# A DECISION MODEL TO INCREASE SECURITY IN A UTILITY NETWORK

**Jochen Janssens[(a)], Luca Talarico[(b)], and Kenneth Sörensen[(c)]**

[(a)(b)(c)]University of Antwerp, Faculty of Applied Economics, ANT/OR – University of Antwerp Operations Research group, Prinsstraat 13, 2000 Antwerp, Belgium

[(a)]jochen.janssens@uantwerpen.be, [(b)]luca.talarico@uantwerpen.be, [(c)]kenneth.sorensen@uantwerpen.be

**ABSTRACT**

In this paper we propose a decision model aimed at increasing security in a utility network (e.g., smart grid, water network). This model assumes that all edges (e.g., pipes, cables) have a certain, not necessary equal, probability of failure, which can de reduced by taking appropriate arc-specific security measures. These are combined in security strategies that should be applied to minimize the risk of disconnecting an origin node from a destination node. We develop a simple but effective metaheuristic approach to solve this problem. Detailed experiments on realistic instances are conducted and the relationships between solutions and problem parameters are tested by simulating different scenarios.

Keywords: network security, metaheuristics, knapsack problem.

## 1. INTRODUCTION

In modern day society, utility networks such as electricity, water, gas, and communication networks are taken for granted. People expect that they function at all times, and are capable of handling all demand placed on them. However, there is a real risk of failures in all types of networks. Those failures might make the network unavailable with a resulting interruption of the service/connection between two network points which are represented by a origin node (i.e., the point from which the service or the product is send to the customer through the network) and a destination node (i.e., the customer or the point to which the product, service is delivered through the network).

Network breakdowns can have *safety*-related causes such as natural phenomena (e.g., earthquakes, storms), human errors, or mechanical defects such as in pumps and valves, caused by the regular wear and tear. In addition, network breakdowns can be due to *security*-related causes such as intentional terrorist attacks and/or malicious sabotages.

After 9/11, the protection of utility networks against intentional attacks has received great attention among network providers. In fact terrorist attacks on utility network are not rare and might cause huge losses in a nation's economy. For these reasons in the remainder of the paper our focus is on network security rather than safety.

Network providers and managers can reduce the risk of a network breakdown after a terrorist attack addressed at one or several network arcs by applying preventive security measures in order to reduce network vulnerabilities.

The security budget that can be spent on these security measures, however, is generally limited. The current economic situation has increased the pressure on limiting even further many budgets and investments in security. In this work, a combination of security measures for one arc is called a security strategy for that arc.

The problem defined in this paper is to reduce the risk of a utility network being (partially) out of service, which is measured as the risk to break the connection between an origin and a destination node, by reducing the risk or the effects of an intentional attack on the network by selecting security strategies from a list of available ones.

Since the budget is limited and the security strategies can only be applied locally, i.e., on a specific link in the network, the security strategies should be chosen in such a way that the reduction of the risk of the network service being down is as large as possible while keeping the total cost of the security strategies within the budget.

Once we consider realistic cases, in which hundreds of links (in our case from 100 up to 500) might compose the network and dozens different security strategies (in this paper from 5 up to 20) might be available for each network arc, the problem can turn out to be so large that it will become computationally infeasible to solve it in a reasonable amount of time with exact algorithms. Therefore we will explore the use of metaheuristics to support this decision problem.

The paper is organized as follows. In Section 2 we give a brief overview of the state of the art. Section 3 clarifies the problem of selecting the best strategies to increase the security of the whole network is described and modelled as an optimisation problem. In Section 4, we present a metaheuristic to solve the network security problem. Section 5 presents some preliminary results about the computational experiments of the metaheuristic presented in this paper. Section 6 concludes the paper and presents some idea of further developments. During the conference more details about the scenarios that have been designed to investigate the relationships between the problem/heuristic parameters and the solutions quality will be presented.

## 2. LITERATURE REVIEW

Following the 9/11 attacks, network security has received growing attention within the scientific community. Although significant research has been done to improve best practices in the field of security, few papers have addressed the relationship between risk-related variables and an objective related to cost-effective network security decisions. Nevertheless, security measure selection problems have received some attention in more recent literature.

The problem of selecting the right security measures given a limited budget is clearly not an easy task. Most security planning models in the literature are qualitative, and only few of them rely on quantitative approaches. In case of a pipeline network, the security risk assessment procedure elaborated by Reniers and Dullaert (2012) may be used. After a careful pipeline security risk assessment, the user is in possession of pipeline segment risk data as well as pipeline route risk data. Assuming that the security risk analyst determines a set of available security measures and defence strategies for application to the different pipeline segments and/or for the pipeline routes, a selection of the most effective security measures with respect to the available budget (either for a single pipeline segment or for a pipeline route) can be calculated. If the cost of the security measures is known in advance a mathematical approach can be used to solve the problem of optimal allocation of security resources by solving a knapsack problem. Reniers et al. (2012) explain how this well-known technique in the field of Operations Research is easy to use in case of security optimisation problems. A practical application to secure an illustrative pipeline infrastructure used to transport oil is described in Talarico et al. (in press 2014).

In Bistarelli et al. (2007) a method for the identification of the assets, the threats and the vulnerabilities of ICT systems is introduced. Furthermore, a qualitative approach for the selection of security measures to protect an IT infrastructure from external attacks is discussed. In particular, two security models based on defence trees (an extension of attack trees) and preferences over security measures are proposed.

In Viduto et al. (2012) the security of a telecommunication network is analysed from a quantitative point of view. Knowledge of potential risks enables organisations to take decisions on which security measures should be implemented before any potential threat can successfully exploit system vulnerabilities. A security measure selection problem is presented in which both cost and effectiveness of an implemented set of security measures are addressed. A Multi-Objective Tabu Search (MOTS) algorithm is developed to construct a set of non-dominated solutions, which can satisfy organisational security needs in a cost-effective manner.

In Sawik (2013) a similar security measure selection problem for an IT infrastructure is formulated as a single- or bi-objective mixed integer programming problem. Given a set of potential threats and a set of available security measures, the decision maker needs to determine which security measure to implement, under a limited budget, to minimize potential losses from successful cyber-attacks and mitigate the impact of disruptions caused by IT security incidents.

The prevention of heavy losses due to cyber-attacks and other information system failures in an IT network is usually associated with continuous investment in different security measures. In Bojanc and Jerman-Blažič (2008) several approaches enabling the assessment of the necessary investments in security technology are addressed from an economical point of view. The paper introduces methods for the identification of risks in ICT systems and proposes a procedure that enables the selection of the optimal level of investments in security measures.

Once security risks have been identified, the potential loss associated with their occurrence, as well as their probability of occurrence must be determined. Determining both probability of occurrence and potential impact of each risk is done in a process called *risk assessment*. Performing a risk assessment phase allows to take decisions regarding the necessary investment in security controls and systems. In our paper we assume that a preliminary risk assessment phase has been conducted by experts, in order to determine the probability of attacks associated with each network arc together with the costs and benefits of each available security measure.

Our approach extends the works of Reniers and Dullaert (2012) and Reniers et al. (2012) by defining a single-objective problem and proposing a quantitative method to select appropriate security measures. A different objective function is used, which relies on the minimization of the risk of the network to be not accessible between a couple of network nodes instead of the maximization of the effectiveness of the security measures used. Moreover, in our work, since a list of security measures is defined for each arc of the network, the model incorporates not only decisions taken at the level of the network, as done in Reniers and Dullaert (2012), Reniers et al. (2012) and Sawik (2013), but it depends on the choices made at the level of single network arcs.

## 3. PROBLEM DESCRIPTION

The utility network can be represented by using a graph $\mathscr{G} = \{\mathscr{N}, \mathscr{A}\}$, where $\mathscr{N}$ represents a set of nodes and $\mathscr{A}$ a set of arcs, connecting the nodes. All arcs $a_i \in \mathscr{A}$ have a probability of being attacked and failing, denoted as $p_i$. A set of security strategies $\mathscr{S}_i$, is defined for each arc $a_i \in \mathscr{A}$ and it comprises all security strategies $s_{ij}$ that are available for this arc.

For each security strategy $s_{ij}$ of arc $a_i$ there are a cost $c_{ij}$ and a value $p_{ij}$, which represents the probability of failure of this arc when $s_{ij}$ is applied. Only one security strategy per arc can be applied. A security strategy can be a combination of single security measures (see e.g., Table 1). A combination of security measures can have a different effectiveness than the sum of the impact of

Table 1: Set of security strategies $\mathscr{S}_i$ for arc $a_i$

| Strategy | Security measures | Cost | Probability |
|---|---|---|---|
| 0 | - | 0 | 0.6 |
| 1 | A | 100 | 0.5 |
| 2 | B | 150 | 0.45 |
| 3 | C | 200 | 0.4 |
| 4 | A&B | 250 | 0.32 |
| 5 | B&C | 300 | 0.25 |

the individual security measures due to some interaction effects. In some cases, combinations of single security measures might not be available due to their incompatibility.

The default security strategy $s_{i0}$, that has a cost $c_{i0} = 0$, is a default state that indicates that no security measures are applied. Its related probability $p_{i0}$ represents the risk of arc $a_i$ failure in case no security measure is selected. It represents the probability of failure of that arc given that an attacker is rational. The probabilities are unique for each arc, and are based on several information such as geographical location, length, criticality of that arc in the network. We assume that these probabilities are predefined in the risk assessment done by a security professional.

The model proposed in this paper makes the assumption that only arcs can be attacked and that nodes are well protected and no viable target for an attack. In future research the model will be extended to a more general case where nodes are targets as well.

Given an origin node $o$ and a destination node $d$ in the network, the quality of a solution (i.e., a selection of a security strategy for each arc) is defined as the probability that no path exists between node $o$ and node $d$. This would make it impossible for a service or good from node $o$ to reach node $d$ (e.g., it would be impossible to make a phone call from node $o$ to node $d$, if all connections to node $d$ were unavailable).

In a communication network it is necessary that the whole network remains connected after an attack in order to guarantee a proper transfer of data between an origin node and a destination node. While extending the analysis to water/gas/electricity networks it is possible that after an attack a sub-network could still operate, but the transfer of a service/product between a supplier (our origin node) and a final user (our destination node) is not possible due to the lack of connections after an attack. In fact some arcs that are not available due to an attack might disconnect the end user from the global utility network.

In this paper, since the decision problem is introduced for the first time, the problem is simplified by making the assumption that only one supplier and one customer exist in the network. However, several intermediate network nodes through which the service/goods pass along the network to reach the customer are considered. In future work, this model will be extended as to evaluate several utility suppliers and several customer in the network, minimizing the risk that any customer is separated from any of the suppliers. In addition supplier capacity, customer demand and importance of either of them might be considered.

Given the fact that we have a single source node and a single destination node, in order to calculate the risk of the network being out of service, we make use of probability theory. Probability theory is used extensively in reliability theory and in reliability studies of systems. For an overview, we refer to Bazovsky (2004); Ministery of Defence (UK) (2011); Romeu (2004).

In order to mathematically state the decision problem associated to the selection of the best set of security strategies to increase the overall network security, we first have to define the risk for the network $\mathscr{G}$ being not available between source node $o$ and destination $d$. For this reason we define a set $\mathscr{C}$. This set contains the combinations of arcs that will disconnect all paths in the network between nodes $o$ and $d$. In other words each element $l$ of set $\mathscr{C}$ represents a combination of arcs, contained in set $\mathscr{A}_l^E$, for which failure happens, and arcs contained in set $\mathscr{A}_l^N$, which do not fail. It should be noted that $\mathscr{A}_l^E \cup \mathscr{A}_l^N = \mathscr{A}$, $\forall l \in \mathscr{C}$. In addition, an element $l$ in set $\mathscr{C}$ contains a critical combination of arc failures (from now on called scenarios) since if the arcs in $\mathscr{A}_l^E$ are out of service, a network breakdown between $o$ and $d$ is generated. The cardinality of set $\mathscr{C}$ depends on the topology of the network $\mathscr{G}$ and the position of nodes $o$ and $d$ within the network. Let $B$ represents the available security budget and $x_{ij}$ a binary variable, that takes values 1 when the security strategy $j$ on arc $i$ is applied, and 0 otherwise.

$$\min \quad \sum_{l \in \mathscr{C}} R_l \tag{1}$$

s.t.

$$\sum_{i \in \mathscr{A}} \sum_{j \in \mathscr{S}_i} c_{ij} \cdot x_{ij} \leq B \tag{2}$$

$$p_i = \sum_{j \in \mathscr{S}_i} p_{ij} \cdot x_{ij} \qquad \forall i \in \mathscr{A} \tag{3}$$

$$R_l = \prod_{i \in \mathscr{A}_l^E} p_i \cdot \prod_{k \in \mathscr{A}_l^N} (1 - p_k) \qquad \forall l \in \mathscr{C} \tag{4}$$

$$\sum_{j \in \mathscr{S}_i} x_{ij} = 1 \qquad \forall i \in \mathscr{A} \tag{5}$$

$$x_{ij} \in \{0,1\} \qquad \forall i \in \mathscr{A}, \forall j \in \mathscr{S}_i \tag{6}$$

The objective function (1) minimizes the total risk for the network being out of service between nodes $o$ and $d$. The total network risk is given by the sum of risks associated to single scenarios happening. Constraint 2 ensures that the total cost associated to the selected security strategies does not exceed the predefined security budget $B$. Equation 3 is used to define the probability $p_i$ associated to a failure of arc $a_i$. Equation 4 gives us the risk for a scenario happening, which disconnects the paths in the network between nodes $o$ and $d$. Equation 5 forces the decision process to select at maximum one security

strategy to protect arc $a_i$. It should be noted that $x_{i0} = 1$ means that for arc $a_i$ no security measures have been applied. Finally, constraint 6 represents the domain of the decision variable, which ensures that no partial security strategies are allowed.

## 4. SOLUTION APPROACH

The decision problem of selecting appropriate security strategies given a budget constraint, in order to reduce the risk for the utility network being down, belongs to the more general category of knapsack problems.

The single objective knapsack problem is one of the best known combinatorial optimisation problems. This problem can be described as follows: given a set of $n$ items, each with a certain weight $w_i$ and a certain profit $p_i$ with $i \in [1,n]$, the objective is to select the subset of items of which the total profit is maximal, and the total weight does not exceed the knapsack capacity $C$.

Applications of the knapsack problem are frequently encountered in several real-world decision-making processes in different fields such as portfolio management, menu planning, design of experiments. For a detailed review of the knapsack problem, the reader is referred to Wilbaut et al. (2008).

Our problem, since the objective function is not linear, belongs to the class of non-linear knapsack problems, also known as the non-linear resource allocation problem. This problem also belongs to the category of combinatorial optimisation problems (see Bretthauer and Shetty (2002)). As the problem instances grow larger, an exact algorithm will require an exponential amount of time. Therefore, we decided to sacrifice the optimality for near optimal solutions that can be calculated in a very short amount of time. To achieve this goal we will make use of metaheuristics.

The metaheuristic that has been developed in this paper is shown in Algorithm 1. It belongs to the category of iterated local search algorithms (ILS). The reader is referred to Lourenço et al. (2010) for a recent survey on ILS. More specifically, a greedy random adaptive search procedure (GRASP) is combined with a variable neighbourhood descent (VND) to improve the current solution and finally two perturbation heuristics are used to escape from local optima. In addition a tabu list is used during the whole execution of the heuristic to avoid an exploration of solutions that have been analysed in previous iterations.

The first step of this iterative solution approach consists of running a GRASP constructive heuristic that selects promising arcs, and selects from that set of promising arcs the best security strategy. This selection is repeated until the security budget does not allow any further security strategies.

After the GRASP procedure is finished, we use local search to improve the current solution by using a VND block. This local search is executed until the algorithm finds no more improvement. Once this is the case, a perturbation is applied to escape the local optimum, and the algorithm continues with a local search from this perturbed solution. If after a predefined number of perturbations no better solution can be found, the algorithm is restarted from a new solution generated by the GRASP constructive heuristic.

**Algorithm 1** Metaheuristic structure

```
Initialize both Problem and Heuristic parameters
let x be the current solution and f(x) its cost
let x* be the best solution found so far and f(x*) its cost
x ← GRASP Heuristic()
x* ← ∅, f(x*) ← ∞
while (max number of iterations not reached) do
   x ← Improvement(x)
   if (f(x) < f(x*)) then
      x* ← x, f(x*) ← f(x)
      update number of iterations without improvement
   end if
   if (max number of iterations without improvement not
   reached) then
      x ← Perturbation(x)
   else
      x ← GRASP heuristic()
   end if
   update number of iterations
end while
return x*
```

## 5. COMPUTATIONAL RESULTS

In this sections we provide some preliminary results of the computational experiments by using the solution approach described before on some realistic instances.

In a first step, the parameters for the solution approach are tuned in order to achieve the best results on average. This step is executed by doing a full factorial experiment on small but realistic instances.

Then, using the best parameter settings for the solution approach, we analyse the influence of each metaheuristic components on both the quality of the solutions and the running time. In particular the VND heuristic on average can improve the initial solutions generated by the GRASP constructive heuristic by 1%. Moreover the perturbation is quite effective since it can efficiently help the solution approach by escaping from local optima and improve the quality of solutions on average by 0.14%.

In Figure 1 we report the evolution of the objective function associated with both the best and the current solutions over time. It can be noticed that our solution approach is able to converge towards good results in a short CPU time also in case of large instances. It should be noted that the marginal improvement of the best solution found so far significantly decreases when the running time is increased.

Analysing the plot associated with the current solution in Figure 1 the behaviour of the solution approach on the quality of the solution should become clear. After the perturbation, that destroys the quality of the solution, small improvements obtained during the VND

heuristic can lead to better solutions. One can clearly distinguish the perturbation strategy that allows the algorithm to efficiently escape from local optima. Starting from the perturbed solution, presented by a higher objective value (thus denoted with a pick), the VND heuristic guides the current solution trough small improvements towards a new local optimum and a hopefully a new and better solution becomes available. The fact that the VND heuristic is able to decrease the value of the perturbed solution and detects new local optima prove the efficiency of the VND.

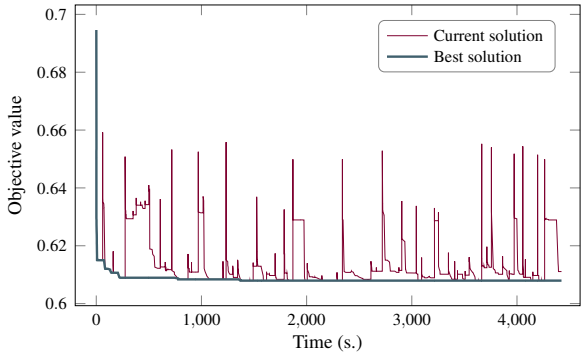


Figure 1: Plot of the objective value over time.

## 6. CONCLUSION & DISCUSSION

In this paper we describe a model for the selection of the appropriate security strategies given a limited budget to increase the security of an infrastructure such as pipelines transportation systems, telecommunication networks, smart grids.

By selecting an origin node and a destination node it is possible to define the risk associated to the interruption of service (or material flow) due to external, malicious attacks (e.g., terrorism, vandalism) directed at the destruction of one or several arcs.

Redundancies in the network might be used by the service provider or network owner in order to keep the service available in case of problems affecting a single arc of the network. However, attacks directed at critical arcs might disrupt the complete infrastructure and service.

An exact evaluation of the risk for the whole network to be down might be a difficult task, especially when several loops are present inside the network. Loops might be added to increase the networks reliability. In order to reduce the complexity of computations, we defined an approach to have an accurate estimate of the risk for the network being down.

This method considers the global impact of a limited number of arcs that are unavailable at the same time and therefore might disconnect the origin node from the destination node. In order to prevent such episodes that could induce significant economic loss, security strategies can be implemented to increase the reliability of each network arc.

We assume that each arc presents different characteristics in terms of vulnerability to external attacks due to internal and external factors such as geographical location, length, materials used, operating conditions. In addition, we assume to have available for each arc a list of security strategies each one with different characteristics in terms of cost and effectiveness. The decision support model presented in this paper attempts to define a ideal mix of such strategies in order to increase the security of the overall network respecting the budget. This budget might restrict the choice between security strategies.

The decision model considered in this paper addresses multilevel decisions, since a decision made at the level of a single arc might affect the security of the whole network. We proposed a heuristic algorithm, which exploits the benefits offered by tabu search combined with a GRASP and an iterated local search solution approach, to solve this combinatorial optimisation problem.

We tested our solution approach on a set of instances that mimic possible realistic scenarios. During the conference we will report the relationship between risk reduction offered by the solutions and the instance parameters such as: vulnerability of the network arcs, cost and effectiveness of the available security strategies, criticality of the segments and security budget allocations.


## ACKNOWLEDGEMENTS

This research was partially supported by the Interuniversity Attraction Poles (IAP) Programme initiated by the Belgian Science Policy Office (COMEX project).


## References


Bazovsky, I., 2004. *Reliability Theory and Practice*. Dover Civil and Mechanical Engineering Series. Dover Publications. ISBN 9780486438672.

Bistarelli, S., Fioravanti, F., and Peretti, P., 2007. Using CP-nets as a guide for countermeasure selection. In *Proceedings of the 2007 ACM symposium on Applied computing*, pages 300–304. March 11 - 15, Seoul, Republic of Korea.

Bojanc, R. and Jerman-Blažič, B., 2008. An economic modelling approach to information security risk management. *International Journal of Information Management*, 28 (5), 413 – 422.

Bretthauer, K. M. and Shetty, B., 2002. The nonlinear knapsack problem – algorithms and applications. *European Journal of Operational Research*, 138 (3), 459 – 472.

Lourenço, H., Martin, O., and Stützle, T., 2010. *Iterated Local Search: Framework and Applications*. Springer New York.

Ministery of Defence (UK), 2011. Chapter 6: Probabilistic R&M Parameters and redundancy calculations. In *Applied R&M Manual for Defence Systems (GR-77), Part D - Supporting Theory*. Abbey Wood, Bristol, UK Ministery of Defence.

Reniers, G. and Dullaert, W., 2012. TePiTri: A screening

method for assessing terrorist-related pipeline transport risks. *Security Journal*, 25 (2), 173–186.

Reniers, G. L., Sörensen, K., and Dullaert, W., 2012. A multi-attribute systemic risk index for comparing and prioritizing chemical industrial areas. *Reliability Engineering & System Safety*, 98 (1), 35–42.

Romeu, J. L., 2004. Understanding series and parallel systems reliability. *Selected Topics in Assurance Related Technologies (START)*, 1 (5), 1 – 8.

Sawik, T., 2013. Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, 55 (1), 156–164.

Talarico, L., Sörensen, K., Reniers, G., and Springael, J., in press 2014. Pipeline security. In Hakim, S. and Shiftan, D. C. Y., editors, *Securing Transportation Systems*. New York, Springer Science and Business Media, LLC.

Viduto, V., Maple, C., and Huang, W.and López-Peréz, D., 2012. A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. *Decision Support Systems*, 53 (3), 599–610.

Wilbaut, C., Hanafi, S., and Salhi, S., 2008. A survey of effective heuristics and their application to a variety of knapsack problems. *IMA Journal of Management Mathematics*, 19 (3), 227–244.

## AUTHORS BIOGRAPHY

**Jochen Janssens** received his Master in Information Management, from the KU Leuven in 2011. Following his graduation, he joined ANT/OR, the University of Antwerp Operations Research Group. To date, he is working there as a doctoral student in the field of metaheuristics and complex optimisation problems. His main interests lie in logistics, Smart Grid optimisation and other network problems.

**Luca Talarico** graduated as an industrial engineer in utility management at the University of Calabria (Italy) in 2005. In 2007 he obtained his master degree in management engineering with a focus on integrated logistics at the University of Calabria. In 2011 he achieved a post graduate degree in business administration (MBA) at the Alma Graduate School of Bologna. He is in the course of getting his PhD in risk management for routing problems. In his former professional career, he worked as a project manager and logistics expert at Ceva logistics and Auchan group.

**Kenneth Sörensen, PhD** obtained his Doctoral degree in Applied Economics at the University of Antwerp in 2003. He is founder of ANT/OR, the University of Antwerp Operations Research Group (http://antor.ua.ac.be) and EU/ME, the metaheuristics community, the largest international forum for researchers in the field of optimization using metaheuristics. He is currently full research professor at the Department of Engineering Management of the Faculty of Applied Economics at the University of Antwerp. His research focuses on (applications of) operations research, mainly optimization.