CHEMICAL ENGINEERING TRANSACTIONS
VOL. 103, 2023
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Petar S. Varbanov, Panos Seferlis, Yee Van Fan, Athanasios Papadopoulos

ISBN 979-12-81206-02-1; **ISSN** 2283-9216
DOI: 10.3303/CET23103046

Stackelberg-Leontief Model for Optimal Defense of Industrial Sites

Kathleen B. Aviso[a,*], Albert Lamberte[b], Joost R. Santos[c], Raymond R. Tan[a], John Frederick D. Tapia[a], Krista Danielle S. Yu[b]

[a]Department of Chemical Engineering, De La Salle University, Manila, Philippines
[b]School of Economics, De La Salle University, Manila, Philippines
[c]Department of Engineering Management and Systems Engineering, The George Washington University, D.C., USA
kathleen.aviso@dlsu.edu.ph

Large industrial facilities offer attractive targets to malicious attacks by terrorists. These attacks can trigger cascading failures, capitalizing on the high levels of integration among the components of highly optimized industrial systems. Any defensive measure will generally be resource-constrained and may be difficult to conceal perfectly. In this work, a novel hybrid Stackelberg-Leontief model is developed for planning optimal defensive measures in industrial sites against targeted attacks. The core of the model represents the industrial site with a physical input-output model, which is embedded in a leader-follower game. The defender acts as the leader, who selects defensive measures to implement from a suite of options. Each selected defensive measure incurs a fixed cost regardless of whether an attack occurs or not; however, the defensive measure also mitigates the economic damage caused by any attack. The attacker acts as the follower, who selects an attack strategy based on a set of options with damage coefficients; the attacker is also resource-constrained and needs to optimize the attack while considering the defensive measures put in place. The defender anticipates the attacker's strategic behavior in developing the defense strategy, resulting in a Stackelberg game formulated as a bilevel mixed integer linear program. The model is illustrated with a didactic case study. In both scenarios considered, the Stackelberg strategy is for the defender to protect the RO module with the attacker targeting the CHP and RO module (Scenario 1) or the CHP, Chiller, and RO module (Scenario 2). This results in the lowest possible mitigation cost (100 USD/h) and a 26 – 27 % increase in the leader's objective relative to a no defense strategy.

1. Introduction

Large industrial facilities like oil refineries and power plants make attractive targets for terrorists. Threats include physical attacks on plants and personnel (Lee, 2022) as well as cyberattacks (Stergiopoulos et al., 2020). As a result, there has been extensive research on vulnerability analysis, security countermeasure planning, and post-attack emergency response for industrial plants (Bajpai and Gupta, 2005). The presence of an intelligent and malicious attacker requires an approach that is fundamentally different from risk analysis and management tools used for natural disasters and industrial accidents (Labib, 2015). Game theoretic models are needed to effectively model the non-cooperative interaction between the attacker and the defender, each of whom seeks a strategy that optimizes its objective (Brown et al., 2006).

A bilevel optimization model consists of a lower-level Mathematical Program (MP) embedded as a constraint in an upper-level MP (Bracken and McGill, 1973). They are used for some classes of chemical engineering design problems, and present computational challenges not encountered with conventional MPs (Clark and Westerberg, 1990). In addition to deterministic algorithms specifically tailored for narrow classes of bilevel MPs, there has been extensive work on evolutionary (Sinha et al., 2018) and fuzzy (Zhang et al., 2016) algorithms to find heuristic solutions. Algorithms for handling bilevel mixed-integer MPs take advantage of the discrete nature of some player decisions (Kleinert et al., 2021). Bilevel MPs are often used to represent static Stackelberg games, which involve the non-cooperative interaction between a leader and a follower

Paper Received: 12 April 2023; Revised: 04 July 2023; Accepted: 27 July 2023
Please cite this article as: Aviso K.B., Lamberte A., Santos J.R., Tan R.R., Tapia J.F.D., Yu K.D.S., 2023, Stackelberg-Leontief Model for Optimal Defense of Industrial Sites, Chemical Engineering Transactions, 103, 271-276 DOI:10.3303/CET23103046

(Kalashnikov et al., 2015). The leader seeks a Stackelberg strategy that optimizes its payoff in anticipation of a rational reaction from the follower. The latter, in turn, optimizes its own payoff in reaction to parameters determined by the leader's prior decision. Bilevel and multi-level MPs have been used for planning the defense of critical infrastructure (Brown et al., 2006). The impact on unprotected system components needs to be considered (Scaparra and Church, 2008). The problem generally involves the cost-effective allocation of potentially limited defense resources (Villa et al., 2017). It is also necessary to mitigate ripple effects that can occur in systems with interdependent components (Aliakbarian et al., 2015).

Risk analysis in process industries should account for the potential cascading effects of disruptions (Sano et al., 2020). Input-output (IO) modeling was first proposed as a computational framework for representing a network of economic sectors with a system of linear algebraic equations (Leontief, 1936). When applied at the level of a single firm, it is known as enterprise IO modeling (Lin and Polenske, 1998). The fundaments of IO models are firmly established and widely used for economic analysis (Miller and Blair, 2009), while variants used for sustainability-oriented uses (Tan et al., 2019). Environmentally-extended IO models have been used to quantify the footprints of industrial sectors (Khongprom et al., 2020) or countries (Wang et al., 2020). IO models have also been used to quantify the ripple effects of disruptive events such as terrorist attacks (Santos and Haimes, 2004) and disease outbreaks (Pichler and Farmer, 2022). MP models based on the IO framework can also be used to optimize damage control measures after adverse events (Jiang and Haimes, 2004). The same approach has also been extended to enterprise IO models (Kasivisvanathan et al., 2013). However, such single-level MP models are not game theoretic. They cannot be used effectively to plan protective measures against deliberate attacks since an intelligent attacker can react to and bypass the defenses.

This work addresses this research gap by developing a novel hybrid Stackelberg-Leontief model for the optimal defense of industrial sites. The Stackelberg game framework adequately models the interaction between a defender and attacker, while the network structure of the industrial facility is represented by an enterprise IO model. The model is formulated as a Bilevel Mixed Integer Linear Program (BMILP) whose solution gives the defender's Stackelberg strategy. The rest of this paper is organized as follows. Section 2 gives the formal problem statement. Section 3 shows the BMILP formulation. Section 4 illustrates the model and algorithm with a polygeneration plant case study. Finally, Section 5 states the conclusions and recommends directions for future research.

2. Formal problem statement

To lay the foundation for the subsequent BMILP problem formulation, the formal problem statement, scope, and associated assumptions are described as follows:

- The focus will be on a given industrial facility that consists of N interdependent process units;
- The industrial facility uses and generates M (raw material, intermediate, and product) streams;
- The defender of the industrial facility, acting as the leader, has the option to protect process units, mitigating potential inoperability (fractional loss of capacity) resulting from an attack;
- The protective measures entail incremental cost, which makes the defender's strategy inherently resource-constrained;
- The attacker, acting as the follower, has the option to attack process units to cause a direct loss of inoperability in selected targets as well as indirect inoperability due to interdependency effects;
- The attacker's strategy is also inherently resource-constrained;

Generally, the attacker seeks to maximize damage to the defender while the defender seeks to minimize damage resulting from an attack. Specifically, the defender seeks to maximize profit (or minimize cost) in case of attack, under the assumption that the attacker uses an optimized attack strategy in response to its transparent defensive strategy. The problem is to determine the leader's Stackelberg strategy of identifying which process unit to defend to maximize the industrial plant's productivity while knowing the rational reaction of the follower whose objective is to maximize the damage done to the industrial facility based on selected attack strategies. This solution is the defender's Stackelberg strategy. Decisions to defend and attack are assumed to be discrete. Linearity assumptions are used so that interdependencies within the industrial plant conform to the IO framework.

3. Bilevel model formulation

The leader's objective function is to maximize the productivity of the system (Eq(1)) where c_i is the price associated to stream i, y_i is the final demand of stream i, α_j is the defense cost coefficient for process j, and q_j is a binary variable which indicates the leader's defense strategy. The leader's decision is to select its defense strategy within an exogenously defined resource limit, L (Eq(2)). The binary variable q_j takes a value of 1 if the

leader defends process unit j and 0 otherwise (Eq(3)). The follower's objective is to maximize the damage caused to the system (Eq(4)) where a_{jj} is the output of stream j in process j, d_j is the attack damage to process j, r_j is a binary variable which indicates the follower's attack, p_j the defense mitigation for process j, and s_j is the conjunction between the attack and defense strategies. It is subject to stream balance requirements (Eq(5)) where a_{ij} is the input or output of stream i in process j and x_j is the total output of process j. The net output of each stream i, y_i, should not be more than the baseline output y_i^o (Eq(6)). The total output of process j, x_j, is potentially reduced due to damages from an attack (Eq(7)). The damage can be reduced if the leader has chosen to defend the process unit which was attacked, variable s_j represents the conjunction of the attack and defense strategies (Eq(8) – Eq(10)) which takes a value of 1 if the leader defends the same process unit as what was attacked, and a value of 0 otherwise. Eq(11) – Eq(13) define the binary variables.

$$\max \sum_{i=1}^{N} c_i y_i - \sum_{j=1}^{M} \alpha_j q_j \tag{1}$$

Subject to:

$$\alpha_j q_j \leq L \qquad \forall j \tag{2}$$

$$q_j \in \{0,1\} \qquad \forall j \tag{3}$$

$$\max \sum_{j}^{M} c_j a_{jj} \left(d_j r_j - p_j s_j\right) \tag{4}$$

Subject to:

$$y_i = \sum_{j=1}^{M} a_{ij} x_j \qquad \forall i \tag{5}$$

$$y_i \leq y_i^{\circ} \qquad \forall i \tag{6}$$

$$x_j \leq x_j^{\circ} - d_j r_j + p_j s_j \qquad \forall j \tag{7}$$

$$s_j \leq q_j \qquad \forall j \tag{8}$$

$$s_j \leq r_j \qquad \forall j \tag{9}$$

$$s_j \geq q_j + r_j - 1 \qquad \forall j \tag{10}$$

$$q_j \in \{0,1\} \qquad \forall j \tag{11}$$

$$r_j \in \{0,1\} \qquad \forall j \tag{12}$$

$$s_j \in \{0,1\} \qquad \forall j \tag{13}$$

This BMILP cannot be solved directly using conventional solvers, but requires specialized algorithms developed for bilevel MPs (Kleinert et al., 2021). A small-scale case study illustrates its use in Section 4.

4. Polygeneration plant case study

Polygeneration systems are known for being highly integrated and efficient, making them more susceptible to cascading failures. This case study uses the data of the polygeneration plant described by Kasivisvanathan et al. (2013). The plant consists of a stand-alone boiler, a combined heat and power (CHP) module, an electric chiller, and a reverse osmosis (RO) module. It produces heat, power, cooling, and treated water. The purchased inputs are fuel oil and fresh water. The waste streams (combustion emissions and RO reject water) are not shown. The balanced process matrix for normal operations is shown in Table 1, where positive and negative entries denote stream outputs and inputs. Note that the process units are mutually interdependent and that the sum of each row gives the net output of the system. The unit prices of the streams are given in Table 2. The hourly operating profit of the plant (excluding capital recovery) can be computed by multiplying the net outputs by the respective unit prices and then taking the total.

Table 1: Balanced process matrix (Kasivisvanathan et al., 2013)

	Boiler	CHP module	Chiller	RO module	Net output
Heat (kW)	6,882	18,118	0	0	25,000
Power (kW)	–69	12,079	–1,600	–410	10,000
Cooling (kW)	0	0	8,000	0	8,000
Treated water (L/s)	–4	–33	0	137	100
Fuel oil (L/s)	–0.23	–1.81	0	0	–2.04
Fresh water (L/s)	0	0	0	–342	–342

Table 2: Unit prices (Kasivisvanathan et al., 2013)

	Unit price
Heat (USD/kWh)	0.05
Power (USD/kWh)	0.12
Cooling (USD/kWh)	0.06
Treated water (USD/L)	0.025
Fuel oil (USD/L)	0.90
Fresh water (USD/L)	0.001

It is assumed that the defender and attacker have one (defense or attack) decision for each process unit of the polygeneration plant. The corresponding exogenously defined parameters are shown in Table 3. The attacker's inoperability factors give the induced inoperability or fractional loss of capacity in the targeted process unit. The defender's inoperability mitigations serve to blunt any attack by reducing this induced inoperability. However, this benefit comes at a price as defined by the mitigation cost. These parameters may be obtained from expert estimates or historical data. The total mitigation cost reduces the plant's profit even if an attack does not occur.

Table 3: Defender and attacker parameters

	Boiler	CHP module	Chiller	RO module
Defender's inoperability mitigation factor	0.2	0.2	0.1	0.1
Defender's mitigation cost (USD/h)	250	400	120	100
Attacker's inoperability factor	0.4	0.3	0.5	0.2

Table 4: Alternative defense and attack strategies in Scenario 1

Solution	Defense strategy vector	Attack strategy vector	Defense cost (USD/h)	Defender's objective (USD/h)	Attacker's objective (USD/h)
1	(0, 0, 0, 0)	(0, 1, 0, 1)	0	3,822.99	2,900.84
2*	(0, 0, 0, 1)	(0, 1, 0, 1)	100	4,827.95	1,667.84
3	(0, 0, 1, 0)	(0, 1, 0, 1)	120	3,702.99	2,900.84
4	(0, 0, 1, 1)	(0, 1, 0, 1)	220	4,707.95	1,667.84
5	(0, 1, 0, 0)	(0, 1, 0, 1)	400	2,127.18	2,610.95
6	(0, 1, 0, 1)	(0, 1, 0, 1)	500	3,132.14	1,377.95
7	(0, 1, 1, 0)	(0, 1, 0, 1)	520	2,007.18	2,610.95
8	(1, 0, 0, 0)	(0, 1, 0, 1)	250	3,572.99	2,900.84
9	(1, 0, 0, 1)	(0, 1, 0, 1)	350	4,577.95	1,667.84
10	(1, 0, 1, 0)	(0, 1, 0, 1)	370	3,452.99	2,900.84
11	(1, 0, 1, 1)	(0, 1, 0, 1)	470	4,457.95	1,667.84

In the first scenario, the attacker is more resource-constrained than the defender. The former can attack at most two process units, while the latter can afford a defense cost of up to 600 USD/h, which is exogenously defined. This small-scale problem can be solved by enumerating all the defender's feasible defensive strategies and then solving the attacker's lower-level MILP problem to determine its rational response. Given a binary decision for each process unit, there are sixteen possible defensive strategies, but five of these exceed the defense budget (not shown in Table 4). The defender can then evaluate its profit or cost for each of these potential attacks and select its Stackelberg strategy based on that criterion. Due to combinatorial explosion, this solution strategy is not viable for large-scale problems; alternative algorithms will be needed for such cases (Kleinert et al., 2021). Table 4 lists the defender's eleven feasible defensive strategies and the

attacker's rational response to each of them, where the comma-separated binary values in Columns 2 and 3 correspond to the following units of the plant: (i) boiler, (ii) CP module, (iii) Chiller, and (iv) RO module. A value of 1 means the unit is chosen to be defended (or attacked), while a value of 0 means otherwise. Both players' objective functions are also shown. The Stackelberg strategy is given by Solution 2, where the defender protects the RO module to elicit an attack response that targets both the CHP and RO modules. This strategy gives an hourly profit of 4,827.95 USD/h. The defender opts to spend only 100 USD/h for defensive measures, which is well below its 600 USD/h limit. The results are non-monotonic due to the interdependence of process units. The over-all objective is thus a consequence of direct and indirect effects of the attack and the mitigation strategy.

Table 5: Alternative defense and attack strategies in Scenario 2

Solution	Defense strategy vector	Attack strategy vector	Defense cost (USD/h)	Defender's objective (USD/h)	Attacker's objective (USD/h)
1	(0, 0, 0, 0)	(0, 1, 1, 1)	0	3,678.99	3,140.84
2*	(0, 0, 0, 1)	(0, 1, 1, 1)	100	4,683.95	1,907.84
3	(0, 0, 1, 0)	(0, 1, 1, 1)	120	3,587.79	3,092.84
4	(0, 0, 1, 1)	(0, 1, 1, 1)	220	4,592.75	1,859.84
8	(1, 0, 0, 0)	(0, 1, 1, 1)	250	3,428.99	3,140.84

In the second scenario, the defender is more resource-constrained than the attacker. The latter now has the resources to mount an attack on up to three process units, while the former's budget for defense is reduced to 250 USD/h. The available strategies are listed in Table 5. Once again, the defender's Stackelberg strategy is to protect the RO module, eliciting a three-pronged attack on the CHP module, chiller, and RO module. This solution gives a profit of 4,683.95 USD/h and requires a defensive strategy that, at 100 USD/h, is still well below the budget limit. Both scenarios also illustrate the possibility of counterintuitive solutions, where the best option for the defender may be to leave parts of the system unprotected to deliberately divert the attacker's strategy while also saving on defensive cost. These effects can be investigated through sensitivity analysis and by applying this model to larger-scale systems.

5. Conclusions

A game theoretic optimization model has been developed in this work for optimal defense of industrial facilities. The model is based on a hybrid Stackelberg-Leontief framework and is formulated as a BMILP. The defender plays the role of the leader, who allocates limited defense resources in anticipation of an attack whose ripple effects can be predicted using the EIO framework. The attacker plays the role of the follower, and implements an optimized attack in response to the leader's defense strategy. The modelling framework is illustrated with a polygeneration plant case study wherein the Stackelberg strategy is for the defender to protect the RO module while the attacker targets the CHP and RO module (Scenario 1) or the CHP, Chiller, and RO module (Scenario 3). The Stackelberg strategy results in a 26 – 27 % increase in the leader's objective in comparison to a no defense strategy. In both scenarios considered, the defender chooses the strategy with the lowest mitigation cost while the attacker maximizes its opportunities to launch an attack. This demonstrates that the best defense strategy can be counterintuitive.

Future work can explore different extensions of this work. Sensitivity analysis can be performed to analyze the effects of price changes in products and defense costs. Impact on population mentality and working attitude can also be considered. The framework can be readily applied with minimal mathematical modification to input-output models of industrial parks, transportation networks, and even entire economies. Deterministic or metaheuristic solution algorithms can also be developed for solving this class of game theoretic models.

Nomenclature

Parameters:
α_j – defense cost coefficient for process unit j
a_{ij} – input or output of stream i in process unit j
c_i – price associated with stream i
d_j – attack damage for process unit j
L – defense resource limit
p_j – defense mitigation for process unit j
x_j° - baseline total output for process unit j
y_i° - baseline final demand for stream i

Variables:
q_j – binary variable indicating leader's defense
r_j – binary variable of follower's attack strategy
s_j – conjunction of attack/defense strategy
x_j – total output of process unit j
y_i – final demand for stream i

Acknowledgments

We acknowledge the support from the National Science Foundation (Award #1832635), Fulbright US Scholar Program, and Philippine-American Educational Foundation (PAEF).

References

Aliakbarian N., Dehghanian F., Salari M., 2015, A bi-level programming model for protection of hierarchical facilities under imminent attacks. Computers and Operations Research, 64, 210–224.

Bajpai S., Gupta J.P., 2005, Site security for chemical process industries. Journal of Loss Prevention in the Process Industries, 18, 301–309.

Bracken J., McGill, J.T., 1973, Mathematical programs with optimization problems in the constraints. Operations Research, 21, 37–44.

Brown G., Carlyle M., Salmerón J., Wood K., 2006, Defending critical infrastructure. Interfaces, 36, 530–544.

Clark P.A., Westerberg, A.W., 1990, Bilevel programming for steady-state chemical process design—I. Fundamentals and algorithms. Computers and Chemical Engineering, 14, 87–97.

Jiang P., Haimes Y.Y., 2004, Risk management for Leontief-based interdependent systems. Risk Analysis, 24, 1215–1229.

Kalashnikov V.V., Dempe S., Pérez-Valdés G.A., Kalashnykova N.I., Camacho-Vallejo J.-F., 2015, Bilevel programming and applications. Mathematical Problems in Engineering, 2015, 310301.

Kasivisvanathan H., Barilea I.D.U., Ng D.K.S., Tan R.R., 2013, Optimal operational adjustment in multi-functional energy systems in response to process inoperability. Applied Energy, 102, 492–500.

Khongprom P., Champanoi S., Suwanmanee U., 2020, An input-output approach for environmental life cycle assessment of cement production. Chemical Engineering Transactions, 81, 1345–1350.

Kleinert T., Labbe M., Ljubic I., Schmidt M., 2021, A survey on mixed-integer programming techniques in bilevel optimization. EURO Journal of Computational Optimization, 9, 100007.

Labib A., 2015, Learning (and unlearning) from failures: 30 years on from Bhopal to Fukushima an analysis through reliability engineering techniques. Process Safety and Environmental Protection, 97, 80–90.

Lee C.-Y., 2022, Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure. Energy Research & Social Science, 87, 102459.

Leontief W.W. 1936, Quantitative Input and Output Relations in the Economic Systems of the United States. Review of Economics and Statistics, 18, 105–125.

Lin X., Polenske K.R., 1998, Input—output modeling of production processes for business management. Structural Change and Economic Dynamics, 9, 205–226.

Miller, R.E., Blair, P.D., 2009, Input-output Analysis: Foundations and Extensions, 2nd ed., University Press, Cambridge, UK.

Pichler A., Farmer J.D., 2022, Simultaneous supply and demand constraints in input–output networks: the case of COVID-19 in Germany, Italy, and Spain. Economic Systems Research, 34, 273–293.

Sano K., Koshiba Y., Ohtani H., 2020, Risk assessment and risk reduction of an acrylonitrile production plant. Journal of Loss Prevention in the Process Industries, 63,104015.

Santos J.R., Haimes Y.Y., 2004, Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures. Risk Analysis, 24, 1437–1451.

Scaparra M.P., Church R.L., 2008, A bilevel mixed-integer program for critical infrastructure protection planning. Computers and Operations Research, 35, 1905–1923.

Sinha A., Malo P., Deb K., 2018, A review on bilevel optimization: From classical to evolutionary approaches and applications. IEEE Transactions of Evolutionary Computation, 22, 276–295.

Stergiopoulos G., Gritzalis D.A., Limnaios E., 2020, Cyber-attacks on the oil gas sector: A survey on incident assessment and attack patterns. IEEE Access, 8, 128440–128475.

Tan R.R., Aviso K.B., Promentilla M.A.B., Yu K.D.S., Santos J.R., 2019, Input-output Models for Sustainable Industrial Systems: Implementation Using LINGO, Springer Nature, Singapore.

Villa V., Reniers G.L.L., Paltrinieri N., Cozzani V., 2017, Development of an economic model for counter terrorism measures in the process-industry. Journal of Loss Prevention in the Process Industries, 49, 437–460.

Wang, X.-C., Klemeš, J.J., Varbanov, P.S., 2020, Water-energy-carbon nexus analysis of the EU27 and China. Chemical Engineering Transactions, 81, 469–474.

Zhang G., Han J., Lu J., 2016, Fuzzy bi-level decision-making techniques: A survey. International Journal of Computational Intelligence Systems, 9, 25–34.