# Table of Contents

1. Introduction
2. The PCSP: Bilevel Programming
3. $\text{PCSP}(G, K, D)$: Polyhedral Investigation
4. Conclusion and Perspectives
Table of contents

1 Introduction

2 The PCSP: Bilevel Programming

3 PCSP(G,K,D): Polyhedral Investigation

4 Conclusion and Perspectives
Motivation

Cybercrimes

$2000 billion by 2019

Risk analysis VS complex systems

Contributions

Risk assessment graphs
Introduction
The PCSP: Bilevel Programming
PCSP(\(G, K, D\)): Polyhedral Investigation
Conclusion and Perspectives

Motivation

Cybercrimes

$2000 billion by 2019

Risk analysis vs complex systems

Cyberdefense

$170 billion by 2020

Risk assessment graphs

Contributions

Optimisation

Security vs Cost

Algorithms

M.Yassine Naghmouchi

The PCSP: Bilevel Programming and Polyhedra
Table of contents

1 Introduction

2 The PCSP: Bilevel Programming
   - Problem Statement
   - Complexity
   - Bilevel Programming
   - PCSP2: A Path-Based Formulation

3 \textit{PCSP(G, K, D)}: Polyhedral Investigation

4 Conclusion and Perspectives
(\(G_i = (V_i, A_i)\))_{i \in I}, \text{ where } I \text{ 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 \(w_{u,v}^i\) representing the propagation difficulty at time \(i\).
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 \( d_{st}^t \).
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 $d_{s,v} = 0$ for all $v \in T \setminus \{t\}$.

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.

\[
\text{"Min" } F(x(y), y) \\
G(x(y), y) \leq 0, \\
H(x(y), y) = 0, \\
x(y) \in \arg\min \{ f(x, y) : g(x, y) \leq 0, h(x, y) = 0 \} 
\] (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.

\[
\begin{align*}
\text{Min } & \sum_{(t, k) \in K} c_t^k x_t^k \\
\sum_{u \in \pi} \sum_{k \in K_v} \alpha_v^k x_v^k & \geq d_s^t - \sum_{u \in \pi} w_{u v}^i \quad \forall i \in I, s \in S, t \in T, \pi \in \pi_{s,t}^i \\
x_t^k & \in \{0, 1\} \quad \forall (t, k) \in K.
\end{align*}
\]
PCSP2: A Path-Based Formulation

Procedure

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

\[
\begin{align*}
\text{Min} \quad & \sum_{(t,k) \in K} c^k_t x^k_t \\
\sum_{uv \in \pi} \sum_{k \in K_v} \alpha^k_v x^k_v & \geq d^t_s - \sum_{uv \in \pi} w^i_{uv} \quad \forall i \in I, s \in S, t \in T, \pi \in \pi^i_{s,t} \\
x^k_t & \in \{0, 1\} \quad \forall (t, k) \in K.
\end{align*}
\]

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

1. Introduction

2. The PCSP: Bilevel Programming

3. PCSP\((G, K, D)\): Polyhedral Investigation
   - Associated Polytope
   - Dimension of PCSP\((G, K, D)\)
   - Facial Investigation
   - Numerical Results

4. Conclusion and Perspectives
The **PCSP** \((G, K, D)\)

For simplicity reasons we set \(|I| = 1\), only one graph.

\[
\sum_{uv \in P, k \in K_v} \alpha^k_x^v \geq d^t_s - V(P) \quad \forall s \in S, t \in T, P \in P_{s,t},
\]

\(0 \leq x^k_t \forall (t, k) \in K,\)

\(x^k_t \leq 1 \forall (t, k) \in K.\)

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

**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 \( \text{PCSP}(G, K, D) \).

**Definition**

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

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

where \( K^* \) is the set of all essential countermeasures of \( \text{PCSP}(G, K, D) \).
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:

\[
\sum_{\nu \in P_0, \nu \neq s_0, (\nu, l) \in K_v \setminus \{(t, k)\}} \alpha'_\nu < d^{t_0}_{s_0} - \nu(P_0)
\]

Theorem

*Finding the essential countermeasures for \(PCSP(G, K, D)\) can be solved in polynomial time.*
Finding the Essential Countermeasures

1. Input: An instance \((G, K, D)\) of \(PCSP\).
2. Output: The set \(K^*\) of essential countermeasures.
3. Step 0: \(K^* \leftarrow \emptyset\),
4. For each \((t, k) \in K\):
5.   Step 1: Select all the countermeasures in \(K \setminus \{(t, k)\}\),
6.   Step 2: Construct \(\tilde{G}(K \setminus \{(t, k)\})\),
7.   Step 3: For each \(s \in S\) and \(t \in T\), compute \(P^*_{s,t}\) in \(\tilde{G}(K \setminus \{(t, k)\})\),
8.   Step 5: Apply Definition:
9.     If \(v(P^*_{s,t}) < d^t_s\):
10.    \(K^* \leftarrow K^* \cup \{(t, k)\}\).
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 $\tilde{G}(K \setminus \{(2, k_2)\})$

(b) The graph $\tilde{G}(K \setminus \{(6, k_6)\})$
### 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 \(\text{PCSP}(G, K, D)\) 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 \( \text{PCSP}(G, K, D) \) 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 $S(G, K \setminus \{J \cup \{(v, l)\}\}, D) \neq \emptyset$
Theorem

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

1) \( \exists (v, l) \in K(P) \) such that \( \alpha_v^l \leq d^t_s - V(P) \),

2) For all \( J \subseteq K^* \cap K(P) \)
   \[ \sum_{(v, l) \in J} \alpha_v^l \leq d^t_s - V(P), \]

3) \( \exists (v, l) \in K(P) \) such that \( (v, l) \in K \setminus K^* \) or
   \[ \alpha_v^l \neq \frac{1}{|K(P)|}(d^t_s - V(P)). \]
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\((G, K, D)\).

\[
\sum_{i=1}^{n} x_{t_i}^{k_i} \geq \left\lceil \frac{n - 1}{2} \right\rceil \tag{6}
\]
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 $|I| = n - \left\lfloor \frac{n-1}{2} \right\rfloor + 1$, $S(G, K \setminus I, D) \neq \emptyset$.

**Theorem**

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

1) $n$ is even,

2) There exists $I \subset J$, $|I| \geq n - \left\lfloor \frac{n-1}{2} \right\rfloor$ such that $S(G, K \setminus I, D) \neq \emptyset$. 
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.
Definition

Let $n, p \in \mathbb{N}^\ast$ such that $n \leq |K| - |K^\ast|$ and $p \in \{2, \ldots, n\}$. Let $J = \{(t_i, k_i) : (t_i, k_i) \in K \setminus K^\ast, i = 1, \ldots, n\}$. Consider $(t_0, k_0) \in K \setminus K^\ast$ 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 $I \in I_n^p$, $\{(t_0, k_0)\} \in (K \setminus I)^\ast$. 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

$I \in I_3^4$

$(t_1, k_1)$ (t_2, k_2) (t_3, k_3)

(t_4, k_4) (t_0, k_0)
\[ p - n - (t_0, k_0) \text{ d.c.s Inequalities} \]

\[ J \text{ a d.c.s, } n=4, \ p=3 \]
\[ p - n - (t_0, k_0) \text{ d.c.s Inequalities} \]

\[ x_{t_0}^{k_0} + \sum_{i=1}^{3} x_{t_i}^{k_i} \geq 1 \quad \forall I \in I_3^3, \text{is valid.} \]

By Chvatal Gomory, we get:

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

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

\[
q x_{t_0}^{k_0} + \sum_{(v,l) \in I} x_l^v \geq q \quad \forall I \in l_n^{p+q-1} \tag{7}
\]
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 $l \in I_n^{p+q-1}$, for all $(t, k) \in K \setminus \{K^*, l, (t_0, k_0)\}$, we have $S(G, K \setminus \{l, (t, k)\}, D) \neq \emptyset$. 
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:

<table>
<thead>
<tr>
<th>Countermeasure</th>
<th>effect</th>
<th>cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>$c_1$</td>
<td>0.1</td>
<td>100</td>
</tr>
<tr>
<td>$c_2$</td>
<td>0.5</td>
<td>10</td>
</tr>
<tr>
<td>$c_3$</td>
<td>0.9</td>
<td>1</td>
</tr>
</tbody>
</table>

- Programming language: Python 2.7.
- Graph library: Networkx.
PCSP2 Objective

![Graph showing OPEX Cost vs Number of nodes](image-url)
PCSP2 CPU Time

- **CPU Time (s)**
- **Number of nodes**

![Graph showing CPU Time vs Number of nodes](image-url)
## Table of contents

1. **Introduction**
2. **The PCSP: Bilevel Programming**
3. **PCSP\((G, K, D)\): Polyhedral Investigation**
4. **Conclusion and Perspectives**
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

