propagating a hazard to the population and the environment. In view of the interest of optimally allocating protection, the basic elements to consider are:

(a) modes of attack;
(b) modes of protection;
(c) impact indicators;
(d) defensive policy.

The last depends on various factors, such as political, societal, economic, and environmental ones, and at the same time is confronted by the uncertain nature of the intentional attacks. Hence, the defensive actions must be evaluated also with respect to their robustness to different adverse scenarios.

2.1 System modelling

Interconnected infrastructure systems can be modelled as generic networks \( G(N;E) \) composed of a set \( N = \{ n_i \} \) of \( n \) nodes linked by a set of edges \( E = \{ e_{ij} \} \), each of which connects two generic nodes \( n_i \) with \( n_j \) in a directed or undirected manner [17]. This general abstraction can be applied to model the topology of numerous types of interconnected systems in nature and engineering.

From the viewpoint of the process of hazard propagation following an attack, several features may be considered in the model, like the edges’ transmission capacity, the intensity of the hazard propagated, or the existence of different modes of attack, among others. Other realistic aspects to be considered are, for example, constraints on the capacity of links and nodes (e.g. which arise in electric [7] or water distribution systems [2]).

In the present methodological work, the modelling is limited to the basic aspects relating to the number of entities at each node which can be potentially damaged by the hazard propagation, the number of nodes attacked by the antagonist, and the time of propagation of the attack’s hazardous effects through the links. This allows concentrating the work on the general aspects of modelling the propagation dynamics through its topology and of optimizing the protective measures, while avoiding the detailed modelling of the physical characteristics of the network system.

Under this viewpoint, as soon as an attack takes place, its harmful effects begin to propagate through the network, from node to node, with consequent impact on the entities associated with such nodes. When the generic node \( n_i \) is hit by the hazard, it propagates the attack to an adjacent node \( n_j \) through link \( e_{ij} \), with a time delay \( TD_{ij} \). As we shall see in this work, time delays are assumed, for simplicity but without loss of generality, to be integer random variables of known distributions; the time evolution of hazard propagation can then be evaluated by a combination of CA and MC simulation [18, 19].

2.2 Consequence assessment

In this work, two indices of attack impact are considered [18, 19].

1. Average number of persons affected (ANPA) or average number of affected entities (ANAE): this is the average number of people or entities which are affected by the propagation. It is proportional to the area below the cumulated curve of people affected by the propagation of the attack as a function of time. For this index, larger values indicate larger impacts.

2. Time to reach all network destination nodes (TTRAD): this is the time that it takes for the hazard to propagate to all nodes of the network. Shorter times indicate larger impacts. This measure is similar to the ‘all-terminal network reliability’ [20], often used in network reliability analysis.

2.3 Allocating protections under uncertainty: robust protections

From a defender’s point of view, the possible strategies against such hazard propagation attacks are to prevent the antagonist from performing the attack or to implement a set of countermeasures to neutralize or mitigate the impact of the attack once it is performed. The decision-making problem considered in the present work corresponds to this latter situation: given an attack, the defender aims at minimizing the impact on the network, subject to his or her amount of available resources \( R_D \).

On the other hand, the antagonist is assumed to be rational so that his or her selection of targets is aimed at maximizing the impact subject to the amount of available resources \( R_A \). Hence, the defender’s problem can be formulated as the identification of
protections to be allocated on the network for minimizing the impact of an attack, subject to the amount of available resources $R_D$.

Naturally, the pattern of attack remains uncertain, even when some information about the preferences of the attacker and his/her resources $R_A$ can be estimated through intelligence gathering.

The key issue for the optimization of the protective measures is the definition of the impact of an attack to the network, which is the quantity to be minimized. For instance, in references [9] to [12] the authors aim at minimizing a utility function that amounts to the expected damage. In this work, ANPA and TTRAD are considered within a multiple-objective optimization problem.

A multiple-objective optimization (MO) problem consists in optimizing a vector $F(x)$ of objective functions $f_i(x)$, $i = 1, 2, \ldots, k$, possibly under specified equality $h(x)$ and inequality $g(x)$ constraints:

$$\text{Opt} \left[ F(x) = (f_1(x), f_2(x), \ldots, f_k(x))^T \right]$$

s.t.: $g_j(x) \leq 0, \quad j = 1, 2, \ldots, q$

$$h_j(x) = 0, \quad j = 1, 2, \ldots, r \quad (q + r = m)$$

where $x = (x_1, x_2, \ldots, x_n)^T \in X$ is the vector of decision variables, and $X$ is the feasible domain.

Assuming for simplicity that the above constraints are such to allow protecting only one single attack point, the question is which one should be protected.

If the defender is confident that the attacker would prefer the non-dominated points maximizing the damage, any rational and robust protection scheme should consider the minimization of the maximal impact, within a so-called min–max policy.

In general the MO analysis considers different – partially conflicting – attributes simultaneously, so that the optimization leads to a set of potential solutions. Considering the proposed measures of impact ANPA and TTRAD, the decision-making problem regarding which node of a network to protect for the minimization of the impact of an attack to the network is formulated in mathematical terms as follows (see reference [21]).

Find the node $n_p$ of the network to be protected such that

$$n_p = \arg \left\{ \min_{n_p} \max_{n_s} \text{ANPA} \land \max_{n_p} \min_{n_s} \text{TTRAD} \right\}$$

(1)

where subscripts $p$ and $a$ indicate the nodes to protect and to attack, respectively.

Notice that the min–max criterion is not the only criterion applicable to decide where to place the protection, although it seems to best fit the management of high-consequence events and is considered ‘particularly appropriate in the design of robust military system’ networks [22]. Moreover, the min–max is the typical criterion adopted for optimizing the robustness of discrete domain systems [21–23].

3 SOLUTION APPROACH

This section provides some basics of the CA, MC simulation, and MOEA that constitute the basis of the solution approach adopted in the present work.

CA are a general class of mathematical models [24] which are appealingly simple and yet capture the complex behaviour of dynamic systems. They offer a significant computational potential owing to their spatially and temporally discrete nature, characterized by local interaction and an inherently parallel form of evolution. Herein, CA are used to quantitatively model the hazard propagation through the network, based on continuity constraints among the nodes.

MC simulation [25] is used for reproducing several realizations of the hazard propagation dynamics in the face of an attack, by sampling the time delays associated with the links and the number of affected persons in every node from known probability distributions.

3.1 Modelling with cellular automata

CA are mathematical models of dynamic systems. The dynamics of CA unfolds at discrete time steps on a discrete lattice of cells $L$, typically assumed homogeneous (all cells bear the same properties) [24]. For example, in a three-dimensional cellular state space, the state at the discrete time $t$ of the generic cell $ijl$, of coordinates $x_i, y_j, z_l$ with $i, j, l \in Z$, is described by the state variable $s_{ijl}(t)$. Each cell of $L$ is a finite automaton which can assume one of a finite number of discrete values in a local value space, $S \equiv \{0, 1, 2, \ldots, k-1\}$.

The generic cell $ijl$ interacts only with a fixed number $n$ of cells that belong to its predefined local neighbourhood $N_{ijl}$. At the next discrete time $t+1$, the cell $ijl$ updates its state $s_{ijl}(t+1)$ according to a transition rule $\phi : S^n \rightarrow S$, which is a function of the state variables at time $t$ of the $n$ cells in $N_{ijl}$ that is, $s_{ijl}(t+1) = \phi(s_{ijl}(t), r_{ijl} \in N_{ijl})$. Notice that the homogeneity assumption implies that the functional form of the rule is assumed to be the same everywhere in the cellular state space, i.e. there is no space index attached to $\phi$. Differences between what is happening at different locations are due only to differences in the values of the state variables of the local neighbourhood, not to the update rule. The rule is also homogeneous in time. One ‘iteration step’ of the dynamic evolution of the CA is achieved after the simultaneous application of the rule $\phi$ to...
each cell in the lattice $L$. The temporal evolution of this CA is obtained by:

(a) specifying the finite size of the lattice $L$;
(b) specifying the boundary conditions;
(c) specifying the initial condition $\mathbf{s}(0) = [s_1(0), s_2(0), ..., s_M(0)];$
(d) simultaneously applying the rule $\phi$ to each of the $L$ lattice cells, in an iterative manner.

For example, consider a network of $m$ binary nodes (step a) whose function is to deliver a given throughput from a source $S$ to a destination node $D$ [26]. Ascertaining the connectivity of the network from source to destination would require knowledge of the system cut or path sets [27], an NP-hard problem [20], or a depth-first procedure [28].

Within a CA computational scheme, each node $i$ is mapped into a spatial cell whose neighbour $N_i$ is the set of network elements which provide their input to it (step b). The state variable $s_i$ of cell $i$ is binary, assuming the value of 1 when node $i$ is operating (active) and of 0 when not operating (passive). Initially all the cells’ state values are passive (step c).

The problem analysed in the present paper must consider that the activation of a node is delayed by the time required to propagate the attack from node to node. Indeed, a cell is activated if it is connected to and receives input from at least one active cell or node in its neighbourhood. When accounting for the hazard propagation process, the cell activation concerning the hazard also depends on the time required to propagate the attack: the arrival time of the propagated attack is determined as the sum of the current time plus the time delay. If several nodes can propagate the attack to a given node, the arrival time of the attack at such a node is determined by the minimum of the times of propagation from all connected nodes in its neighbourhood.

Assume now that the generic connecting element (arc) $j_i$ from node $j$ to $i$ can be in two states, active ($w_{ji}(t) = 1$) or passive ($w_{ji}(t) = 0$). The $j_i$ arc state variable $w_{ji}(t)$ defines the ‘operational’ state of the arc. Initially all $w_{ji}(t) = 0$. As soon as node $j$ is reached by the attack, the state of $w_{ji}(t)$ changes from 0 to 1, for $t = t + TD_{ji}$.

The transition rule governing the evolution of the generic cell $i$ consists of the application of the following rule

$$s_i(t) = [w_{pi}(t) \lor w_{qi}(t) \lor ... \lor w_{ri}(t)], \quad p, q, ..., r \in N_i$$

The basic algorithm proceeds as follows:

1. $t=0$.
2. Set all the cells, state values and $w_{ji}(t)$ to 0 (passive).
3. Set $s_i(0) = 1$ and $w_{ji}(t+TD_{ji}) = 1$ (source activated and arcs from $s$ activated at $t = t + TD_{ji}$).
4. Update each cell state by means of the transition rule and update all exiting arcs from each cell at $t = t + 1$.
5. If $s_D(t) = 1$, stop (destination activated); else go to (4).

To account for the time to reach every node in the network, an additional node is introduced that is activated only when all nodes are activated. The network under analysis is assumed to be operational, so that there is at least one spanning tree [28].

To illustrate the procedure, consider the network in Fig. 1. Numbers in each arc represent the propagation delays between its nodes, in arbitrary units. For example, when node 1 is activated by an attack, it will activate node 2 after 2 time units and node 3 after 3 time units.

The sequence of events along the network is as follows.

$t = 0$: Node 1 is activated and the attack begins to propagate to nodes 2 and 3. The arrival time at node 2 is $0 + 2 = 2$ and at node 3, $0 + 3 = 3$. This means that nodes 2 and 3 will be activated at $t = 2$ and $t = 3$, respectively ($w_{12}(2) = 1$ and $w_{13}(3) = 1$).

$t = 1$: No nodes are activated by an attack during this time step and the hazard propagation does not reach any nodes.

$t = 2$: The hazard reaches node 2, which is then activated ($s_2(2) = [w_{12}(2) \lor w_{22}(2)] = 1$). The attack begins to propagate from node 2 to the connected node 4 which will be reached at $2 + 2 = 4$ ($w_{24}(4) = 1$).

$t = 3$: The hazard reaches node 3, which is activated. The attack begins to propagate from node 3 to the connected nodes 2, 4, and 5 with arrival times at $3 + 1 = 4$, $3 + 2 = 5$, and $3 + 2 = 5$, respectively. However, node 2 is already active and node 4 will be activated earlier, at $t = 4$, through the 1–2–4 path.

$t = 4$: The hazard reaches node 4 from node 2. The attack begins to propagate from node 4 to nodes 5 and 6 with arrival times at $4 + 2 = 6$ and $4 + 3 = 7$, respectively.

$t = 5$: The hazard reaches node 5 from node 3. The attack begins to propagate from node 5 to node 6 with arrival time at $5 + 1 = 6$. 

Fig. 1 Network with time delays
$t = 6$: The hazard reaches destination node 6 from node 5.

Figure 2 shows the CA evolution corresponding to the hazard propagation through the network. The $x$-axis contains the node indices; along the $y$-axis the CA time evolution is displayed proceeding from the top. The dots represent the active cells at the current iteration step. Note that node 4 is activated at time 12, so $\text{TTRAD} = 12$. If time delays were not considered, the destination node would be activated at $t = 3$.

3.2 Multiple-objective evolutionary algorithms

In the present work, the search for an optimal solution to the problem (equation (1)) of identifying which node of the network to protect for minimal impact of an attack is tackled by means of MOEA. This family of evolutionary algorithms is designed to deal with multiple-objective problems, possibly with constraints. The approach does not guarantee the determination of the true Pareto front, nor does any other heuristic approach for that matter. Nevertheless, a number of comparisons performed in evolutionary multi-criteria optimization on benchmark problems have shown that the results obtained using different instances of MOEA are very close to the exact solution [29, 30].

This group of algorithms combines the basic concepts of dominance with the general characteristics of evolutionary algorithms. Therefore, MOEA are able to deal with non-continuous, non-convex, and/or non-linear spaces, as well as problems whose objective functions are not explicitly known, as in the case of the output of MC simulation codes.

Herein, the non-dominated sorting genetic algorithm (NSGA-II) is used [30]. It is a very efficient MOEA, which incorporates elitism and a rule for adaptation of the population chromosomes that takes into account both the rank and the distance of each solution with respect to its neighbours in the population.

Our NSGA-II implementation allows integer, real, and mixed chromosomes. For the particular problem studied here, only integer variables were used. The recombination mechanism is one-point crossover (for more implementation details see reference [31]).

4 COMPUTATIONAL EXAMPLE

As stated in section 1, an important characteristic of security risk assessment is the need to consider the presence of ‘a malevolent intelligence directed toward maximum social disruption’ [13]. Then, it is expected that the attacker would choose the target that maximizes the amount of harm delivered. Adopting a multiple-objective perspective, the attacker would arrive at the definition of a group of non-dominated points of attack, e.g. nodes in our network model.

In order to illustrate the approach, suppose that an attacker plans to set on the 52-node network depicted in Fig. 3 [32]. Such a network is composed of bidirectional links, so the propagation of the attack at any node spreads immediately to its neighbours. Nevertheless, the time to accomplish such propagation is considered variable from link to link. In this particular example, propagation time delays are randomly selected, without loss of generality, using a discrete uniform distribution $U(0,10)$. The numbers of persons affected at the different nodes are also uniform random variables within the ranges reported in Table 1. Five hundred MC evaluations have been performed to assess the consequences of any particular attack. Note that the simulation may consider the protection in any node as well as the simultaneous attack of any group of nodes. However, attacks in cascade are not considered here.

![Fig. 3 Network used to evaluate the effect of attacks on different nodes [32]](image-url)
For the sake of simplicity, let us consider scenarios made by attacks on individual nodes in the network. In Fig. 4, the consequence of each scenario is represented as a point on the two-dimensional plane of the objective functions TTRAD and ANPA. The dotted line constitutes the non-dominated front comprising those nodes the individual attack of which maximizes the impact on TTRAD (node 22 with minimal TTRAD) and ANPA (node 24 with maximal ANPA). So, there is no other node outside this non-dominated set that can be rationally preferred for an attack, if the damage is to be maximized according to ANPA and TTRAD criteria.

Suppose that some kind of protection can be implemented inside the network, for curtailing or rejecting terrorist attacks. The nature of such protections is obviously strongly related to the type of network under consideration. For example, in water distribution networks the attacks can be avoided or rejected by single surveillance of some nodes of the network, and the propagation can be curtailed by means of interruption of selected lines [1]. Nevertheless, in practice the number and nature of the protective actions that can be effectively implemented on the system are constrained by many factors, economic, technical, and political ones among others.

For example, the decision maker can a priori propose a protective scheme at node 22 in order to delay the single attack propagation. Figure 5 shows the effect on the average TTRAD when node 22 is immunized, i.e. it does not propagate the hazard and one single node (on the x-axis) is attacked. As expected, if the attack initiates right at node 22, the protective action avoids the hazard propagation to the rest of the network.

Figure 6 shows the maximal impact that can be achieved should a single attack take place in the network, for different protected nodes. A simple way to investigate the Pareto frontier is to fix the protected node and to determine the set of non-dominated points of attack that maximizes the impact given the protection. This procedure amounts to a complete enumeration of scenarios ‘node attacked–node protected’, which is evidently affordable only if the number of nodes is small. Even if the network under study has only 52 nodes, we use an MOEA (as tested in references [33] and [34]).

Table 1 Minimum and maximum values of the ranges for the number of people affected by an attack to a single node in the network shown in Fig. 3

<table>
<thead>
<tr>
<th>Node</th>
<th>Min</th>
<th>Max</th>
<th>Node</th>
<th>Min</th>
<th>Max</th>
<th>Node</th>
<th>Min</th>
<th>Max</th>
<th>Node</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17</td>
<td>32</td>
<td>14</td>
<td>17</td>
<td>35</td>
<td>27</td>
<td>15</td>
<td>39</td>
<td>40</td>
<td>11</td>
<td>38</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>36</td>
<td>15</td>
<td>12</td>
<td>37</td>
<td>28</td>
<td>10</td>
<td>40</td>
<td>41</td>
<td>13</td>
<td>32</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>33</td>
<td>16</td>
<td>20</td>
<td>40</td>
<td>29</td>
<td>19</td>
<td>35</td>
<td>42</td>
<td>14</td>
<td>34</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>38</td>
<td>17</td>
<td>12</td>
<td>31</td>
<td>30</td>
<td>17</td>
<td>37</td>
<td>43</td>
<td>20</td>
<td>39</td>
</tr>
<tr>
<td>5</td>
<td>19</td>
<td>38</td>
<td>18</td>
<td>15</td>
<td>31</td>
<td>31</td>
<td>14</td>
<td>37</td>
<td>44</td>
<td>18</td>
<td>32</td>
</tr>
<tr>
<td>6</td>
<td>19</td>
<td>33</td>
<td>19</td>
<td>18</td>
<td>34</td>
<td>32</td>
<td>17</td>
<td>31</td>
<td>45</td>
<td>15</td>
<td>34</td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td>30</td>
<td>20</td>
<td>13</td>
<td>30</td>
<td>33</td>
<td>10</td>
<td>38</td>
<td>46</td>
<td>20</td>
<td>33</td>
</tr>
<tr>
<td>8</td>
<td>14</td>
<td>31</td>
<td>21</td>
<td>15</td>
<td>33</td>
<td>34</td>
<td>17</td>
<td>40</td>
<td>47</td>
<td>19</td>
<td>36</td>
</tr>
<tr>
<td>9</td>
<td>19</td>
<td>40</td>
<td>22</td>
<td>10</td>
<td>31</td>
<td>35</td>
<td>18</td>
<td>39</td>
<td>48</td>
<td>16</td>
<td>38</td>
</tr>
<tr>
<td>10</td>
<td>15</td>
<td>38</td>
<td>23</td>
<td>18</td>
<td>39</td>
<td>36</td>
<td>11</td>
<td>33</td>
<td>49</td>
<td>11</td>
<td>31</td>
</tr>
<tr>
<td>11</td>
<td>13</td>
<td>39</td>
<td>24</td>
<td>16</td>
<td>32</td>
<td>37</td>
<td>11</td>
<td>37</td>
<td>50</td>
<td>16</td>
<td>37</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>39</td>
<td>25</td>
<td>14</td>
<td>40</td>
<td>38</td>
<td>13</td>
<td>35</td>
<td>51</td>
<td>18</td>
<td>36</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>34</td>
<td>26</td>
<td>15</td>
<td>36</td>
<td>39</td>
<td>16</td>
<td>34</td>
<td>52</td>
<td>13</td>
<td>35</td>
</tr>
</tbody>
</table>
The set of curves shown provides valuable information to define the protection policy. The largest reduction on the consequences of a single attack is achieved by protecting node 24 (min–max criterion). Such protection is considered robust because the reduction in the amount of consequences is maximal under the assumption of one single attack, although the probability of any node being attacked remains not quantified. Moreover, the size of the displacement between the non-dominated fronts of the unprotected system and the protected ones gives an insight into the actual reduction of risk that can be achieved with the protection of each node. It would be interesting to investigate how the protection decision is affected by the probability of attack to different nodes.

Since the analysis of the topology of the network is an important source of information [35], the node degree centrality (DC) (number of nodes adjacent to a given node) [36] was evaluated. In this case note that node 24 is not the node with the highest degree centrality. Indeed, \( DC_{24} = 4 \), while \( DC_{42} = 5 \) (see Fig. 3).

An alternative network centrality measure [36], the ‘betweenness centrality’ (BC), was also evaluated. Considering that the communication between two nodes \( j \) and \( k \) that are not adjacent depends on the nodes that are in the path connecting \( j \) and \( k \), the BC measure is the number of times that a node lies along the shortest path between two others [37]. Table 2 presents the highest normalized BC (BCn) for the network under consideration. Note that nodes reported in Fig. 4 belong to the set of nodes with high BC. This a priori information of the ‘topological importance’ of some nodes could be used in order to reduce the computational effort for determining the robust protective scheme in larger networks (e.g. by a MOEA-estimation distribution algorithm).

If we analyse the nodes that constitute the non-dominated front for the maximal impact when node 24 is protected (see Fig. 7), it is possible to identify a cluster of nodes. These nodes must be kept under surveillance if an additional reduction of risk is required (see Fig. 8). Again, some nodes belong to the set of nodes with high BC.

For illustrative purposes the second non-dominated front (i.e. the non-dominated front that would be

![Fig. 6](image6.png)

**Fig. 6** Analysis of the min–max-based robust protection scheme

<table>
<thead>
<tr>
<th>Node</th>
<th>BCn</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>29.982</td>
</tr>
<tr>
<td>26</td>
<td>27.773</td>
</tr>
<tr>
<td>24</td>
<td>24.904</td>
</tr>
<tr>
<td>18</td>
<td>22.943</td>
</tr>
<tr>
<td>38</td>
<td>22.331</td>
</tr>
<tr>
<td>36</td>
<td>22.331</td>
</tr>
<tr>
<td>10</td>
<td>19.244</td>
</tr>
<tr>
<td>31</td>
<td>18.201</td>
</tr>
<tr>
<td>42</td>
<td>17.132</td>
</tr>
<tr>
<td>14</td>
<td>16.893</td>
</tr>
</tbody>
</table>

**Table 2** The ten nodes with highest betweenness centrality
found if the current front is removed) is included in Fig. 7. Such fronts are topologically related in the network and define the zone of highest vulnerability in case of a single attack.

5 CONCLUSIONS

The present paper has reported on a methodological approach which embeds CA modelling and MC simulation within an MO scheme for identifying effective protective schemes of network systems exposed to terrorist attacks. An example of application of the methodology on a hypothetical network clearly demonstrates that the methodology is capable of identifying a set of nodes that, if properly protected, would minimize the consequences of the attack. Additional research efforts are needed to include quantitative probabilistic considerations and to include topological parameters as prior information for driving the MOEA search of Pareto optimal solutions in the case of large networks.

REFERENCES


25 Marceseguerra, M. and Zio, E. Basics of the Monte Carlo method with application to system reliability, 2002 (LiLoLe-Verlag, Hagen).

26 Rocco, S. C. M. and Zio, E. Solving advanced network reliability problems by means of cellular automata and


