Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in DISCRETE MATHEMATICS

Electronic Notes in Discrete Mathematics 64 (2018) 295–304 www.elsevier.com/locate/endm

A Bilevel Programming Model for Proactive Countermeasure Selection in Complex ICT Systems

A. Ridha Mahjoub[1], M. Yassine Naghmouchi[1,2], Nancy Perrot[2]

Abstract

We consider the Proactive Countermeasure Selection Problem (PCSP) for complex Information and Communication Technology (ICT) systems. Given 1) the Risk Assessment Graphs (RAGs), a set of digraphs, in which a node is either an access point which is the start point of an attacker, or an asset-vulnerability node to be secured; 2) a positive security threshold for each access point and each asset-vulnerability node; and 3) a set of countermeasures to deploy on the asset-vulnerability nodes, the PCSP consists in selecting the countermeasures placement with minimal cost, guaranteeing the security of all the most likely paths- from attackers point of view- between each access point and each asset-vulnerability node.

We propose a bilevel programming model for the PCSP. We present two single-level reformulations of the bilevel program. The first formulation is a compact one, based on primal-dual optimality conditions. The second formulation is an extended one, employing an exponential number of path constraints. We propose a branch-and-cut algorithm to solve this formulation to optimality. Several series of experiments are conducted on random instances showing the efficiency of the branch-and-cut algorithm to solve the extended formulation. In addition, preliminary computational comparisons between the two formulations are discussed.

Keywords: Bilevel programming, Risk Assessment Graphs, Countermeasure selection, Branch-and-cut.

1 Introduction

Today ICT Systems are becoming more and more complex. They include a large number of heterogeneous elements connected by non-linear interactions,

[1] Université Paris-Dauphine, PSL Research University, CNRS, LAMSADE, 75016, Paris, France.
Email: mahjoub@lamsade.dauphine.fr,
[2] Orange Labs, France.
Email: firstname.lastname@orange.com

https://doi.org/10.1016/j.endm.2018.02.004

and evolve frequently over the time. Such systems are subject to intruder threats, and their risk management is of major concern. Generally, there are two main steps of risk management [8]: the risk assessment and the risk treatment. Recently in [1], we have proposed a new risk assessment framework to supervise the state of complex ICT systems. We have introduced the concept of the *Risk Assessment Graphs* (RAGs) and a quantitative risk evaluation approach. The purpose of this paper concerns the risk treatment process and is strongly related to our risk assessment framework developed in [1].

The RAGs capture the security information in terms of vulnerabilities and topological information. A node in the RAG is either an access point from which an intruder starts an attack, or an asset-vulnerability node to be secured. An arc between two nodes exists if there is a topological access between them allowing the exploitation of the target node. Each arc is weighted by the *arc propagated potentiality*, which is a scalar between 0 and 1 measuring how easy it is for an attacker to exploit the target node of an arc from the source one. These graphs are adaptive to the system change over the time.

In [1], we have proposed a quantitative risk evaluation approach. Our basic security metric is *the path propagated risk* from an access point u to an asset-vulnerability node w, at a time slot t. This is the maximum product of the arc propagated potentialities, over all the $u - w$ paths. The resulting path is the path of maximum propagated risk, called *the most likely path*. By labelling the arcs of the RAGs with the log of the inverse of the arc propagated potentiality (i.e, *the arc propagation difficulty* of an attacker), the $u - w$ most likely path at time t is nothing but the path minimizing the sum of the arc propagation difficulties (the $u - w$ shortest path). Finding the $u - w$ most likely path at each time slot t is crucial. Indeed, when such path is secured (i.e, its shortest path value is greater then a given *path propagation difficulty* threshold), all the $u - w$ paths are so, and the system is said to be secured at time t.

The risk treatment is the final step of the risk management process. It uses the output of the risk assessment, and should give efficient protection decisions. To this end, a set of countermeasures must best be utilized to reduce the risk. However, the deployment of countermeasures might be expensive. In this paper, we aim at selecting the location of countermeasures guaranteeing the security of all the most likely paths at each time slot, while minimizing the total cost of deployment–OPerational EXpenditure (OPEX) cost. We simulate the effect of placing a countermeasure on a node by increasing the ongoing arcs the propagation difficulty of this node with the countermeasure effect. The protection strategy we consider is proactive, i.e, the countermeasures placement is selected at the initial state of the system to be fixed over the time, and this is based on the pre-constructed RAGs.

Our problem can be seen as a "game" between a defender and several attackers. Attackers try to find the most likely paths. But they are forced to act according a certain hierarchy. In fact, the defender who will select the

countermeasures placement in order to make all the most likely paths secured. To get the placement decision of minimal cost, the defender will anticipate the reactions of the attackers to its decisions. From a mathematical programming point of view, the problem is a bilevel programming one [5]. That is an optimization problem (the leader) having other parametric optimization problems (the followers) as part of its constraints.

Bilevel programming is one of the most popular new topics to solve several security problems. In [9] the authors study the electric grid security under disruptive threat problem. In [10] a bilevel programming model for transmission network expansion planning with security constraints is proposed. The most related works to ours are *Shortest Path Network Interdiction Problems* (SPNIPs) [7], [2], [3], and [4], which consist in interdicting the arcs in order to maximize the shortest s-t path length.

We refer to our problem as the Proactive Countermeasures Selection Problem (PCSP). We formulate the PCSP as a bilevel program in which the leader will play the role of the defender and each follower will play the role of an attacker. We propose two single-level reformulations of the model. The first formulation is based on primal-dual optimality conditions. This gives a compact Integer Linear Programming (ILP) formulation that is directly solved using the ILP solver CPLEX [6]. The second one enumerates all possible paths between each access point and each asset-vulnerability node in order to ensure the safety of all of them. This gives an extended formulation with an exponential number of constraints, and will be solved to optimality using a branch-and-cut algorithm.

The rest of the paper is organized as follows. In Section 2, we present the problem and study its complexity. In Section 3, we formulate the PCSP as a bilevel program. In Section 4, we give the compact and the extended single-level reformulations of the bilevel program. Numerical results are discussed in Section 5, and concluding remarks are given in Section 6.

2 The PCSP Statement and Complexity

In this section, we state the PCSP and study its complexity. We consider the RAGs model as introduced in [1]. That consists of a set of directed graphs $(G_t = (V, A_t))_{t \in I}$, where $I = [|1, \ldots, T|]$ is a discrete time interval. The set of nodes V is partitioned into two specified subsets U and W. A node in U represents an attacker access point, and a node in W represents an asset-vulnerability pair. An arc from $w_1 = (a_1, v_1)$ to $w_2 = (a_2, v_2)$ of W represents the possibility of exploiting the vulnerability v_2 of the asset a_2 after exploiting the vulnerability v_1 of the asset a_2. An arc from u to w exists if the exploitation of w from the access point u is possible. Note that the subgraph induced by the nodes U is a stable set. With each arc $ij \in A_t$ is associated a weight w_{ij}^t representing the arc propagation difficulty.

We have a set of countermeasures K to deploy in W. The placement of a

countermeasure $k \in K$ on a node $w \in W$ has a cost c_k, and yields an increase of the weight of the ongoing arcs of w by an effect $\alpha_k \in \mathbb{R}^+$. For each $u \in U$ and $w \in W$, we have a path propagation difficulty threshold $d_{u,w} \in \mathbb{R}^+$ on the length of the $u - w$ shortest path to respect. The goal of the PCSP consists in finding a placement of the countermeasures of K on W in such a way that the cost of deployment is minimum and the shortest path from each $u \in U$ to each $w \in W$ in G_t is at least $d_{u,w}$, for all $t \in I$. We have the following result.

Theorem 2.1 *The PCSP is NP-Complete.*

Proof. We will use a reduction from the Minimum Vertex Blocker to Short Paths Problem (MVBP). Given a directed graph $G = (V, A)$, two nodes $s, t \in V$, the length $l_{ij} \in \mathbb{R}^+$ of each arc $ij \in A$, and an integer d, the MVBP consists in finding a subset $V' \subseteq V$ of minimum cardinality such that the shortest path from s to t in $G \setminus V'$ is at least d. This problem is NP-Complete [2]. We construct an instance of the PCSP as follows. Let $T = 1$; there is only one RAG G_1. Let $G_1 = G$, $U = \{s\}$ and $t \in W = V \setminus \{s\}$. We choose $|K| = 1$; there is only one countermeasure with $c_1 = 1$ and $e_1 = +\infty$. We set $d_{s,t} = d$, and $d_{s,w} = 0$ $\forall w \in W \setminus \{t\}$. Remark that the placement of a countermeasure of effect e_1 on a node w is the same as deleting w, since the effect of the ongoing arcs of w becomes infinite. On the other hand, $|V'|$ is equal to the cost of placement of c_1, since we have a countermeasure with a unit cost. For this particular instance of PCSP, we have exactly the MVBP problem. □

Our work is a generalization of SNIPs [7], [2], [3], and [4], where instead of removing arcs, the leader can pay a given price to increase the length of all the ongoing arcs of a given node. In addition, we consider all the shortest paths between each access point and each asset-vulnerability node in the RAGs.

3 The Bi-level Model

In this section, we formulate the PCSP as a bilevel problem in which the leader controls the countermeasure deployment, and forces the shortest paths between each access point $u \in U$, and each asset-vulnerability node $w \in W$, at each $t \in I$, to be at least $d_{u,w}$. On the other hand, several followers will play the role of the attackers. For each $t \in I$, $u \in U$, and $w \in W$ each follower will compute the $u - w$ shortest paths after the leader acts (countermeasures placement). That is the *tuw-follower problem.*

3.1 tuw-Lower Level Problem Formulation

Let x_{kw}, $k \in K, w \in W$ be the binary variable used to indicate if the countermeasure k is deployed on the node w or not. We denote by $l^t_{uw}(x)$ the length of the shortest path, at time $t \in I$, from u to w, after the leader acts. Each tuw-follower problem aims at finding the value $l^t_{uw}(x)$.

The weight of an arc $ij \in A_t$ after applying a countermeasure k in the node j is $w_{ij}^t(x) = w_{ij}^t + \alpha_k x_{kj}$. Now, let $z_{ij}^{uw,t}$ $\forall t \in I u \in U, w \in W, ij \in A_t$ be the binary variable indicating whether or not an arc ij belongs to the $u-w$ shortest path at time t. Hence, we have $l_{uw}^t(x) = \sum_{ij \in A_t} w_{ij}^t(x) z_{ij}^{uw,t}$

For all $t \in I, u \in U, w \in W$, the tuw-follower formulation is then equivalent to:

$$\text{(tuw-}F\text{)} \begin{cases} \text{Min } l_{uw}^t(x) = \sum_{ij \in A_t} (w_{ij}^t + \sum_{k \in K} \alpha_k x_{kj}) z_{ij}^{uw,t} & \\ \sum_{j \in \Gamma^+(i)} z_{ij}^{uw,t} - \sum_{j \in \Gamma^-(i)} z_{ji}^{uw,t} = \begin{cases} 1 & \text{if } i = u \\ 0 & \text{if } i \notin \{u, w\} \\ -1 & \text{if } i = w \end{cases} & \forall i \in V, \\ z_{ij}^{uw,t} \geq 0 & \forall ij \in A_t. \end{cases}$$

The LP dual of $tuw-$F $\forall t \in I, u \in U, w \in W$ is :

$$\text{(tuw-}FD\text{)} \begin{cases} \text{Max } \lambda_w^{uw,t} - \lambda_u^{uw,t} & \\ \lambda_j^{uw,t} - \lambda_i^{uw,t} \leq w_{ij}^t + \sum_{k \in K} \alpha_k x_{kj} & \forall ij \in A_t, \\ \lambda_i^{uw,t} \text{ free} & \forall i \in V. \end{cases}$$

3.2 The Bi-level Formulation

The leader controls the countermeasure deployment respecting the security constraints: given the most likely paths thresholds $d_{u,w}$ for each $u \in U$ and $w \in W$, the leader forces the shortest paths returned by the tuw-followers to be at least $d_{u,w}$, at each time slot $t \in I$. The objective function is to minimize the total cost of the countermeasure deployment. The PCSP is then equivalent to the following bilevel program:

$$\text{Min} \sum_{w\in W}\sum_{k\in K} c_k x_{kw}$$

$$\sum_{ij\in A_t} (w_{ij}^t + \sum_{k\in K} \alpha_k x_{kj}) z_{ij}^{uw,t} \geq d_{u,w}, \qquad \forall t \in I, u \in U, w \in W,$$

$$\forall tuw - F \begin{cases} \text{Min} \sum_{ij\in A_t} (w_{ij}^t + \sum_{k\in K} \alpha_k x_{kj}) z_{ij}^{uw,t}, \\ \\ \sum_{j\in\Gamma^+(i)} z_{ij}^{uw,t} - \sum_{j\in\Gamma^-(i)} z_{ji}^{uw,t} = \begin{cases} 1 & \text{if } i = u \\ 0 & \text{if } i \notin \{u,w\} \\ -1 & \text{if } i = w \end{cases} \quad \forall i \in V, \\ \\ z_{ij}^{uw,t} \in \{0,1\} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \forall ij \in A_t. \end{cases}$$

$$x_{kw} \in \{0,1\} \qquad\qquad\qquad\qquad \forall k \in K, w \in W.$$

4 Single-Level Reformulations

Here, we present two different single-level reformulations of our PCSP bilevel model. First, primal-dual optimality conditions are used to obtain a single level compact formulation of the problem [5]. Second, we present a non compact formulation, controlling all the possible paths between each $u \in U$ and $w \in W$.

4.1 Compact Single-Level Formulation

According to the weak and strong duality theorems, every LP problem can be replaced with the primal feasibility constraints, the dual feasibility constraints, and the weak duality equation. Hence, by replacing the follower with its primal-dual optimality conditions, we obtain a single level formulation of the bilevel PCSP model described in Section 3. Note that the primal-dual transformation holds because the linear relaxation of the shortest path problem is integral. To linearize the term $x_{jk}z_{ij}^{uw,t}$, we introduce a binary variable $y_{k,ij}^{uw,t}$ that takes the value 1 if x_{kj} and $z_{ij}^{uw,t}$ are both equal to 1, and 0 otherwise. These operations yield the following compact ILP formulation $\forall t \in I, u \in U, w \in W$:

$$\text{PCSP1: Min} \sum_{w\in W}\sum_{k\in K} c_k x_{kw}$$

$$\sum_{ij\in A_t} (w_{ij}^t z_{ij}^{uw,t} + \sum_{k\in K} \alpha_k y_{k,ij}^{uw,t}) \geq d_{u,w},$$

$$\sum_{j\in\Gamma^+(i)} z_{ij}^{uw,t} - \sum_{j\in\Gamma^-(i)} z_{ji}^{uw,t} = \begin{cases} 1 & \text{if } i = u \\ 0 & \text{if } i \notin \{u,w\} \\ -1 & \text{if } i = w \end{cases} \quad \forall i \in V,$$

$$\lambda_j^{uw,t} - \lambda_i^{uw,t} \leq w_{ij}^t + \sum_{k\in K} \alpha_k x_{kj} \qquad \forall ij \in A_t,$$

$$\sum_{ij\in A_t} (w_{ij}^t z_{ij}^{uw,t} + \sum_{k\in K} \alpha_k y_{k,ij}^{uw,t}) = \lambda_w^{uw,t} - \lambda_u^{uw,t},$$

$$y_{k,ij}^{uw,t} \leq 1/2(x_{kj} + z_{ij}^{uw,t}) \qquad \forall ij \in A_t,$$

$$y_{k,ij}^{uw,t} \geq x_{k,j} + z_{ji}^{uw,t} - 1 \qquad \forall ij \in A_t,$$

$$x_{kw}, z_{ij}^{uw,t}, y_{k,ij}^{uw,t} \in \{0,1\} \qquad \forall ij \in A_t, k \in K.$$

4.2 Extended Single-Level Formulation

A second single-level reformulation of the bilevel model consists in controlling all the paths from each $u \in U$ to each $w \in W$, for all $t \in I$, to be greater or equal than $d_{u,w}$. In fact, if all the paths are at least of length $d_{u,w}$ the shortest one is so, and vice versa. Let $\pi_{u,w}^t$ be the set of all paths between u and w at time t. The following extended ILP formulation is equivalent to the PCSP bilevel model:

$$\text{PCSP2: Min} \sum_{w\in W}\sum_{k\in K} c_k x_{kw}$$

$$\sum_{ij\in\pi}\sum_{k\in K} \alpha_k x_{kj} \geq d_{u,w} - \sum_{ij\in\pi} w_{ij}^t \quad \forall t \in I, u \in U, w \in W, \pi \in \pi_{u,w}^t \qquad (1)$$

$$x_{kw} \in \{0,1\} \qquad \forall w \in W, k \in K.$$

The number of constraints (1) could be exponential in $O(n)$, we use a branch-and-cut algorithm to solve the problem to optimality. The separation problem corresponds to a shortest path problem: for a given $t \in I$ if the shortest path between an access point u and an asset-vulnerability node w is greater than $d_{u,w}$, it is so for all $u - w$ paths.

5 Experimental Results

In this section, numerical results are discussed for a set of instances randomly generated.

5.1 Instances Description and Implementation Environment

We set $I = [|1, \ldots, 12|]$ and $|U| = \frac{1}{2}|W|$. For each time slot in I, two specific subsets of arcs are randomly generated: the arcs induced by the nodes of W, denoted by $A_t(W)$, and the arcs connecting the nodes of U with those of W, denoted by $A_t(U, W)$. The sub-graph induced by the nodes of W is an Erdös-Renyi random graph [11] of parameters W and $p = 0.5$. This is generated by randomly connecting $|W|$ nodes. Each arc in $A_t(W)$ is included with probability 0.5 independent from every other arc.

On the other hand, the arcs $A_t(U, W)$ are constructed as follows: Let W_1 be the subset of W whose out degree is greater than or equal to those in $W \backslash W_1$ and such that $|W_1| = 1/2|W| = |U|$. We randomly connect each node in U to exactly one node in W_1. The weights of the arcs are randomly generated. The thresholds vary in $[|1, 10|]$. Finally, three countermeasures available for each node in W are used and described in Table 1.

We implement our formulations with the ILP solver CPLEX 12.6. We use Python 2.7 as programming language and Networkx as graph library. In the following we show, for PCSP2, the variation of the CPU time and the objective value with the number of the nodes. Further preliminary results are also provided for PCSP1.

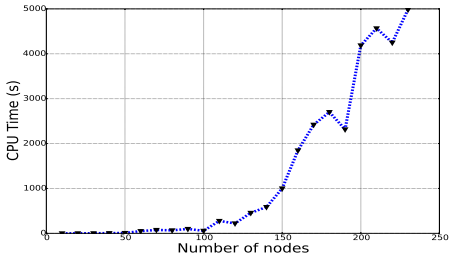
Countermeasure	effect	cost
c_1	10	100
c_2	5	10
c_3	1	1

Table 1
Countermeasures

5.2 PCSP2 Numerical Results

In Figure 1(a), we vary the number of the nodes of the RAGs $|V|$ from 10 to 240. The execution time is short from 10 to 100, relatively short between 100 and 150 nodes, and becomes critical from 150 nodes onwards. A future polyhedral analysis could potentially improve the CPU time for these critical instances, by identifying a set of efficient valid inequalities of the polytope PCSP2.

In Figure 1(b), we observe a non monotone cost variation in function of the number of the nodes. This is explained by the fluctuation of the risk from an instance to another, independently of its size. In fact, an instance of a big size may have a lower risk than another one with a smaller size. This generates a smaller cost of countermeasure deployment for the bigger instance. In Figure 1(b), this can be seen with the instances $|V| = 110$ and $|V| = 120$.



(a) CPU Time (b) Objective Function

Fig. 1. Computational Results

5.3 PCSP1 and PCSP2 Preliminary Comparison

In Table 2, we present some results of PCSP1 compared to those obtained by solving PCSP2. We refer to the objective value by OPT, to the CPU time by CPU, and to the preprocessing time by PP. First, we notice the same values of objective functions. However, these preliminary results show that, even with small instances, the execution time of solving PCSP2 with the branch-and-cut algorithm is less than the one of solving the PCSP1 using CPLEX. Furthermore, PCSP1 preprocessing time is much larger than the one of the PCSP2. Indeed, it uses six different types of constraints, and contains a large number of variables (i.e, at most $|W|[(|T||U|\max_t\{|A_t|\}(|K|+1))+|K|]$) compared to PCSP2 (i.e, $|K||W|$).

$\|V\|$	PCSP1			PCSP2		
	OPT	PP(s)	CPU(s)	OPT	PP(s)	CPU(s)
12	1360	1920	13.16	1360	180	0.15
13	2160	11400	17.91	2160	320	0.17
15	4160	19703	29.39	4160	382	0.2
22	8324	40319	116.24	8324	514	0.6

Table 2
PCSP1 and PCSP2 Comparison

6 Conclusion and Ongoing Work

In this paper, we considered a bilevel model for the Proactive Countermeasure Selection Problem (PCSP), in complex ICT systems. We proposed two single-level reformulations of the model. The first one, PCSP1, was compact and based on primal-dual optimality conditions. The second formulation, PCSP2, was an extended one and based on listing all possible paths between each access point and each asset-vulnerability node in the RAGs. A branch-and-cut algorithm was used to solve the extended formulation. We conducted computational results for PCSP2 with a set of random instances. Numerical results showed that PCSP2 is better than PCSP1.

This paper gave preliminary results on the PCSP. Polyhedral analysis of PCSP2 is in progress in order to strengthen the linear relaxation. Another interesting direction consists in the use of robust optimization to investigate the PCSP with uncertain parameters such as the accessibilities between the assets.

References

[1] Naghmouchi, M. Y, Kheir, K., Mahjoub, A. R. , Perrot, N., Wary, J. P. , *A New Risk Assessment Framework Using Graph Theory for Complex ICT Systems* , Proceedings of the 2016 International Workshop on Managing Insider Security Threats, ACM, 2016.

[2] Khachiyan, L., Boros, E., Borys, K., Elbassioni, K., Gurvich, V., Rudolf, G., and Zhao, J. , *On short paths interdiction problems: Total and node-wise limited interdiction* , *Theory of Computing Systems*, **43(2)** (2008), 204-233.

[3] Golden, B. , *A problem in network interdiction* , *Naval Research Logistics Quarterly*, **25(4)** (1978), 711-713.

[4] Ball, M. O., Golden, B. L., and Vohra, R. V. , *Finding the most vital arcs in a network* , *Operations Research Letters* , **8(2)**, (1989), 73-76.

[5] Dempe, S. , "Foundations of bilevel programming" , *Springer Science & Business Media.* (2002).

[6] CPLEX, IBM ILOG, Users Manual for CPLEX , *International Business Machines Corporation*, **46(53)** (2009).

[7] Israeli, E., and Wood, R. K. ,*Shortestpath network interdiction.* , *Networks*, **40(2)** (2002), 97-111.

[8] Purdy, G. , *ISO 31000: 2009setting a new standard for risk management* , *Risk analysis*, **30(6)** (2010), 881-886.

[9] Motto, A. L., Arroyo, J. M., and Galiana, F. D. , *A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat* , *IEEE Transactions on Power Systems*, **20(3)** (2005), 1357-1365.

[10] Fan, H., and Cheng, H. , *Transmission network expansion planning with security constraints based on bilevel linear programming* , *European transactions on electrical power*, **19(3)** (2009), 388-399.

[11] Erdös, P., and Rényi, A. , *On random graphs, I. Publicationes Mathematicae (Debrecen)*, **6** (1959), 290-297.