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