

12 July 2010

A Bilevel Fixed Charge Location Model for Facilities under Imminent Attack

Deniz Aksen

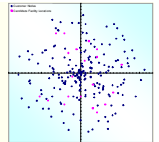
*Koç University
College of Administrative Sciences
and Economics
Sarıyer, İSTANBUL*

Necati Aras and Nuray Piyade

*Boğaziçi University
Dept. of Industrial Engineering
Bebek, İSTANBUL*

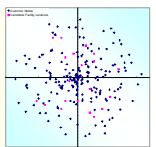


AGENDA



- PROBLEM DEFINITION and DESCRIPTION
- LITERATURE REVIEW
- BFCLP MODEL
- SOLUTION METHODS
- COMPUTATIONAL RESULTS
- CONCLUSION





PROBLEM DEFINITION

Interdiction of a Geographically Distributed Service or Supply Network System

□ Definition:

An intentional strike against a network system which is anticipated in the form of a man-made threat

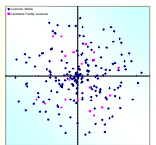
Examples: sabotage, riot, enemy attack, terrorist action

□ Target:

Critical facilities - the ones which, if lost, would pose a significant threat to needed supplies, services, and communications or a significant loss of service coverage or significant loss of efficiency in service delivery.

Examples:

- **Needed supplies:** food, energy, medicines, water
- **Needed services:** police, fire, emergency medical services, transportation (airports, ports, terminals), purification and sanitation
- **Needed communications:** antenna towers, base stations, switch offices, radars



PROBLEM DEFINITION

Interdiction of a Geographically Distributed Service or Supply Network System

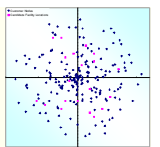
□ Consequences:

- Disruption in the service provision/delivery
- Decay in service system efficiencies

- Disruption in the supply distribution
- Decay in service coverage

r-Interdiction Median Problem (RIM)

r-Interdiction Coverage Problem (RIC)



PROBLEM DEFINITION: RIM

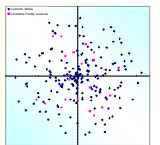
r - Interdiction Median Problem

□ Definition:

- Among p facilities,
find a subset of r facilities, which—when removed—yields the highest level of demand-weighted distance (cost) in total.
- **Anti-thesis of the world-famous p -median problem.**

□ Purpose:

- Identification of r most critical facilities in a network consisting of p service/supply and n demand nodes.
- Prediction of the most disruptive action of an Attacker.



PROBLEM DEFINITION: RIMF

r - Interdiction Median Problem with Protection

□ Definition:

Of the p different facilities, find the subset of q , which—when protected—provides the best outcome against a subsequent optimal (worst-case) r -interdiction strike leading to the definitive loss of r non-protected facilities.

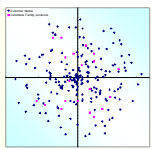
$$(q + r \leq p)$$

PUBLIC FACILITIES

service delivery NOT on customer site!

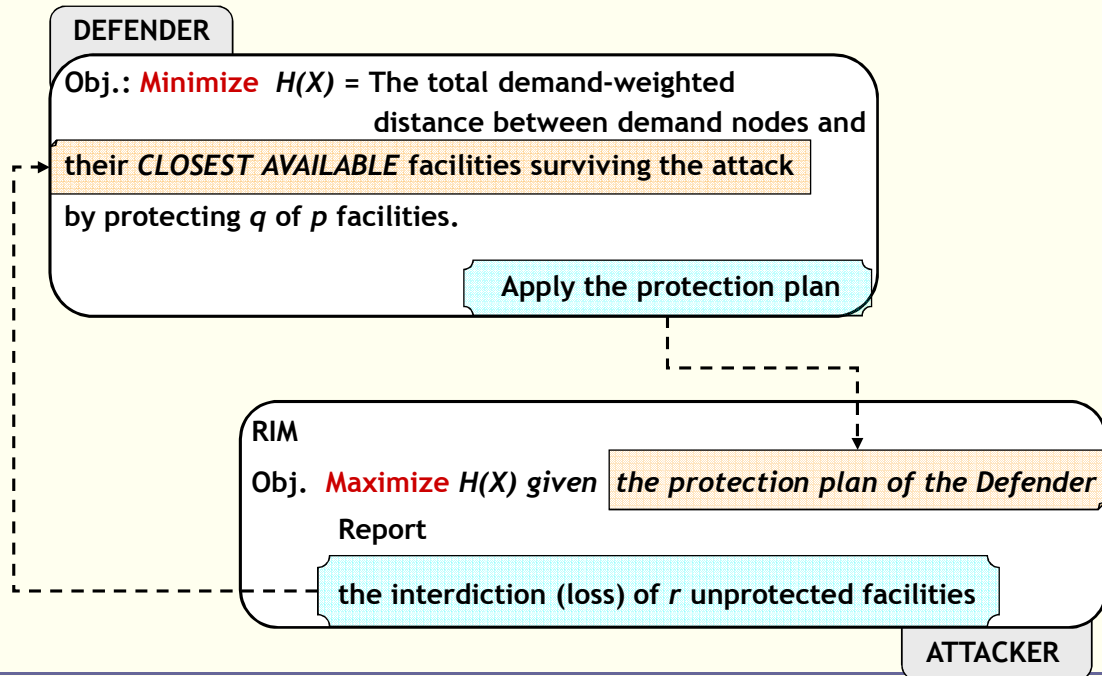
□ Objective:

Minimize the post-attack cost of accessibility from demand nodes to the **CLOSEST AVAILABLE** supply/service nodes.



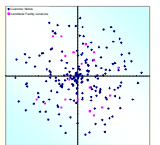
PROBLEM DEFINITION: RIMF

The Bilevel Programming (Stackelberg Game) Formulation of the r - Interdiction Median Problem with Protection



By Deniz Aksen on July 12th 2010 in Lisbon

7



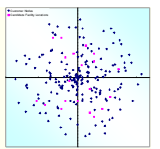
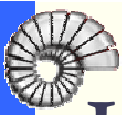
AGENDA

- PROBLEM DEFINITION and DESCRIPTION
- LITERATURE REVIEW
- BFCLP MODEL
- SOLUTION METHODS
- COMPUTATIONAL RESULTS
- CONCLUSION



By Deniz Aksen on July 12th 2010 in Lisbon

8



LITERATURE REVIEW

Review of critical infrastructure, reliability and disruption models for facility location and supply chain networks

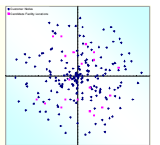
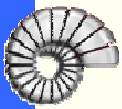
Snyder LV, Daskin MS. Reliability models for facility location: the expected failure cost case. (*Trans Sci* 2005;39)

Snyder LV, Scaparra MP, Daskin MS, Church RL (2006). Planning for disruptions in supply chain networks. In: Greenberg HK (ed), (*TutORials in Operations Research, INFORMS, Baltimore*)

Murray AT, Grubescic TH (eds) (2007). *Critical infrastructure: reliability and vulnerability. Advances in spatial sciences.* Springer-Verlag, Berlin, Heidelberg.

By Deniz Aksen on July 12th 2010 in Lisbon

9



SOURCES OF INSPIRATION

□ RIM + RIC + an annotated bibliography

Church RL, Scaparra MP, Middleton RS (2004). Identifying critical infrastructure: the median and covering facility interdiction problems. *Annals of the Association of American Geographers* 94(3):491-502.

□ IMF : Single level problem solved with Cplex 7.0

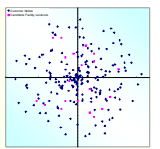
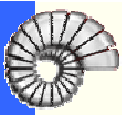
Church RL, Scaparra MP (2007). Protecting critical assets: the *r*-interdiction median problem with fortification. *Geographical Analysis* 39(2):129-146.

□ Maximal Covering Problem with Precedence Constraints (MCPC): an alternative way of reformulating IMF

Scaparra MP, Church RL (2008a). An exact solution approach for the interdiction median problem with fortification. *European Journal of Operational Research* 189(1):76-92.

By Deniz Aksen on July 12th 2010 in Lisbon

10

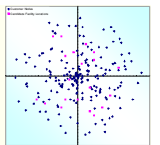
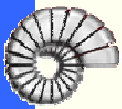


SOURCES OF INSPIRATION

- **RIMF: Bilevel problem solved with implicit enumeration and Cplex 9.0**

Scaparra MP, Church RL (2008b). A bilevel mixed integer program for critical infrastructure protection planning. Computers & Operations Research 35(6):1905-1923.

- *Requires at most $(r^{q+1}-1)/(r-1)$ RIM problems to be solved conditional on the protection plan of the Defender.*



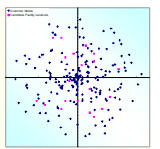
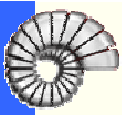
SOURCES OF INSPIRATION

BCRIMF-CE

- **The budget constrained r -interdiction median problem with capacity expansion**

Aksen D, Aras N, Piyade N (2010). Central European Journal of Operations Research.

- ✓ Benefits from the binary enumeration tree (BET) method proposed in Scaparra and Church (*Comp. & OR, 2008*)
- ✓ Adds a budget constraint on the protection resources of the defender instead of a fixed number of facilities that can be protected.
- ✓ Incorporates capacity expansion decisions in accordance with customer-facility reassignments in the wake of interdiction.
- ✗ Assumes that facility locations were already predetermined.



SOURCES OF INSPIRATION

BPPCF

- A Bilevel p -Median Model for the Planning and Protection of Critical Facilities

Aksen D, Aras N, Piyade N (2009, under review)

- ✓ Incorporates also the facility location decisions into the problem setting of BCRIMF-CE

- ✓ This makes BPPCF a triplet problem in a bilevel framework :

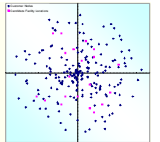
location + protection by the Defender, interdiction by the Attacker.

- ✗ Still based on the p -median idea

- ✗ The protection budget is not a cost component in the Defender's objective, but rather an a priori known limited resource.

By Deniz Aksen on July 12th 2010 in Lisbon

13



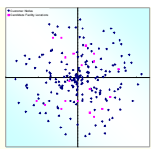
AGENDA

- PROBLEM DEFINITION and DESCRIPTION
- LITERATURE REVIEW
- BFCLP MODEL
- SOLUTION METHODS
- COMPUTATIONAL RESULTS
- CONCLUSION



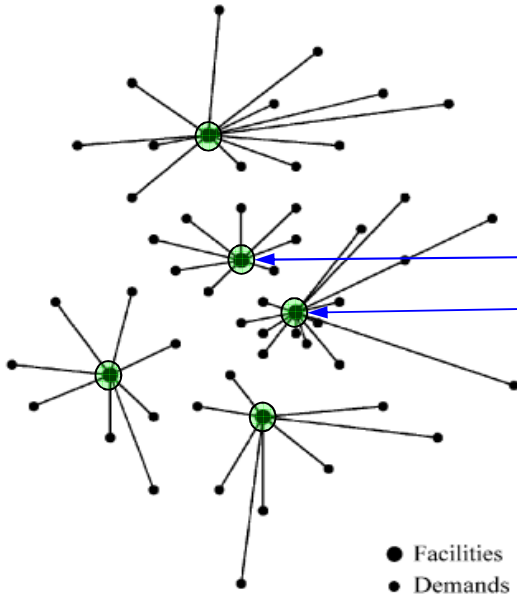
By Deniz Aksen on July 12th 2010 in Lisbon

14



PROBLEM DESCRIPTION: RIM

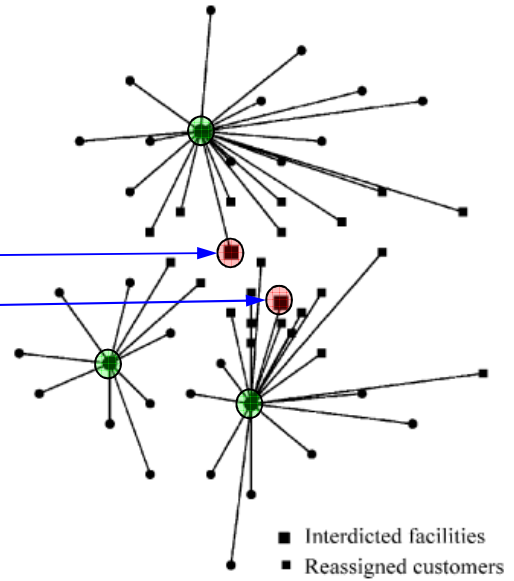
Weighted Distance: 2950.41



● Facilities
● Demands

Figure 2a. Optimal solution to the p -median problem ($p = 5$).

Weighted Distance: 6124.53

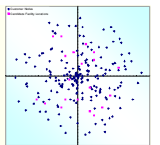
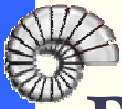


■ Interdicted facilities
■ Reassigned customers

Figure 2b. Optimal interdiction of the p -median solution given in Figure 2a ($r = 2$).

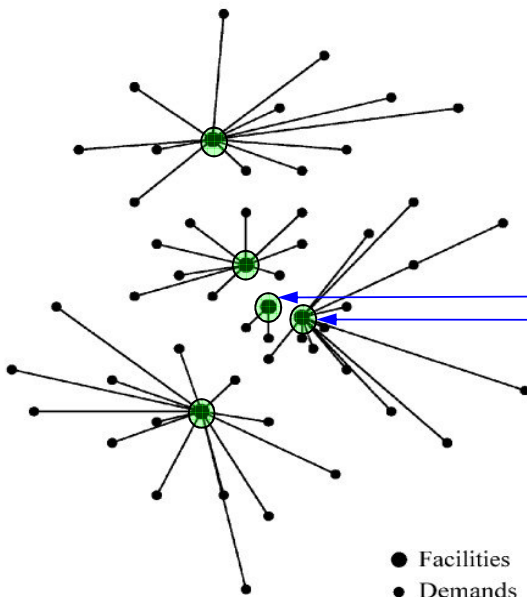
Source: Church RL, Scaparra MP, Middleton RS (2004). Identifying critical infrastructure: the median and covering facility interdiction problems. *Annals of the Association of American Geographers* 94(3):491-502.

By Deniz Aksen on July 12th 2010 in Lisbon



PROBLEM DESCRIPTION: RIM

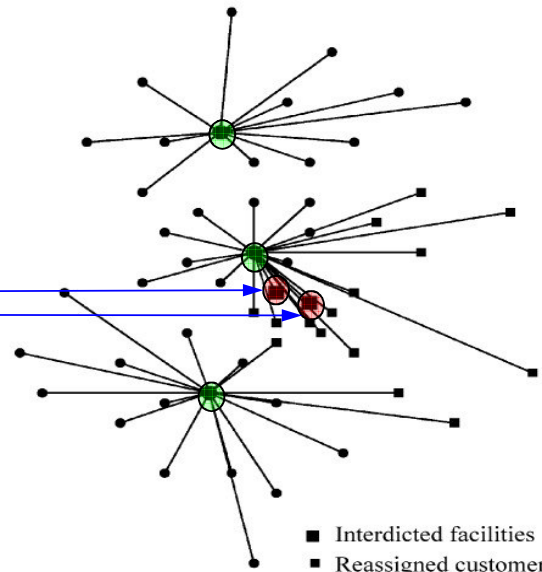
Weighted Distance: 3055.10



● Facilities
● Demands

Figure 3a. A close-to-optimal solution to the p -median problem ($p = 5$).

Weighted Distance: 4613.17



■ Interdicted facilities
■ Reassigned customers

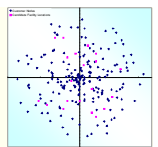
Figure 3b. Optimal interdiction of the p -median solution given in Figure 3a ($r = 2$).

Source: Church RL, Scaparra MP, Middleton RS (2004). Identifying critical infrastructure: the median and covering facility interdiction problems. *Annals of the Association of American Geographers* 94(3):491-502.

By Deniz Aksen on July 12th 2010 in Lisbon



RIM: side-by-side comparison



Weighted Distance: 2950.41

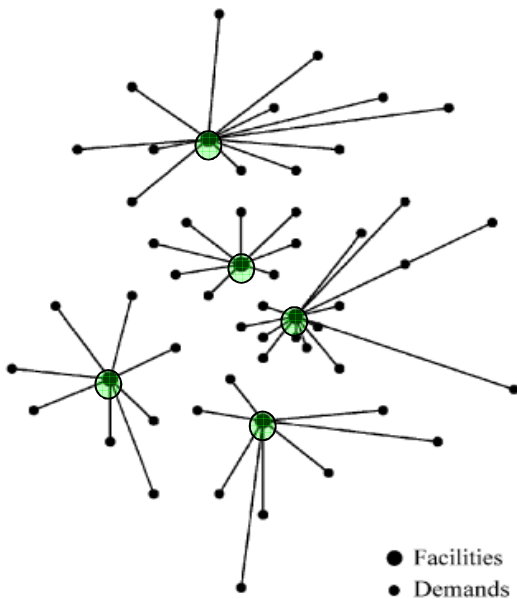


Figure 2a. Optimal solution to the p -median problem ($p = 5$).

Post-attack DWTC: 6124.53
($r = 2$)

Weighted Distance: 3055.10

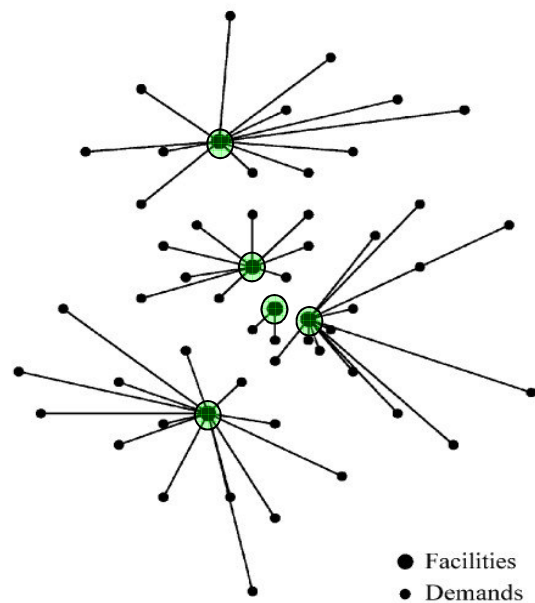


Figure 3a. A close-to-optimal solution to the p -median problem ($p = 5$).

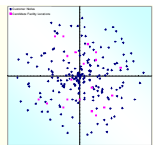
Post-attack DWTC: 4613.17
($r = 2$)

By Deniz Aksen on July 12th 2010 in Lisbon

17



NEW MODEL: BFCLP

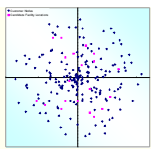


A Leader-Follower Game (*static Stackelberg Game*) for the Planning and Protection of Critical Facilities

- In the upper level (*Leader's problem*), the Defender decides:
 - Given a finite and discrete set of candidate locations,
 - how many facilities should be opened where?
 - what should be their initial capacity installations?
 - and what should be their initial status (protected *or* unprotected)?
- Each facility location has different opening costs for the unprotected and protected modes.

By Deniz Aksen on July 12th 2010 in Lisbon

18



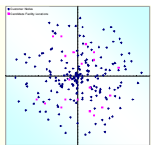
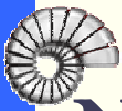
NEW MODEL: BFCLP

ASSUMPTIONS

- Given the decisions of the Defender in the upper level problem, the Attacker in the lower level problem (*Follower's problem*) chooses:
 - **At most r facilities to interdict (r is given).**
- An interdicted facility is destroyed beyond repair.
- Partial interdiction of a facility is not possible.
- The Attacker has perfect information about the protection status of every opened facility.
- A facility opened in the protected mode (*more expensive!*) is immune to any attack.
- **EACH CUSTOMER DESIRES TO GO TO THE CLOSEST OPERATIONAL FACILITY.**

By Deniz Aksen on July 12th 2010 in Lisbon

19



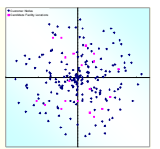
NEW MODEL: BFCLP

THE DEFENDER'S COST COMPONENTS BEFORE INTERDICTION

- **BI-1.** The total fixed cost of opening facilities either in the protected or unprotected mode.
- **BI-2.** The sum of capacity acquisition costs at the opened facilities, which may vary from one facility to another depending on the unit capacity acquisition cost and the total customer demand met.
- **BI-3.** The sum of demand-weighted traveling costs between customers and the respective nearest opened facilities before interdiction.

By Deniz Aksen on July 12th 2010 in Lisbon

20



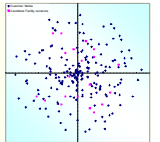
NEW MODEL: BFCLP

THE DEFENDER'S COST COMPONENTS AFTER INTERDICTION

- **AI-1.** The sum of capacity expansion costs incurred by the non-interdicted facilities due to the re-allocation of the customer demand originally satisfied by the interdicted facilities.
- **AI-2.** The sum of extra demand-weighted traveling costs arising due to the re-allocation of the customers from the facilities severed by the attacker.

THE ATTACKER'S COST COMPONENTS

- **AI-1** +
- **AI-3.** The sum of post-attack demand-weighted traveling costs between all customers and their respective nearest facilities surviving the attack.



BFCLP :: Notation

□ Sets:

$I =$ Set of demand nodes (customers), $I = \{1, \dots, n\}$

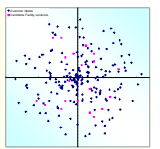
$J =$ Set of candidate facility sites, $J = \{1, \dots, m\}$

□ Parameters

d_{ij}	=	traveling cost between facility site j and demand node i .
q_i	=	demand of customer i .
f_j	=	fixed cost of opening a facility at site j in the unprotected mode.
$f_j + b_j$	=	fixed cost of opening a facility at site j in the protected mode.
c_{1j}	=	unit capacity acquisition cost for the facility at site j
c_{2j}	=	unit capacity expansion cost for the facility at site j
r	=	the max. number of facilities that can be interdicted by the attacker.



BFCLP :: Notation



Binary Decision Variables:

$$X_j = \begin{cases} 1 & \text{if site } j \text{ is chosen to open a facility,} \\ 0 & \text{otherwise.} \end{cases}$$

$$Y_j = \begin{cases} 1 & \text{if the facility at site } j \text{ is protected,} \\ 0 & \text{otherwise.} \end{cases}$$

$$S_j = \begin{cases} 1 & \text{if the facility at site } j \text{ is lost due to an interdiction,} \\ 0 & \text{otherwise.} \end{cases}$$

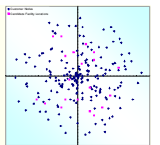
$$U_{ij} = \begin{cases} 1 & \text{if customer } i \text{ is assigned to the facility at site } j \text{ before the attack,} \\ 0 & \text{otherwise.} \end{cases}$$

$$V_{ij} = \begin{cases} 1 & \text{if customer } i \text{ is assigned to the facility at site } j \text{ after the attack,} \\ 0 & \text{otherwise.} \end{cases}$$



BFCLP Model

$$\mathcal{F}_{ij} = \{k \in \mathbf{J} \mid d_{ik} \leq d_{ij}\}$$



Defender's (Upper Level) Problem

$$\min Z_{\text{def}} = \sum_{j \in \mathbf{J}} f_j X_j + \sum_{j \in \mathbf{J}} b_j Y_j + \sum_{i \in \mathbf{I}} \sum_{j \in \mathbf{J}} (c_{1j} + d_{ij}) q_i U_{ij} + \sum_{i \in \mathbf{I}} \sum_{j \in \mathbf{J}} (c_{2j} + d_{ij}) q_i (1 - U_{ij}) V_{ij} \quad (1)$$

$$\text{Subject to } \sum_{j \in \mathbf{J}} U_{ij} = 1 \quad \forall i \in \mathbf{I} \quad (2)$$

$$\sum_{i \in \mathbf{I}} U_{ij} \leq n X_j \quad \forall j \in \mathbf{J} \quad (3)$$

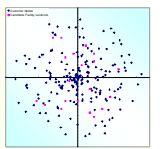
$$\sum_{k \in \mathcal{F}_{ij}} U_{ik} \geq X_j \quad \forall i \in \mathbf{I}, \forall j \in \mathbf{J} \quad (4)$$

$$Y_j \leq X_j \quad \forall j \in \mathbf{J} \quad (5)$$

$$U_{ij}, X_j, Y_j \in \{0, 1\} \quad \forall i \in \mathbf{I}, \forall j \in \mathbf{J} \quad (6)$$



$$\mathcal{F}_{ij} = \{k \in \mathbf{J} \mid d_{ik} \leq d_{ij}\}$$



Attacker's (Lower Level) Problem

$$\max Z_{\text{att}} = \sum_{i \in \mathbf{I}} \sum_{j \in \mathbf{J}} c_{2j} q_i (1 - U_{ij}) V_{ij} + \sum_{i \in \mathbf{I}} \sum_{j \in \mathbf{J}} q_i d_{ij} V_{ij} \quad (7)$$

$$\text{Subject to } \sum_{j \in \mathbf{J}} V_{ij} = 1 \quad \forall i \in \mathbf{I} \quad (8)$$

$$\sum_{j \in \mathbf{J}} S_j \leq r \quad (9)$$

$$S_j \leq X_j - Y_j \quad \forall j \in \mathbf{J} \quad (10)$$

$$\sum_{i \in \mathbf{I}} V_{ij} \leq n X_j (1 - S_j) \quad \forall j \in \mathbf{J} \quad (11)$$

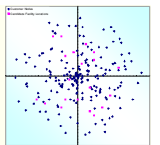
$$\sum_{k \in \mathcal{F}_{ij}} V_{ik} \leq 1 + S_j - X_j \quad \forall i \in \mathbf{I}, \forall j \in \mathbf{J} \quad (12)$$

$$V_{ij} \geq U_{ij} (1 - S_j) \quad \forall j \in \mathbf{J} \quad (13)$$

$$S_j, V_{ij} \in \{0, 1\} \quad \forall i \in \mathbf{I}, \forall j \in \mathbf{J} \quad (14)$$

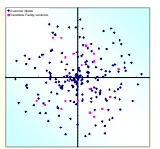
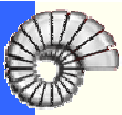


AGENDA



- PROBLEM DEFINITION and DESCRIPTION
- BILEVEL PROGRAMMING
- LITERATURE REVIEW
- BFCLP MODEL
- SOLUTION METHODS
- COMPUTATIONAL RESULTS
- CONCLUSION

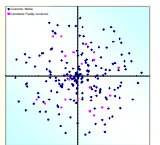
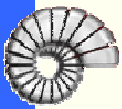




SOLVING BILEVEL PROBLEMS

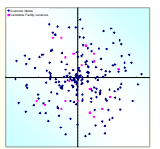
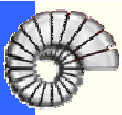
BFCLP has binary variables in both the upper and lower level problems.

- Moore and Bard (*OR*, 1990) showed that MIBPPs are *NP-hard*.
- When the integrality constraints of a given MIBPP are relaxed, the solution of the relaxed problem does not provide a valid lower bound on the global optimum of the MIBPP even if that solution is integral.
- A branch-and-bound type of enumerative solution algorithm to tackle the MIBPP
 - The number of integer variables in either the leader's or the follower's subproblem is at most 10, which reveals the restricted applicability of Moore and Bard's algorithm.



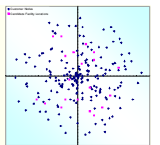
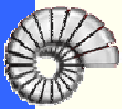
SOLVING BILEVEL PROBLEMS

- Gümüş and Floudas (*Comp. Mgmt Sci*, 2005): a novel deterministic global optimization framework combined with a reformulation/linearization technique originally developed by Sherali and Adams (*SIAM Journal on Discrete Mathematics*, 1990).
- It solves a variety of mixed-integer nonlinear BPPs including the purely integer linear BPP.
 - This technique is used to transform the mixed-integer inner problem constraint set of the given BPP into the continuous domain.
 - The transformation results in a polytope—provided that the inner problem is bounded—with all vertices defined by binary values.



SOLVING BILEVEL PROBLEMS

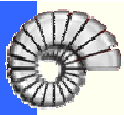
- Gümüő and Floudas (*Comp. Mgmt Sci*, 2005):
 - This polytope is actually equivalent to the convex hull of all integer feasible solutions of the respective inner problem.
 - The reformulation/linearization technique renders the inner problem linear in inner variables.
 - The inner problem can be then replaced with the set of equations that define its necessary and sufficient Karush-Kuhn-Tucker (KKT) optimality conditions.
 - In this way, the original BPP is reduced into a single level optimization problem that should be solved to global optimality.
 - Cplex accomplishes this final job if the problem is a mixed-integer linear problem.
- Impractical even for a 10-facility and 100-customer instance of the BFCLP, since such a modest instance would require as many as 2,030 binary decision variables and 2,251 constraints.



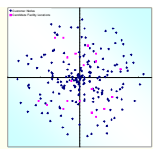
SOLVING BILEVEL PROBLEMS

A HEURISTIC METHOD FOR SOLVING MIBPPs

- Hecheng and Yuping (*Journal of Systems Engineering and Electronics*, 2008)
 - An exponential-distribution based genetic algorithm (GA)
 - For MIBPPs where the follower's objective function and constraints are separable with respect to the follower's variables,
 - For MIBPPs where they are convex when the follower's variables are not restricted to integers.
 - The GA essentially fixes the leader's decision variables, and obtains with a simplified branch-and-bound method (B&B) a proven optimal solution to the linear relaxation (LR) of the follower's MIP.
 - The algorithm proceeds according to the principles of genetic search.



Method-1: TABU SEARCH with HASHING



Features of the applied *tabu search algorithm with hashing (TSH)*

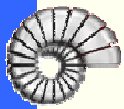
1. Initial Solution

If $r < m$, we randomly select $p = \max\{r + 1, \lceil \log_2 m \rceil\}$ facilities and open them in the unprotected mode.

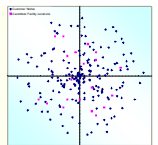
- Solve the attacker's problem by Cplex as a **RIM** problem since none of the initial p facilities is protected.

2. Neighborhood Structure

TSH capitalizes on a large-scale neighborhood structure comprising five types of moves.



Method-1: TABU SEARCH with HASHING



2. Neighborhood Structure (cont.)

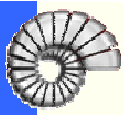
1-Drop : One of the opened facilities will be closed.

1-Add : One of the closed facilities will be opened either in the protected or unprotected mode.

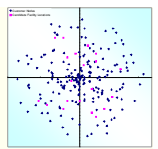
1-Flip : The protection status of an opened facility will be switched on or off.

1-Swap-Int : Two facilities opened in opposite protection modes will swap their protection modes.

1-Swap-Ext: One of the opened facilities will be replaced by one of the closed facilities, where the latter will be opened either in the protected or unprotected mode.



Method-1: TABU SEARCH with HASHING

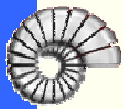


2. Neighborhood Structure (cont.)

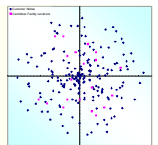
Table 1. Properties of the move types used in TSH

Move Type	Changes p ?	Changes π ?	Max. Neigh. Size
<i>1-Add</i>	yes	possible	$2(m-p)$
<i>1-Drop</i>	yes	possible	p
<i>1-Flip</i>	no	yes	p
<i>1-Swap-Int</i>	no	no	$\pi(p-\pi)$
<i>1-Swap-Ext</i>	no	possible	$\begin{cases} \lceil 2p(m-p)/RNS \rceil & \text{if } p > 1, \\ 2(m-1) & \text{otherwise.} \end{cases}$

RNS is short for *ratio of neighborhood size*.

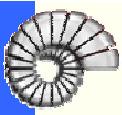


Method-1: TABU SEARCH with HASHING

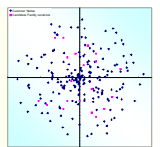


3. Infeasible Solutions

- Throughout the TSH iterations, we do not allow any move to create an infeasible solution for the BFCLP.
- An infeasible solution is where the facility location-protection plan of the defender is too weak to ensure the sustainability of the service system in the wake of the worst-case attacks.
 - A facility location-protection plan of the defender is infeasible if $p \leq r$ and $\pi = 0$.
 - In response to such a plan, the attacker would interdict all facilities present, thereby paralyze the whole system.



Method-1: TABU SEARCH with HASHING



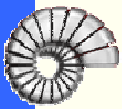
4. Stopping Conditions

■ Condition-1

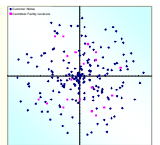
- completing the maximum number of iterations (Max_Iter), which is set equal to 200.

■ Condition-2

- reaching the maximum number of successive iterations during which the incumbent does not improve (Max_Nonimp_Iter), which is set equal to 100.



Method-1: TABU SEARCH with HASHING



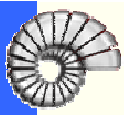
4. Probabilistic Nature and Diversification of **TSH**

■ **TSH** involves randomness which stems from:

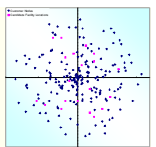
- I. the random selection of an initial feasible facility location-protection plan, and
- II. the granularity of the **1-Swap-Ext** neighborhood which is controlled by the value of the coefficient **RNS**.

- **TSH** starts with a different initial solution in each run. Hence, it needs to be run multiple times with different random number seeds in order to get the best solution overall.

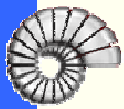
☞ In fact, we run **TSH** five times where each run is executed with a different random number seed.



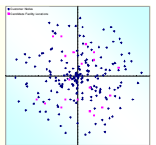
Method-1: TABU SEARCH with HASHING



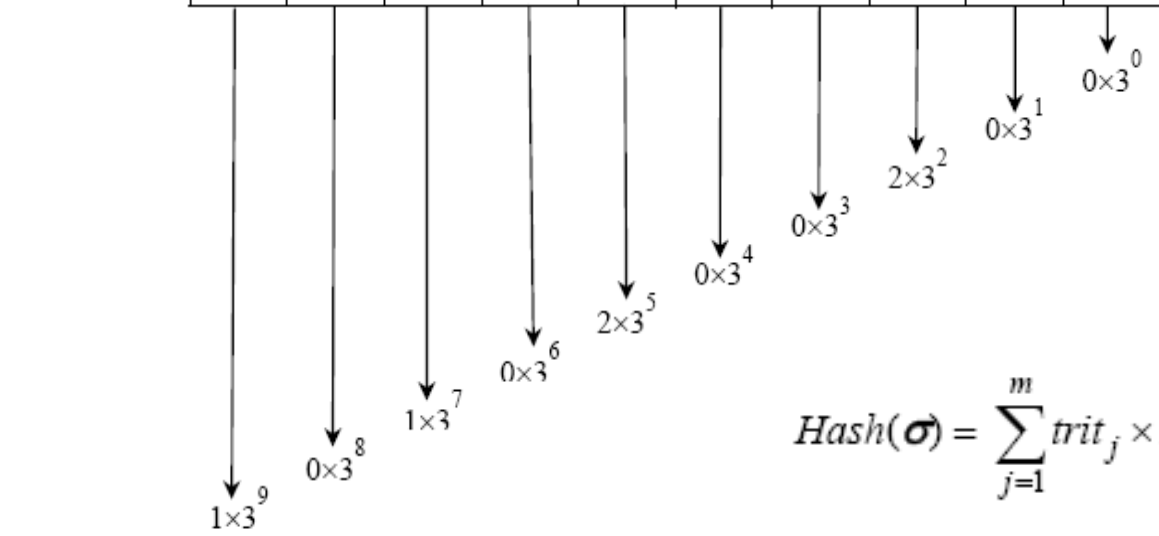
- Applying the **tabu search (TS) principles** by the book...
- **Hashing vectors for tabu search:**
 - First proposed by **Woodruff and Zemel** (*Annals of Operations Research, 1993*)
 - Any search algorithm should be prevented from falling back to a recently visited solution; otherwise can never escape local optima (**Woodruff and Zemel, 1993**).



Method-1: TSH — *how to hash?*



Facility ID →	1	2	3	4	5	6	7	8	9	10
Status trit →	1	0	1	0	2	0	0	2	0	0

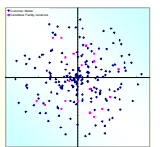
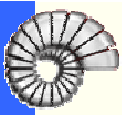


$$\text{Hash}(\sigma) = \sum_{j=1}^m \text{trit}_j \times 3^{m-j}$$

Hash value → $3^9 + 3^7 + 2 \times 3^5 + 2 \times 3^2 = 22,374$

Figure 1.

The **unique ternary string** representation and **hash value** of a sample BFCLP solution

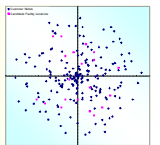
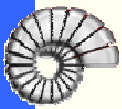


Hashing in TSH

Table 2.

Computation of the **hash value** of a neighborhood solution in TSH

Move Type	ID of Fac.1 added or flipped	ID of Fac.2 dropped or flipped	Formula of $hash_{neigh}$ given the current solution σ and its has value $hash_{neigh}$
1-Add	j	—	$(hash_{curr} + trit_j \times 3^{m-k})$
1-Drop	—	k	$(hash_{curr} - trit_k \times 3^{m-j})$
1-Flip	j	—	$(hash_{curr} + 3^{m-j})$ if $trit_j$ was 1 in σ ; $(hash_{curr} - 3^{m-j})$ otherwise.
1-Swap-Int	j	k	$(hash_{curr} + 3^{m-j} - 3^{m-k})$ where $trit_j$ was 1 and $trit_k$ was 2 in σ .
1-Swap-Ext	j	k	$(hash_{curr} + trit_j \times 3^{m-j} - trit_k \times 3^{m-k})$



Hashing in TSH

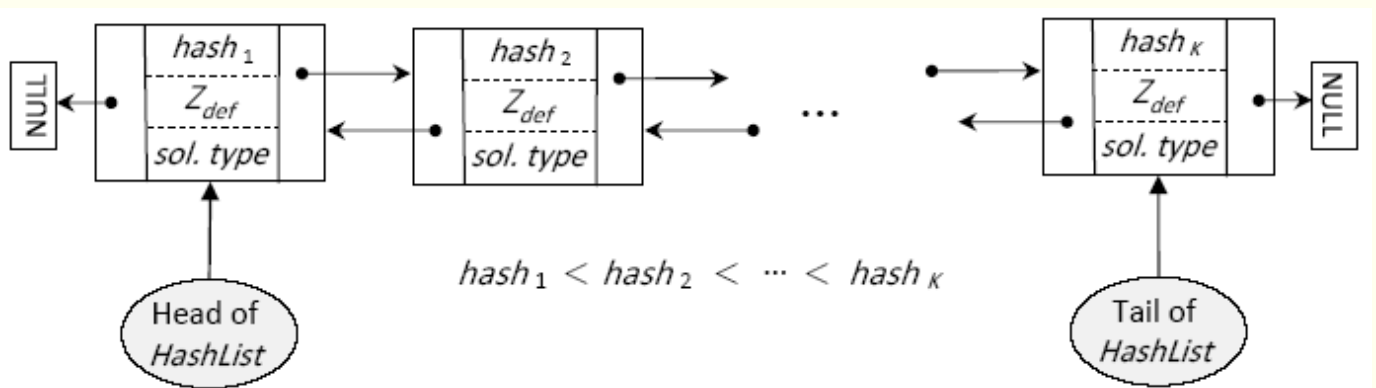
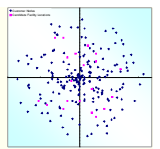
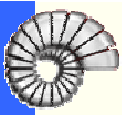


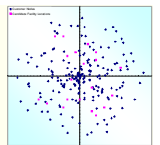
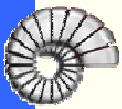
Figure 2.

The doubly linked **HashList** to store the hash values in ascending order



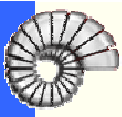
Improving the Efficiency of TSH

- **Woodruff and Zemel (1993)** have listed the following three goals an effective pair of a hash function and hash list should meet:
 1. Computation and update of the hash values should be as easy as possible.
 2. The integers generated should be in a range that requires reasonable storage and comparison effort.
 3. The *probability of collision* (also known as *hashing error*) should be low.
 - A collision occurs when the hash function returns the same hash value for two different solution vectors.

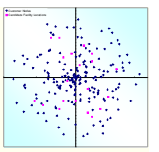


Method-2: Sequential Solution Method (SSM)

- **SSM** achieves—compared to **TSH**—considerably faster CPU times in yielding a good feasible solution to the **BFCLP**.
- In **SSM**, the facility location and protection decisions of the defender are decoupled into a pair of pure fixed charge facility location and facility interdiction with protection problems which are solved sequentially in two stages.
- The two problems solved sequentially to yield a quick and favorable solution to **BFCLP** are formulated next.



Method-2: Sequential Solution Method (SSM)



SSM Stage-1 Problem: FCLP_{def}

$$\min Z_1 = \sum_{j \in J} f_j X_j + \sum_{i \in I} \sum_{j \in J} (c_{1j} + d_{ij}) q_i U_{ij} \quad (16)$$

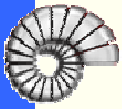
$$\text{Subject to } \sum_{j \in J} X_j \geq r + 1 \quad (17)$$

$$\sum_{j \in J} U_{ij} = 1 \quad \forall i \in I \quad (18)$$

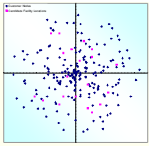
$$\sum_{i \in I} U_{ij} \leq n X_j \quad \forall j \in J \quad (19)$$

$$\sum_{k \in J_{ij}} U_{ik} \geq X_j \quad \forall i \in I, \forall j \in J \quad (20)$$

$$U_{ij}, X_j \in \{0, 1\} \quad \forall i \in I, \forall j \in J \quad (21)$$



Method-2: Sequential Solution Method (SSM)



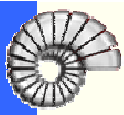
SSM Stage-2 Problem: RIMF-CE

$$\min Z_{\text{def}}(\mathbf{J}_p^*) = \sum_{j \in \mathbf{J}_p^*} b_j Y_j + \sum_{i \in I} \sum_{j \in \mathbf{J}_p^*} (c_{2j} + d_{ij}) q_i (1 - U_{ij}^*) V_{ij} \quad (22)$$

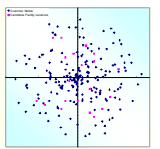
$$\text{Subject to } Y_j \in \{0, 1\} \quad \forall i \in I, \forall j \in \mathbf{J}_p^* \quad (23)$$

where \mathbf{Y} solves:

$$\max Z_{\text{att}}(\mathbf{J}_p^*) = \sum_{i \in I} \sum_{j \in \mathbf{J}_p^*} c_{2j} q_i (1 - U_{ij}^*) V_{ij} + \sum_{i \in I} \sum_{j \in \mathbf{J}_p^*} q_i d_{ij} V_{ij} \quad (24)$$



Method-2: Sequential Solution Method (SSM)



$$\text{Subject to } \sum_{j \in J_p^*} V_{ij} = 1 \quad \forall i \in I \quad (25)$$

$$\sum_{j \in J_p^*} S_j \leq r \quad (26)$$

$$S_j \leq 1 - Y_j \quad \forall j \in J_p^* \quad (27)$$

$$\sum_{i \in I} V_{ij} \leq n(1 - S_j) \quad \forall j \in J_p^* \quad (28)$$

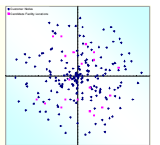
$$\sum_{k \notin J_{ij}^*} V_{ik} \leq S_j \quad \forall i \in I, \forall j \in J_p^* \quad (29)$$

$$V_{ij} \geq U_{ij}^*(1 - S_j) \quad \forall j \in J_p^* \quad (30)$$

$$S_j, V_{ij} \in \{0,1\} \quad \forall i \in I, \forall j \in J_p^* \quad (31)$$



AGENDA

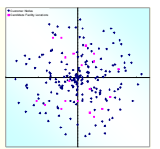


- PROBLEM DEFINITION and DESCRIPTION
- BILEVEL PROGRAMMING
- LITERATURE REVIEW
- BFCLP MODEL
- SOLUTION METHODS
- COMPUTATIONAL RESULTS
- CONCLUSION





Computational Results



□ Computing Platform

- Microsoft Visual C++ 2005
- Workstation with Intel Xeon X5460 3.16 GHz Quad-Core processor and 28 GB RAM. Each core on this computing platform's processors attains a speed of approximately 4800 MIPS (million instructions per second).
- The attacker's problem conditional on the present protection plan obtained at each node of the binary enumeration tree (**BET**) solved to optimality with Cplex 11.2.



Computational Results

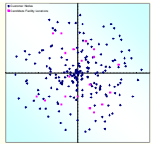


Table 3.

Random problem generation template for 48 BFCLP instances

Parameters	Values
m	{10, 15, 20, 25}
n	$10m$
r	{1, 2, 3}
(R, L)	(1000, 1500)
(cx_i, cy_i)	Let $R_i = R \times U(0,1)$, $\theta_i = 2\pi \times U(0,1)$. Then, $cx_i = \lfloor R_i \cos \theta_i \rfloor$ and $cy_i = \lfloor R_i \sin \theta_i \rfloor$.
(fx_j, fy_j)	$fx_j = -0.5L + \frac{L}{m} \times U[0, m]$ and $fy_j = -0.5L + \frac{L}{m} \times U[0, m]$
q_i	$10 + 5 \times U[0, 18]$
f_j	$10,000 + 1,250 \times U[0, 8]$
$(b_j)_{low}$	$0.5 \times f_j$
$(b_j)_{high}$	$3.0 \times f_j$
$c_{1j} = c_{2j}$	$10 + 2.5 \times U[0, 4]$
$(d_{ij})_{low}$	$0.1 \times distance(i, j)$
$(d_{ij})_{high}$	$0.2 \times distance(i, j)$



Computational Results

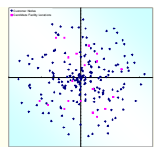


Table 4.

Comparison of TSH and SSM on instances with $(d_{ij})_{low} = 0.1 \times \text{distance}(i, j)$.

Instance	TSH				SSM			
	Min Z_{def}^*	Avg. Z_{def}^*	CPU _{min} (sec)	CPU _{avg} (sec)	Z_{def}^{SSM}	CPU (sec)	PD_{best} (%)	PD_{avg} (%)
(10,1,lo)	383,583	383,583	0.3	0.6	402,397	0.3	4.90	4.90
(10,1,hi)	465,833	468,419	3.6	20.6	562,647	0.3	20.78	20.12
(10,2,lo)	383,583	383,583	0.3	0.5	426,613	0.2	11.22	11.22
(10,2,hi)	465,833	488,041	0.3	14.3	666,113	0.2	42.99	36.49
...								
(25,2,lo)	917,001	917,001	21.0	227.9	917,001	3.2	0.00	0.00
(25,2,hi)	1,153,094	1,153,094	3,318.8	4,775.2	1,247,001	3.2	8.14	8.14
(25,3,lo)	917,001	917,001	49.2	237.9	917,001	5.3	0.00	0.00
(25,3,hi)	1,240,523	1,244,311	8,390.5	10,513.5	1,247,001	5.3	0.52	0.22
Average	718,542	727,791	553.8	882.7	789,041	1.5	11.53	10.11



Computational Results

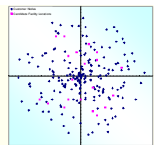
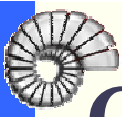


Table 5.

Comparison of TSH and SSM on instances with $(d_{ij})_{low} = 0.2 \times \text{distance}(i, j)$.

Instance	TSH				SSM			
	Min Z_{def}^*	Avg. Z_{def}^*	CPU _{min} (sec)	CPU _{avg} (sec)	Z_{def}^{SSM}	CPU (sec)	PD_{best} (%)	PD_{avg} (%)
(10,1,lo)	625,715	625,715	0.6	3.8	625,715	0.4	0.00	0.00
(10,1,hi)	706,085	736,985	1.3	17.7	860,860	0.2	21.92	16.81
(10,2,lo)	625,715	625,715	0.6	1.0	625,715	0.2	0.00	0.00
(10,2,hi)	843,632	853,590	12.6	53.4	875,965	0.2	3.83	2.62
...								
(25,2,lo)	1,425,903	1,547,308	35.5	504.3	1,450,013	2.0	1.69	-6.29
(25,2,hi)	1,680,009	1,706,407	2004.3	3119.5	1,944,672	2.0	15.75	13.96
(25,3,lo)	1,425,903	1,508,689	309.3	1268.6	1,450,013	3.8	1.69	-3.89
(25,3,hi)	1,803,353	1,869,447	957.1	11287.1	2,150,013	3.7	19.22	15.01
Average	1,081,253	1,120,756	276.3	980.9	1,170,775	1.1	7.82	4.07



Computational Results

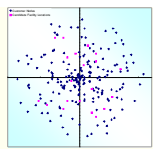


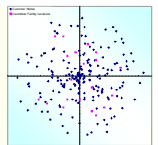
Table 6.

Change of the defender's objective value with respect to problem parameters

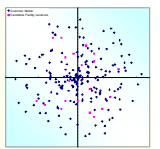
	$(d_{ij})_{low}$		$(d_{ij})_{high}$		Grand Avg.
	$(b_j)_{low}$	$(b_j)_{high}$	$(b_j)_{low}$	$(b_j)_{high}$	
$r = 1$	631,468	739,834	979,986	1,082,604	860,027
$r = 2$	631,468	818,270	979,986	1,214,888	911,153
$r = 3$	631,468	858,747	979,986	1,250,072	936,578
Grand Avg.	718,547		1,081,253		899,898



Computational Results



- The columns of Table 6 corresponding to $(b_j)_{high}$ reveal that as r increases the Defender's objective value Z_{def} takes on larger values.
 - This is a consequence of the demand-weighted traveling costs increased by extra interdictions.
 - However, that is true only when the protection costs are high and the cost of protecting added facilities exceeds the cost of capacity expansions induced by extra interdictions.
 - When the protection costs are low, on the other hand, the defender can afford to protect all the opened facilities, and the value of r does not have any effect on the average Z_{def} .
 - It is also expected that Z_{def} is higher when d_{ij} is high.



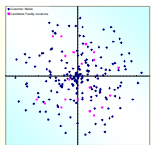
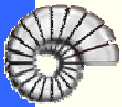
AGENDA

- PROBLEM DEFINITION and DESCRIPTION
- BILEVEL PROGRAMMING
- LITERATURE REVIEW
- BFCLP MODEL
- SOLUTION METHODS
- COMPUTATIONAL RESULTS
- CONCLUSION



By Deniz Aksen on July 12th 2010 in Lisbon

53



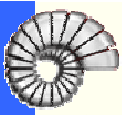
Conclusion

The main contribution of the paper is:

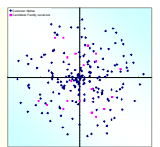
- the simultaneous consideration of facility location and protection decisions of the defender as well as the interdiction decision of the attacker *for the first time in the literature*.
- Moreover, the number of facilities opened is a decision variable as is the case in the well-known uncapacitated facility location problem (**UFLP**).

By Deniz Aksen on July 12th 2010 in Lisbon

54

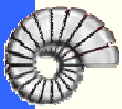


Conclusion

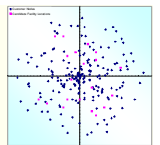


We developed two heuristic methods to solve the **BFCLP**.

1. **TSH** : a probabilistic TS algorithm with a hash list which records the objectives and hash values of all solutions explored to prevent **cycling**.
 - The use of **hashing** helps avoid cycling and boosts the efficiency of the tabu search by minimizing the number of objective function evaluations.
2. **SSM (sequential solution method)** : sequentially rather than concurrently.
 - First, a **UFLP** is solved disregarding the attacker, and an optimal subset of unprotected facility locations is obtained.
 - Given this optimal subset, the defender determines in a bilevel programming framework which facilities to protect against the attacker to minimize his own post-attack costs.

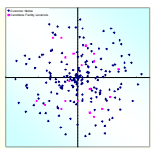
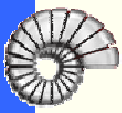


Conclusion



The results obtained on a test bed of 48 randomly generated instances indicate that:

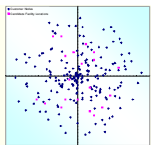
- **TSH** outperforms the **SSM** method in solution quality, but requires much longer CPU times.
 - The objective value of the defender found by **SSM** is on average **9.67% inferior** to the minimum objective value obtained in a 5-run multi-start implementation of **TSH**.
 - One can choose either of **TSH** and **SSM** depending on the desired accuracy and urgency of the solution to the problem at hand.



Conclusion

There can be two extensions of this work.

1. Formulating the same BFCLP model such that partial interdiction of facilities is allowed.
 - This means that facilities will not be rendered totally inoperative after an attack, but will continue to provide service with less than full capacity depending on the degree of interdiction.
2. Considering partial protection of facilities for a better utilization of the limited protection resources.



Thanx for your listening!

All critiques, comments,
and questions are candidly
appreciated!

