The PCSP: Bilevel Programming and Polyhedra

M.Yassine Naghmouchi

PGMO, 14 November 2017

With A. Ridha Mahjoub, Nancy Perrot

Table of Contents

Table of contents

Motivation

Challenges

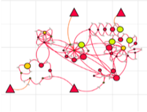
Cybercrimes

$ 2000 billion by 2019

Risk analysis VS complex systems

Contributions

Risk assessment graphs



Contributions

Motivation

Challenges

Cybercrimes

$ 2000 billion by 2019

Risk analysis VS complex systems

SDN
Software Defined Networking

5G orange

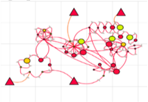
Vidéo à la demande orange

Cyberdefense

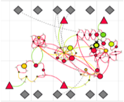
$ 170 billion by 2020

Contributions

Risk assessment graphs

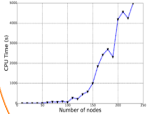


Contributions



Optimisation

Security VS Cost



Algorithms

Table of contents

The RAG model (CCS, 2016)

- $(G_i = (V_i, A_i))_{i \in I}$, where I is a discrete time interval.
- The set of nodes V_i is partitioned into two specified subsets S_i and T_i.
- A node in S_i represents an attacker access point.
- A node in T_i represents an asset-vulnerability pair.
- An arc from $t_1 = (a_1, v_1)$ to $t_2 = (a_2, v_2)$ of T_i exists if the exploitation of the vulnerability v_1 on the asset a_1 makes possible the exploitation of v_2 on a_2.
- With each arc $(u, v) \in A_i$ is associated a weight $w^i_{u,v}$ representing the propagation difficulty at time i.

Problem Statement

Input

An instance of the PCSP: (G, K, D)

- G: the set of the RAGs, with each arc $(u, v) \in A_i$ is associated a weight w^i_{uv} representing the arc propagation difficulty.
- K: the set of countermeasures $K = \{(t, k) : k \in K_t, t \in T\}$ such that K_t is the set of countermeasures associated with t. The placement of k on t: $c^k_t \in \mathbb{R}_+$, $\alpha^k_t \in \mathbb{R}^*_+$
- D: the difficulty propagation thresholds: $D = (d^t_s)_{s \in S, t \in T} \in \mathbb{R}^{|S|\times|T|}_+$.

Problem Statement

Output

Selecting a set of countermeasures, at minimal cost, such that for each $s \in S$ and $t \in T$ the length of the $s - t$ shortest path is at least d_s^t.

NP-Completeness

Theorem

The PCSP is NP-Complete.

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.

The transformation

Let $|I| = 1$, let $G_1 = G$, $S = \{s\}$ and $T = V \setminus \{s\}$.
We choose $|K| = 1$, $c_1 = 1$ and $e_1 = +\infty$.
We set $d_{s,t} = d$, and $d_{s,v} = 0$ $\forall v \in T \setminus \{t\}$.
We have exactly the MVBP problem.

History

First formulation dates back to 1934 by H.v. Stackelberg.

Hierarchical problems

- Optimization problem having a second (parametric) optimization problem as part of its constraints.

$$
\begin{aligned}
&\text{"}\underset{y}{Min}\text{"} F(x(y), y) \\
&\qquad G(x(y), y) \leq 0, \\
&\qquad H(x(y), y) = 0, \\
&\qquad x(y) \in argmin\{f(x, y) : \underset{x}{g(x, y)} \leq 0, h(x, y) = 0\}
\end{aligned} \tag{1}
$$

- NP-Hard problems.

Our bilevel problem

- The attackers are represented by the follower: a shortest path formulation.
- The defender is represented by the leader: ensuring that each $s - t$ shortest path is of length greater than or equal to the corresponding threshold.

Reformulations

- PCSP1: compact formulation based on primal-dual optimality conditions. (INOC, 2017)
- PCSP2: extended formulation based on enumerating all the $s - t$ paths.

PCSP2: A Path-Based Formulation

procedure

Enumerating all the paths between each access point and each asset-vulnerability node.

PCSP2: A Path-Based Formulation

procedure

Enumerating all the paths between each access point and each asset-vulnerability node.

$$\mathrm{M}in \sum_{(t,k)\in K} c_t^k x_t^k$$

$$\sum_{uv\in\pi} \sum_{k\in K_v} \alpha_v^k x_v^k \geq d_s^t - \sum_{uv\in\pi} w_{uv}^i \quad \forall i \in I, s \in S, t \in T, \pi \in \pi_{s,t}^i$$

$$x_t^k \in \{0,1\} \quad \forall (t,k) \in K.$$

PCSP2: A Path-Based Formulation

procedure

Enumerating all the paths between each access point and each asset-vulnerability node.

$$\mathrm{M}in \sum_{(t,k)\in K} c_t^k x_t^k$$

$$\sum_{uv\in\pi} \sum_{k\in K_v} \alpha_v^k x_v^k \geq d_s^t - \sum_{uv\in\pi} w_{uv}^i \quad \forall i \in I, s \in S, t \in T, \pi \in \pi_{s,t}^i$$

$$x_t^k \in \{0,1\} \quad \forall (t,k) \in K.$$

Only one type of binary variables, but an extended formulation.

Table of contents

The $PCSP(G, K, D)$

For simplicity reasons we set $|I| = 1$, only one graph.

$$\sum_{\substack{uv \in P, \\ k \in K_v}} \alpha_v^k x_v^k \geq d_s^t - V(P) \quad \forall s \in S, t \in T, P \in P_{s,t}, \tag{2}$$

$$0 \leq x_t^k \quad \forall (t, k) \in K, \tag{3}$$

$$x_t \leq 1 \quad \forall (t, k) \in K. \tag{4}$$

$$PCSP(G, K, D) = conv\{c^T x | x \in \{0, 1\}^{|K|} : \text{x satisfies } (2) - (4)\}$$

Theorem

The linear relaxation of $PCSP(G, K, G)$ can be solved in polynomial time.

What is an essential countermeasure?

$S(G, K, D)$ define the set of solutions of $PCSP(G, K, D)$.

Definition

If $S(G, K, D) \neq \emptyset$, a countermeasure $(t, k) \in K$ is said to be *essential* for $PCSP(G, K, D)$ if and only if the set $S(G, K \backslash \{(t, k)\}, D) = \emptyset$.

$$x_t^k = 1 \quad \forall (t, k) \in K^* \tag{5}$$

where K^* is the set of all essential countermeasures of $PCSP(G, K, D)$.

Characterisation of Essential Countermeasures

Definition

$(t, k) \in K$ is essential for $PCSP(G, K, D)$ if and only if $\exists$ $s_0 \in S$, $t_0 \in T$, and $P_0 \in P_{s_0,t_0}$ such that:

$$\sum_{\substack{v \in P_0, v \neq s_0, \\ (v,l) \in K_v \setminus \{(t,k)\}}} \alpha_v^l < d_{s_0}^{t_0} - v(P_0)$$

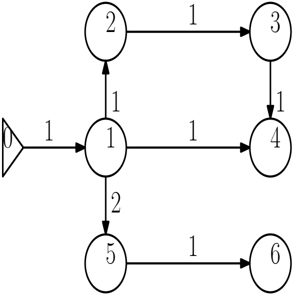
Theorem

Finding the essential countermeasures for $PCSP(G, K, D)$ can be solved in polynomial time.

Finding the Essential Countermeasures

Input: An instance (G, K, D) of $PCSP$.
Output: The set K^* of essential countermeasures.
Step 0: $K^* \leftarrow \emptyset$,
For each $(t, k) \in K$:
    Step 1: Select all the countermeasures in $K \backslash \{(t, k)\}$,
    Step 2: Construct $\tilde{G}(K \backslash \{(t, k)\})$,
    Step 3: For each $s \in S$ and $t \in T$, compute $P^*_{s,t}$ in $\tilde{G}(K \backslash \{(t, k)\})$,
    Step 5: Apply Definition:
        If $v(P^*_{s,t}) < d^t_s$:
            $K^* \leftarrow K^* \cup \{(t, k)\}$.

An Instance of PCSP with Essential Countermeasures



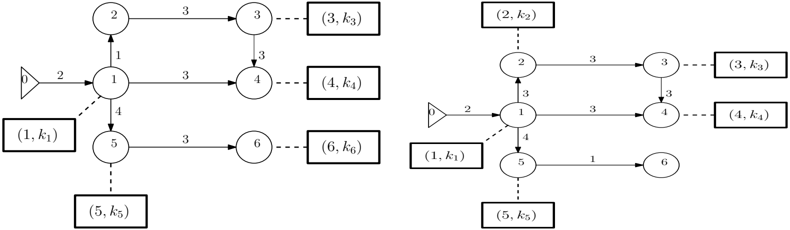
$K_1 = \{(1, k_1)\}, \alpha_{(1,k_1)} = 1$

$K_w = \{(w, k_w)\}, \alpha_{(w,k_w)} = 2,$

$d_{0,1} = 1, d_{0,6} = 5,$

$d_{0,w} = 4 \forall w \in \{2, 3, 4, 5\}.$

Essential Countermeasures of the Instance



(a) The graph $\tilde{G}(K \backslash \{(2, k_2)\})$

(b) The graph $\tilde{G}(K \backslash \{(6, k_6)\})$

Dimension

Proposition

Consider $ax = \alpha$ an equation of $PCSP(G, K, D)$. Then $ax = \alpha$ is a linear combination of equations (5)

Theorem

$dim(PCSP(G, K, D)) = |K| - |K^*|$

Corollary

$PCSP(G, K, D)$ is full dimensional if and only if $K^* = \emptyset$

Trivial Inequalities

Theorem

Let $(t, k) \in K$. Inequality $x_t^k \leq 1$ defines a facet of $PCSP(G, K, D)$ if and only if $(t, k) \in K \setminus K^*$.

Trivial Inequalities

Theorem

Let $(t,k) \in K$. Inequality $0 \leq x_t^k$ defines a facet of $PCSP(G,K,D)$ if and only if

1) $(t,k) \in K \setminus K^*$,
2) $(K \setminus \{(t,k)\})^* = K^*$.

Sufficient Conditions for Security Inequalities to be Facet Defining

Theorem

Let $s \in S$, $t \in T$ and $P \in P_{s,t}$. Security inequality defines a facet of $PCSP(G, K, D)$ if

1) *For all $(v, l) \in K(P)$, $\alpha_v^l = \alpha$,*
2) *$\exists r \in \mathbb{N}$ such that $1 \leq r \leq |K(P)|$ and $r\alpha = d_s^t - V(P)$,*
3) *For all $J \subseteq K(P) \setminus K^*$ such that $|J| = |K(P)| - r$, for all $(v, l) \in K \setminus \{K^* \cup K(P)\}$, we have $S(G, K \setminus \{J \cup \{(v, l)\}\}, D) \neq \emptyset$*

Necessary Conditions for Security Inequalities to be Facet Defining

Theorem

Let $s \in S$, $t \in T$ and $P \in P_{s,t}$. Security inequality defines a facet of $PCSP(G, K, D)$ only if

1) $\exists (v, l) \in K(P)$ *such that* $\alpha_v^l \leq d_s^t - V(P)$,
2) *For all* $J \subseteq K^* \cap K(P)$ $\sum_{(v,l) \in J} \alpha_v^l \leq d_s^t - V(P)$,
3) $\exists (v, l) \in K(P)$ *such that* $(v, l) \in K \setminus K^*$ *or* $\alpha_v^l \neq \frac{1}{|K(P)|}(d_s^t - V(P))$.

e.i.c.s Inequalities

Definition

Let $J = \{(t_i, k_i) : (t_i, k_i) \in K \setminus K^*, (t_{i+1}, k_{i+1}) \in (K \setminus \{(t_i, k_i)\})^*, i = 1, \ldots, n-1\ n \leq |K| - |K^*|\}$. The set J is said to be a set of essentially interdependent countermeasures. We refer to such set as e.i.c.s.

Theorem

Let J be an e.i.c.s. The following inequality is valid for $PCSP(G, K, D)$.

$$\sum_{i=1}^{n} x_{t_i}^{k_i} \geq \lceil \frac{n-1}{2} \rceil \tag{6}$$

Sufficient and Necessary Conditions for e.i.c.s Inequalities to be Facet Defining

Theorem

Let J be a e.i.c.s. Inequality (6) defines a facet of $PCSP(G, K, D)$ if for all $I \subseteq K \setminus K^*$ such that $|I| = n - \lceil \frac{n-1}{2} \rceil + 1$, $S(G, K \setminus I, D) \neq \emptyset$.

Theorem

Inequality (6) define a facet of $PCSP(G, K, D)$ only if

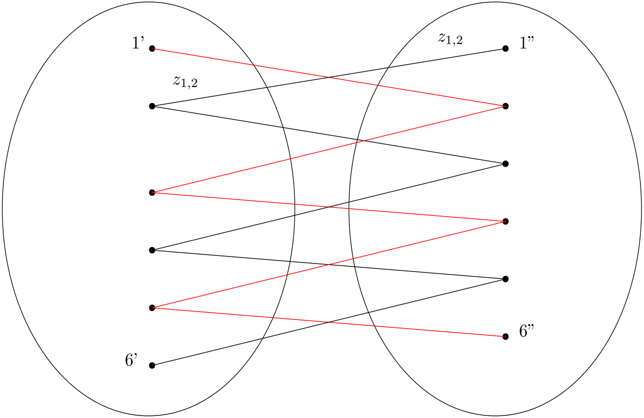
1) *n is even,*
2) *There exists $I \subset J$, $|I| \geq n - \lceil \frac{n-1}{2} \rceil$ such that $S(G, K \setminus I, D) \neq \emptyset$.*

Separation of e.i.c.s Inequalities

1) Let $x \in \mathbb{R}^K$, and let J be a e.i.c.s where n is even,
2) Let $z_{i,i+1} = (x_i + x_{i+1}) - 1$ for all $i = 1, \ldots, n-1$. We have $z_{i,i+1} \geq 0$ for all $i = 1, \ldots, n-1$,
3) $\sum_{i=1}^{n-1} z_{i,i+1} \geq 1 - x_0 - x_n$,
4) If $\sum_{i=1}^{n-1} z_{i,i+1} < 1 - x_0 - x_n$, the e.i.c.s inequality with respect to J and n is violated.

Separation of e.i.c.s Inequalities

Finally, find a shortest path between u' and v'' in the following graph.



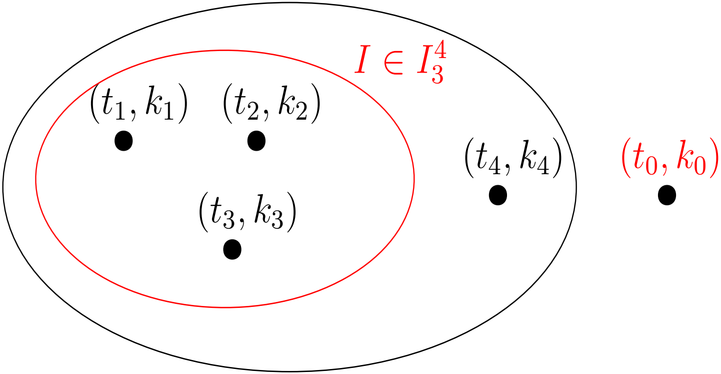
$p-n-(t_0,k_0)$ d.c.s

Definition

Let $n,p \in \mathbb{N}^*$ such that $n \leq |K| - |K^*|$ and $p \in \{2,\dots,n\}$. Let $J = \{(t_i,k_i) : (t_i,k_i) \in K \setminus K^*, i = 1,\dots,n\}$. Consider $(t_0,k_0) \in K \setminus K^*$ and $I_n^p = \{I \subset J, |I| = p\}$. The set J is said to be $p-n-(t_0,k_0)$ dependent countermeasures if for all $I \in I_n^p$, $\{(t_0,k_0)\} \in (K \setminus I)^*$. We refer to such set as d.c.s.

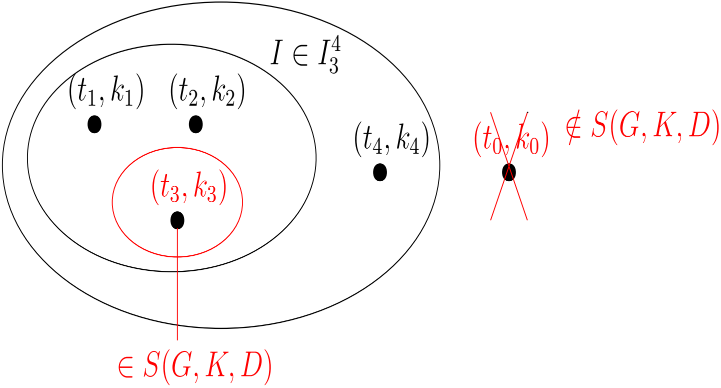
$p - n - (t_0, k_0)$ d.c.s Inequalities

J a d.c.s, n=4, p=3



$p - n - (t_0, k_0)$ d.c.s Inequalities

J a d.c.s, n=4, p=3



$p - n - (t_0, k_0)$ d.c.s Inequalities

$$x_{t_0}^{k_0} + \sum_{i=1}^{3} x_{t_i}^{k_i} \geq 1 \quad \forall I \in I_4^3, \text{is valid.}$$

By Chvatal Gomory, we get:

$$2x_{t_0}^{k_0} + \sum_{i=1}^{4} x_{t_i}^{k_i} \geq 2 \quad \forall I \in I_4^4, \text{is valid.}$$

$p - n - (t_0, k_0)$ d.c.s Inequalities

Theorem

Let J a $p - n - (t_0, k_0)$ d.c.s. The following inequality is valid for $PCSP(G, K, D)$ for all $q \in \{1, \ldots, n - p + 1\}$

$$q x_{t_0}^{k_0} + \sum_{(v,l) \in I} x_v^l \geq q \quad \forall I \in I_n^{p+q-1} \tag{7}$$

Sufficient Conditions $p - n - (t_0, k_0)$ d.c.s Inequalities to be Facet Defining

Theorem

Let J a $p - n - (t_0, k_0)$ d.c.s. Inequality (7) defines a facet of $PCSP(G, K, D)$ if for all $I \in I_n^{p+q-1}$, for all $(t, k) \in K \setminus \{K^*, I, (t_0, k_0)\}$, we have $S(G, K \setminus \{I, (t, k)\}, D) \neq \emptyset$.

Instances Description and Implementation

- $I = [|1, \ldots, 12|]$
- $|S| = \frac{1}{2}|T|$.
- The sub-graph induced by the nodes of T is an Erdös-Renyi random graph of parameters $|T|$ and p.
- Connecting each $s \in S$ to one node in T, starting by the one having the biggest out-degree
- The weights of the arcs are calculated based on the difficulty of propagation metric.

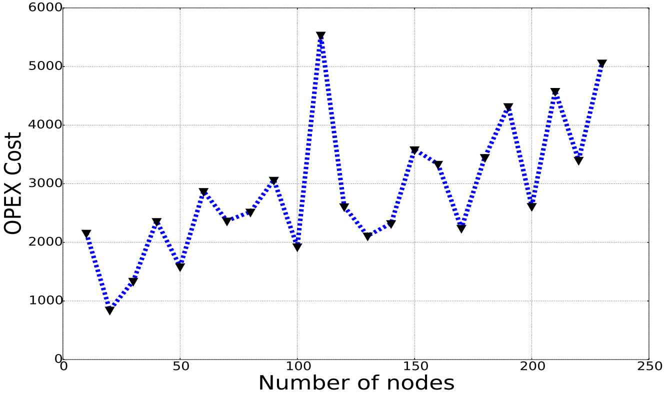
Instances Description and Implementation

- The thresholds vary in $[|1, 10|]$.
- Countermeasures:

Countermeasure	effect	cost
c_1	0.1	100
c_2	0.5	10
c_3	0.9	1

- Solver: CPLEX 12.6.
- Programming language: Python 2.7.
- Graph library: Networkx.

PCSP2 Objective



PCSP2 CPU Time

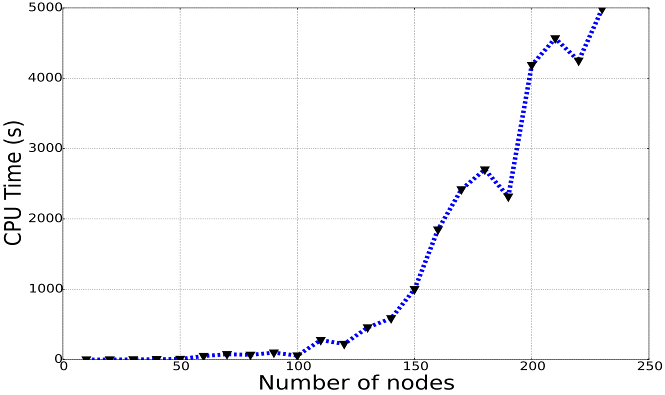


Table of contents

Conclusion

- A bilevel model for optimal countermeasure selection.
- Polyhedral investigation of the extended formulation PCSP2.

Ongoing and future work

- Separation of d.c.s Inequalities.
- Efficiency of e.i.c.s and d.c.s inequalities.

References

[1] A.Ridha Mahjoub, Mohamed Yassine Naghmouchi, Nancy Perrot, *A Bi-level Programming Model for Proactive Countermeasure Selection in Complex ICT Systems*, INOC 2017, Lisbonne, Portugal.

[2] M.Yassine Naghmouchi ; Nancy Perrot ; Nizar Kheir ; A.Ridha Mahjoub ; Jean-Philippe Wary, *A New Risk Assessment Framework Using Graph Theory for ICT Complex Systems*. CCS, MIST octobre 2016, Vienne, Autriche.

References

[3] M.Yassine Naghmouchi ; Nancy Perrot ; Nizar Kheir ; A.Ridha Mahjoub ; Jean-Philippe Wary, *On assessing the risk of complex systems. Journal annals of telecommunications*.

[4] M.Yassine Naghmouchi, Nancy Perrot, Nizar Kheir, Jean-Philippe Wary, *Procédé et dispositif de surveillance de la sécurité dun système dinformation*, institut national de la propriété industrielle (INPI), Juillet 2016, France