Playing chemical plant protection game with distribution-free uncertainties

Reference:
Zhang Laobing, Reniers Genserik, Qiu Xiaogang.- Playing chemical plant protection game w ith distribution-free uncertainties
Reliability engineering and system safety - ISSN 0951-8320 - 191(2019), p. 1-11
Full text (Publisher's DOI): https://doi.org/10.1016/J.RESS.2017.07.002

Playing Chemical Plant Protection Game with Distribution-free Uncertainties

Laobing Zhang[a], Genserik Reniers[a,b,c,*] , Xiaogang Qiu[d]

[a] Faculty of Technology, Policy and Management, Safety and Security Science Group (S3G), TU Delft, 2628 BX Delft, The Netherlands.

[b] Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), University Antwerp, 2000 Antwerp, Belgium.

[c] CEDON, KULeuven, Campus Brussels, 1000, Brussels, Belgium

[d] Research Center of Computational Experiments and Parallel System Technology, College of Information System and Management, National University of Defense Technology, Changsha 410073, China

(*) Author to whom correspondence should be addressed.

tel. (+31)15 27 83749

e-mail: G.L.L.M.E.Reniers@tudelft.nl

Abstract

A common criticism on game theoretic risk analysis of security threats is that it requires quantitative parameters of both the defender and the attacker, whereby the parameters of the attackers are difficult to estimate. In the present paper, a game theoretic model for chemical plant protection, being able to deal with defender's distribution-free uncertainties on the attacker's parameters (Interval CPP Game), is proposed. The Interval CPP Game only requires the intervals that the attacker's parameters will locate in, instead of the exact number. Two algorithms are developed, namely the Interval Bi-Matrix Game Solver (IBGS) and the Interval CPP Game Solver (ICGS), for solving general bi-matrix games with interval payoff uncertainties and special for solving interval CPP games, respectively. Both two algorithms are based on mixed integer linear programming (MILP). Theoretic analysis as well as case study show that the defender's uncertainties on the attacker's parameters would reduce her equilibrium payoff.

Highlights

1) First developed chemical plant protection game which is able to deal with interval inputs;

2) Algorithms for solving general bi-matrix game with interval payoff uncertainties as well as special for solving interval CPP game are proposed.

Keywords

Chemical plant protection; game theory; distribution-free uncertainty

1. Introduction

The New York 9/11 attack shift the risk analysis paradigm from non-intentional disasters (i.e. natural disasters) to intentionally caused events, and the recently happened terrorism attack at Paris and Brussel furthermore stimulated this shift. Chemical industry, which normally associated with extreme producing conditions as well as dangerous materials, is listed as one of the 13 critical infrastructures by the U.S. government [1] [2]. Though some risk analysis projects concluded that a malicious attack on some chemical sites might cause millions of casualties as well as irreversible environmental pollution [3], the protection of chemical plants (clusters) has not drawn enough attention yet [4].

The ANSI/API Standard 780 Security Risk Assessment (SRA) methodology [5], which is currently the extensively employed security risk analysis framework in the chemical industries, has its drawbacks of not considering the intelligent interactions between the defender and the attacker. Cox [6] pointed out numbers of limitations of SRA methodologies which are based on the "$risk = TVC$" formula, such as being not adequate for resources allocation, being not able to deal with intelligent attackers etc. Cox [6, 7] emphasised in his paper that intelligent interactions between the defender and attacker are the key properties of security risk assessment procedure, furthermore, game theory shows a great potentiality to be used in security risk assessment.

In chemical security domain, Reniers and co-authors [8-13] systematically studied cooperation on safety/security investment within chemical clusters, in a game theoretic approach. In their models, different chemical plants in one cluster share similar threats due the existence of domino effects, and their games focus on analysing whether the stakeholders of plants should invest on safety/security or not. Talarico et al. [14] proposed a game theoretic model named “MISTRAL” for protecting multi-modal chemical transportation network. Zhang and Reniers [15] developed a simultaneous game-theoretic model to protect chemical plants from terrorist attacks (CPP game), and later on they extended their model to sequential games played by a first moving defender and several types of following attackers [16]. Feng et al. [17] employed a simultaneous and complete information game theoretic model to study allocation of defensive resources for protecting multiple chemical facilities

in a city. All these mentioned game theoretic models for protecting chemical plants ask for quantitative inputs, such as the probabilities of intrusion, consequences of an attack etc. However, these quantitative inputs are practically difficult to obtain, which makes these models difficult to be used in realistic cases.

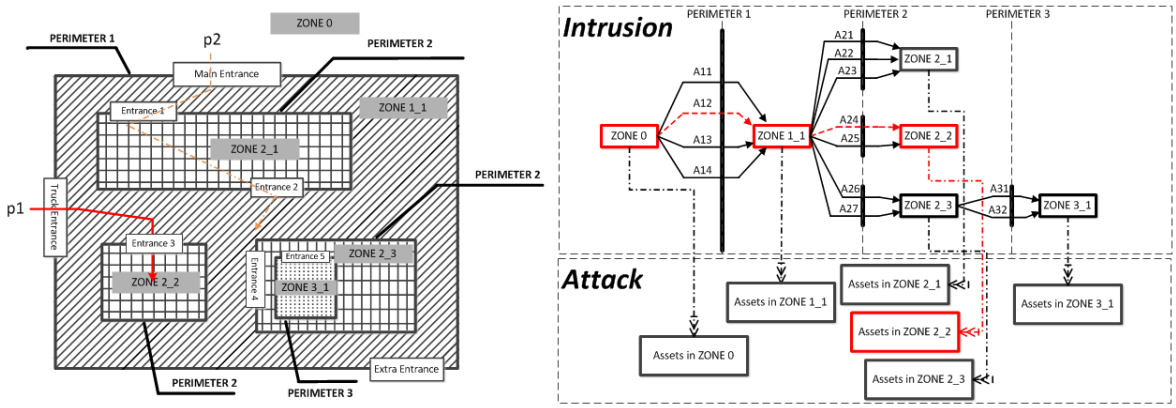
Though the exact numerical inputs are difficult to obtain, the intervals of them are relatively easier to estimate. In this paper, the previously proposed chemical plant protection (CPP) game [15, 16] is extended to dealing with distribution-free/interval inputs. In the remainder of this paper, Section 2 gives a brief introduction of the Chemical Plant Protection (CPP) game. Section 3 is the main body of this paper, in which the CPP game is extended to interval CPP game, algorithms for solving general interval bi-matrix games as well as special for solving interval CPP game are both proposed. A case study is conducted in Section 4 to illustrate how the models and algorithms proposed in these paper work. Finally, conclusions are drawn in Section 5.

2. Baseline models

This paper is a follow up research of two previous research paper, namely the CPP game paper [15], and the Bayesian Stackelberg CPP game paper [16]. In this section, the general intrusion detection approach in chemical plants, and the game theoretic model developed based on this intrusion detection approach, are briefly introduced. More details can be found in Zhang and Reniers [15, 16] and Reniers et al.[18].

2.1. General Intrusion Detection Approach in Chemical Plants

Figure 1(a) shows the multi-layer physical intrusion detection approach in the chemical plants. In such a system, different layers of perimeter divide the area into different levels of zones, and each perimeter is assigned with one or more accesses. A “typical” in this system is defined as a summation of technological items constituting a security barrier [18]. Thus in figure 1(a), the accesses assigned on each perimeters and the different zones are “typical”, since the defender can implement counter-terrorism-measures on these parts.



(a) Multi-layers Protection System

(b) Intrusion Attack Procedure

Figure 1. General Physical Intrusion Detection system in a chemical plant

Figure 1(b) shows the intrusion attack procedure, from the attacker's perspective, and it is based on figure 1(a). The attacker would, firstly, decide which target to attack, secondly, decide how to reach the target, and thirdly, decide what attack scenario to use. The red (also dash) line in figure 1(b) (reflects the p1 in figure 1(a)) represents the attacker's behaviour as he[a] will attack a target located in zone 2_2 (second subzone in zone level 2), and he will start from zone level 0 (i.e. the outside of the plant), pass perimeter 1 from the track entrance, reaching zone level 1, and then pass perimeter 2 from the entrance 3, reaching zone level 2.

The intruder is assumed that he would never step into the same level of zone twice. For example, the p2 in figure 1(a) is excluded due to this assumption, since if the intruder follows p2, he would step into zone level 1 twice. This assumption is reasonable due to the fact that otherwise the intruder will pass more "typicals", increasing the probability of being detected. This assumption is also necessary: with this assumption, the analysis of the attacker's intrusion path becomes easier, since the complex paths are excluded (e.g., p2 in figure 1(a)).

Based on above analysis, the probability of successfully reaching the target can be calculated by formula (1). In which I denotes the zone level that the target locates in; P^z denotes the probability of successfully passing different levels of zones; P^p denotes the probability of passing the different layers of perimeters.

[a] In security game, we normally denote the defender as she/her/her, while denote the attacker as he/him/his.

$$P = \prod_{i=0}^{I} P_i^z \cdot \prod_{j=1}^{I} P_j^p. \quad (1)$$

2.2. Chemical Plant Protection Game (CPP Game)

The Chemical Plant Protection (CPP) game is played by two players: the industrial defender and the potential attacker (whereby different types, e.g., terrorists, activists etc., are possible).

The defender's pure strategy is defined as combination of Security Alert Levels (SAL) on each "typicals", as formulated in formula (2). The attacker's pure strategy is defined as combination of the attack target, the intrusion path, and the attack scenario, as formulated in formula (3). Defender's (attacker's) pure strategy set can be denoted as S_d (S_a), while the mixed strategy set can be defined as $Y = \left\{ y \in R^{|S_d|} \middle| \sum y_i = 1, y_i \in [0,1] \right\}$ and $X = \left\{ x \in R^{|S_a|} \middle| \sum x_i = 1, x_i \in [0,1] \right\}$, for the defender and the attacker, respectively.

$$s_{di} = z^0 \times \prod_{r=1}^{Q} (A_1^r \times A_2^r \times \ldots \times A_{ent(r)}^r \times z_1^r \times z_2^r \times \ldots \times z_{sub(r)}^r) \quad (2)$$

$$s_{ai} = a \times \prod_{r=1}^{I} j_r \times e \quad (3)$$

In which s_{di} is a specific defence decision, also called 'pure strategy' in game-theoretic terminology, of the defender; z_i^r is the detect level in i^{th} sub zone in zone level r, z^0 denotes the detect level in zone level 0; A_i^r is the detect level at the i^{th} access of perimeter r; $ent(r)$ is the number of accesses in perimeter r; $sub(r)$ is the number of sub zones in zone level r; Q is the total zone levels in the plant; $\times$ denotes cross product; s_{ai} is a specific attack action, also called 'pure strategy' in game-theoretic terminology, of the attacker; a is the target asset; j_r denotes an access on the r^{th} perimeter, and $j_r = 1,2,\ldots,ent(r)$; e denotes the attack scenario, specially, $e = Null$ means no attack scenario is implemented, i.e., the attacker is deterred.

An example of the attacker's pure strategy, which is shown as red (dash) line in figure 1(b), is that the attacker wants to attack a target (assuming its index is $\mathcal{L}$) in ZONE 2_2, and he intrudes following path p1, and further assume that he aims at shutting down a critical machine. The example strategy can be formally denotes as $s_{ai} = \mathcal{L} \times Truck\ Ent \times Ent3 \times Shutting\ down\ a\ machine$.

Payoffs are defined in formula (4) and (5), for the defender and the attacker respectively. P ($\tilde{P}$) denotes the successful probability that the attacker can reach the target, as defined in formula (1); PL_y ($\widetilde{PL}_y$) represents the expected consequence of an attack on the target, which equals the product of successful probability that the attack will be executed P_y ($\tilde{P}_y$) and the estimated consequence of a successful attack on the target L_y ($\tilde{L}_y$); C_d (C_a) denotes the cost of the defence (attack) plan; from the defender's (attack's) perspective.

$$u_d(s_a, s_d) = -(P(s_a, s_d) \cdot PL_y(s_a) + C_d(s_d)) \quad (4)$$

$$u_a(s_a, s_d) = \tilde{P}(s_a, s_d) \cdot \widetilde{PL}_y(s_a) - C_a(s_a) \quad (5)$$

2.3. Bayesian Stackelberg CPP Game

In Zhang and Reniers [15], the CPP game is assumed to be played simultaneously, thus the Nash Equilibrium is used to predict the outcome of the game. Later on in Zhang and Reniers [16], they argue that in most cases, the players in CPP game move sequentially, and in reality, the defender always faces multiple types of attackers. Thereby, they extended the CPP game to Bayesian Stackelberg CPP game, which is the baseline model of this paper.

In the Bayesian Stackelberg CPP game, the defender moves first, followed by multiple types of possible attackers with full observation of the defender's implemented action. The defender does not know exactly which attacker will execute an attack, but she knows the prior probabilities ρ that each type of attacker would occur.

Knowing the defender's strategy, each types of attackers would play their best responses to the defender's strategy. Defender knows that rational attackers would play their best responses, and she could also work out the attackers' best responses, thus she plays optimally. A Bayesian Stackelberg Equilibrium (BSE) $(\tilde{k}^1, \tilde{k}^2, \dots, \tilde{k}^{|\aleph|}, \tilde{y})$ for the Bayesian Stackelberg CPP game is defined by formulas (6) and (7).

$$\tilde{y} = \underset{y \in Y}{\operatorname{argmax}} \sum_{l \in \aleph} \rho^l \cdot U_d^l(\tilde{k}^l, :) \cdot y \quad (6)$$

$$\tilde{k}^l = \underset{k \in M^l}{\operatorname{argmax}} U_a^l(k,:) \cdot y \,, l \in \aleph \quad (7)$$

In which $\tilde{k}^l$ ($l \in \aleph$) represents the l^{th} attacker's best response; $\aleph$ denotes the set of different types of attackers (e.g., $\aleph = \{terrorist, activist\}$); ρ^l denotes the prior probability that the l^{th} attacker would occur; U_d^l and U_a^l represent the defender and the attacker's payoff matrix, respectively; $M^l = \{1,2,\dots,m^l\}$, and m^l denotes the number of pure strategies of the l^{th} attacker. For the convenience of expression, we also define $N = \{1,2,\dots n\}$, in which n denotes the number of pure strategies of the defender. The players' payoff matrix can be obtained by calculating the payoff units for each strategy tuple, by employing formulas (4) and (5). Notice that since different types of attackers would result in different payoff, thus the payoff matrix are all assigned with the type of the attacker.

Besides, a MaxiMin solution $(\overline{x}, \overline{y})$ for the Bayesian Stackelberg CPP game can be defined by formulas (CMT).

$$(\overline{x}, \overline{y}) = arg \max_{y \in Y} [\sum_{l \in \aleph} \rho^l \cdot \min_{x_l \in X_l} (x_l{}' \cdot U_d^l \cdot y)] \quad \text{(CMT)}$$

In which X_l denotes the l^{th} attacker's mixed strategy space. MaxiMin solution is a very conservative solution for the Bayesian Stackelberg CPP game, since its definition indicates the attacker aims at minimizing the defender's payoff, instead of maximizing his own payoff.

It is worth noting that the attacker's payoff matrix is not involved in the definition of the defender's MaxiMin solution. To this end, the defender could play her BSE strategy only when she knows the attacker's payoff matrix, namely, the U_a^l. In case that the defender does not know any information of the attacker, or all her information about the attacker is not reliable, the MaxiMin solution can be employed.

Observation 1. Defender's equilibrium payoff from the BSE is higher than or equal to the payoff from the MaxiMin solution.

Remark: Its proof can be easily shown as $P_{MM} = \max_{y \in Y}[\sum_{l \in \aleph} \rho^l \cdot \min_{x_l \in X_l}(x_l{}' \cdot U_d^l \cdot y)] \leq$ $\max_{y \in Y}[\sum_{l \in \aleph} \rho^l \cdot \min_{k^l \in M^l}(U_d^l(k^l, :) \cdot y)] \leq \max_{y \in Y}(\sum_{l \in \aleph} \rho^l \cdot U_d^l(\tilde{k}^l, :) \cdot y) = P_{BSE}$. This observation reflects the value of information of the attackers, as pointed out by the ancient Chinese military strategist Sun Tzu: "if you know your enemies and know yourself, you will not be put at risk even in a hundred battles."

Paruchuri et al. [19] proposed an efficient exact algorithm named "DOBSS" for calculating BSE, while algorithms for calculating MaxiMin solution can be found in Pita et al. [20], among others.

3. Interval CPP GAME

In this section, firstly, the Bayesian Stackelberg CPP game is extended to interval CPP game, in sub-section 3.1; then an algorithm for solving general bi-matrix game with interval payoff uncertainties is illustrated, in sub-section 3.2; sub-section 3.3 discusses the parameter coupling problem in the interval CPP game; a specific algorithm for dis-coupling this parameter coupling problem for interval CPP game is proposed, in sub-section 3.4.

3.1. Definition of Interval CPP Game

To implement the CPP game for realistic chemical plants protection, two works should be carried out: i) transfer the chemical plant protection problem to its formal representation as shown in figure 1; ii) get a set of quantitative inputs, such as the values of the targets, the vulnerability of each entrances etc. The currently available SRA methodologies (e.g., the API SRA methodology [5]), which were extensively implemented in chemical plants, though have been criticized for not being able to model the intelligent interactions between the defender and the attacker, is helpful for obtaining the inputs for CPP game. However, exact numeral inputs are still difficult to obtain, while an interval estimation would be much easier.

In the current research, the defender is assumed to have exact parameters of herself, but she could only know the intervals that the attacker's parameter will locate in, without knowing neither the

exact numbers nor the distribution. Cases that defender either does not know parameters of herself need extra research, thus can be a future research.

Fed with interval estimation of input parameters, the units of the payoff matrix of the CPP game will also associate with interval uncertainties. Assuming that the defender cannot exactly know the attacker's parameter σ (e.g., $\tilde{P}_i^z, \widetilde{PL}$), , but she believes that $\sigma \in [\sigma^{min}, \sigma^{max}]$, and she does not know how σ is distributed between $[\sigma^{min}, \sigma^{max}]$. Combining formulas (1) and (5), the attacker's payoff can be written as $u_a(s_a, s_d) = \prod_{i=0}^{I} \tilde{P}_i^z \cdot \prod_{j=1}^{I} \tilde{P}_j^p \cdot \widetilde{PL}_y - C_a$. Since all the parameters (i.e. $\tilde{P}_i^z$, $\tilde{P}_j^p$, $\widetilde{PL}_y$, and C_a) in this formula are greater than 0, hereby the u_a can be easily bounded as:

$$u_a^{min} = \prod_{i=0}^{I} \tilde{P}_i^{z\,min} \cdot \prod_{j=1}^{I} \tilde{P}_j^{p\,min} \cdot \widetilde{PL}_y{}^{min} - C_a{}^{max} \quad (8)$$

$$u_a^{max} = \prod_{i=0}^{I} \tilde{P}_i^{z\,max} \cdot \prod_{j=1}^{I} \tilde{P}_j^{p\,max} \cdot \widetilde{PL}_y{}^{max} - C_a{}^{min} \quad (9)$$

Therefore, the interval CPP game can be represented as

$$\mathrm{ICG} = \left\{ (U_d^l, \underline{U_a^l}, \overline{U}_a^l) \middle| l \in \aleph \right\} \quad (10)$$

In which $\underline{U_a^l}$ ($\overline{U}_a^l$) denotes the defender's estimation of the l^{th} type attacker's lower (upper) bound of payoff matrix.

3.2. Interval Bi-Matrix Game Solver

In interval CPP game as shown in formula (10), if the defender commits a mixed strategy, then she could not work out the attacker's best response to her strategy, since she does not know the exact U_a^l (see formula (7)). Being not able to calculate the attacker's best response, the defender could not be able to calculate her optimal strategy y either.

Fortunately, the development of robust linear programming[21, 22] and robust game theory[23] enables us to deal with games with distribution-free (interval) uncertainties. More specific in security game domain, Nikoofal and Zhuang [24] employed robust game theory for solving critical infrastructure protection games considering attacker's distribution-free private information. They studied how the budget of uncertainties can influence the allocation of resources in a real data case.

Kiekintveld et al. [25] developed a polynomial time binary search algorithm (named as "ISG Solver") to solve interval security games (ISG). "ISG Solver" is developed for security games which can be descript in a compact way as defined in Kiekintveld et al [26]. However, games in this paper could not be descript in the compact way. Pita et al. [20, 27] proposed a mixed integer linear programming (MILP) algorithm (named as "BRASS") which is able to deal with $\varepsilon - optimal$ adversaries. Though BRASS was developed for solving games played by bounded rational adversaries, its idea of separating the attacker's theoretic best response and the realistic possible responses makes it easily to be extended to solve the games with interval uncertainties, as also pointed out in Kiekintveld et al. [25]. Following Pita el al.'s work, an MILP algorithm based Interval Bi-Matrix Game Solver (IBGS) was proposed, as shown in the following formulas.

The basic idea in IBGS is that, though the defender could not work out the attacker's best response, she could judge that some attacker strategies is definitely worse than others. And the rule for this judgement is that, knowing the defender's strategy y, if the attacker upper bound payoff by playing strategy i is lower than the attacker lower bound payoff by playing some strategies, then strategy i can be excluded from the attacker's possible choices.

$$\max \sum_{l\in\Psi} \rho^l \gamma^l$$

$$s.t.\begin{cases} c1.\ \ 0 \le R^l - \underline{U}_a^l(i,:)\cdot y \le (1-h_i^l)\cdot\Gamma, \quad \forall i \in M^l \\ c2.\ \ (q_i^l - 1)\cdot\Gamma \le \overline{U}_a^l(i,:)\cdot y - R^l \le q_i^l \cdot\Gamma, \quad \forall i \in M^l \\ c3.\ \ \Gamma\cdot(1-q_i^l) + U_d^l(i,:)\cdot y \ge \gamma^l, \quad \forall i \in M^l \\ c4.\ \ q_i^l \ge h^l{}_i, \quad \forall i \in M^l \\ c5.\ \ q_i^l, h_i^l \in \{0,1\} \\ c6.\ \ \sum h^l = 1 \\ c7.\ \ \sum y = 1, y_i \in [0,1] \\ c8.\ \ R^l, \gamma^l \in R \end{cases} \tag{11}$$

In IBGS, $U_d^l(i,:)$ denotes the i^{th} row of the defender's payoff matrix; $\overline{U}_a^l(i,:)$ and $\underline{U}_a^l(i,:)$ denotes the i^{th} row of the attacker's upper and lower bound payoff matrix respectively; M^l represents the

attacker's pure strategy index set; Γ is a constant big real number, e.g., 10^6. The cost function represents that the defender aims at maximizing expected payoff, w.r.t. different types of adversaries. Constraint c1, c5, and c6 calculate the attacker's maximal value of the lower bound payoff, i.e., R^l, and the maximal value reaches if and only if $h_i = 1$. Notice that in c1, $h_i = 1$ indicates that $R^l = \underline{U}_a^l(i,:) \cdot y$, while $h_i = 0$ indicates that $R^l \geq \underline{U}_a^l(i,:) \cdot y$. Constraint c2 picks out all the strategies which have upper bound payoffs greater than the R^l. Notice that in c2, if $\overline{U}_a^l(i,:) \cdot y > R^l$, then $q_i^l = 1$, if $\overline{U}_a^l(i,:) \cdot y < R^l$, then $q_i^l = 0$, while if $\overline{U}_a^l(i,:) \cdot y = R^l$, then q_i^l can be either 0 or 1. Constraint c3 represents the idea that, among all the possible strategies of the attacker (i.e., strategies picked out by c6, or $q_i^l = 1$), the defender conservatively thinks that the worst strategy to herself is the attacker's best response, and thus she can ensure a payoff of γ^l. Constraint c4 enforces the strategy which has the maximal lower bound payoff to be a possible strategy.

IBGS does not depend on any specific property of the CPP game, thus it can be used for any security games which can be expressed in bi-matrix form.

3.3. Parameters Coupling in Interval CPP Game

The IBGS, though general enough, could be too conservative for interval CPP game. Look back on formulas (8) and (9) , the uncertainties on parameters lead to uncertainties on the attacker's payoffs, and notice that some attack strategies share the same parameters. To this end, the interval uncertainties on the attacker's payoffs are coupled, instead of independent.

For example, if strategy $s_{a1}, s_{a2} \in S_a$, and the only difference is that they have different attack target. Without loss of generality, assume that s_{a1} represents the strategy of attacking target 1 in ZONE 0 with a specific scenario, while s_{a2} represents attacking target 2 also in ZONE 0 with the same attack scenario. Further assume that defender plays a pure strategy $\dot{y}$ (pure strategy set belongs to mixed strategy set) which makes the game having the parameters as shown in table I.

Feeding formulas (8) and (9) with parameters in table I, we have: $u_a^{min}(s_{a1}) = 60, u_a^{max}(s_{a1}) = 74.456, u_a^{min}(s_{a2}) = 71.2, u_a^{max}(s_{a2}) = 95.84$. Ignoring other possible strategies, then we would have $R^l = u_a^{min}(s_{a2}) > u_a^{min}(s_{a1})$. Since $u_a^{max}(s_{a1}) > R^l$, according to the IBGS algorithm, both s_{a1}, s_{a2} are the attacker's possible best responses to $\dot{y}$.

Table I. illustrative parameters

Strategy s_{a1}			Strategy s_{a2}		
Para	min	max	Para	min	min
$\tilde{P}_0^z$	0.8	0.9	$\tilde{P}_0^z$	0.8	0.9
C_a	10	12	C_a	10	12
$\tilde{P}_y$	0.9	0.92	$\tilde{P}_y$	0.8	0.84
$\tilde{L}$	100	102	$\tilde{L}$	130	140

However, s_{a1}, s_{a2} share the same parameters $\tilde{P}_0^z$ and C_a. Substituting the independent parameters to the payoffs and keep the coupled parameters remain, we would have:

$u_a(s_{a1}) = \tilde{P}_0^z \cdot PL_1 - C_a$, and $u_a(s_{a2}) = \tilde{P}_0^z \cdot PL_2 - C_a$

In which $PL_1 \in [90,93.84], PL_2 \in [104,117.6]$. Although the defender has uncertainties on $\tilde{P}_0^z$ and C_a, but no matter what values they are, as long as that $\tilde{P}_0^z > 0$, the defender can predict that $u_a(s_{a1}) \leq 93.84 \cdot \tilde{P}_0^z - C_a < 104 \cdot \tilde{P}_0^z - C_a \leq u_a(s_{a2})$. To this end, the defender can judge that, for the attacker, s_{a2} is a better response than s_{a1}. Therefore, a strategic attacker would not play s_{a1}.

This example implies that the IBGS is over-conservative for interval CPP game, making the prediction of the attacker's behaviour more difficult. Following text formulates the idea used in above example, preparing for the algorithm specific to solve interval CPP game.

Given a defender's committed strategy $y, \forall k, t \in M$, define $\Delta_{kt} = U_a(k,:) \cdot y - U_a(t,:) \cdot y$, which denotes the differences of the attacker's payoff when responding k or t to y. Furthermore, define Tp_k as the set of typicals that attack strategy k has to pass, and Tp_t analogously. Substituting formulas (1) and (5) into Δ_{kt}, resulting that:

$$\Delta_{kt} = \sum_{j\in N}(\prod_{i\in Tp_k}\tilde{p}_{ij}\cdot\widetilde{PL}_k - C_k)\cdot y_j - \sum_{j\in N}(\prod_{i\in Tp_t}\tilde{p}_{ij}\cdot\widetilde{PL}_t - C_t)\cdot y_j \quad (12)$$

Defining $Tp_{kt} = Tp_k \cap Tp_t$, in order to dis-coupling the parameters, formula (12) can be re-organized as:

$$\Delta_{kt} = \sum_{j\in N}[(\prod_{i\in Tp_{kt}}\tilde{p}_{ij})\cdot(\prod_{i\in Tp_k - Tp_{kt}}\tilde{p}_{ij}\cdot\widetilde{PL}_k - \prod_{i\in Tp_t - Tp_{kt}}\tilde{p}_{ij}\cdot\widetilde{PL}_t)]\cdot y_j + C_t - C_k \quad (13)$$

Following texts demonstrate how to bound Δ_{kt} according to defender's interval uncertain knowledge on the attacker's parameters. The demonstration will be explained from 4 different cases, namely, whether strategy k and t use the same attack scenario ($e_k = e_t$), whether they attack the same target ($a_k = a_t$).

Case 1: $e_k = e_t$, $a_k = a_t$, thus $C_t = C_k$, $\widetilde{PL}_k = \widetilde{PL}_t$.

In this case, Δ_{kt} can be simplified as:

$$\Delta_{kt} = \sum_{j\in N}[(\prod_{i\in Tp_{kt}}\tilde{p}_{ij})\cdot\widetilde{PL}_k\cdot(\prod_{i\in Tp_k - Tp_{kt}}\tilde{p}_{ij} - \prod_{i\in Tp_t - Tp_{kt}}\tilde{p}_{ij})]\cdot y_j \quad (14)$$

In formula (14), for the two different strategies, only the $\tilde{p}_{ij}$ ($i \in Tp_k - Tp_{kt}\ or\ i \in Tp_t - Tp_{kt}$) are independent, thus their values are not coupled. Considering again that all parameters are greater than 0, we have:

$$\Delta_{kt} \geq \sum_{j\in N}\left[(\prod_{i\in Tp_{kt}}\tilde{p}_{ij})\cdot\widetilde{PL}_k\cdot(\prod_{i\in Tp_k - Tp_{kt}}\tilde{p}_{ij}{}^{min} - \prod_{i\in Tp_t - Tp_{kt}}\tilde{p}_{ij}{}^{max})\right]\cdot y_j \quad (15)$$

Define $\xi_{ktj}^{min} = (\prod_{i\in Tp_k - Tp_{kt}}\tilde{p}_{ij}{}^{min} - \prod_{i\in Tp_t - Tp_{kt}}\tilde{p}_{ij}{}^{max})$. For each $j \in N$ in formula (15), if $\xi_{ktj}^{min} \leq 0$, then inequality (16) holds, and vice versa.

$$\left[(\prod_{i\in Tp_{kt}}\tilde{p}_{ij})\cdot\widetilde{PL}_k\cdot\xi_{ktj}^{min}\right]\cdot y_j \geq \left[(\prod_{i\in Tp_{kt}}\tilde{p}_{ij}^{max})\cdot\widetilde{PL}_k^{max}\cdot\xi_{ktj}^{min}\right]\cdot y_j \quad (16)$$

To this end, we have:

$$\Delta_{kt} \geq \sum_{j\in N}\left[\left(\prod_{i\in Tp_{kt}}\tilde{p}_{ij}^{\varphi}\right)\cdot\widetilde{PL}_k^{\varphi}\cdot\xi_{ktj}^{min}\right]\cdot y_j = \Delta_{kt}^{min} \quad (17)$$

In which:

$$\varphi = \begin{cases} max, & if\ \xi_{ktj}^{min} \leq 0 \\ min, & otherwise \end{cases}$$

Analogously, we have:

$$\Delta_{kt}^{max} = \sum_{j\in N}\left[\left(\prod_{i\in Tp_{kt}}\tilde{p}_{ij}^{\varphi}\right)\cdot\widetilde{PL}_k^{\varphi}\cdot\xi_{ktj}^{max}\right]\cdot y_j \quad (18)$$

In which:

$$\xi_{ktj}^{max} = \left(\prod_{i \in Tp_k - Tp_{tk}} \tilde{p}_{ij}{}^{max} - \prod_{i \in Tp_t - Tp_{tk}} \tilde{p}_{ij}{}^{min}\right)$$

$$\varphi = \begin{cases} max, & if\ \xi_{ktj}^{max} \geq 0 \\ min, & otherwise \end{cases}$$

For the following 3 cases, we give the result of Δ_{kt}^{min} and Δ_{kt}^{max} directly, since they are obtained analogously as in case 1. [CMT the following 3 cases are quite similar to the case 1, and we give the result directly. It is a little bit like repeat work, shall we move the following 3 cases to the appendix?]

Case 2: $\boldsymbol{e_k = e_t}$, $\boldsymbol{a_k \neq a_t}$, thus $\boldsymbol{C_t = C_k}$.

$$\Delta_{kt}^{min} = \sum_{j \in N} \left[\left(\prod_{i \in Tp_{kt}} \tilde{p}_{ij}^{\varphi}\right) \cdot \xi_{ktj}^{min}\right] \cdot y_j$$

In which:

$$\xi_{ktj}^{min} = \left(\prod_{i \in Tp_k - Tp_{kt}} \tilde{p}_{ij}{}^{min} \cdot \widetilde{PL}_k^{min} - \prod_{i \in Tp_t - Tp_{kt}} \tilde{p}_{ij}{}^{max} \cdot \widetilde{PL}_t^{max}\right)$$

$$\varphi = \begin{cases} max, & if\ \xi_{ktj}^{min} \leq 0 \\ min, & otherwise \end{cases}$$

And,

$$\Delta_{kt}^{max} = \sum_{j \in N} \left[\left(\prod_{i \in Tp_{kt}} \tilde{p}_{ij}^{\varphi}\right) \cdot \xi_{ktj}^{max}\right] \cdot y_j$$

In which:

$$\xi_{ktj}^{max} = \left(\prod_{i \in Tp_k - Tp_{kt}} \tilde{p}_{ij}{}^{max} \cdot \widetilde{PL}_k^{max} - \prod_{i \in Tp_t - Tp_{kt}} \tilde{p}_{ij}{}^{min} \cdot \widetilde{PL}_t^{min}\right)$$

$$\varphi = \begin{cases} max, & if\ \xi_{ktj}^{max} \geq 0 \\ min, & otherwise \end{cases}$$

Case 3: $\boldsymbol{e_k \neq e_t}$, $\boldsymbol{a_k = a_t}$, thus $\boldsymbol{\widetilde{PL}_k = \widetilde{PL}_t}$.

$$\Delta_{kt}^{min} = \sum_{j \in N} \left[\left(\prod_{i \in Tp_{kt}} \tilde{p}_{ij}^{\varphi}\right) \cdot \widetilde{PL}_k^{\varphi} \cdot \xi_{ktj}^{min}\right] \cdot y_j + C_t^{min} - C_k^{max}$$

In which:

$$\xi_{ktj}^{min} = \left(\prod_{i \in Tp_k - Tp_{kt}} \tilde{p}_{ij}{}^{min} - \prod_{i \in Tp_t - Tp_{kt}} \tilde{p}_{ij}{}^{max}\right)$$

$$\varphi = \begin{cases} max, & if\ \xi_{ktj}^{min} \leq 0 \\ min, & otherwise \end{cases}$$

And,

$$\Delta_{kt}^{max} = \sum_{j \in N} \left[\left(\prod_{i \in Tp_{kt}} \tilde{p}_{ij}^{\varphi}\right) \cdot \widetilde{PL}_k^{\varphi} \cdot \xi_{ktj}^{max}\right] \cdot y_j + C_t^{max} - C_k^{min}$$

In which:

$$\xi_{ktj}^{max} = \left(\prod_{i \in Tp_k - Tp_{kt}} \tilde{p}_{ij}{}^{max} - \prod_{i \in Tp_t - Tp_{kt}} \tilde{p}_{ij}{}^{min}\right)$$

$$\varphi = \begin{cases} max, \ if \ \xi_{ktj}^{max} \geq 0 \\ min, \quad otherwise \end{cases}$$

Case 4: $e_k \neq e_t, a_k \neq a_t$.

$$\Delta_{kt}^{min} = \sum_{j \in N} \left[\left(\prod_{i \in Tp_{kt}} \tilde{p}_{ij}^{\varphi}\right) \cdot \xi_{ktj}^{min}\right] \cdot y_j + C_t^{min} - C_k^{max}$$

In which:

$$\xi_{ktj}^{min} = \left(\prod_{i \in Tp_k - Tp_{kt}} \tilde{p}_{ij}{}^{min} \cdot \widetilde{PL}_k^{min} - \prod_{i \in Tp_t - Tp_{kt}} \tilde{p}_{ij}{}^{max} \cdot \widetilde{PL}_t^{max}\right)$$

$$\varphi = \begin{cases} max, \ if \ \xi_{ktj}^{min} \leq 0 \\ min, \quad otherwise \end{cases}$$

And,

$$\Delta_{kt}^{max} = \sum_{j \in N} \left[\left(\prod_{i \in Tp_{kt}} \tilde{p}_{ij}^{\varphi}\right) \cdot \xi_{ktj}^{max}\right] \cdot y_j + C_t^{max} - C_k^{min}$$

In which:

$$\xi_{ktj}^{max} = \left(\prod_{i \in Tp_k - Tp_{kt}} \tilde{p}_{ij}{}^{max} \cdot \widetilde{PL}_k^{max} - \prod_{i \in Tp_t - Tp_{kt}} \tilde{p}_{ij}{}^{min} \cdot \widetilde{PL}_t^{min}\right)$$

$$\varphi = \begin{cases} max, \ if \ \xi_{ktj}^{max} \geq 0 \\ min, \quad otherwise \end{cases}$$

Proposition 1. Δ_{kt}^{min} and Δ_{kt}^{max} are the lower and upper bound of Δ_{kt}, and they can be reached.

Remark: It is straightforward according to the definition of Δ_{kt}. Δ_{kt}^{min} and Δ_{kt}^{max} can be reached when all the parameters are valued as the value in the definition of Δ_{kt}^{min} and Δ_{kt}^{max}, since all these parameters are dis-coupled in the definition.

Proposition 2. $\Delta_{kt}^{min} = -\Delta_{tk}^{max}$.

Remark: Proof of this proposition is due to the fact that for each cases of the above mentioned 4 cases, we have $\xi_{ktj}^{min} = -\xi_{tkj}^{max}$. According to this proposition, in the remainder of this paper, we focus on the Δ_{kt}^{min} for each attacker strategy pairs.

Proposition 3. If $\Delta_{kt}^{min} > 0$, then strategy k is always a better response than t, to the defender's committed strategy y.

Remark: Its proof is straightforward since $0 < \Delta_{kt}^{min} \leq \Delta_{kt} = U_a(k,:) \cdot y - U_a(t,:) \cdot y$. Proposition 3 illustrates a new approach for the defender to calculate the attacker's possible best responses, comparing to the c6 in IBGS.

Another interesting property of the Δ_{kt}^{min} is that, it is a linear polynomial of y. Define a 3-dimension coefficient matrix $\Omega^l(M^l, M^l, N)$, and the coefficient of y_j in Δ_{kt}^{min} as its unit $\Omega^l(k,t,j)$.

3.5. Interval CPP Game Solver

Combining the idea of IBGS and the proposition 3, an algorithm named Interval CPP Game Solver (ICGS) is proposed.

For each $k^l \in M^l$, solve the following MILP problem, obtaining the optimal payoff for the defender $\mathcal{H}(k^1, k^2, \ldots, k^{|\aleph|})$. Finally the maximal value of the $\mathcal{H}$ and its corresponding strategies are the optimal solution of the interval CPP game.

$$\max \sum_{l \in \Psi} \rho^l \gamma^l$$

$$s.t. \begin{cases} \text{c9.} \ \underline{U}_a^l(i,:) \cdot y \leq \underline{U}_a^l(k^l,:) \cdot y, \quad \forall i \in M^l \\ \text{c10.} \ -q_t^l \cdot \Gamma \leq \Omega^l(k^l,t,:) \cdot y \leq (1-q_t^l) \cdot \Gamma, \quad \forall t \in M^l \\ c11. \ \Gamma \cdot (1-q_i^l) + U_d^l(i,:) \cdot y \geq \gamma^l, \quad \forall i \in M^l \\ c12. \ q_i^l \in \{0,1\}, q_{k^l}^l = 1 \\ c13. \ \sum y = 1, y_i \in [0,1] \end{cases} \tag{20}$$

In ICGS, $\underline{U}_a^l$ and U_d^l represent the lower bound of the attacker's payoff and the defender's payoff, respectively. $\Omega^l(k^l,t,:)$ denotes the vector in k^l row, t column of matrix Ω^l. Constraint c9 makes sure that the k^l strategy has the highest lower bound payoff, which is similar to the c1 in IBGS. Constraint c10 can be explained as: giving the condition that k^l strategy has the highest lower bound payoff, if strategy t, satisfying $\Omega^l(k^l,t,:) \cdot y > 0$, then $q_t^l = 0$; if satisfying $\Omega^l(k^l,t,:) \cdot y < 0$, then $q_t^l = 1$; otherwise, q_t^l can be either 0 or 1. Constraint c10 picks out attacker's possible best responses based on the idea in proposition 3, instead of using the c2 in IBGS, which is the key innovation of ICGS. Constraint 11 represents the idea that, among all the possible strategies of the

attacker (i.e., strategies picked out by c13, or $q_i^l = 1$), the defender conservatively thinks that the worst strategy to herself is the attacker's best response, as the same in c3 in IBGS. c12 enforces that the k^l strategy is a possible strategy, the same as in c4 in IBGS.

Proposition 4. Defender's equilibrium payoff from ICGS is higher than or equal to her equilibrium payoff from IBGS.

Proof: $\forall y \in Y$, without loss of generality, assume that $\underline{A}_{\pi^l}^l \cdot y \geq \underline{A}_i^l \cdot y$, for all $i \in M^l$.

In IBGS, from c1 we have $R^l = \underline{A}_{\pi^l}^l \cdot y$. From c2 we know that $\forall t \in M^l$, if $\overline{A}_t^l \cdot y < R^l$, then $q_t^l = 0$, which means that the strategy t will definitely not be the attacker's best response. Define $E_B^l = \left\{t \in M^l - \{\pi^l\} \middle| \overline{A}_t^l \cdot y < R^l\right\}$. According to c3, we have $\gamma_B^l = \min_{i \in M^l - E_B^l} \{U_d^l(i,:) \cdot y\}$.

In ICGS, from c9 we have $k^l = \pi^l$. From c10 we know that $\forall t \in M^l$, if $\Omega^l(k^l, t, :) \cdot y > 0$, then $q_t^l = 0$, which means that strategy k^l is always a better response than strategy t, or, strategy t will definitely not be the attacker's best response. Define $E_C^l = \{t \in M^l - \{\pi^l\} | \Omega^l(k^l, t, :) \cdot y > 0\}$. According to c11, we have $\gamma_C^l = \min_{i \in M^l - E_C^l} \{U_d^l(i,:) \cdot y\}$.

We prove that $E_B^l \subseteq E_C^l$. $\forall t \in E_B^l$, we have $0 < \underline{A}_{\pi^l}^l \cdot y - \overline{A}_t^l \cdot y \leq \min(A_{\pi^l}^l \cdot y - A_t^l \cdot y) = \Omega^l(k^l, t, :) \cdot y$, thereby $t \in E_C^l$.

Since $E_B^l \subseteq E_C^l$, thus we have $\gamma_B^l \leq \gamma_C^l$, thus $\sum_{l \in \aleph} \rho^l \gamma_B^l \leq \sum_{l \in \aleph} \rho^l \gamma_C^l$.□

4. Case study

In this section, a case study is conducted to show how models and algorithms proposed in this article work. Sub-section 4.1 gives some basic information of the case study, while sub-section 4.2 demonstrates the results by implementing different models and algorithms.

4.1. Definition of the Case Study

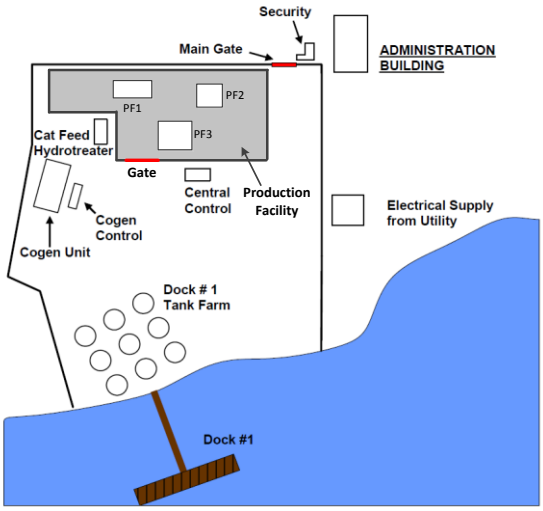
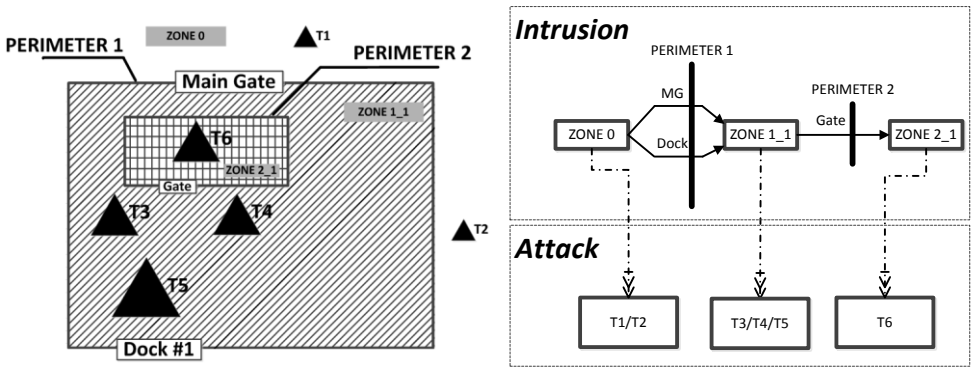


Figure 2. Layout of the case study (PF=Production Facility)

Figure 2 shows an refinery which is also an case study used in Zhang and Reniers [15, 16], Lee et al. [28], and API SRA report [5].



(a) Abstract Description of the Plant (b) Intrusion and Attack Procedure

Figure 3. Formalized representation of the plant as figure 1

Figure 3 illustrates the formalized representation of the plant, from the CPP game perspective. Appendix A gives the map of the notations used in figure 3 (a) and figure 2. In this case study, the defender has 6 "typicals" to implement counter-measures, namely: i) ZONE 0; ii) the Main Gate (MG); iii) the Dock #1 (Dock); iv) ZONE 1; v) the Gate; vi) ZONE 2. Further assume that the defender can have 3 different security alert levels at each typical. Recalling formula (2), in this case study, the defender's strategy can be denote as a cross product of 6 digital numbers which denotes the security alert levels at these 6 typicals. For instance, $s_d = 2 \times 1 \times 3 \times 2 \times 3 \times 1$ denotes that the security alert levels at ZONE 0 (Main Gate, Dock #1, ZONE 1, Gate, ZONE2) are 2 (1,3,2,3,1) respectively.

Figure 3(b) shows that for each given attack scenario, the attackers could have 10 pure strategies, they are: (1 and 2) attack T1 or T2 in ZONE 0; (3-8) attack T3 or T4 or T5 in ZONE 1, passing perimeter 1 through MG or Dock; (9 and 10) attack T6 in ZONE 2, pass perimeter 1 through MG or Dock. Two types of adversaries (together with scenario) are considered: a) terrorist with vehicle-borne improvised explosive device (VBIED T); b) environmental activist (EA). Different to previous two researches [15, 16], the adversary passing perimeters by stepping over the perimeters are not considered in this case study, for the sake of simplicity. Also, as the VBIED T could not be able to intrude from the Dock, thus the strategies contain Dock in the intrusion path are all ignored for the terrorist, that is to say, the VBIED T would have only 6 strategies. Furthermore, the EA is assumed to aim at shutting down the plant, thus the office building (T1) and the tank farm (T5) would not be his target, since attack on these two targets might cause casualties. Table II and III list all the attackers' pure strategies for this case study, expressed as defined in formula (3).

Table II. VBIED T's pure strategy list

Index	Strategy
s_{v1}	$T1 \times VBIED$
s_{v2}	$T2 \times VBIED$
s_{v3}	$T3 \times MG \times VBIED$
s_{v4}	$T4 \times MG \times VBIED$
s_{v5}	$T5 \times MG \times VBIED$
s_{v6}	$T5 \times MG \times Gate \times VBIED$

Table III. EA's pure strategy list

Index	Strategy
s_{e1}	$T2 \times EA$
s_{e2}	$T3 \times MG \times EA$
s_{e3}	$T3 \times Dock \times EA$
s_{e4}	$T4 \times MG \times EA$
s_{e5}	$T4 \times Dock \times EA$
s_{e6}	$T6 \times MG \times Gate \times EA$
s_{e7}	$T6 \times Dock \times Gate \times EA$

According to the data from API Standard 780[5], the threat of a VBIED T and a EA is 3 and 4 respectively, thus the prior probabilities of these two types of adversaries can be calculated as $\rho = (3/7\,, 4/7)$.

Series parameters are given in table IV through table IX, for illustrative purpose. It is worth noting that if the models are implemented on industrial practice, all these parameters should be given by security experts (e.g., the API SRA team[5]). It is also worth noting that all these information are estimations from the defender's point of view.

Table IV. Basic probabilities of successful intrusion for the VBIED T

Typical	From	To	p_d	$\tilde{p}_a^{min}$	$\tilde{p}_a^{max}$	$\tilde{p}_a^{nominal}$	Coe_2	Coe_3
zone0		T1 or T2	0.95	0.95	0.99	0.95	0.68	0.45
MG			0.3	0.3	0.5	0.3	0.65	0.38
zone1	MG	Gate	0.78	0.78	0.85	0.78	0.68	0.46
zone1	MG	T3	0.8	0.8	0.9	0.8	0.68	0.46
zone1	MG	T4	0.8	0.8	0.9	0.8	0.68	0.46
zone1	MG	T5	0.7	0.7	0.85	0.7	0.68	0.46
Gate			0.2	0.2	0.3	0.2	0.61	0.32
Zone2	Gate	T6	0.9	0.9	0.99	0.9	0.66	0.39

Table V. Basic probabilities of successful intrusion for the EA

Typical	From	To	p_d	$\tilde{p}_a^{min}$	$\tilde{p}_a^{max}$	$\tilde{p}_a^{nominal}$	Coe_2	Coe_3
zone0		T1 or T2	0.95	0.9	0.97	0.95	0.68	0.45
MG			0.3	0.2	0.32	0.3	0.65	0.38
Dock			0.2	0.16	0.23	0.2	0.53	0.30
zone1	MG	Gate	0.78	0.7	0.8	0.78	0.68	0.46
zone1	MG	T3	0.8	0.72	0.8	0.8	0.68	0.46
zone1	MG	T4	0.8	0.72	0.8	0.8	0.68	0.46
zone1	Dock	Gate	0.78	0.7	0.78	0.78	0.68	0.46
zone1	Dock	T3	0.8	0.74	0.8	0.8	0.68	0.46
zone1	Dock	T4	0.8	0.74	0.8	0.8	0.68	0.46
Gate			0.2	0.15	0.21	0.2	0.61	0.32
Zone2	Gate	T6	0.9	0.8	0.9	0.9	0.66	0.39

Table IV and V give the probabilities of successfully passing typical or from some typical/asset to another typical/asset. p_d represents defender's estimation of the probabilities, $\tilde{p}_a^{min}$ ($\tilde{p}_a^{max}$, $\tilde{p}_a^{nominal}$) represents the defender's estimation of the attacker's minimal (maximal, nominal) estimation of the probabilities. These four columns are the probabilities when the security alert levels are all set to be

lowest level (i.e., level 1). Considering that terrorists are normally risk-seeking, and activists are normally risk-aversion, thus in table IV and V, we intentionally set that for terrorists, p_d is very close to $\tilde{p}_a^{min}$, while for activists, p_d is very close to $\tilde{p}_a^{max}$.

When security alert levels are not the lowest level , for the sake of simplicity, instead of giving extra 2 tables of assumed data, we assume that the intrusion probabilities will decrease concavely[29]. The Coe_2 and Coe_3 columns shows the coefficients, which is randomly produced according to the concave rule, as shown in figure 4. For example, in table IV, the defender's estimation of p_d is 0.3 when the security alert level on the main entrance is level 1, and this probability would be $p_d \cdot Coe_2$ (i.e., $0.3 \times 0.65 = 0.195$) when the SAL is level 2 while when the SAL is level 3, the probability would be $p_d \cdot Coe_3$. $\tilde{p}_a^{min}$ ($\tilde{p}_a^{max}$, $\tilde{p}_a^{nominal}$) are all calculated analogously.

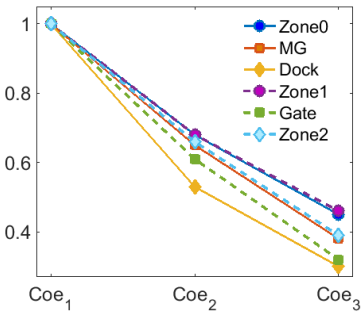


Figure 4. The coefficients in table IV and V

Table VI. In condition of successfully arriving the target, probabilities of damage and consequences (k€), for VBIED T

Target	p_y	$\tilde{p}_y^{min}$	$\tilde{p}_y^{max}$	$\tilde{p}_y^{nominal}$	L	$\tilde{L}^{min}$	$\tilde{L}^{max}$	$\tilde{L}^{nominal}$
T1	0.1	0.1	0.2	0.1	1000	1900	2100	2000
T2	0.9	0.9	0.95	0.9	100	140	160	150
T3	0.7	0.7	0.8	0.7	300	240	260	250
T4	0.6	0.6	0.8	0.6	800	880	920	900
T5	0.9	0.9	1	0.9	2000	3000	3600	3000
T6	0.99	0.99	1	0.99	10000	4000	5200	5000

Table VII. In condition of successfully arriving the target, probabilities of damage and consequences (k€), for EA

Target	p_y	$\tilde{p}_y^{min}$	$\tilde{p}_y^{max}$	$\tilde{p}_y^{nominal}$	L	$\tilde{L}^{min}$	$\tilde{L}^{max}$	$\tilde{L}^{nominal}$
T2	0.7	0.5	0.74	0.7	100	200	220	200
T3	0.7	0.4	0.6	0.5	300	280	310	300
T4	0.7	0.4	0.6	0.5	800	880	940	900
T6	0.9	0.85	0.95	0.9	1000	1800	2200	2000

Table VI and VII give the estimation of conditional probabilities that an attack would be successfully executed and the estimated consequences/gains. Table VIII and IX give the materialized defensive and attack costs respectively.

Table VIII. Materialized costs (k€) for defender

	Zone0	MG	Dock	Zone1	Gate	Zone2
SAL:1	40	20	20	20	20	20
SAL:2	60	30	25	30	25	30
SAL:3	100	50	40	50	40	50

Table IX. Materialized costs (k€) for attackers

VBIED T			EA		
C_a^{min}	C_a^{max}	$C_a^{nominal}$	C_a^{min}	C_a^{max}	$C_a^{nominal}$
5	15	10	0.2	2	1

4.2. Results and Discussion

Fed formulas (4) and (5) with the defender's data and the attacker's nominal data given in table IV through table IX, we get the Bayesian Stackelberg CPP game $\{(U_d^{VBIED}, U_a^{VBIED}), (U_d^{EA}, U_a^{EA})\}$. Fed formulas (8) and (9) with the attacker's minimal and maximal parameters, we get the bi-matrix form interval CPP game $\{\left(U_d^{VBIED}, \underline{U}_a^{VBIED}, \overline{U}_a^{VBIED}\right), \left(U_d^{EA}, \underline{U}_a^{EA}, \overline{U}_a^{EA}\right)\}$. Fed formulas (17) etc., we get the $(\Omega^{VBIED}, \Omega^{EA})$.

In case that the defender does not have any information about the attackers, thus she could protect the plant using the "balanced protection" principle, or, in game theoretic terminology, the MaxiMin strategy. Using U_d^{VBIED} and U_d^{EA} as inputs for the algorithm for calculating MaxiMin[20], we get the defender's MaxiMin strategy as shown in table X, and the corresponding payoff, which is €-256,832.1.

Table X Defender's MaxiMin Strategy

s_d	Probability
$2 \times 2 \times 1 \times 2 \times 2 \times 1$	0.4850
$2 \times 2 \times 1 \times 2 \times 2 \times 2$	0.1334
$2 \times 2 \times 2 \times 2 \times 2 \times 1$	0.0714
$2 \times 2 \times 2 \times 2 \times 2 \times 2$	0.3102

The probabilities means that the defender plays strategy $2 \times 2 \times 1 \times 2 \times 2 \times 1$ at probability 0.4850, plays strategy $2 \times 2 \times 1 \times 2 \times 2 \times 2$ at probability 0.1334, and so forth.

Table XI Defender's Payoff w.r.t. different attacker strategies (k€)

VBIED T	
s_a	Def Payoff
s_{v1}	-255.9439
s_{v2}	-249.4839
s_{v3}	-205.7347
s_{v4}	-224.2372
$\boldsymbol{s_{v5}}$	**-283.8563**
s_{v6}	-283.8563
EA	
s_a	Def Payoff
$\boldsymbol{s_{e1}}$	**-236.5639**
s_{e2}	-205.7347
s_{e3}	-229.7194
s_{e4}	-208.3014
s_{e5}	-236.5639
s_{e6}	-196.9507
s_{e7}	-198.1642

Table XI shows the defender's payoff when the attackers play different strategies. It is shown that though the defender does not have any information of the attackers, by playing the MaxiMin strategy, she could guarantee a minimal payoff at $-283.8563 \times \frac{3}{7} - 236.5639 \times \frac{4}{7} = -256{,}832.1$ euro.

In case that the defender believes that her estimations of the attacker's parameters (i.e., the nominal values) are exact, thus she could protect the plant by using the BSE. Using $\left(U_d^{VBIED}, U_a^{VBIED}\right)$ and $\left(U_d^{EA}, U_a^{EA}\right)$ as inputs for the DOBSS algorithm[19], we get the BSE, as shown in table XII, XIII, and XIV, and the corresponding payoffs, which is €-246,167.5.

Table XII. Defender's BSE strategy

s_d	Probability
$2 \times 2 \times 1 \times 2 \times 1 \times 1$	0.8641
$2 \times 2 \times 2 \times 2 \times 1 \times 1$	0.1359

Table XIII. Players' payoff w.r.t. different VBIED T strategy (k€) (attacker's best response is bold)

s_a	Atk Payoff	Def Payoff
s_{v1}	67.5200	-245.2794
s_{v2}	65.5820	-238.8194
s_{v3}	1.9923	-195.0702
s_{v4}	27.0049	-213.5727
$\boldsymbol{s_{v5}}$	**128.7686**	**-273.1917**
s_{v6}	79.2976	-359.2745

Table XIV. Players' payoff w.r.t. different EA strategy (k€) (attacker's best response is bold)

s_a	Atk Payoff	Def Payoff
$\boldsymbol{s_{e1}}$	**48.7420**	**-225.8994**
s_{e2}	9.2792	-195.0702
s_{e3}	36.0049	-219.0549
s_{e4}	12.8172	-200.0235
s_{e5}	48.7420	-232.2637
s_{e6}	20.6479	-191.5033
s_{e7}	28.0991	-195.2289

As shown in table XIII and XIV, the defender knows the attacker's information, thus she could predict the attackers' best responses to her strategy, and play accordingly. It is worth noting that if the VBIED T plays s_{v6} and the EA plays s_{e5}, the defender would have a low payoff as $-359.2745 \times \frac{3}{7} - 232.2637 \times \frac{4}{7} = -286.6969$ euro. However, the defender believes that both the two types of attackers are rational, and they would not play other strategies but their best response strategies. As shown in table XIV, it is also worth noting that for the EA, playing strategies s_{e1} and s_{e5} are indifferent, from which the EA can have a payoff at 48.7420. In this cases, the strategy which brings the defender higher payoff is assumed to be the attacker's best response, for more discussion of this assumption, interested readers are referred to von Stengel and Zamir [30], Pita et al. [20].

In case that the defender does not know the attacker's exact parameters, but she believes that these parameters locate between the minimal and maximal values as given in previous section, thus she could protect the plant by using the conservative results from the interval CPP game. Using $\left(U_d^{VBIED}, \underline{U}_a^{VBIED}, \overline{U}_a^{VBIED}\right)$ and $\left(U_d^{EA}, \underline{U}_a^{EA}, \overline{U}_a^{EA}\right)$ as inputs for IBGS, we get the optimal strategy and the corresponding payoffs, which is €-253,424.4. Using U_d^{VBIED}, U_d^{EA}, $\underline{U}_a^{VBIED}$, $\underline{U}_a^{EA}$, and

$(\underline{\Delta}^{VBIED}, \underline{\Delta}^{EA})$ as inputs for ICGS, we get the optimal strategy and the corresponding payoffs, which is €-247,396.2.

Table XV. Defender's optimal solution from IBGS

s_d	Probability
$2 \times 2 \times 1 \times 2 \times 2 \times 1$	0.6184
$2 \times 2 \times 2 \times 2 \times 2 \times 1$	0.2788
$2 \times 2 \times 2 \times 2 \times 2 \times 2$	0.1028

Table XVI. Defender's optimal solution from ICGS

Index	s_d	Probability
$s_{d-ICGS-1}$	$2 \times 2 \times 1 \times 2 \times 1 \times 1$	0.6184
$s_{d-ICGS-2}$	$2 \times 2 \times 2 \times 2 \times 1 \times 1$	0.3816

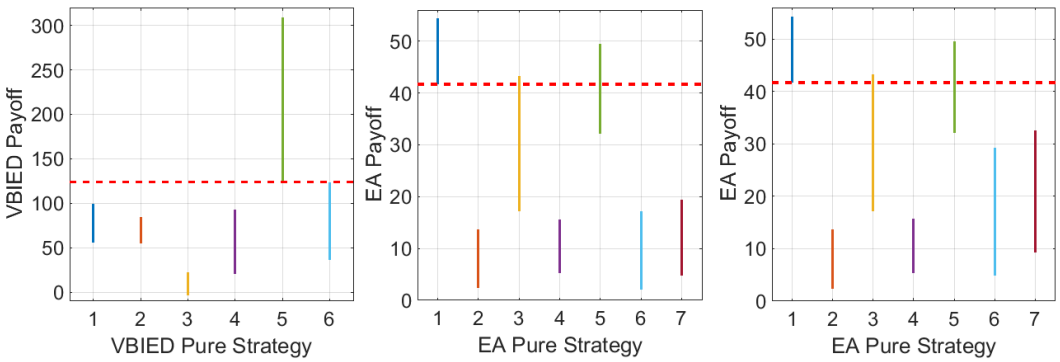


Figure 5. Attackers' payoff range (the Left sub-figure (L): VBIED T's payoff range corresponding to defender's IBGS strategy; the Middle sub-figure (M): EA's payoff range corresponding to defender's IBGS strategy; the Right sub-figure (R): EA's payoff range corresponding to defender's ICGS strategy)

Figure 5 (L) and (M) illustrate the attackers' payoff range, corresponding to the defender's IBGS strategy as given in table XV. Different to the analytics of table XIII and XIV, in IBGS, the defender has interval uncertainties on the attackers' payoffs, thus she could not work out the attackers' best responses. However, based on her knowledge of the interval uncertainties, she could know that the upper bound payoffs of some attacker's strategies (i.e., the s_{v1}, s_{v2}, s_{v3}, s_{v4}, and s_{v6} in (L), the s_{e2}, s_{e4}, s_{e6}, and s_{e7} in (M)) are lower than the lower bound payoffs of some others (i.e., the s_{v5} in (L), the s_{e1} in (M)), hereby, the fore strategies would not be the attackers' possible best responses. To keep consistency with IBGS, we have that $R^{VBIED\,T} = 123.7686, R^{EA} = 41.6968, h_5^{VBIED\,T} = 1, h_1^{EA} = 1, q_5^{VBIED\,T} = 1, q_{1,3,5}^{EA} = 1$.

Figure 5 (R) illustrates the attackers' payoff range, corresponding to the defender's ICGS strategy as given in table XVI. It shows that EA's strategy s_{e3} has a upper bound payoff higher than the lower bound payoff of strategy 1, thereby, the defender can judge that strategy s_{e3} could also be a possible best response of the EA, from the IBGS idea. However, noting that EA's strategy s_{e1} and s_{e3} share the some parameters, they are, the intrusion probability P_0^Z in ZONE 0 and the attack cost C_a. Substituting the interval estimations of all the parameters, except the P_0^Z and the C_a, into formulas (8) and (9), we have:

$$u_a^{min}(s_{d-ICGS-1}, s_{e1}) = P_0^Z \cdot 0.68 \cdot 105 - C_a = P_0^Z \cdot 71.4 - C_a$$

$$u_a^{max}(s_{d-ICGS-1}, s_{e3}) = P_0^Z \cdot 0.32 \cdot 0.65 \cdot 0.8 \cdot 0.68 \cdot 0.64 \cdot 910 - C_a = P_0^Z \cdot 65.8997 - C_a$$

$$u_a^{min}(s_{d-ICGS-2}, s_{e1}) = P_0^Z \cdot 0.68 \cdot 105 - C_a = P_0^Z \cdot 71.4 - C_a$$

$$u_a^{max}(s_{d-ICGS-2}, s_{e3}) = P_0^Z \cdot 0.32 \cdot 0.65 \cdot 0.8 \cdot 0.68 \cdot 0.64 \cdot 910 - C_a = P_0^Z \cdot 65.8997 - C_a$$

Thus we have:

$$\Delta_{13} = 0.6184 \cdot \left[u_a^{min}(s_{d-ICGS-1}, s_{e1}) - u_a^{max}(s_{d-ICGS-1}, s_{e3})\right] + 0.3816 \cdot \left[u_a^{min}(s_{d-ICGS-2}, s_{e1}) - u_a^{max}(s_{d-ICGS-2}, s_{e3})\right] = P_0^Z \cdot 5.5003 > 0$$

This result means that with these interval uncertainties, the defender could be able to judge that strategy s_{e1} is always a better response than strategy s_{e3} for the EA. IBGS is not able to assist the defender to make this judgement, as shown in figure 5 (R), but the ICGS could, and this is the reason that ICGS could bring the defender higher equilibrium payoff.

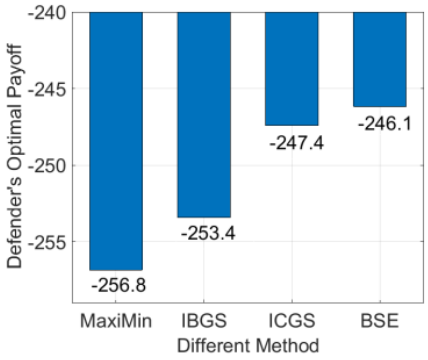


Figure 6. Defender's optimal payoff from different methods

Figure 6 illustrates the defender's optimal payoffs from the above mentioned 4 methods. The results show that knowing more about the attacker (from MaxiMin to IBGS (ICGS), to BSE), the defender

could have a higher optimal payoff (from -256.8k€ to -253.4k€ (-247.4k€), to -246.1k€). The results also show that with the same information of the attacker, the ICGS solution could bring the defender higher payoff than the IBGS solution, which is theoretically analysed in proposition 4.

4.3. Sensitivity Analysis

In this section, we study how the interval uncertainties on the attackers would affect the defender's optimal payoffs. Two experiments are defined, namely, the s1, in which the defender has interval uncertainties on all the attackers' parameters, and s2, in which the defender only has interval uncertainties on the attackers' monetary parameters. In both experiments, the defender's parameters are the same as given in table IV through table IX, while the attacker's parameters are defined by following rules: 1) an interval radius $\mu \geq 0$ is used; 2) all the monetary parameters (i.e., $\tilde{L}_y, C_a$) are bounded in the interval $\left[\sigma^{nominal} \cdot (1-\mu), \sigma^{nominal} \cdot (1+\mu)\right]$, and the $\sigma^{nominal}$ are the nominal values of the attackers' parameters as given in table IV through table IX. In experiment s1, all the probabilistic parameters (i.e., $\tilde{P}_i^Z, \tilde{P}_i^p, \tilde{p}_y$) are bounded in the interval $\left[\sigma^{nominal} \cdot (1-\mu), \sigma^{nominal} \cdot (1+\mu)\right] \cap [0,1]$, and the $\sigma^{nominal}$ are the nominal values of the attackers' parameters as given in table IV through table IX. In experiment s2, all the probabilistic parameters (i.e., $\tilde{P}_i^Z, \tilde{P}_i^p, \tilde{p}_y$) are the same as the nominal values as given in table IV through table IX.

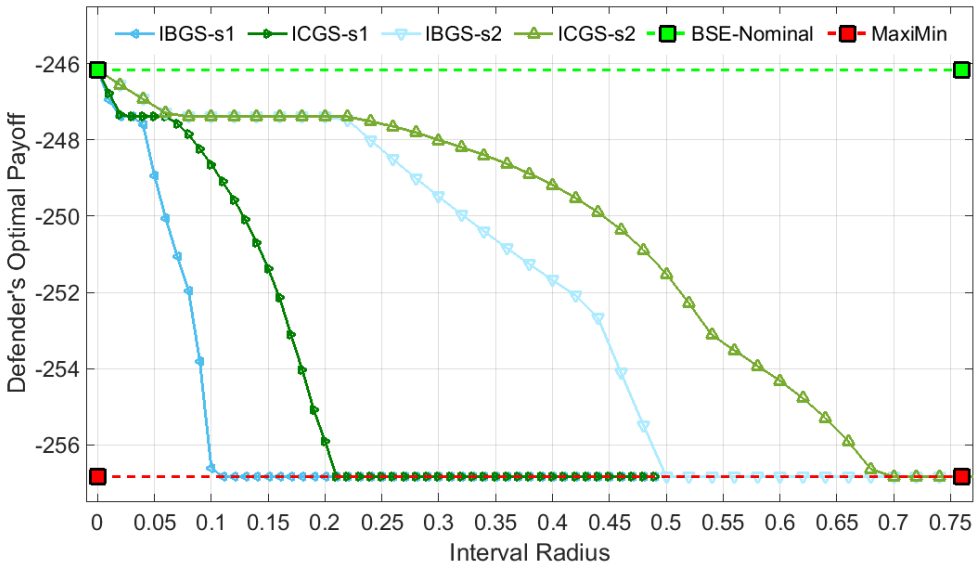


Figure 7. Defender's optimal payoff corresponding to the interval radius

Results shown in figure 7 demonstrates that the increase of interval radius μ would result in decrease on the defender's optimal payoff. When $\mu = 0.0$, which means no interval uncertainty exists, the defender could have a payoff equal to the payoff from the BSE. When $\mu \geq \mu^*$ (in experiment s1, $\mu^* = 0.11$ for IBGS and $\mu^* = 0.21$ for ICGS, while in s2, $\mu^* = 0.50$ for IBGS and $\mu^* = 0.70$ for ICGS), the defender's payoff could be as low as her MaxiMin payoff. This means that, in Bayesian Stackelberg CPP game, if the defender could not effectively bound the attacker's parameters into a relatively narrow interval, then her information of the attacker is useless.

Figure 7 also shows that with the same interval radius, the ICGS solution could always bring the defender higher payoff than the IBGS solution.

5. Conclusion

Security risk analysis is difficult because of the lack of historical data as well as the adaptive attackers. Game theory, being able to model intelligent interactions between defenders and adaptive attackers, has been introduced as a promising way, for improving security in many domains. Current game theoretic studies on security domain, however, are criticized for its requirement of lots of quantitative inputs, which is quite difficult to obtain.

In this paper, for the purpose of protecting chemical plants from intentional attacks, the interval Chemical Plant Protection (CPP) game is proposed. The interval CPP game considers the fact that the defender always have distribution-free uncertainties on her opponents' parameters, thereby the interval CPP game could assist the defender to make defence decisions accordingly. Two Mixed-Integer Linear Programming based algorithms are proposed, namely, the IBGS and the ICGS, for solving general interval bi-matrix games and interval CPP game respectively. Based on the work in this paper, some existed security risk assessment methods (e.g., the API SRA framework) could transfer their qualitative (or semi-quantitative) results to the CPP game model, as inputs for the latter.

This article can be extended by also considering bounded rational attackers. Although attackers are believed to be strategic in some academia studies and government reports, they could have some emotional factors when making decisions. There are some studies on bounded rational attackers in the security game domain, but no available models or algorithms existed in the chemical plant protection domain.

Appendix A. Symbols in Figure 2 and 3 (a)

Table A. Symbols map between Figure 2 and Figure 3 (a)

Symbol in Fig 3 (a)	Symbol in Fig 2
ZONE0	Outdoor Area
ZONE1_1	Area within Enclosure
ZONE2_1	Production Facility
PERIMETER 1	the boundary of the plant
PERIMETER 2	The boundary of the production facility
Main Gate	Main gate
Dock #1	Dock #1
Gate	The entrance of the production facility
T1	Administration Building
T2	Electrical Supply from Utility
T3	Cogen Unit/ Cogen Control/Cat Feed Hydrotreater
T4	Central control
T5	Tank Farm
T6	Production facilities in production facility area

Reference

[1] Brown G, Carlyle M, Salmerón J, Wood K. Defending critical infrastructure. Interfaces. 2006;36(6):530-44.
[2] (DHS) DoHS. National strategy for homeland security. 2002.
[3] Paul Orum RR. Chemical Security 101, What You Don't Have Can't Leak, or Be Blown Up by Terrorists. 2008.
[4] Reniers G. Terrorism security in the chemical industry: Results of a qualitative investigation. Secur J. 2011;24(1):69-84.
[5] Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, (2013).
[6] Cox Jr LAT. Some limitations of "Risk= Threat× Vulnerability× Consequence" for risk analysis of terrorist attacks. Risk Anal. 2008;28(6):1749-61.
[7] Cox Jr LAT. Game theory and risk analysis. Risk Anal. 2009;29(8):1062-8.

[8] Pavlova Y, Reniers G. A sequential-move game for enhancing safety and security cooperation within chemical clusters. J Hazard Mater. 2011;186(1):401-6.
[9] Reniers G. An external domino effects investment approach to improve cross-plant safety within chemical clusters. J Hazard Mater. 2010;177(1-3):167-74.
[10] Reniers G, Cuypers S, Pavlova Y. A game-theory based Multi-plant Collaboration Model (MCM) for cross-plant prevention in a chemical cluster. J Hazard Mater. 2012;209-210:164-76.
[11] Reniers G, Dullaert W, Karel S. Domino effects within a chemical cluster: A game-theoretical modeling approach by using Nash-equilibrium. J Hazard Mater. 2009;167(1-3):289-93.
[12] Reniers G, Dullaert W, Visser L. Empirically based development of a framework for advancing and stimulating collaboration in the chemical industry (ASC): Creating sustainable chemical industrial parks. J Clean Prod. 2010;18(16-17):1587-97.
[13] Reniers G, Soudan K. A game-theoretical approach for reciprocal security-related prevention investment decisions. Reliab Eng Syst Saf. 2010;95(1):1-9.
[14] Talarico L, Reniers G, Sörensen K, Springael J. MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. Reliab Eng Syst Saf. 2015;138:105-14.
[15] Zhang L, Reniers G. A Game-Theoretical Model to Improve Process Plant Protection from Terrorist Attacks. Risk analysis : an official publication of the Society for Risk Analysis. 2016.
[16] Laobing Zhang GR. Applying a Bayesian Stackelberg game for securing a chemical plant. Risk Anal. 2016.
[17] Feng Q, Cai H, Chen Z, Zhao X, Chen Y. Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. J Loss Prev Process Ind. 2016;43:614-28.
[18] Reniers G, Van Lerberghe P, Van Gulijk C. Security risk assessment and protection in the chemical and process industry. Process Saf Prog. 2015;34(1):72-83.
[19] Paruchuri P, Pearce JP, Marecki J, Tambe M, Ordonez F, Kraus S, editors. Playing games for security: an efficient exact algorithm for solving Bayesian Stackelberg games. Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems-Volume 2; 2008: International Foundation for Autonomous Agents and Multiagent Systems.
[20] Pita J, Jain M, Tambe M, Ordóñez F, Kraus S. Robust solutions to Stackelberg games: Addressing bounded rationality and limited observations in human cognition. Artificial Intelligence. 2010;174(15):1142-71.
[21] Soyster AL. Technical note—convex programming with set-inclusive constraints and applications to inexact linear programming. Operations research. 1973;21(5):1154-7.
[22] Ben-Tal A, Nemirovski A. Robust solutions of uncertain linear programs. Operations research letters. 1999;25(1):1-13.
[23] Aghassi M, Bertsimas D. Robust game theory. Mathematical Programming. 2006;107(1-2):231-73.
[24] Nikoofal ME, Zhuang J. Robust allocation of a defensive budget considering an attacker's private information. Risk Anal. 2012;32(5):930-43.
[25] Kiekintveld C, Islam T, Kreinovich V, editors. Security games with interval uncertainty. Proceedings of the 2013 international conference on Autonomous agents and multi-agent systems; 2013: International Foundation for Autonomous Agents and Multiagent Systems.
[26] Kiekintveld C, Jain M, Tsai J, Pita J, Ordóñez F, Tambe M, editors. Computing optimal randomized resource allocations for massive security games. Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1; 2009: International Foundation for Autonomous Agents and Multiagent Systems.
[27] Pita J, Jain M, Ordóñez F, Tambe M, Kraus S, Magori-Cohen R, editors. Effective solutions for real-world stackelberg games: When agents must deal with human uncertainties. Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1; 2009: International Foundation for Autonomous Agents and Multiagent Systems.

[28] Lee Y, Kim J, Kim J, Kim J, Moon I. Development of a risk assessment program for chemical terrorism. Korean Journal of Chemical Engineering. 2010;27(2):399-408.
[29] Zhuang J, Bier VM. Balancing terrorism and natural disasters-defensive strategy with endogenous attacker effort. Operations Research. 2007;55(5):976-91.
[30] Von Stengel B, Zamir S. Leadership with commitment to mixed strategies. 2004.