A Bilevel Model for Risk Treatment in Complex ICT Systems

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

[1] Université Paris-Dauphine, PSL Research University, CNRS, LAMSADE, 75016, Paris, France.
mahjoub@lamsade.dauphine.fr

[2] Orange Labs, France.
{prénom.nom}@orange.com

Keywords : *Bilevel programming, Risk Treatment, Branch-and-cut.*

1 Introduction

Today Information and Communication Technology (ICT) Systems are becoming more and more complex, and evolve frequently over the time. Such systems are subject to intruder threats, and their risk management is a major issue for network operator. In this paper, we are interested in the risk treatment of such systems. We use the Risk Assessment Graphs (RAGs) [1] as an input of our model. The RAGs capture the security information in terms of vulnerabilities and topological information, as well as the way the system evolves over the time. 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 *propagation difficulty*, which is a positive scalar measuring how it is difficult for an attacker to exploit the target node of an arc from the source one. *the most likely path*, from an attacker point of view is the path allowing the minimum propagation difficulty.

Our problem can be seen as a "game" between several attackers trying to minimize the length of their most likely paths, and one defender selecting the countermeasures placement to ensure that all the most likely paths are secured. From a mathematical programming point of view, the problem is a bilevel programming one [2]. We refer to our problem by the Proactive Countermeasures Selection Problem (PCSP). We propose two single-level reformulations of the model ; PCSP1 and PCSP2. The first formulation is based on primal-dual optimality conditions. This gives a compact ILP formulation that is directly solved using the ILP solver CPLEX. 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 a non-compact formulation with an exponential number of constraints, and it is solved to optimality using a branch-and-cut algorithm. In Section 2, we present the bilevel formulation. In Section 3, we conduct numerical results. We conclude in Section 4.

2 Bilevel Formulation

We consider the RAGs model as introduced in [1]. It 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 (access points, attackers) and W (asset-vulnerability pairs, nodes to be secured). A weight w_{ij}^t representing the propagation difficulty is associated to each arc $(i, j) \in A_t$. The set of countermeasures to deploy in W is denoted by C. The placement of a countermeasure $k \in C$ 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 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 $k \in C$

on W at minimal cost and such that the shortest path from each $u \in U$ to each $w \in W$ in G_t is at least $d_{u,w}$, for all $t \in I$.

Let x_{kw}, $k \in C, w \in W$ be the binary variable used to indicate if the countermeasure k is deployed on the node w or not. Let $z_{ij}^{uw,t}$ $\forall t \in I u \in U, w \in W, (i,j) \in A_t$ be the binary variable indicating whether or not an arc (i,j) belongs to the $u-w$ shortest path at time t. The PCSP is equivalent to the following bilevel formulation :

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

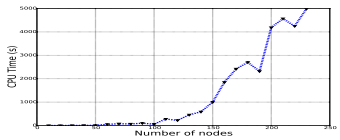
$$\sum_{ij \in A_t} (w_{ij}^t + \sum_{k \in C} \alpha_k x_{kj}) z_{ij}^{uw,t} \geq d_{u,w}, \qquad \forall t \in I, u \in U, w \in W,$$

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

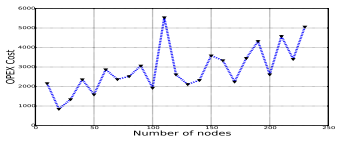
$$x_{kw} \in \{0,1\} \qquad \forall k \in C, w \in W.$$

3 Numerical Results

The results for PCSP2 are presented in Figure 1. The execution time (Figure 1(a)) is short from 10 to 100, relatively short between 100 and 150 nodes, and becomes critical from 150 nodes. We observe a non monotone cost variation in function of the number of the nodes (Figure 1(b)). This is explained by the fluctuation of the risk from an instance to another, independently of its size. Furthermore, we notice an average CPU time gain of 63.6% by solving PCSP2, compared to PCSP1.



(a) PCSP2 CPU Time



(b) PCSP2 Objective Function

FIG. 1 – Computational Results

4 Concluding Remarks

We have considered a bilevel model for the PCSP, in complex ICT systems. We propose two single-level reformulations of the model : a compact formulation PCSP1, and a non-compact formulation PCSP2. We conduct computational results for PCSP2 with a set of random instances. We show that PCSP2 is more efficient than PCSP1. Polyhedral analysis of PCSP2 is in progress in order to enforce the linear relaxation.

Références

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