This item is the archived peer-reviewed author-version of:

A game-theoretical model to improve process plant protection from terrorist attacks

Reference:

Zhang Laobing, Reniers Genserik.- A game-theoretical model to improve process plant protection from terrorist attacks
Risk analysis / Society for Risk Analysis [New York] - ISSN 0272-4332 - 36:12(2016), p. 2285-2297
Full text (Publisher's DOI): <https://doi.org/10.1111/RISA.12569>
To cite this reference: <https://hdl.handle.net/10067/1396690151162165141>

**A game-theoretical model to improve chemical plant
protection from terrorist attacks**

ABSTRACT

The New York City 9/11 terrorist attacks urged people from academia as well as from industry to pay more attention to operational security research. The required focus in this type of research is human intention. Unlike safety-related accidents, security-related accidents have a deliberate nature, and one has to face intelligent adversaries with characteristics that traditional probabilistic risk assessment techniques are not capable of dealing with. In recent years, the mathematical tool of game theory, being capable to handle intelligent players, has been used in a variety of ways in terrorism risk assessment. In this article, we analyse the general intrusion detection system in process plants, and propose a game-theoretical model for security management in such plants. Players in our model are assumed to be rational and they play the game with complete information. Both the pure strategy and the mixed strategy solutions are explored and explained. We illustrate our model by an illustrative case, and find that in our case, no pure strategy but a mixed strategy Nash equilibrium exists.

KEY WORDS: Process Plant Security, Strategic Adversaries, Terrorism Risk Assessment, Game theory

1. INTRODUCTION

Since the 9/11 attacks in New York City, security research, and especially the protection of critical infrastructure, has gained even more attention from both academia and industry. The American Department of Homeland Security, for example, identified the following 13 critical infrastructures: agriculture, banking and finance, chemical industry, defence industrial base, emergency services, energy, food, government, information and telecommunications, postal and shipping, public health, transportation, and water⁽¹⁾, due to their extreme importance for society and their vulnerability. The importance of protecting industrial process plants (including those in the chemical industry, the food supply industry, the energy industry, and others) cannot be underestimated. They play important roles in modern society, from producing daily necessities such as food and energy, to making modern medicine, and therefore they are truly essential for our modern way of living. Energy comes in the form of power and fuels. In addition, the product gamma of importance to mankind is even much larger, think of materials in general, with particular ones such as fibers, medicine and electronic materials. Process plants thus usually store dangerous goods in some quantities, which can be an important threat to themselves as well as to their surroundings. Moreover, due to a variety of benefits of scale, process plants tend to build their factories geographically together, potentially aggravating the danger.

Different to safety research that focuses on natural and randomly (non-strategic) hazards, security research has to face intelligent and strategic adversaries. Traditional methods or concepts used in safety science such as probabilistic risk assessments, historical data analysis and etc., no longer can be readily and easily used. When dealing with security problems, the adversaries' strategies should be taken into consideration instead of the incidents' probabilities.

Game theory, which originated in economic sciences, is a good choice to handle problems that contain intelligent players. Game theory has very rigor mathematical foundations, and if adequately used in the chemical security, we can obtain more accurate and more defensible quantitative results,

besides the qualitative assessments and results used nowadays in chemical plants. In recent years, a lot of attention in academia has been laid on the combination of game theory and critical infrastructure protection. Tambe (2011)⁽²⁾ and his group used game theory to improve the security situation in airport patrolling, air marshals' allocation, and coast line protection. They developed several decision support systems based on their research, and these systems now work in reality. Bier (2008)⁽³⁾ and her group researched the combination of game theory and security assessment methods from a theoretical viewpoint. They answered the questions why game theory has an important role in security research, and illustrated the advantages and disadvantages of using game theory in operational security. Talarico⁽²⁷⁾ presented a multi-modal security-transportation model to allocate security resources within a chemical supply chain which is characterized by the use of different transport modes, each having their own security features.

Although there are already some researches on using game theory to improve operational security, in fact in the process security, no research has been done as yet, to the best of the authors' knowledge. Security problems in the process industries are different to those in aviation or the electric power grid for example, although they are all critical infrastructures. We cannot readily apply game theoretical models now being used in aviation, within the process industries directly. Different security models are implemented in different types of industries. For instance, in Tambe's model⁽²⁾, air marshals are allocated to defend an air plane, and therefore the players' strategies are limited to "protect" (that is, to allocate an air marshal on the plane) or not (that is, no air marshal on the plane), and "attack" or not. However, in case of security in the process industries, the model is more complex, the strategies may be at a different alert level (discrete model) or at a different investment level (continuous model). Moreover, specific of the process industry is the nature of the consequences: explosion fire and toxic spread. Actually, an attacker may want trying to get as much escalation as possible. This is by knowing what effects hazardous material releases will have. For a more detailed discussion of this, please see Reniers⁽²⁶⁾.

Section 2 illustrates the intrusion detection model in process plants. A generic setup of security within process plants is given and the intrusion procedure is analysed in this section. Section 3 defines the game theoretical security model in process plants. An illustrative example is given in section 4, to show how our model works in practice. In the last section conclusions are drawn and future research pathways are provided.

2. INTRUSION DETECTION MODEL IN PROCESS PLANTS

Since chemical plants are often very large and complex entities and house a lot of installations and equipment, often linked together with pipework, protection in such plants goes hand in hand with assessing different perimeters and different zones of protection. The general intrusion detection model in process plants is illustrated in Figure 1, where the terms “perimeter” and “zone” are used⁽⁵⁾. Typically, in process plants, perimeters are used to distinguish and isolate critical areas from uncritical areas. In case of certain perimeters, there should be some access(es), from where authorised visitors and/or vehicles can come in to, or go out of, the critical areas and unauthorised visitors and/or vehicles cannot. Perimeters distinguish different levels or parts of critical areas, which are the so-called zones.

Figure 1. General Intrusion Preventing in Process Plants

In order to describe our model more conveniently, we index zones in a hierarchical way, or, in different levels. The zone level starts from 0, which is the outdoor area, and zone level $i+1$ is located in zone level i . There may be several sub-zones in one zone level, for example, in Figure 1, there are 3 sub-zones in zone level 2. Based on these notations, we can say that if the attack target is located in zone level i , then the attacker has to pass zone level $0, 1, 2, \dots, i$. In the model, we assume that the attacker will not pass the same zone level more than a single time. For example, if the attacker would like to attack the installation in ZONE 3_1, he will follow the path “ZONE 3_1 through zone 0, perimeter 1, zone 1_1, perimeter 2, zone 2_3, perimeter 3, zone 3_1”, and he will thus never go into zone 2_1 from zone 1_1 and then go out from zone 2_1 to zone 1_1 again. This is a reasonable assumption, since if he would follow the latter path, he would come into zone level 1 and 2 twice, which would be irrational. According to the Detection/Delay/Response Principle⁽⁶⁾, the plant can install some equipment (cameras, scanners, etc.), or employ some guards to detect the

unauthorised intruders; the plant can also deploy some barriers within the zone area to delay the intrusion, and there are other possible measures to take. To indicate the possible security measures that can be taken at a certain point, the term “typical “ is sometimes employed. A typical is a summation of technological items constituting a security barrier and thus describes the specific detailed technical characteristics of a security measure installed at a plant or at a part thereof⁽⁵⁾. An intentional attack usually starts with a successful intrusion, and culminates into an attack at a certain target (e.g., tank farms, administration building, process facilities, and etc.). In the intrusion period, the attacker needs to decide which means to use to execute the attack, and needs to choose a critical intrusion path. In the attack period, the attacker reaches the target and executes his attack.

Figure 2. The Intrusion and Attack Procedure

Figure 2, which is a plot from the attacker’s viewpoint, illustrates the intrusion and attack procedure to a process plant, as shown in Figure 1. A_{ij} means the j^{th} possible access to pass perimeter i . For example, perimeter 1 in Figure 1 has four accesses: the main entrance, the truck entrance, the extra

entrance, as well as the enclosure/fence. Without loss of generality, we can map A11 in Figure 2 to the main entrance of perimeter 1 in Figure 1, A12 can be mapped to the truck entrance, etc. Note here that we can see the enclosure or the fence also as a gate, because the attacker can step over the enclosure or the fence, but to make things easier, we treat the whole circle as one gate. For example, we map A14 in Figure 2 to the enclosure/fence in perimeter 1. In the following part of this paper, we always treat the enclosure/fence also as an access.

In order to attack a certain target which is located in a certain zone, the attacker will have a critical path, which he thinks is the easiest way to reach the target. For example, if the target is located in zone 2_1, the attacker has to first pass zone 0, then pass perimeter 1 (through a certain access, A11 for instance) to reach zone 1_1, and then pass zone 1_1 to access A21 or A22 and pass perimeter 2 to reach zone 2_1; finally he also has to walk in the zone 2_1 for a certain distance to reach the target.

In the above example, we assume that the attacker can successfully pass zone level i with probability P_i^z . P_i^z is a function of the defender's detection level in zone level i and of the time t_i^z that the attacker will stay in zone level i . The higher the detection level, the lower P_i^z . The higher t_i^z , the lower P_i^z .

The possibility of successfully passing perimeter i is noted P_i^p . Since the perimeter has several accesses, the attacker will choose one of them to pass it, so P_i^p will be equal to the possibility of successfully passing the chosen access k , represented as P_{ik}^p . Note that although different accesses have different difficulties to pass, the attacker will not always choose the easiest access, because in our model, the attacker can also be detected in certain zones. For example, under a certain detection level and intrusion effort, the access k is easier than access l to pass, indicating that $P_{ik}^a > P_{il}^a$, but access l is closer to the target or to the access of the next perimeter than access k , and thus the attacker might choose the access l after all.

Based on these notations, the probability that the attacker can reach the target is given by the following formula:

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

The notation I in formula (1) indicates that the target is located in zone level I . Detection starts from 0 since security experts suggest that the outdoor area should also be taken into consideration in one way or another, for adequate security management in a chemical plant⁽⁵⁾.

3. GAME-THEORETICAL MODEL FOR CHEMICAL PLANT PROTECTION (CPP GAME)

A game-theoretical model mainly consists of three parts: the players, the strategy sets, and the payoff matrix. The three parts will be discussed in the following sub-sections, and afterwards, the game and its solutions will be developed and discussed.

3.1. Players of the CPP Game

It is obvious that in a security game for process plants, there are only two players: one is the defender and the other is the attacker. Questions that are valuable to be discussed here are whether the players are rational and whether they have complete information of the game. For the first question, whether the players are rational, a lot of papers state that adversaries will analyse defences, and then plan accordingly^(7,8). They can thus be assumed to be rational. The defenders, who in our case are the security managers in companies, with abundant experience and highly educated, can also be assumed rational. However, one of the basics of attack philosophy is surprise in place, time and means. So, the attacker will have most success when he enters following a trajectory not expected by the defender, hence irrational. Conversely, if the game is played to make an optimum investment given a certain budget than the assumption is obviously justified. As regards the second question, whether players have complete information of the game, it is difficult to assess.

Since the adversary preferably will collect extensive security information of the plant, and some researches show that based on the media, the terrorists can collect at least 80% (sometimes even 100%) of the information that is needed to execute a successful attack⁽¹⁾, it may indeed be reasonable to assume that the adversaries have complete information of the game, including the strategy sets of both themselves and the defender, as well as the payoffs when both players choose certain strategies. Unfortunately, it is difficult to say that defenders have complete information of the security game, since up to now, we do not have enough knowledge about the attackers. A possible solution to face this shortage is the Bayesian game⁽⁹⁾. In a Bayesian game, we can define different types of attackers as well as different attack scenarios. For each of them, we can estimate their occurrence probabilities. Then Harsanyi's theory can be employed to translate the incomplete information game to an imperfect game⁽¹⁰⁾. In this paper, we assume that we are dealing with a specific type of attacker, therefore we assume that the defender has complete information of the game. Bayesian games can be an interesting path for future research. For a more detailed discussion of 'rationality', 'complete information', and also common knowledge of a security game, the interested reader is referred to Guikema⁽¹¹⁾.

Thus research on this paper assumes: (i) both defender and attacker are rational players, and the rationality is a common knowledge; (ii) both two players have complete information of the game.

3.2. Strategy Sets of the CPP Game

There are three options of attack in a chemical plant: intrusion, inside job, and a remote attack. The focus of this paper is intrusion, since this is the most visible part of anti-terrorism security policies in chemical plant. Most chemical plants are also focused on this type of security in current industrial practice. Attacks from insiders as well as remote attacks (e.g. using drone technology) are of a different nature, and require their own research activity.

To secure a process plant, security managers need to decide for each typical where to implement it in which security alert level. To execute an attack, the attacker needs to decide which targets to attack first, and then choose the critical intrusion path.

The defender's Strategies are given by:

$$S_d = \{s_1, s_2, \dots, s_{N_d}\} \quad (2)$$

With:

$$s_i = z_0 \times \prod_{i=1}^Q (A_{i1} \times \dots \times A_{iM_i} \times z_{i-1} \times z_{i-2} \times \dots \times z_{i-N_i}) \quad (3)$$

Where:

S_d : defender's strategy set

s_i : a specific defence decision, also called 'pure strategy' in game-theoretic terminology, of the defender

N_d : number of pure strategies of the defender

z_{i-x} : detect level in x^{th} sub zone in zone level i

A_{ij} : detect level at the j^{th} access of perimeter i

M_i : number of accesses in perimeter i

N_i : number of sub zones in zone level i

Q : total zone levels in the plant

$\times$: cross product

Assume further that a process plant has k security alert levels, for example, $k = 3^{(5)}$ or $k = 5^{(12)}$, then we can compute the number of possible defender's strategies using the following formula:

$$N_d = k^{1 + \sum_{i=1}^Q (M_i + N_i)} \quad (4)$$

Furthermore, the attacker's Strategies are:

$$S_a = \{s_1, s_2, \dots, s_{N_a}\} \quad (5)$$

With:

$$s_i = a_{I-X-y} \times \prod_{t=1}^I A_{tj_t} \times e \quad (6)$$

Where:

S_a : attacker's strategy set

s_i : a specific attack action, also called 'pure strategy' in game-theoretic terminology, of the attacker

N_a : number of pure strategies of the attacker

a_{I-X-y} : the target asset, which is the y^{th} asset located in the X^{th} sub zone in zone level I

I : the target asset located in zone level I

A_{tj_t} : the access to pass the t^{th} perimeter

e : attack efforts

To be easier understandable, we can see the attacker's pure strategy as which asset to attack, how to intrude to reach the asset, and with what effort level.

The number of attacker's pure strategies can be computed by employing the following formula:

$$N_a = k^e \cdot \sum_{i=1}^Q \sum_{j=1}^{N_i} (N_{i-j}^a \cdot \prod_{l=1}^i M_l^s) \quad (7)$$

Where k^e is the number of different attack efforts.

According to formula (4), (7), we do realize that N_d and N_a will increase dramatically as the scale of the plant grows. But in practise, limited budgets/resources are available for both defenders and attackers, thus N_d and N_a can be reduced, see for example Talarico⁽²⁷⁾.

For the convenience of expressing the players' strategies, a code protocol which can map to the strategies as well as the strategy index is needed. Since the defender's strategies depend on the security alert level at each typical, we can easily code his strategies as a series of numbers $d_1 d_2 \dots d_{Nt}$, where d_i equals the detection level at the i^{th} typical and Nt indicates the total number of typicals (we also have $Nt = 1 + \sum_{i=1}^Q (M_i + N_i)$). We also code the attacker's strategy as a series of numbers by

using the code protocol shown in Figure 3.

Figure 3. Code Protocol of Attacker's Strategies

For instance, the defender's strategy code "1111 2222" means that there are 8 typicals in the plant, and the detection levels at the first 4 typicals are '1' while at the later 4 typicals are '2'. As an example of an attacker's strategy code, "3151" indicates that the attacker will attack the target '5' which is located in zone level 1, and he will do so with effort '3', and he will pass perimeter 1 to intrude zone level 1 through access 1.

3.3. Payoffs of the CPP Game

In any game, payoffs are numbers which represent the motivations of players, for instance, profit, quantity, "utility," or other continuous measures (cardinal payoffs), or may simply rank the desirability of outcomes (ordinal payoffs) ⁽¹³⁾. Usually, a payoff should be some function of the strategy tuple played by all players.

The intruder aims at causing some damages to the target, as analysed in the previous section, and to do so, he first should choose a target to reach and then plan an intrusion path. After reaching the target, he will attack the target, with a certain probability of success due to the difficulties of having to surpass the defences related to the target. Note that in this article, as we are dealing with terrorists and not with thieves, and therefore we do not consider the exit and rewarding stage which are sometimes mentioned as a part of a successful intrusion process⁽¹⁴⁾. Irrespective of the fact whether the intrusion and the attack are successful, an attack has a financial aspect attached to it (that is, it will cost money), with the exact amount depending on the efforts spent.

The defender aims at preventing losses from an attack. If he doesn't invest in security, the intruders can more easily intrude the plant and execute a successful attack. In this article, we assume that security investments are only used to reduce the probability of successful intrusion.

Based on the above analysis, the attacker and defender's payoff can be computed by the following two formulas:

$$U_a(s_a, s_d) = P_{I-X}(s_a, s_d)P_y L_{I-X-y} - C_a(s_a) \quad (8)$$

$$U_d(s_a, s_d) = \bar{P}_{I-X}(s_a)P_y L_{I-X-y} - (P_{I-X}(s_a, s_d)P_y L_{I-X-y} + C_d(s_d)) \quad (9)$$

Where:

U_a : the intruder's payoff

U_d : the defender's payoff

P_{I-X} : the probability of successfully reaching the target, under a certain defence level

P_y : the probability of successfully attacking the target after reaching the target

L_{I-X-Y} : the estimated loss of the target. In practise, the loss can be computed as $L_{I-X-Y} = \alpha C + \beta E + \gamma P$, where casualties (C), direct and indirect economic loss (E), and environmental pollution (P) are considered. Coefficients (α, β, γ) can be used to transfer them into money (in Euro).

C_a : the cost of certain intrusion effort

$\bar{P}_{I-X}$: the probability of successfully reaching the target, without any defence

C_d : the cost of a certain defence effort

The numbers of P_y , L_{I-X-y} , C_d can be provided by security managers, eventually supported by risk analysis theory^(15,16), so we will not discuss the computation of them in this article. Based on formula (1), the computation of P_{I-X} and $\bar{P}_{I-X}$ depend on P_i^p and P_i^z . For each P_i^p and P_i^z , they are functions of the defender's strategy as well as the attacker's strategy. We assume that an equally proportionate change (the proportion parameter is represented as λ) in the efforts of both defender and attacker would leave the P_i^p and P_i^z unaffected, that is

$$P_i^z(\lambda e, \lambda z_{i-x}) = P_i^z(e, z_{i-x}) \text{ and } P_i^p(\lambda e, \lambda A_{ik}) = P_i^p(e, A_{ik}) \quad (10)$$

Under this assumption (10), we can apply the power form of an extended Contest Success Function (CSF)^(17,18) to compute P_i^p and P_i^z , as following:

$$P_i^z = \frac{e}{e + \alpha_{ix} z_{i-x}} \quad (11)$$

$$P_i^p \in \{P_{i1}^p, P_{i2}^p, \dots, P_{iM_i}^p\} \quad (12)$$

$$P_{ik}^p = \frac{e}{e + \beta_{ik} A_{ik}} \quad (13)$$

Where α , β indicate the defence effectiveness ratios, or the difficulty of defence, based on perception and experience/expertise of security management. The higher α , β are, the easier to defend that zone or perimeter. For example, zone 1 is much bigger than zone 2 in area, then we would say even under the same intrusion effort and detect level, we will have $P_2^z < P_1^z$, that is to say, $\alpha_2 > \alpha_1$.

As we analysed in previous section, the detect probabilities of the intrusion in zones not only depend on the detection level and the intrusion effort, but also depend on how long the intruder stays in the zone. We therefore add the time factor into formula (11) to compute the probabilities in zones as following:

$$P_i^z = \frac{e}{e + \alpha_{ix} z_{i-x}} e^{-\frac{t_{i-x}}{\tau}} \quad (14)$$

Since zone level 0 is defined as the open area, the time that the attacker stays in this zone will be infinite. Obviously, plant security management is unable to defend the whole zone level 0 area. Instead, plant security will only patrol or install equipment in a very close area of the plant. Therefore

we assume that the time that the attacker stays in zone level 0 is a constant number, independent to his next action.

To make things easier, we also assume that if the attacker chooses to step over the enclosure/fence to pass a certain perimeter, his time in the next zone will be a constant number, independent from his next action. This is a simplification of the model, but it does not limit the generalization of the model in any way.

The computation of C_a depends on the type of the adversary and attack, where a reasonable estimation of C_a should be scenario-based. For example, in the scenario of a suicide bomb attack, the bomber's cost C_a contains the cost of the bomb, the bomber's life, the vehicle he uses to intrude the plant, and other costs. Furthermore, different types of bombs, different bombers (well trained or not), different vehicles related to different attack efforts, and a different effort related to a different attack cost, can be conceptualized and mapped.

3.4. Solutions of the CPP Game

A pure strategy is a specific move/action/decision that a player will follow. The strategy sets discussed in section 3.2 are pure strategies for the defender and attacker.

A mixed strategy is a strategy consisting of possible moves and a probability distribution (collection of weights) which corresponds to how frequently each move is to be played. For example, a mixed strategy for defender can be represented as:

$$P_d = (p_{d1}, p_{d2}, \dots, p_{dN_d})$$

Where $p_{d1} + p_{d2} + \dots + p_{dN_d} = 1$, and p_{dk} means the defender will play the pure strategy s_k at probability p_{dk} . Similarly, an attacker's mixed strategy can be defined as:

$$P_a = (p_{a1}, p_{a2}, \dots, p_{aN_a})$$

Where $p_{a1} + p_{a2} + \dots + p_{aN_a} = 1$.

When a mixed strategy is used, the players' payoffs should be computed as the expected payoffs under certain probability distributions on pure strategies.

$$v_d(p_a, p_d) = \sum_{j=1}^{N_d} \sum_{i=1}^{N_a} p_{dj} p_{ai} U_d(s_{ai}, s_{dj}) \quad (15)$$

$$v_a(p_a, p_d) = \sum_{i=1}^{N_a} \sum_{j=1}^{N_d} p_{ai} p_{dj} U_a(s_{ai}, s_{dj}) \quad (16)$$

A solution of a game is a pair (not necessarily unique) of strategies, which is so-called the pure strategy solution, or a probability distribution of each of the strategies, which is the so-called mixed strategy solution, that a rational pair of players might use⁽¹⁹⁾. A Nash Equilibrium (for two players) is a solution where a change in strategies by either player will lead him to obtain less payoff if the other player remained with his current strategy, or, in other words, a Nash Equilibrium point is a stable point of the players' strategies, where no one has motivations to change his strategy. A pure strategy Nash Equilibrium for the CPP Game can be defined as (s_a^*, s_d^*) such that:

$$u_d(s_a^*, s_d^*) \geq u_d(s_a^*, s_d) \quad \forall s_d \in S_d \quad (17)$$

and

$$u_a(s_a^*, s_d^*) \geq u_a(s_a, s_d^*) \quad \forall s_a \in S_a \quad (18)$$

A mixed strategy Nash Equilibrium of the CPP Game is a pair of strategies (p_a^*, p_d^*) such that

$$v_d(p_a^*, p_d^*) = \max_{p_d} v_d(p_a^*, p_d) \quad (19)$$

and

$$v_a(p_a^*, p_d^*) = \max_{p_a} v_a(p_a, p_d^*). \quad (20)$$

For algorithms to find Nash Equilibriums, interested readers are referred in case of pure strategy Nash equilibria to Gibbons⁽²²⁾ and for mixed strategy Nash Equilibria to Lemke and Howson⁽²⁰⁾.

In 1950, Nash⁽²¹⁾ proved that in a finite game (that is, there are finite players and each player has a finite number of pure strategies), a Nash Equilibrium (NE) always exists (either as a pure strategy NE, or as a mixed strategy NE). Gibbons⁽²²⁾ states that “in any game in which each player would like to outguess the other(s), there is no Nash Equilibrium (at least no pure strategy Nash Equilibrium)”. The CPP Game evidently meets these conditions with two players, each player having N_d and N_a pure strategies respectively, and the defender and attacker being eager to outguess each other.

4. AN ILLUSTRATIVE CASE FOR THE CPP GAME

In this section, we use an illustrative case of a refinery in a dock area to elaborate and explain how the model of the CPP Game, as explained in the previous section, works in practice.

4.1. Layout of the Illustrative Case

Figure 4 shows a refinery in a dock area. This case is also used in ^(23,24), but we add some concrete production facilities in the production facility zone, to make the case more interesting and also more realistic.

Figure 4. Layout of the Plant (PF=Production Facility)

4.2. Game-theoretical Modelling for the Illustrative Case

We can easily transfer Figure 4 into our Intrusion Detect Model (explained in section 2) as displayed in Figures 5(a) and 5(b).

Figure 5 Intrusion Detect Model of the Case – description of the plant (left panel (a)) and attacker's viewpoint (right panel (b))

Table I further provides the various symbols used in Figures 4 and 5 and their meanings, and also offers some background information.

Table I. Symbols map between Figure 4 and Figure 5

Symbol in Fig 5	Symbol in Fig 4	Background information
ZONE0	Outdoor Area	
ZONE1_1	Area within Enclosure	
ZONE2_1	Production Facility	
PERIMETER 1	the boundary of the plant	The left/up/right side are enclosures and the down side is the coastline
PERIMETER 2	The boundary of the production facility	
Main Gate	Main gate	
Dock #1	Dock #1	An attacker may intrude from dock #1 as well as from a ship, for example
Gate	The entrance of the production facility	
T1	Administration Building	Some staff of the plant works in the building
T2	Electrical Supply from Utility	
T3	Cogen Unit/ Cogen Control/Cat Feed Hydrotreater	
T4	Central control	
T5	Tank Farm	They are very close to each other and they always contain dangerous materials. If one of the tanks belonging to the farm is attacked, then all tanks are assumed to be destroyed due to domino effects.
T6	Production facilities in production facility area	They are very close to each other and they always contain dangerous materials. If one of the production facilities is attacked, then all of them are assumed to be destroyed due to domino effects.

Table II gives an indication of the time that is needed to travel from point A to point B in a variety of locations for our illustrative case study.

Table II. Cross Zone Time (illustrative figures)

Zone 0 (Time is indicated in minutes)					
<div> <div>To</div> <div>From</div> </div>	T1	T2	Main Gate	Dock #1	Wall
Anywhere	5	5	5	5	5
Zone 1_1 (Time is indicated in minutes)					
<div> <div>To</div> <div>From</div> </div>	T3	T4	T5	Gate	Wall 2
Main Gate	10	10	15	10	5
Dock #1	6	7	3	10	12
Wall 1	5	5	5	5	5
Zone 2_1 (Time is indicated in minutes)					
<div> <div>To</div> <div>From</div> </div>	T6				
Gate	3				
Wall 2	3				

Table III provides the monetary consequences of the different assets that, if they would be attacked, would materialize.

Table III. Consequence Table (illustrative figures)

Asset Index	Estimated Consequences (Thousand euros)
T1	1000
T2	100
T3	300
T4	800
T5	2000
T6	10000

Consequence estimation should, amongst others, take direct economic loss, casualties, business interruption, environment pollution, as well as potential domino effects to other assets into

consideration. For example, if an attack on T3 will also cause losses in T5 due to domino effects (L_{35} for example), then when measuring the consequences in T3, L_{35} should also be considered.

Table IV. Parameters in each Typical and Assets (illustrative figures)

Typical	Parameter	Values
ZONE 0	α_0	1
ZONE 1_1	α_{1_1}	3
ZONE 2_1	α_{2_1}	6
Main Gate	β_{11}	1
Dock #1	β_{12}	3
Enclosure 1	β_{13}	2
Gate	β_{21}	2
Enclosure 2	β_{22}	3
T1	P_{y1}	0.1
T2	P_{y2}	0.9
T3	P_{y3}	0.7
T4	P_{y4}	0.6
T5	P_{y5}	0.9
T6	P_{y6}	0.99

We assume that while under the same detection level and attack level, zone 2_1 is easier to protect than zone 1_1 and in its turn, zone 1_1 is easier to protect than zone 0, due to some practical reasons (size, for example, since the smaller the area, the easier to protect). Under these assumptions, we have $\alpha_{2_1} > \alpha_{1_1} > \alpha_0$. Similarly, we assume that in perimeter 1, the main entrance is the most difficult access to detect intruders, because there are too many people/vehicles coming in/going out from the main entrance. Dock #1 is the most easy access with respect to intruder detection. Under these assumptions, we have $\beta_{11} < \beta_{13} < \beta_{12}$. Analogously, we use identical assumptions for the accesses of perimeter 2. Regarding P_y , T2/T5/T6 are some sensitive assets, so if

an attacker is able to reach them and carry out an attack, they are very easily destroyed. T1/T3/T4 are some buildings or some equipment that, even in the event that an attacker executes an attack on them, they are difficult to destroy.

Table V provides the cost for the attacker per level of attack, while Table VI gives some figures on the cost of the defender.

Table V. Cost of Attack level (illustrative figures)

Attacker level	Cost (thousand euros)
1	10
2	20
3	40

Table VI. Cost of defend Level (illustrative figures)

Typical	Detect level	Cost (thousand euros)		Detect level	Cost (thousand euros)
Detect in Zone 0	1	40	Detect in Zone 1_1	1	20
	2	60		2	30
	3	100		3	50
Detect at Main Gate	1	20	Detect at Gate	1	20
	2	30		2	25
	3	50		3	40
Detect at Dock #1	1	20	Detect in Zone 2_1	1	20
	2	25		2	30
	3	40		3	50
Detect at Enclosure 1	1	20	Detect in Enclosure 2	1	10
	2	30		2	20
	3	50		3	40

Under the conditions that $k = 3$, $k^e = 3$, $Q = 2$, $M_1 = 3$, $M_2 = 2$, $N_1 = N_2 = 1$, $N_0^a = 2$, $N_1^a = 3$,

$N_2^a = 1$, and let $\tau = 100$, the following information can be computed.

The defender's number of strategies: $N_d = k^{1+\sum_{i=1}^Q (M_i + N_i)} = 6561$

The attacker's number of strategies: $N_a = k^e \cdot \sum_{i=0}^Q \sum_{j=1}^{X_i} (N_{i-j}^a \cdot \prod_{l=1}^i M_l^s) = 51$

There are 8 ($1 + \sum_{i=1}^Q (M_i + N_i) = 8$) typicals in this case, therefore we can map the defender's strategies to strategy codes consisting of 8 digit numbers (a definition of strategy codes was given at the end of section 3.2). The meanings of each number are shown in table VII.

Table VII. The meanings of the 8 typicals in case of our illustrative case

Notation	Meaning	Notation	Meaning
d ₁	Security Alert Level (SAL) in zone 2_1	d ₅	SAL at main entrance in perimeter 1
d ₂	SAL at gate in perimeter 2	d ₆	SAL at dock #1
d ₃	SAL at the enclosure/fence in perimeter 2	d ₇	SAL at the enclosure/fence in perimeter 1
d ₄	SAL in zone 1_1	d ₈	SAL in zone 0

For example, strategy 1122 2321 means that the detection level in zone 2_1 is 1, the detection level at the gate (perimeter 2) is 1, the detection level at the enclosure/fence (perimeter 2) is 2, and so on.

4.3. Solutions of the Illustrative Case-study using the CPP Game

4.3.1. Pure Strategy

Using the parameters given in section 4.2, no Pure Strategy Nash Equilibrium exists in our game theoretical model. The reason no Pure Strategy Nash Equilibrium exists is that in the CPP Game, the two players are outguessing each other's actions. As discussed in section 3.4, when all players are trying to outguess each other(s) action, there is no Pure Strategy Nash Equilibrium. Nonetheless, we find that no matter what the defender's strategy is, the attacker will always attack T5 and T6, as can be seen in Figure 6.

Figure 6. Distribution of Attacker's Best Response

This result is quite reasonable because the most attractive parts of this chemical plant are the production tank area and the product facility area. Other assets, the administration building for example, are either too low-impact or too difficult to attack. The tank area and the production facilities are what makes the chemical plant different from other infrastructures.

4.3.2. Mixed Strategy

If the parameters from section 4.2 are employed, there exists at least one mixed strategy Nash Equilibrium⁽²¹⁾. A general algorithm able to find out all the mixed strategy Nash Equilibria for a game does not exist yet, up to the authors' knowledge. However, Lemke and Howson⁽²⁰⁾ gave an algorithm to find out one mixed strategy Nash Equilibrium.

Table VIII shows one mixed strategy Nash Equilibrium for our illustrative case. Although the defender has 6561 pure strategies, he will only play 3 of them at some probabilities, while the attacker will also only play 3 of his pure strategies at some probabilities.

Table VIII. Mixed Strategy Nash Equilibrium

Pure Strategy of Defender	Probability
$d_1: 1\ 1\ 1\ 3\ 2\ 1\ 1\ 2$	$p_{d_1}: 0.286$

$d_2: 1\ 1\ 1\ 3\ 2\ 1\ 2\ 2$	$p_{d_2}: 0.333$
$d_3: 1\ 2\ 1\ 3\ 2\ 1\ 1\ 2$	$p_{d_3}: 0.381$
Pure Strategy of Attacker	Probability
$a_1: 3\ 1\ 5\ 1$	$p_{a_1}: 0.644$
$a_2: 3\ 1\ 5\ 3$	$p_{a_2}: 0.239$
$a_3: 3\ 2\ 6\ 1\ 1$	$p_{a_3}: 0.117$

Based on formula (15) and (16), the payoffs that players can get from this mixed strategy Nash Equilibrium are in case of the defender €1,941,800 and in case of the attacker €92,634.

In this mixed strategy NE, the defender plays d_1 , d_2 , and d_3 with probability 0.286, 0.333, and 0.381 respectively, while the attacker plays a_1 , a_2 , and a_3 with probability 0.644, 0.239, and 0.117 respectively. Thus there are 9 possible strategy tuples that may happen, which are $\{d_1, d_2, d_3\} \times \{a_1, a_2, a_3\}$. Under each tuple $\{d_i, a_j\}$, we can compute the probability $p_{s(i,j)}$ that the attacker can reach the target successfully, by employing formula (1), and formulas (11)~(14). Table IX shows the results.

Table IX. probability $p_{s(i,j)}$ that the attacker can reach the target successfully

$s_d \backslash p_s$	a_1	a_2	a_3
d_1	0.0737	0.0814	0.0150
d_2	0.0737	0.0582	0.0150
d_3	0.0737	0.0814	0.0107

Thus the expected probability that the attacker will reach the target is $\sum_{i=1}^3 \sum_{j=1}^3 p_{d_i} p_{a_j} p_{s_{i,j}} = 0.0666$.

The investment of the defender in this mixed strategy NE is shown in table X:

Table X. defence investment of each strategy

s_d	C_d
-------	-------

d_1	230
d_2	240
d_3	235

Thus the expected cost of the defence is: $\sum_{i=1}^3 C_{d_i} p_{d_i} = \text{€}235,235$.

If the defender doesn't invest in security, then the probability that the attacker can reach his target $p_{s(0,j)}$ can be computed by employing formula (1), and formulas (11)~(14). Table XI shows the result.

Table XI. probability $p_{s(0,j)}$ that the attacker can reach target when there is no defence

s_a	p_s
a_1	0.8187
a_2	0.9048
a_3	0.8353

The expected probability that he can reach the target is: $\sum_{j=1}^3 p_{s(0,j)} * p_{a_j} = 0.8412$.

In one sentence, we can present the result like: the defender invests €235,235 to improve the intrusion detection probability from $1 - \sum_{j=1}^3 p_{s(0,j)} * p_{a_j} = 0.1588$ to $1 - \sum_{i=1}^3 \sum_{j=1}^3 p_{d_i} p_{a_j} p_{s_{i,j}} = 0.9334$, in such a plant.

5. CONCLUSIONS AND FUTURE RESEARCH

Research in this article explores how game theory can be employed to improve security in chemical process plants. A new mathematical description of a process plant's layout is proposed for easy use by security plant management. The mathematical layout can easily be extended to a multi-plants' layout, in which case there are several sub-zones in zone level 1, and where each sub-zone can be treated as a single plant. Based on the mathematical model, a game-theoretical model called CPP, being single-plant-oriented, is suggested in this article to optimally decide on defences against terrorist intrusion and attack in process plants. An illustrative case is provided to show the applicability of our model in industrial practice.

Our future research will focus on several aspects. First, there is the multi-targets situation. In this article, we assume that the attacker will only attack one target at one time. But more practically, the attacker may deploy bombs simultaneously, or have attack actions at several targets sequentially. Our future research will therefore extend the CPP Game to a multi-targets situation. A second path of further promising research is investigating the sequential game situation. A sequential game is one in which players make decisions (or select a strategy) following a certain predefined order, and in which at least some players can observe the moves of players who preceded them. In the security domain, it is difficult to assess whether the defender can secrete his strategy very effectively, because the attacker will try to get information through various approaches. However, in some situations, the defender will have first-mover advantage. In this situation, the defender will make his strategy known to the public. The third path of future research is that of the incomplete information game. Research in this article assume that players have complete information of their adversaries, which can be true in some situations, but not always. To meet this problem, a Bayesian game can be elaborated and employed.

REFERENCES

- [1]. Brown G, Carlyle M, Salmerón J, Wood K. Defending critical infrastructure. *Interfaces*. 2006;36(6): 530-544.
- [2]. Tambe M (eds). *Security and game theory: Algorithms, deployed systems, lessons learned*. New York: Cambridge University Press, 2011.
- [3]. Bier V, Azaiez M (eds). *Game theoretic risk analysis of security threats*. New York: Springer Science & Business Media, 2008.
- [4]. Tsai J, Kiekintveld C, Ordóñez F, Tambe M, Rathi S. IRIS-a tool for strategic security allocation in transportation networks[J]. 2009

- [5]. Reniers G, Lerberghe P, Gulijk C. Security risk assessment and protection in the chemical and process industry. *Process Safety Progress*. 2014;34(1):72-83.
- [6]. Garcia M L. Design and evaluation of physical protection systems. Oxford: Butterworth-Heinemann, 2007.
- [7]. Zhuang J, Bier V. Balancing terrorism and natural disasters-defensive strategy with endogenous attacker effort. *Operations Research*. 2007;55(5): 976-991.
- [8]. National Commission on Terrorist Attacks upon the United States The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States(2004) (W. W. Norton and Company, New York)
- [9]. Harsanyi J. Games with Incomplete Information Played by "Bayesian" Players, I–III: Part I. The Basic Model&. *Management Science*. 2004 DEC; 50(12_supplement): 1804-1817.
- [10].Harsanyi J, Selten R. A generalized Nash solution for two-person bargaining games with incomplete information. *Management Science*. 1972;18(5-part-2): 80-106.
- [11].Guikema S D. Game theory models of intelligent actors in reliability analysis: An overview of the state of the art. Chapter 2 in Bier VM, Azaiez MN (eds). *Game Theoretic Risk Analysis of Security Threats*. New York: Springer, 2009.
- [12].Homeland Security Advisory Council HSAC. Homeland security advisory system, task force report and recommendations. Technical report, U.S. Department of Homeland Security, September 2009.
- [13].Shor, Mikhael, "payoff". Dictionary of Game Theory Terms, Game Theory .net, <<http://www.gametheory.net/dictionary/payoff.html>>
- [14].Institute of Security Belgium, Handbook "BasisopleidingbestemdvoorLeidendPersoneel van beveiligingsondernemingen" (in Dutch), Ministry of Home Affairs, Brussels, 2013.
- [15].Cox Jr L A T. Game theory and risk analysis. *Risk Analysis*. 2009;29(8): 1062-1068.
- [16].Ezell B C, Bennett S P, Von Winterfeldt D, Sokolowski J, Collins A J. Probabilistic risk analysis and terrorism risk. *Risk Analysis*. 2010;30(4): 575-589.

- [17].Skaperdas S. Contest success functions. *Economic Theory*. 1996;7(2): 283-290.
- [18].Clark D J, Riis C. Contest success functions: an extension. *Economic Theory*. 1998;11(1): 201-204.
- [19].Reniers G, Pavlova Y. Using Game theory to improve safety within chemical industrial parks. London: Springer, 2013; page 40-41.
- [20].Lemke C E, Howson, Jr J T. Equilibrium points of bimatrix games. *Journal of the Society for Industrial & Applied Mathematics*. 1964;12(2): 413-423.
- [21].Nash J F. Equilibrium points in n-person games. *Proceedings of the national academy of sciences*. 1950;36(1): 48-49.
- [22].Gibbons R. A primer in game theory. New York: Harvester Wheatsheaf; 1992. 267p.
- [23].Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, API Recommended Practice 780, 2012
- [24].Lee Y, Kim J, Kim J, Moon I. Development of a risk assessment program for chemical terrorism[J]. *Korean Journal of Chemical Engineering*. 2010; 27(2): 399-408.
- [25].Shor, Mikhael, "sequential game," Dictionary of Game Theory Terms, Game Theory .net, http://www.gametheory.net/dictionary/sequential_game.html
- [26].Reniers G L L, Sørensen K, Khan F, Amyotte P. Resilience of chemical industrial areas through attenuation-based security. *Reliability Engineering & System Safety*. 2014; 131: 94-101.
- [27].Talarico L, Reniers G, Sørensen K, Springael J. MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. *Reliability Engineering & System Safety*. 2015; 138: 105-114.