Optimal patrol scheduling of hazardous pipelines using game theory

Optimal patrol scheduling of hazardous pipelines using Game theory

Amirali Rezazadeh[a,b], Laobing Zhang[b], Genserik Reniers[b,c,d], Nima Khakzad[b]
Valerio Cozzani[a]

a: LISES – Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali, Alma Mater Studiorum – Università di Bologna, via Terracini n.28, 40131 Bologna, Italy
b: Safety and Security Science Group (S3G), Faculty of Technology, Policy and Management, TU Delft, 2628 BX Delft, Netherlands.
c: Faculty of Applied Economics, Research Groups ANT/OR, University of Antwerp, Prinsstraat 13, 2000 Antwerp, Belgium
d: CEDON, KULeuven, Campus Brussels, 1000, Brussels, Belgium

Abstract:

An approach based on game theory is proposed to schedule security patrolling for a pipeline system. The method developed proposes numbers of patrolling paths according to the risk of security incidents on the pipeline system to allow the patrol covering high-risk segments more than low-risk segments. Patrolling of the pipeline system was modelled mathematically, based on time and distance discretization. Patrolling of a single unit that can be a motorcycle, vehicle, a drone or an helicopter was considered, depending on its velocity. The overall approach also examines the presence of security countermeasures on a pipeline system, and their effects on the patrolling schedule. The application of the method is explained by an illustrative case study.

1. Introduction:

Nowadays game theory is widely used in the security domain from cyber security to physical security, and for the allocation of limited security resources to scheduling the patrolling in critical infrastructures. The application of game theory to security is well explained by Tambe (2012), and Bier and Azaiez (2009).

Game-theoretic analyses of conflicts require modeling the probable consequences of each choice of strategies by the players and assessing the expected utilities of these probable consequences. According to Tambe (2012), game theory provides a sound mathematical approach for deploying limited security resources to maximize their effectiveness. The Bayesian Stackelberg game is one special class of game theory and has recently been used for security applications (see Tambe (2012)). In this class of game the players may have incomplete information about either the actions or the payoffs representing other players. Incomplete information is modeled by assuming that players can have different types. Thus the players that know their types will outguess each other's type with the probability distribution over possible types of the other player (that is why it is called Bayesian game). This security game is a sequential or extensive form of games in which the defender starts the game as a leader while the followers, defined as different types of attackers, will observe and respond to the leader.

As mentioned before, one of the applications of game theory in the security domain is to schedule patrolling. Patrolling can be defined as an act of traveling within an area in regular intervals so as to secure it against different threats.

Pita et al. (2008) developed a security game for Randomizing schedules for patrolling, checking, or monitoring in an airport surrounding. Their model called ARMOR (Assistant for Randomized Monitoring over Routes) casts this patrolling/monitoring problem as a Bayesian Stackelberg game. ARMOR has been successfully deployed since August 2007 at the Los Angeles International Airport (LAX) to randomize checkpoints on the roadways entering the airport as well as canine patrol routes within the airport terminals.

Tsai et al. (2009) addressed strategic randomization of security resources by a security game. They developed the Intelligent Randomization in Scheduling (IRIS) system, which is a software to schedule the Federal Air Marshals (FAMs) that provide law enforcement aboard U.S. commercial flights. In IRIS, Tsai et al. (2009) model the problem as a Stackelberg game, with FAMS as leaders that commit to a flight coverage schedule, and terrorists as followers that attempt to attack a flight.

A further application of a security game is Port Resilience Operational/Tactical Enforcement to Combat Terrorism, which is called PROTECT. Bo An et al. (2012) developed this algorithm for United States Coast Guard (USCG) in the port of Boston to schedule its patrols. Fang et al. (2016) employed a Green Security Game to design optimal patrolling paths for protection of wildlife.

An application of a security game for scheduling randomized patrols for fare inspection in transit systems like the Los Angeles (LA) Metro Rail system was studied by Yin et al. (2012). They introduced an algorithm called TRUSTS, which models and schedules patrol units moving along the transit system, inspecting the tickets of passengers.

Also, Aguirre and Taboada (2012) deployed a game theory concept to define a multi-agent patrolling strategy on a national border to achieve a secure country through border protection. Similar works have been done by Basilica et al. (2012) and Gatti (2008).

Alpern et al. (2016), Alpern, Morton, and Papadaki (2011) and Papadaki et al. (2016) mathematically defined graph patrolling games and perfectly solved the game on some special graphs, such as the line graph, etc. However, they modeled the graph patrolling games as a zero-sum game, and in their line graph patrolling game, which is quite similar to the patrolling of a pipeline, the quantitative risk assessment of the line was absent.

Besides patrol scheduling, for other applications of game theory in the chemical security domain, we can refer to Rezazadeh et al. (2016) for securing Oil & Gas pipelines, Zhang and Reniers (2016) and Feng et al. (2016) for protecting process plants from terrorist attacks, and Talarico et al. (2015) for allocating security measures to the chemical transportation network.

In the security risk assessment domain Srivastava and Gupta (2010) introduced a Security Risk Factor Table (SRFT) and created a Stepped Matrix Procedure (SMP) to assess the security risk of oil and gas industry as well as the other chemical process industries. While the SRFT deals with the effects of individual threats, the SMP deals with the cascading (domino) effects. After that Bajpai et al. (2010) have modified the SRFT model by using the concepts of fuzzy logic. These models can be applicable for Oil&Gas pipelines.

Reniers and Dullaert (2011) have made a TePiTri method to determine relative terrorist-related security risk levels of a pipeline transportation system. In the TePiTri method a likelihood grade and a consequence grade are determined by discretizing the pipeline route through an analysis procedure, and these grades define the security risk level of a segment. One of the determining factors of security risk is threat assessment which is well planned by Reniers et al.(2013) in the TARP model for the chemical industry. TARP lists different security threats and proposes a decision flowchart for the assessments and a guideline for revising this threat assessment periodically or if needed.

CCPS (2008) explained qualitative and semi-quantitative approaches for evaluation of safety and security risks using either risk indexing or risk ranking matrixes. CCPS (2010) and API780 (2012) propose a Security Risk Assessment method (SRA) which defines the security risk as a function of Vulnerability, Attractiveness, and Consequences. Also, they define a procedure by which the security risk can be found from a ranking matrix through asset-based and scenario-based approaches.

Moore (2013) examined the key elements of this API SRA process and discussed how forward thinking organizations might use risk-based performance metrics to analyze facility security postures and identify appropriately scaled systematically and fiscally responsible countermeasures based on current and projected threats.

In this paper, we apply the Bayesian Stackelberg game for scheduling the patrolling on a pipeline system. This game theoretical model is called **P**ipeline **P**atrolling **G**ame (**PPG**). PPG is a Bayesian Stackelberg game in which the defender is the leader whereas the attacker is the follower. In this methodology, there is only one type of the defender, but the attacker can have different types. Like the ARMOR and the IRIS, PPG focuses on one security activity per application, which is patrolling. For dealing with several security activities, however, we refer to Game-theoretic Unpredictable and

Randomly Deployed Security (GUARDS) by Pita et al. (2011), used by the United States Transportation Security Administration (TSA) in resource allocation tasks for airport protection at over 400 airports. The PPG has been built based on a credible security risk assessment. Each part of the pipeline system due to its location, design and operation characteristics can be more vulnerable in comparison to other parts. These different parts can have a different attraction or perceived value from the attacker and the defender points of view. Therefore a risk analysis framework is required to systematically examine the components and characteristics of the risk of different pipeline segments and then presents the results in a rank ordering form, to build the utility functions that estimate the gain or loss of the players.

Among the abovementioned security risk assessments methods, the API SRA method, providing a risk ranking baseline, will be manipulated for the security risk assessment in the PPG model.

In this paper, section 2 discusseses the players of the game. Modeling of the patrolling is treated in section 3. Section 4 explains security risk assessment of PPG. For solving the proposed security game the PPG algorithm is introduced in section 5. In section 6 we will explain an illustrative case study in addition to its results and discussion. Finally, in section 7 conclusions are provided. Some details of calculation are given in Annex 1 and 2.

2. Modelling the players of the game

Today security forces are faced with different types of adversaries with various characteristics. Each of them has its specific intention and capabilities. They may plan different malicious acts to achieve their separate goals. Accordingly, when the security of pipelines or any other facility is discussed, at first, the type of facing an attacker should be clarified. Also, it is important to categorize them and evaluate their intentions, capabilities to attack and the level in which they are active in a region.

For developing the PPG, only one patrolling unit that can be a vehicle, helicopter or drone and only one intruder who can be any type of attacker are considered. The pipeline route will be separated into some segments to model patrolling paths. In this game, the main assumption is that, if the patrol is present at a pipeline segment location, this will guarantee to stop the attacker at that location, and the attack cannot occur successfully. Moreover, it is assumed that if the security barriers of the pipeline system detect any malicious act, the defender again can stop the attack or prevent it from happening. The attacker has complete information about the probability of which the patrol may be present at a segment, and they are fully rational, but they do not know the exact patrolling plan of security forces.

The PPG game is a 2-player game, namely, the patrol and the attacker. Since “defender” is a general term who can be a security department of a pipeline company planning patrolling paths for a patrol, indeed the front player of the attacker is the patrol; from now on, we call leader or defender the patrol. Therefore the players of the PPG game are the patrol and the attacker. To reduce ambiguity, the Patrol is considered as a female and the attacker as a male so that in the remainder of the paper, the pronoun “he” will be used for an attacker and “she” for a patrol.

2.1. Categorization of attacker types

We are going to categorize the different types of attackers systematically. Therefore we applied API 780 (2012) categorizing attackers to international and domestic terrorists ($k = 1$), criminals ($k = 2$), disgruntled personnel ($k = 3$), or extreme activists ($k = 4$). These different adversaries pose different threats to a pipeline system. Accordingly in this paper we are going to carry out a security risk analysis for the different types of adversaries separately.

2.2. Scenario identification

For evaluating the consequence of a security incident, a scenario analysis should be applied. To do so, experts of the security department of a pipeline company should list all the expected scenarios from the adversaries, and then categorize them according to the type of the attacker. In Table 1 some of the common scenarios are illustrated.

Table 1, typical scenarios for various adversaries

	Terrorist	Criminal	Disgruntled insider	Activist
Scenario	Causing an explosion	Operation disruption	Operation disruption	Operation disruption
	Release of chemical	Release of chemical	Release of chemical	Damage to properties
	Theft	Theft	Theft	-
	-	-	Damage to properties	-

If more than one scenario is possible, the security department can choose either the worst case scenario or the most credible scenario for each type of the attacker, based on their policies, and consider it for further processing (consequence assessments). Thus each type of attacker is paired with a particular scenario. As an illustration, the consequence of a terrorist attack can be a pipeline explosion, while the consequence of a criminal or a disgruntled insider may be a theft or an operation disruption, and the consequence of activist interference can be damages to properties resulting in operation disruption.

2.3. Threat assessment

According to CCPS (2010), threats can come from these three sources:

- Internal
- External
- Collusion (Internal and External)

Threat Acts may be perpetrated by insiders, outsiders or a combination of the two. Insiders are those personnel that has internal knowledge routine and unescorted access to areas where outsiders are not allowed without an escort. Collusion between the two may be the result of monetary incentive, ideological sympathy, or coercion.

The threat can also be defined as the intention and capability of a threat to undertake actions that would be detrimental to the pipeline system. Threat assessment is an important part of a PPG security assessment, especially in light of today's international terrorism. There is a need to determine the threats facing the pipeline system properly in building the present security game. This section describes a threat assessment approach which is derived from API 780 (2012).

In characterizing the threat to a pipeline segment, the security department examines the historical record of security events and obtains available general and location-specific data and intelligence information from governmental organizations and other sources. Then they should classify these threats based on the general history of threats and their capability and intent to attack pipeline system. The threat of an attacker of kind k can be expressed as an integer value ranging from 1 to 5. Table 2 reports a five-level ranking system for defining threat ranking in each *Pipeline Segment*.

Table 2, Threat Classification for attacker of type k

T^k	Description	Level	Conditional Probability
0	Indicates little or no credible evidence of capability or intent, and no history of actual or planned threats against the asset or similar assets (for example: "No expected attack in the life of the facility's operation").	Very Low	0.2
1	Indicates that there is a low threat against the asset or similar assets and that few known adversaries would pose a threat to the asset (for example: "> or = 1 event is possible in the life of the facility's operation").	Low	0.4
2	Indicates that there is a possible threat to the asset or similar assets based on the threat's desire to compromise similar assets, but no specific threat exists for the facility or asset (for example: "> or = 1 event in 10 years of the facility's operation").	Medium	0.6
3	Indicates that a credible threat exists against the asset or similar assets based on knowledge of the threat's capability and intent to attack the asset or similar assets, and some indication exists of the threat specific to the company, facility, or asset (for example: "> or = 1 event in 5 years of the facility's operation").	High	0.8

4	Indicates that a credible threat exists against the asset or similar assets and that the threat demonstrates the capability and intent to launch an attack, and that the subject asset or similar assets are targeted or attacked on a frequently recurring basis, and that the frequency of an attack over the life of the asset is very high (for example: "1 event / event per year").	Very High	1

For instance, from Table 2, if the terrorist threat is very high, their threat Level will be equal to 4, and it is presented by T^1=4.

In fact in a Bayesian Stackelberg game, the probability distribution of different types of a player should be known. Consequently, we are going to define a conditional probability for each type of the attacker to show how likely this type of attacker will contribute in a security incident in comparison to the others. Thus for solving the PPG, the probability distribution over four types of the attacker is identified as ρ^K, which represents the conditional probability if the attacker has type k. The ρ^K is defined based on the threat level from Table 2:

Equation 1

$$\rho^K = \frac{T^k}{\sum_{i=1}^{4} T^i}$$

For example, if ρ^2 is equal to 0.4, the attacker type 2 is 40% probable to be a criminal.

2.4. Identify player types

Concerning API 780 (2012), we classified the expected consequences of security incidents to:

I. Fatalities and injuries
II. Environmental impacts
III. Property damage
IV. Business interruption
V. Damage to reputation or negative publicity

These types of consequences will provide us a framework for categorizing attacker types. Since each type of adversary has its intention and follows distinguished objectives, each kind of consequences has a specific value for them. In other word, based on the characterization of attacker types, the same consequences may have a different value for them. Therefore, in the PPG security risk assessment we identify these various perceived values by a discrete set of weighing factors (indicated by WF)) for each kind of consequences, it means for different attacker types, the experts of the security department should define a distinct set of WF for separate kinds of consequences of a security incident (expert based). It is clear that, these kinds of consequences will have a different contribution to the PPG security risk assessment.

In this study, disparate types of adversaries are presented by distinct sets of WFs associated with each type of consequences. Table 3 shows example sets of WFs for characterizing the attacker in PPG. Similarly, the consequences have different values for the patrol. So, in Table 3 also the patrol is characterized by a set of WFs indicating her perceived values of the consequences.

Table 3, set of WF identifying player types

Kind of consequence	WF				
	Terrorist	Criminal	Disgruntled insider	Activist	patrol
Fatalities and injuries	3	0	0	0	3
Environmental impacts	1	0	1	3	1
Property damage	2	3	1	2	2
Business interruption	2	0	2	2	1
Damage to reputation or negative publicity	3	0	3	3	2

3. Strategy Modelling

PPG player's strategies are modelled in this section. First of all, the pipeline system being patrolled as well as the patrolling time are segmented in sub-section 3.1. Based on this segmentation, the patrolling routes are defined in sub-section 3.2. Finally in sub-section 3.3 and 3.4 the game strategies for the attacker and the patrol are defined.

3.1. Segmentation

In PPG we discretize the time and route into intervals that are called ***Time Segment*** and ***Pipeline Segment***, respectively. To do this, first of all, we divide the time into equal segments. Then the pipeline route is discretized according to equal time intervals into various *Pipeline Segments*.

In the first step of segmentation, the discretization of time is performed according to three factors: (i) the speed of patrol, (ii) the length of the pipeline, and (iii) the length of the time of patrolling. Then a number of time intervals and their duration are estimated. The duration of time intervals should be equal.

In the second step, the pipeline route is discretized to *Pipeline Segments*. The length of each *Pipeline Segment* is not necessarily equal to each other.

Division of the pipeline route is based on the main assumption of PPG. For this purpose, these segments should be thoroughly visible for the patrol as long as she is present in that segment. In other words, as she enters the *Pipeline Segment* and until she leaves, she should be able to detect any movement from the attacker in that segment. Therefore the two determining factors for pipeline route segmentation are natural or man-made visual obstacles.

The *Time Segments* are presented with nodes indicated by j. There will be two nodes, one for the beginning and the other for the end of the *Time Segment*. For example, in case of 20 *Time Segments*, there will be 21 nodes from $j = 0$ to $j = 21$. In this description, the nth *Time Segment* is from node $j = n - 1$ to node $j = n$. (See Figure 1, x axis)

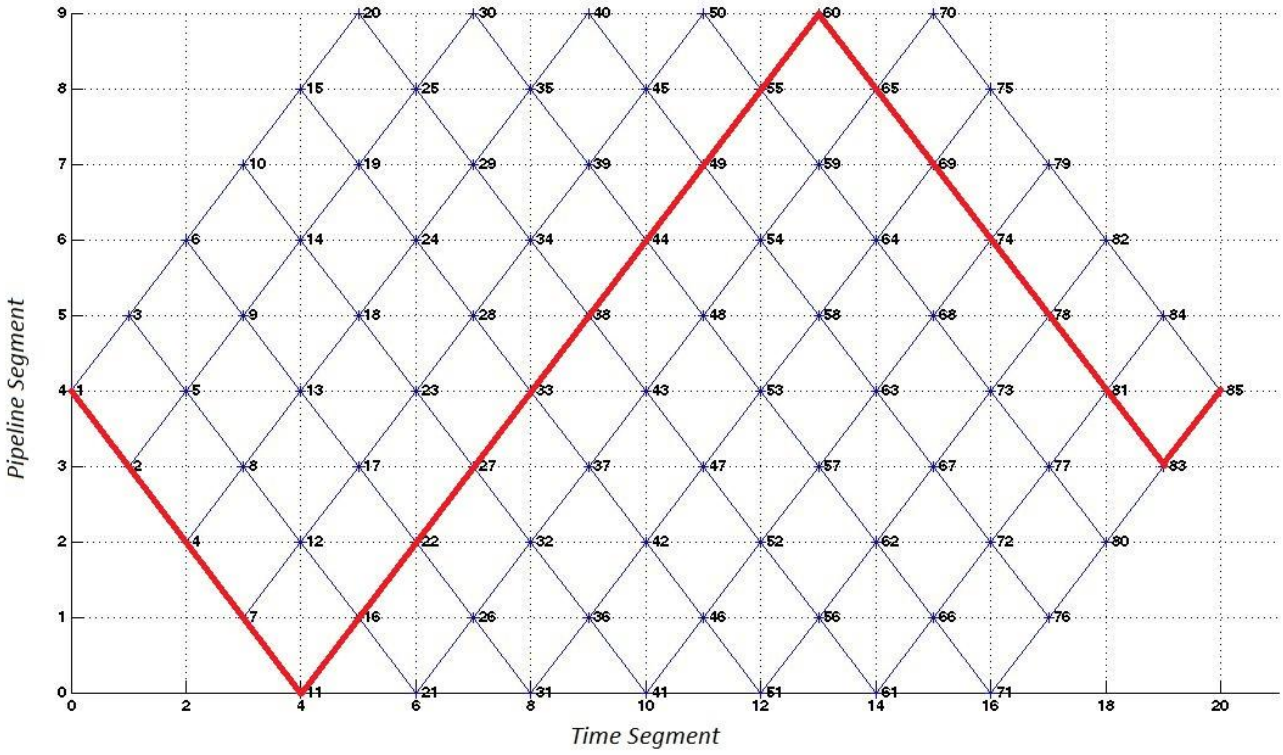

Figure 1, Graphical model of patrolling path

The PPG is designed to schedule patrolling in day or night separately. Thus the game should be run one time to schedule the patrolling during the day and one time to schedule it in the night. Also, the relatively lower visibility at night is a determining factor that changes the length of segments.

In PPG, the *Pipeline Segment*s are determined by nodes. For each *Pipeline Segment,* we define two nodes at both ends. So two adjacent *Pipeline Segments* have one shared node that is the end of the first segment and the beginning of the second one. These nodes are indicated by i and if we have 9 *Pipeline Segment*s, there will be 10 nodes from $i = 0$ to i$= 9$. Consequently the nth *Pipeline Segment* is between node $i = n - 1$ and node $i = n$ (See Figure 1, the y axis).

Subsequently, a Length Examination test should be performed to identify whether or not the length of *Time Segment* is enough to pass and inspect the *Pipeline Segments* completely. If not, the algorithm goes back to step one to modify the time segmentation and repeat the iteration to reach an applicable segmentation in which all the *Pipeline Segments* can be inspected thoroughly with dedicated *Time Segment*.

This segmentation procedure is presented schematically in Figure 2. For example, assume that the security department of a pipeline company intends to schedule the patrolling on a 5 km sweet gas pipeline between city A and B in a day shift of 1.8hr by one patrolling unit, which has an average speed of about 20km/hr. The time can be divided into 20 *Time Segments*, each of about 6 min, and 9 *Pipeline Segments* are defined on this pipeline route. Considering the accessibility of *Pipeline Segment*s and the obstacles that limit the visibility, these *Pipeline Segments* have a lenght between 0.5 to 0.8 km.

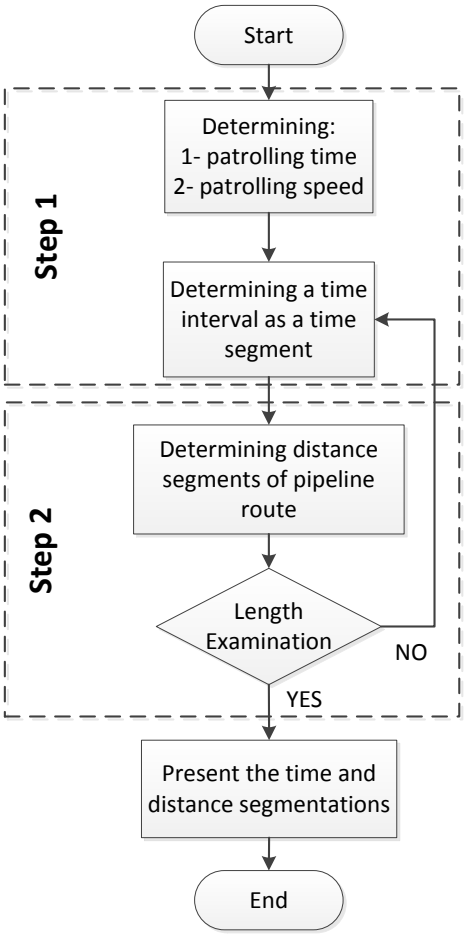

Figure 2, Flowchart of segmentation procedure

3.2. Route identification

Following previous subsection, there is a fixed number of *Route* and *Time Segment*s. The patrol starts from *Time Segment* one and as time goes on she passes all *Time Segments* till the end of her duty. In each *Time Segment,* the patrol stays in one *Pipeline Segment,* and she inspects that segment

thoroughly. As time passes from one *Time Segment* to the next, the patrol should decide where to go for the next time interval. Since each *Pipeline Segment* is shown with two nodes at the both ends, at the end of each *Time Segment* the patrol will be at one of these two nodes. Then they have two options: to come back to the previous node which means stay in their current *Pipeline Segment* or go to the next node to inspect the next *Pipeline Segment*. In this patrolling schedule, as time is passing, *Time Segment*s proceed; and the patrol can go forward, backward or stay in the same segment.

The temporal and spatial starting points are arbitrary, but the entire patrolling should take place during the day or night. Because the visibility in night and day can be different, the PPG should schedule the patrolling for day and night separately. Also, the weather condition and thus visibility variation can result in different segmentation: the PPG will have a separate schedule in this case.

The patrolling schedule can be represented graphically. For instance, following the example of section 3.1, a Patrolling path can be defined by the bold red colour line in Figure 1. In that illustration path, patrol started inspecting the pipeline system from the end of *Pipeline Segment* 4 and then she went backward to the beginning of the pipeline route. After that, she went straight to the end of the route, *Pipeline Segment* 9. Then she came back to *Pipeline Segment* 4 and inspected it in two *Time Segments* till the patrolling time ended. As you see, she finished inspection at the end of *Pipeline Segment* 4 where she started the patrolling.

The number of feasible paths would increase exponentially as the number of pipeline segments and time segments increase. For instance, the case shown in Figure 1, has more than 1000 paths. PPG will examine which paths are better to follow by the patrol to secure the pipeline system more effectively. Hence, individual patrolling paths are deemed as available strategies for the patrol, and this will be explained more in subsection 3.4 as the patrol's strategy.

3.3. Attacker strategy

The attacker faces a whole pipeline system with its different *Pipeline Segment*s as available options for his attack. Accordingly, the attacker's strategies are different segments of the pipeline route.

Equation 2

$$S_a^n = The\ n^{th}\ stratgy\ of\ the\ attacker = The\ n^{th} Route\ Segment$$

From the previous example shown in Figure 1, there will be nine strategies for attacking. The attacker will analyze to attack one of either *Pipeline Segment* one, as his first strategy, or *Pipeline Segment* 2 as his second strategy, till *Pipeline Segment* 9 to obtain the highest results.

3.4. Patrol strategy

The patrol strategies are derived from the probability of being present in a *Pipeline Segment*. This probability is called the Probability of Coverage(PoC). For each *Pipeline Segment,* PoC is defined as:

Equation 3

$$PoC = \frac{Number\ of\ Time\ Segments\ that\ the\ Defender\ spends\ in\ a\ route\ segment}{Total\ number\ of\ Time\ Segments}$$

The patrol has some different paths to choose from. Each patrolling path presents one set of PoC on different *Pipeline Segments*. Therefore along with Fig.1, the patrolling paths can be represented as sets of PoCs which the patrol provides for a pipeline route. This set of PoCs for the bold patrolling path of Fig.1 can be shown in Table 4:

Table 4, example of PoC distribution on pipeline *Pipeline Segments*

Pipeline Segment	1	2	3	4	5	6	7	8	9
PoC	$^2/_{20}$	$^2/_{20}$	$^2/_{20}$	$^4/_{20}$	$^2/_{20}$	$^2/_{20}$	$^2/_{20}$	$^2/_{20}$	$^2/_{20}$

If all the patrolling paths are represented as in Table 4, it can be inferred that some of them have the same distribution of PoC s on different *Pipeline Segments*, meaning that they are equivalent. Consequently, we can combine these equivalent patrolling paths. This combination plays a crucial role in solving the PPG in the case of facing long pipeline routes and several *Pipeline Segments*; because otherwise, the game may become very large and complicated and hence difficult or impossible to solve.

Therefore, many patrolling paths may become equivalent, and they can be categorized in a set of paths with the same distribution of PoC. These categories are indicated by Γ_n where n refers to the n^{th} patrolling path category. Hereinafter each of these patrolling path categories is considered as one of the patrol's strategies. As a result the patrol strategy is shown as:

Equation 4

$$S_d^n = \text{The } n^{th} \text{ strategy of the patrol} = \Gamma_n$$

Definition 1. A path category is called Feasible Path Category (FPC) if at least one patrolling route can be generated.

For example, in the case shown in figure 1, $\Gamma = (0,0,2,4,2,2,2,0,0)$ is a FPC, since at least the bold path shown in figure 1 can be generated according to Γ, while $\Gamma = (2,2,2,0,2,2,2,0,0)$ is not an FPC, since the patrol cannot spend some time in segment 1,2,3 and 4,6,7 respectively but spend no time in segment 4. Thus no route can be generated according to this Γ.

Observation 1. Any path categories $x = (x_1, x_2, \dots, x_{nSeg})$ which satisfies the following constraints c1 to c6 is an FPC (sufficient condition), and any FPC should satisfy these six constraints (necessary condition).

$$\sum_{i=1}^{nSeg} x_i \le nT \quad \text{(c1)}$$
$$x_i \in \mathbb{Z}_0^+, x_i \; is \; a \; even \; number \quad \text{(c2)}$$
$$x_i \le nT - 2 \cdot (i - s - 1), \quad i = s+1, s+2, \dots, nSeg \quad \text{(c3)}$$
$$x_i \le nT - 2 \cdot (s - i), \quad i = 1,2, \dots, s \quad \text{(c4)}$$
$$x_i \ge \varepsilon \cdot x_{i+1}, \quad i = s+1, s+2, \dots, nSeg - 1 \quad \text{(c5)}$$
$$x_{i+1} \ge \varepsilon \cdot x_i, \quad i = 1,2, \dots, s-1 \quad \text{(c6)}$$

In which $nSeg$ denotes the number of route segments, nT denotes the number of time segments, $s = 0,1, \dots, nSeg$ is the start point, $\varepsilon > 0$ is a small positive real number.

Proof: For the sufficient condition, we construct a patrolling path for the given plan category which satisfies these constraints c1 to c6. Given the x which satisfies these constraints, the patrol starts from the start node, goes to one direction until the last segment k which satisfies $\mathrm{x_k} > 0$, and she oscillates in this segment until she stays enough time in this segment, then she goes to the segment $\mathrm{x_{k-1}}$, and she oscillates in this segment until she stays enough time in this segment, and so forth. When she comes back to the start point, she goes to another direction and repeats the procedure. By obeying these steps, the patrol will find a patrolling path which satisfies the coverage constraint.

For the necessary condition, constraint c1 is obvious; constraint c2 reflects that the patrol will start from one node, and finally will come back to the start node; in this case, she will definitely stay in each segment for even times; constraint c3 and c4 reflect the fact that, starting from node i, the time the patrol is spending on further pipeline segments will not exceed the total time minus the time she walks from the starting node to the further segments. In Figure 1, c3 and c4 are shown as the trapezoid shape of the graph. constraint c5 and constraint c6 indicates that if the patrol spends some time on further segments, she should spend some time on closer segments since she has to walk to further segments through the closer segments.

Each of these defensive strategies consists of a patrolling path. It is assumed that if the security measure of pipeline system detects the malicious act, the patrol can stop the attack. For specifying this assumption, according to Owen (2013), the ability of security barriers for detection is defined as Probability of Detection (PoD) and formulated as Equation 5:

Equation 5

$$PoD = \frac{Number\ of\ correct\ detections}{Number\ of\ experiments}$$

Countermeasures can be classified in Table 5 with refers to Talarico, Sorensen, et al. (2015). These security measures are installed on a pipeline system to reduce the likelihood and/or the consequences of the security incident.

Table 5: classification of countermeasures for the pipeline system

Goal: Reducing Likelihood Countermeasures		
Group	Description	Abbreviation
Traditional Countermeasures*	Lighting	Li
	Fences	Fe
	Access Control ID	AC
	Integrated electronic access control	IEA
	Ground Patrol	GP
	Arial Patrol	AP
Advanced Countermeasures*	Open-Air Intrusion Detection Sensors	PIDS
	Not Open-Air Sensor	NOAS
	Remote Sensing Systems	RSS
	Drones Unmanned Aerial Vehicle	DUAV
Recent Technologies*	Distributed acoustic sensing	DAS
	Thermal Infrared Sensor	TIS
	Other ground sensors	GS
Goal: Reducing Consequences Countermeasures		
Other Countermeasures	Trained Personnel	TP
	Isolation Valve and ESD	ESD
	Non-flammable supports	NFS
	Procedures and emergency response plans	ERP
	Non-flammable valves and gaskets	NFVG
	PMS or monitoring system	PMS

As mentioned before, in PPG, it is assumed that if the patrol is present in a pipeline segment, she will catch the attacker and stop the attack. Therefore catching the attacker and stop the security incident depends on two factors, the Probability of Coverage (PoC) and Probability of Detection (PoD). The prospect of stopping adversarial attempts or security incidents is described with Probability of Stop (PoS) and can be clarified as Equation 6:

Equation 6

$$PoS = Probability(\ patrolling\ coverage \cup countermeasures\ detection) = PoD + PoC - [PoD * PoC]$$

The security countermeasures are designed and installed on pipeline system, so they have a constant PoD, nonetheless the PoC is variable and we are examining its different values as patrol strategies.

The PoD and the PoC are derived from two independent events, the former reflects the effectiveness of a physical security countermeasures and the latter indicates the activities of the patrol.

4. Payoff modeling:

The PPG is built based on the security risk assessment (API780) of the pipeline system to identify the patrolling schedules. The PPG risk assessment provides the basis for rank ordering of the penalties and the rewards of players in a defined *Pipeline Segment* according to their specific types. The penalty and the reward indicate benefits that the players can gain or lose in the game. These outcomes are calculated according to the consequences of the identified scenarios and their perceived values for both sides of the game. For this purpose, each *Pipeline Segment* is subjected to independent security risk assessment. Thus, PPG risk assessment will be applied to each *Pipeline Segment* separately. It should be stated that for every attacker type in each *Pipeline Segment,* based on the associated scenario, his penalty and reward of attack is different. For example, having four types of attackers leads to four sets of penalty and reward ranks in any *Pipeline Segment.*

From sub-section 4.1 to 4.4 all the penalties and rewards of attacking and defending the pipeline system for the patrol and attacker are evaluated. Later on, in sub-section 4.5, these disparate sets contribute to the calculation of payoff functions.

4.1. Attacker's Reward

As stated before the probable consequences of security incidents are characterized by five different kinds. According to API recommanded practice 780 each consequence kind is classified from A to E, where A indicates the lowest level of impacts while E shows the highest level. Table 6 presents these ranking in a descriptive way.

Table 6, Ranking of Fatalities and injuries

Kind	Description of classes	Class
i. ii. iii. iv. v.	Possibility of minor injury No environmental impacts. Up to $25,000 loss in property damage. Very short-term (up to 1 week) business interruption/expense. Very low or no impact or loss of reputation or business viability; mentioned in the local press.	A
i. ii. iii. iv. v.	Serious Injuries but no fatalities Minor environmental impacts to the immediate incident area only, less than one year(s) to recover. $25,000 to $100,000 loss in property damage. Short term (>one week to 1 months) business interruption/expense. Low loss of reputation or business viability; query by a regulatory agency; significant local press coverage.	B
i. ii. iii. iv. v.	Serious Injuries and up to 5 fatalities Environmental impact, ten year(s) to recover. $100,000 to $1000,000 loss in property damage. Medium term (1 to 6 month) business interruption/expense. Medium loss of reputation or business viability; the attention of regulatory agencies; national press coverage	C
i. ii. iii. iv. v.	Possibility of 5 to 20 fatalities; Very large environmental impact, between 10 and 100 years to recover. $1000,000 to $10,000,000 loss in property damage. Long term (6 months to 2 years) business interruption/expense. High loss of reputation or business viability; prosecution by the regulator; extensive national press coverage.	D
i. ii. iii. iv. v.	Possibility of more than 20 fatalities from large-scale toxic or flammable release; Major environmental impact (e.g. large-scale toxic contamination of public waterway), the poor chance of recovery. Over $10,000,000 loss in property damage. Very long-term (>two years) business interruption/expense; large-scale disruption to the national economy, public or private operations; loss of critical data. Very high loss of reputation or business viability; international press coverage.	E

After determining the class of each kind of consequences, we can summarize these evaluations in Table 6, in which each class has a relevance of 1, 2, 3, 4 and 5 for A, B, C, D and E, respectively. Because different types of attackers are seeking to various outcomes, the value of the results or their rewards in the case of a successful attack is different. Then the calculation of the Reward for each type of the attacker, whenever he attacks successfully to a specific *Pipeline Segment* (e.g., if the terrorist explodes

the pipeline) can be done in a way which is illustrated in Table 7. WFs are derived from Table 3 and in this example WFs are belong to terrorist.

Table 7, Calculation of the attacker's reward

R_a^1							
Type of consequence	WF	A	B	C	D	E	Score
		1	2	3	4	5	
Fatalities and injuries	3		3*2				6
Environmental impacts	1			1*3			3
Property damage	2	2*1					2
Business interruption	2					2*5	10
Damage to Reputation or Negative Publicity	3				3*4		12
						Sum	33

Like Table 7, for each type of attacker, we can find the rewards separately. Specifically, there are four types of attackers, so four disparate attacker's rewards will be found. For example R_a^1 and R_a^2 indicate the Rewards of Terrorists and criminals, respectively, for attacking the pipeline.

4.2. Patrol's Penalty

From the patrol's point of view, the consequences of security incidents on the pipeline system have particular effects on the company and also on the society where the incident happens. The fatalities, environmental impact or other kinds of damages have different values for the patrol compared to the attacker.

Following Table 6, the security department has assigned a set of WFs for various kinds of consequences. These WFs reflect the perceived values of each kind of consequences and their contributions to estimating the patrol's penalty when a security incident happens.

Next, similar to the calculation of the attacker's reward through Table 7, the Penalty for the patrol after a successful attack can be estimated by the same procedure. It should be noted that the penalty of the patrol is the same for all types of attackers.

4.3. Patrol's Reward

Before, we discussed the outcomes in case the security incident takes place. Now we are going to find the gains of both players – attacker and patrol – if the patrol stops the incident from happening.

Aside from preventing direct consequences, stopping the security incidents can have some benefits for the patrol, such as obtaining critical information about the vulnerabilities and weak points in the security measures, gaining a positive impact on the effectiveness of the security team along with favorable feedbacks from public media. Accordingly, the calculation of the reward of the patrol facing attacker's type k (indicated as R_d^k) can be formulated like Table 8. For instance R_d^1 means the Reward of the patrol if she stops the terrorist from any security incident while R_d^2 is her reward in preventing such an incident from criminals. In this table, for each type of attacker, a score can be assigned to specific kinds of consequences, and the summation of the scores can be deemed as the patrol's Reward. Table 8 presents an example of Patrol's Reward calculation (later it will be used in our case study).

Table 8, calculating the patrol's Reward

Kinds of consequence	R_d^k			
	R_d^1	R_d^2	R_d^3	R_d^4
	Terrorist	Criminal	Disgruntled insider	Activist
Information (5-10)	9	5	7	6
Media (1-5)	5	4	1	3
Reputation (1-5)	5	5	3	4
Sum	19	14	11	13

4.4. Attacker's Penalty

After an unsuccessful attack to a *Pipeline Segment,* the attacker may be caught by the security forces, and he will lose all of his investments. The most important loss of the attacker is the information that he will give to the patrol. This information can have more significant value if he belongs to a larger group. Also, the unsuccessful security incidents make the security measures stricter and actually improve the security level.

The Penalty of the attacker of type k, indicated by P_a^k, when he is stopped by the patrol, can be estimated similar to Patrols Rewards. There are three kinds of consequences for the attacker after being stopped by the patrol such as Information, Investment attack, Sentenced to the jail. For each kind, a score from 1 to 5 can be given. Like Table 8, the summation of these scores presents the attacker's Penalty.

Here P_a^1 means the Penalty of the terrorists when they are stopped by the patrol whereas P_a^4 is the activist's Penalty for the unsuccessful attack.

4.5. Payoff function:

For calculating the payoff to each player when the patrol faces the attacker of type k and in case of the patrol's pure strategy i (the patrol covers the pipeline system with Γ_i) and attacker's pure strategy j (a *Pipeline Segment* j is the attacker's choice); if the attack fails, then the patrol would gain the reward R_d while the attacker would receive a penalty P_a ; otherwise the patrol would receive a penalty P_d and the attacker would gain a reward R_a .

The U_a^k is defined as a payoff for the attacker of type.

Equation 7

$$U_a^k(S_d^i, S_a^j) = (1 - PoS) * R_a^k - PoS * P_a^k$$

Similarly the U_d^k is the patrol payoff facing the attacker of type k.

Equation 8

$$U_d^k(S_d^i, S_a^j) = PoS * R_d^k - (1 - PoS) * P_d$$

The PoS is the probability of stopping the attacker by the patrol. The whole process of PPG model can be presented schematically in Figure 3.

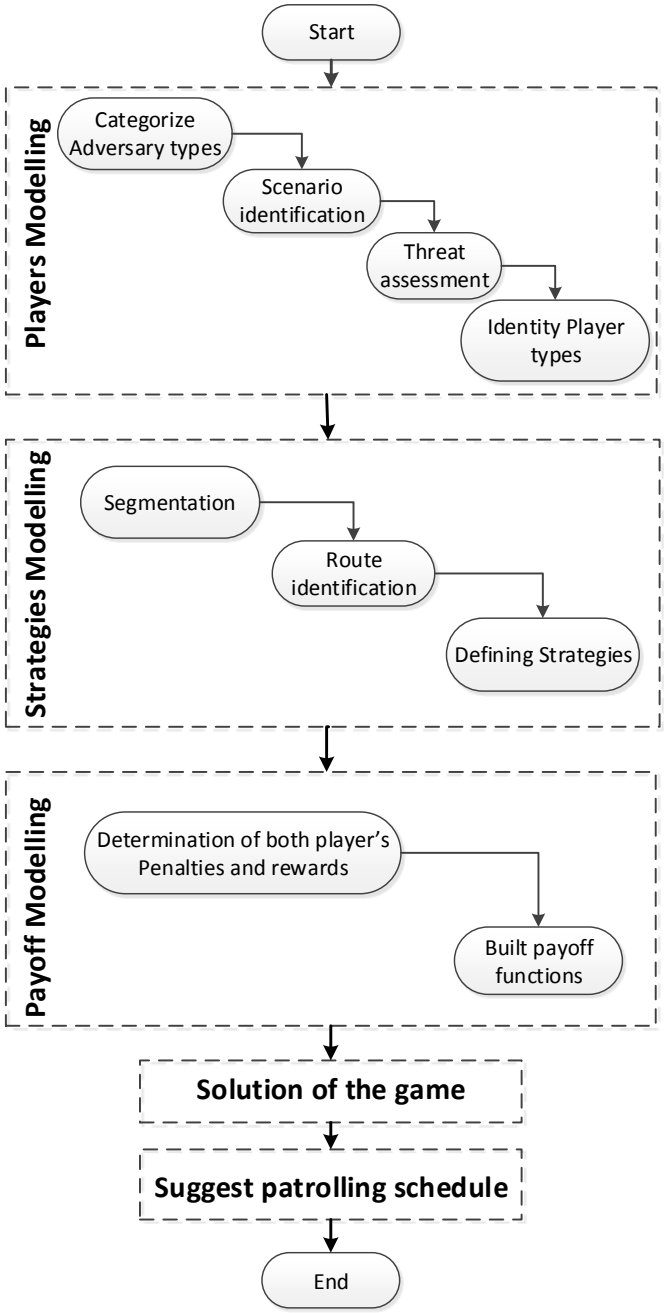

Figure 3, schematic presentation of PPG process

5. PPG algorithm

The PPG is a Bayesian Stackelberg game: the defender moves first, considering the potential different types of attackers, and knowing that the attackers will play their best response to her committed strategy, thus she plays accordingly. To this end, the so-called Strong Stackelberg Equilibrium can be used to predict the output of the game.

Definition 2: A Strong Stackelberg Equilibrium (SSE) (x^*, q) for the PPG can be defined as:

$$x^* = arcmax(\sum_{k=1}^{4} \rho^k \cdot U_d^k(x, q^k(x)))$$

$$q^k(x) = arcmax U_a^k(x, q^k), \forall \mathrm{k} = 1,2,3,4$$

In which x is the FPC as defined in definition 1 in section 3.4, a vector with length of number of route segments; ρ is the Bayesian probability of different types of attacker, as defined in Equation 1 in

section 2.3; U_d^k (U_a^k) is the patrol's (attacker's) payoff when facing the k^{th} type of attacker, as defined in Equation 7 and 8, in section 4.5; q denotes the attacker's best response to the patrol's committed strategy.

For solving the PPG game and finding the SSE, an mixed-integer linear programming (MILP) algorithm is proposed. For the sake of clarity, all the inputs of the algorithm are summarized in Table 9, and variables are presented in Table 10.

Table 9, Input of the algorithm

Notation	Definition	comments
Ψ	Set of different attacker types	terrorist, criminal, activist, etc.
$nSeg$	Number of route segments	
nT	Patrolling time segments	
s	Patrolling start point	s can be a integer from 0 to $nSeg$
RA^k	Reward vector for the k^{th} type of attacker	It is a $1 \times nSeg$ vector, for all $k \in \Psi$
RD^k	Patrol's Reward vector for the k^{th} type of attacker	It is a $1 \times nSeg$ vector, for all $k \in \Psi$
PA^k	Penalty vector for the k^{th} type of attacker	It is a $1 \times nSeg$ vector, for all $k \in \Psi$
PD^k	Patrol's Penalty vector for the k^{th} type of attacker	It is a $1 \times nSeg$ vector, for all $k \in \Psi$
PoD	Probability of detection	It is $1 \times nSeg$ vector
ρ^k	probability if the attacker has type k	
T	Threat of each attackers	It is a $1 \times \lvert\Psi\rvert$ vector

Table 10, Variables of the algorithm

Notation	Definition	comments
x^*	time segments allocation plan	It is a $1 \times nSeg$ vector, and $\sum x_i \leq nT$
q^k	Strategy vector of the k^{th} type of attacker	It is a $1 \times nSeg$ vector, and $q_j^k \in \{0,1\}$, and $\sum q_j^k = 1$, for all $l \in \Psi$
a	Attacker's optimal payoff	It is a $1 \times \lvert\Psi\rvert$ vector
γ^k	Patrol's optimal payoff facing attacker of type k	

Algorithm 1 finding the optimal PoC.

$$max \sum_{k\in\Psi} \rho^k \cdot \gamma^k \quad \text{(OF)}$$

$$\sum_{i=1}^{nSeg} x_i \leq nT \quad (1)$$

$$\sum_{i=1}^{nSeg} q_i^k = 1 \quad (2)$$

$$0 \leq a^k - \left[\left(1 - \mathrm{PoS_j}\right) \cdot RA_j^k - \mathrm{PoS_j} \cdot PA_j^k\right] \leq \left(1 - q_j^k\right) \cdot M, \quad \forall j = 1,2,\dots,nSeg \quad (3)$$

$$M \cdot \left(1 - q_j^k\right) + \left[\mathrm{PoS_j} \cdot RD_j^k - \left(1 - \mathrm{PoS_j}\right) \cdot PD_j^k\right] \geq \gamma^k \quad (4)$$

$$q_j^k \in \{0,1\}, \ \forall j = 1,2,\dots,nSeg \quad (5)$$

$$\mathrm{PoS_j} = \frac{x_j}{nT} + PoD_j - PoD_j \cdot \frac{x_j}{nT} \quad (6)$$

$$a^k \in \mathcal{R}, \gamma^k \in \mathcal{R} \quad (7)$$

$$x_i \in \mathbb{Z}_0^+, x_i \ is \ a \ even \ number \quad (8)$$

$$x_i \leq nT - 2 \cdot (i - s - 1), \quad i = s+1, s+2, \dots, nSeg \quad (9)$$

$$x_i \leq nT - 2 \cdot (s - i), \quad i = 1,2,\dots,s \quad (10)$$

$$x_i \geq \varepsilon \cdot x_{i+1}, \quad i = s+1, s+2, \dots, nSeg - 1 \quad (11)$$

$$x_{i+1} \geq \varepsilon \cdot x_i, \quad i = 1,2,\dots,s-1 \quad (12)$$

The objective function "OF" indicates that the patrol faces several types of adversaries, and she wants to maximize her expected payoff concerning these different adversaries.

Constraint (1) indicates that the sum of time spent in each route segment cannot exceed the total patrolling time. Constraints (2), (3), and (5) mean that observing the patrol's strategy, each type of adversary will play its best response, which is a pure strategy. Note that in (3), $q_j^l = 1$ indicates the attacker's best response, and thus: $a^k = \left(1 - \mathrm{PoS_j}\right) \cdot RA_j^k - \mathrm{PoS_j} \cdot PA_j^k$; otherwise, $q_j^k = 0$, and thus: $a^k \geq \left(1 - \mathrm{PoS_j}\right) \cdot RA_j^k - \mathrm{PoS_j} \cdot PA_j^k$.

For constraint (4), the inequality will be tight only in case of $q_j^k = 1$, indicating that the γ^k is the defender's payoff when the attacker chooses route segment j to attack. Constraint (6) refers to equation (6) in section 3.4. Constraints (8) to (12) are used to make sure that the allocation of the time segment is a FCP as defined in definition 1 in section 3.4.

Note that constraint (8) is not a standard linear constraint. However, when the algorithm is implemented, all the x_i can be replaced by a $x_i = 2y_i$, which will not change the linear property of other constraints.

Algorithm 1 only computes the optimal allocation of time segments, or the so-named path category. The pipeline security management department needs the exact patrolling routes. To this end, the algorithm 2 is proposed to generate patrolling routes from the given optimal path category, and it is a depth-first-search (DFS) based algorithm.

Patrolling routes are generated by **Algorithm 2** from the path category (See Annex 1). The input of the algorithm is the patrolling graph TG (as shown in Figure 1), and the path category x^*. The output of this algorithm is the entire route list which belongs to this path category.

6. Case study

In order to understand the PPG, a short piece of the pipeline route has been chosen for finding an optimum patrolling schedule. Sub-section 6.1. defines this case study and results are discussed in sub-section 6.2

6.1. Case study definition

We follow the example of Section 3 (strategy modelling), in which all the patrolling paths can be modeled through Figure 1. This pipeline route is presented more specifically in Table 11, in which the patrol starts from, and ends to, the starting point of segment 5:

Table 11, pipeline route

Number	Section	Description	Route Length(km)	length
1	1. industrial area	Under river	0.5	1.5
2		Pass a road	0.5	
3		Warehouse	0.5	
4	2. Urban area	Metering and branching	0.6	2.7
5		pass a river	0.5	
6		Pass a highway	0.5	
7		Roadhouse	0.5	
8		Pass a highway	0.6	
9	3. Country side	Hiking path	0.8	0.8

The duration of patrolling is 1.8 hour, and the length of pipeline is 5 km. This patrolling game is modeled by 9 *Pipeline Segment*s and 20 *Time Segments*. Consequently, there are nine attack strategies for the attacker. Based on all available patrolling paths, each possible set of PoC distribution can be one of the patrol strategies. These PoCs were illustrated in Table 4.

On these 9 *Pipeline Segments,* we can install some countermeasures to increase the security level of the pipeline system. As stated before, in PPG scheduling the patrolling is based on implemented countermeasures. We will solve the PPG in two cases: the first one in the absence of any physical countermeasure on the pipeline and the second in the presence of a set of countermeasures. These two cases are presented in Table 12 with the efficiency of the measures.

Table 12, two cases for physical countermeasures

	PoD								
	RT 1	RT 2	RT 3	RT 4	RT 5	RT 6	RT 7	RT 8	RT 9
Case 1	0	0	0	0	0	0	0	0	0
Case 2	0	0	0	0	40%	30%	50%	40%	0

Note: The *Route Segment* is abbreviated with RT

Following player modelling, there are four types of attackers. These types of attackers in addition to the patrol can be characterized by sets of WFs similar to what is presented in Table 3. In this illustration, just one scenario for the security incident system is considered for all types of the attacker, which is an explosion of the pipeline.

In the payoff modeling part, the consequences of this unique scenario are evaluated according to the risk ranking system of Section 4 and the results are estimated for these 9 *Pipeline Segments* in Table 13.

Table 13, ranking different kinds of consequences

	1. industrial area			**4. urban area**					**3. Countryside**
	***Route Segment* Number**								
kinds of consequences	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Fatalities and injuries	3	4	3	3	3	4	5	4	3
Environmental impacts	3	2	2	2	3	2	2	2	4
Property damage	2	4	4	5	3	4	5	4	3
Business interruption	2	3	3	4	2	3	3	3	2
Damage to Reputation or Negative Publicity	4	4	4	5	5	5	5	5	4

The threat assessment of these adversaries in this illustrative case results in level 4 for the terrorist ($T^1 = 4$), level 3 for the criminals ($T^2 = 3$), level 2 for the activists ($T^4 = 1$), and level 1 for the disgruntled insider ($T^3 = 2$). Accordingly, the ρ^ks are calculated (see Annex 2).

Now through Eq.7 the payoff for the leader – the patrol in this work – can be estimated and similarly for the follower - the attacker in the present work - the outcomes can be approximated through Eq.8. (See Annex 2)

6.2. Results and discussion:

The illustrative pipeline system was explanied before, in this subsection, we are solving it through the PPG algorithm introduced in section 5. Our illustration has two cases, as mentioned before, the first case has not any security countermeasures whereas the second case has a set of countermeasures as shown in Table 12.

In the first case, with the PoC distribution shown in Table 14 the patrol can have the highest possible payoff. It means if she schedules her patrolling path based on these PoCs, in comparison to the other choices, she will secure the pipeline system in the best possible way.

Table 14, defender strategy and probability of stopping the attack in case one

Pipeline Segment	1	2	3	4	5	6	7	8	9
PoD	0%	0%	0%	0%	0%	0%	0%	0%	0%
PoC	0%	10%	10%	20%	10%	20%	20%	10%	0%
PoS	0%	10%	10%	20%	10%	20%	20%	10%	0%

Since there isn't any countermeasure on this pipeline system, all the PoSs are equal to the PoCs. This means that if the attacker wants to attack *Pipeline Segment* 8, the probability of presence of the patrol is 10%, consequently the probability of getting caught is only of 10%.

On the other hand, different types of the attacker are predicted to decide on strategies shown in Table 15. Since the attacker is assumed completely rational, these strategies, which lead him to the highest payoff, are the most probable ones to be chosen.

Table 15, attacker's strategies and both players' payoffs in case one

Type of the attacker	His chosen Strategy	Attacker payoff	Patrol payoff
terrorist	*Pipeline Segment 8*	37.4	-29.6
criminal	*Pipeline Segment 4*	9.6	-25.2
disgruntled insiders	*Pipeline Segment 8*	23.4	-30.4
activists	*Pipeline Segment 9*	34	-29

In addition to payoffs of different types of the attacker, the defender expected payoffs in the face of each type of the attacker are presented in Table 15. Nevertheless, by considering the condition probability on each type of the attacker, the overall defender's payoff with PoCs of Table 14 is equal to -28.24. According to Table 14, in case one, the PPG algorithm provides us a set of 36 patrolling paths having the optimum probability of the coverage (PoC). Some of these paths are presented in Figure 4.

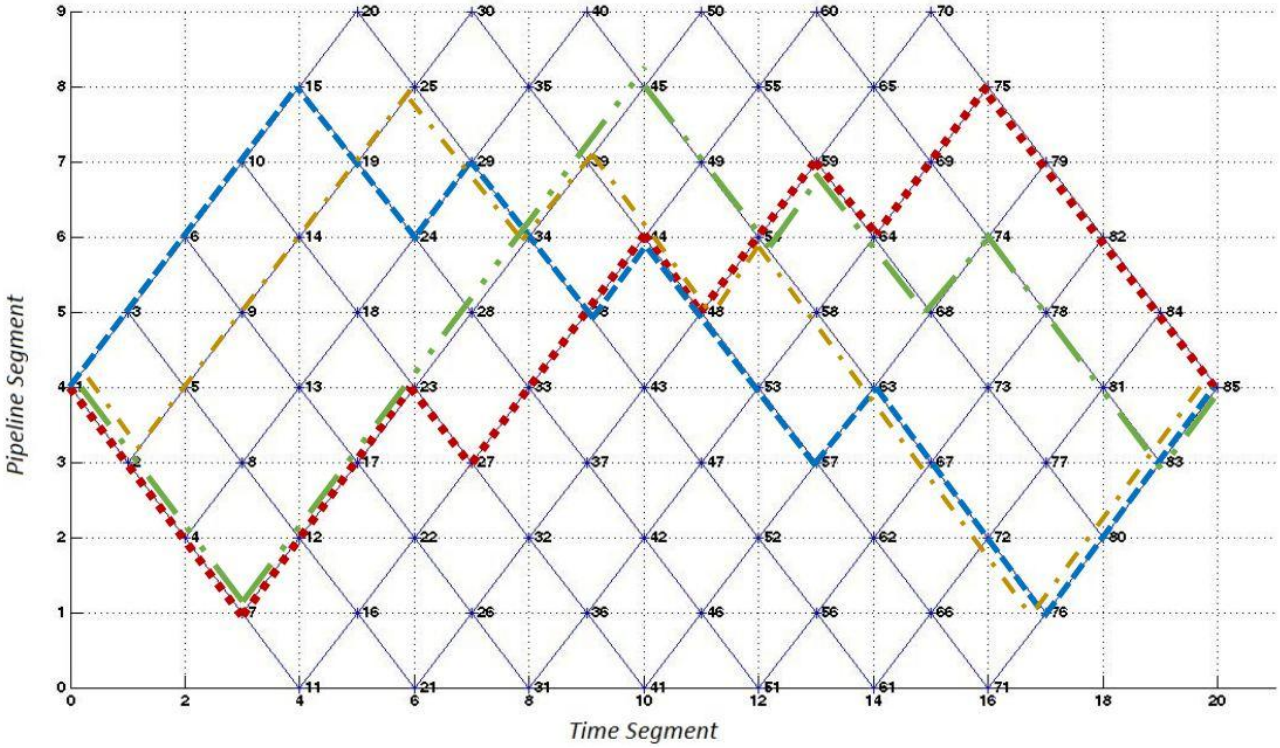

Figure 4, patrolling paths in case one

In the second case, in the presence of countermeasures, it is better for the patrol to plan a patrolling in which the *Pipeline Segments* have PoCs presented in Table 16.

Table 16, defender strategy and probability of stopping the attack in case two

Pipeline Segment	1	2	3	4	5	6	7	8	9
PoD	0%	0%	0%	0%	40%	30%	50%	40%	0%
PoC	0%	20%	10%	20%	10%	10%	10%	10%	10%
PoS	0%	20%	10%	20%	46%	37%	55%	46%	10%

As shown in Table 16, by implementing a set of countermeasures on this ilustrative pipeline system, the probability of catching the attacker in some *Pipeline Segments* has slightly increased. For instance, the probability of exiting a patrol in *Pipeline Segment* 6 is 10%, but by installing a countermeasure with PoD of 30% the probability of stopping the malicious act increases to 37%. For *Pipeline Segment* 6, although the attack consequences are higher than *Pipeline Segment* 3, the duration of patrol inspection are the same, both for 2 *Time Segments*, because a countermeasure implementation in *Pipeline Segment* 6 provides a PoS of 37% and patrol doesn't need to spend more time in that location.

From Table 14 and 16, the effect of installing a set of countermeasures on the pipeline system can be found. *Pipeline Segment* 7 is more critical than other *Pipeline Segments*, therefore in case one, the patrol should spend more time inspecting this *Pipeline Segment* than the others. However, if a countermeasure with a PoD of 50% is installed on that segment, the criticality is decreased so as to the patrol can inspect it less or like the other segments (in 2 *Time Segments*). For *Pipeline Segment* 2 the situation is different. Before installing any countermeasure, the patrol should plan to inspect this *Pipeline Segment*, which is passing a road, in two *Time Segments* to have the highest payoffs. Having a countermeasure implemented on other *Pipeline Segment*s decreases the probability of a successful attack in those segments. Thus in comparison to other segments this *Pipeline Segment* becomes more critical and the patrol is better to inspect it in four *Times Segment*s to have higher payoffs. In *Pipeline Segment* 5, installation of a countermeasure with 40% PoD can increase the probability of stopping the attack from 10% to 46%, nonetheless the number of patrol inspections is the same.

Table 17 represents the most probable strategies for the four types of attacker in case two, which leads them to the highest payoff. In this table, you can find the payoffs of the attacker choosing these strategies. Moreover, payoffs for the patrol facing these types of attacker are shown separately. If we consider the conditional probability distribution on each type of the attacker, it can be calculated that the overall expected payoff for the defender, following the strategies of Table 16, is equal to-24.78

Table 17, attacker's strategies and both players' payoffs in case two

Type of the attacker	His chosen Strategy	Attacker payoff	Patrol payoff
terrorist	*Pipeline Segment 4*	32.6	-24.2
criminal	*Pipeline Segment 4*	9.6	-25.2
disgruntled insiders	*Pipeline Segment 4*	22.2	-25.8
activists	*Pipeline Segment 9*	29.7	-24.8

For the second case, Figure 5 shows 6 generated patrolling routes by PPG algorithm. All these paths have the same PoC distribution as in Table 16.

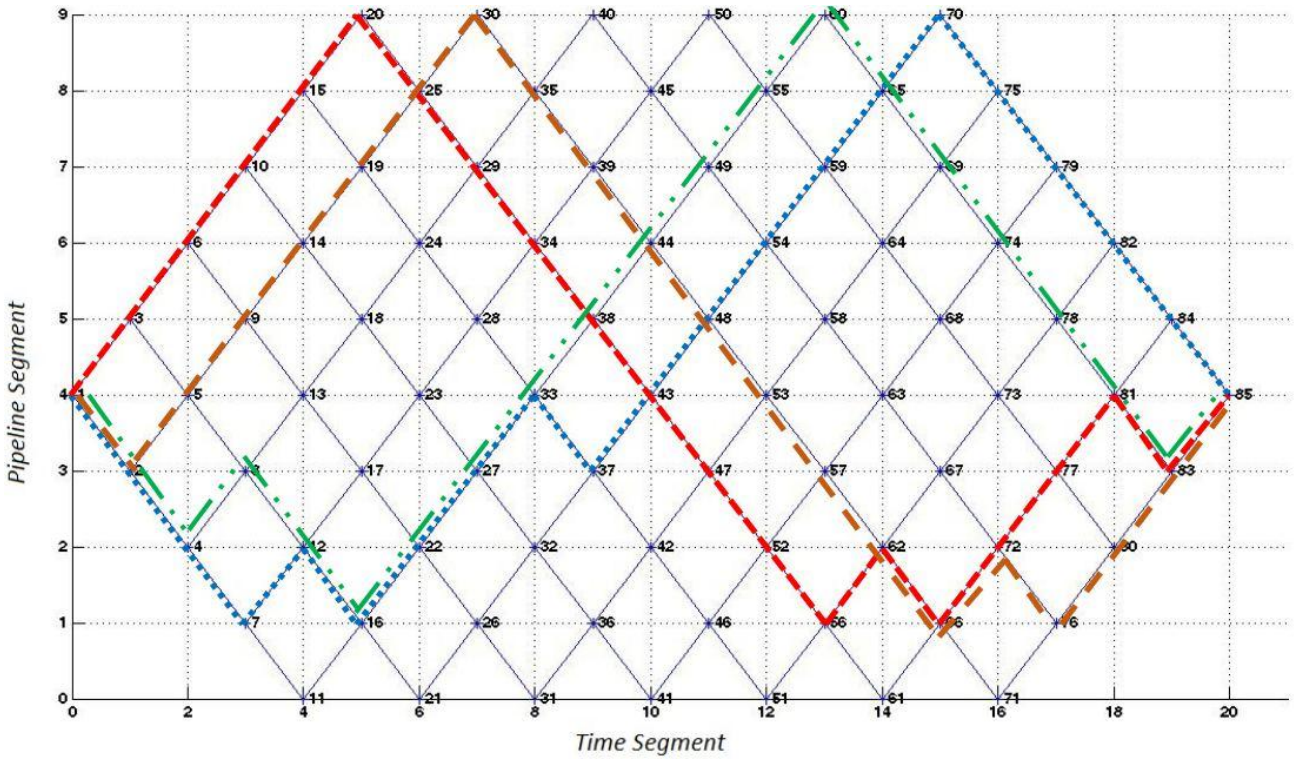

Figure 5, patrolling paths in case two

The illustrative case study thus shows that PPG properly produces the optimum paths for the pipeline considered. Improving the algorithm to cover longer routes is the subject of future work. Moreover, the PPG can be developed for other applications in chemical or Oil&Gas industries.

Moreover, the illustration shows that PPG considers the effectiveness of countermeasures and how they can change the optimal patrolling paths. This feature gives the security department of a pipeline company an advantage of considering the physical protection system in their patrol route and managing their schedule by installing additional countermeasures on their system.

7. Conclusions

In this methodology, however, we assumed that both players are completely rational. Since rationality is not always applied in real security challenges, modelling of the bounded rationality of the players should be taken into account in future research, as theQuantal Response Equilibrium, described by McKelvey and Palfrey (1995) and (1998), that has a superior ability to model human behaviour in simultaneous and extensive move games. Bo An et al. (2012) for instance used this model in the algorithm of their patrol scheduling game, and the application of such bounded rationality models is postponed for further development of PPG.

We have developed a methodology – the so-called **P**ipeline **P**atrolling **G**ame (PPG) – based on a security game to identify the optimal patrolling schedule on the pipeline system. The method is based on a discretization of patrolling time and distance. This discretization provides a framework to model the patrolling paths mathematically. In this framework, we can implement a risk rank ordering system to assess the security risk on the whole pipeline system. The developed methodology produces different patrolling paths according to the results of security risk assessments by which the pipeline system can be protected by an optimal strategy.

By the PPG a pipeline company can ensure that their pipeline system is protected in the best way. Since PPG can produce a set of patrolling paths that except security department nobody knows which of them will be chosen. Security Department can choose one of these paths randomly and be confident that they will inspect the high risky areas more than less risky parts. According the assumptions, although the attacker can know the importance of different sections or guess the frequency of inspecting a section, they don't know the exact plan of the security department and they won't be successful more than specific level.

Annex

Annex 1:

Algorithm 2 generating patrolling routes from the path category

```
GPP (TG, x*)
          Set RouteList := {};
          Stack S := {};    ( start with an empty stack )
          for each vertex u, list u.visitedset := {};
          push S, s;
          while (S is not empty) do
             v := top S;
             node set cv := nodes which can be reached from v by one step
             for each node i in cv
                if i∉S AND i∉v.visitedset
                   push S, i;
                   add v.visitedset i;
                end if
             end for
             nv := top S;
             if nv and v the same
                clear v.visitedset
                pop S;
             else if S not satisfy x*
                pop S;
             else if nv and t the same
                add Routelist S;
                pop S;
             end if
          end while
END GPP
```

Annex 2:

The threat level and the probability distribution over types of the attacker are given in Table A1.

Table A1, threat level and probability if the attacker has type k in illustrated case study

	Terrorist K=1	Criminal k=2	Disgruntled insider k=3	Activist k=4
T^k	4	3	1	2
ρ^K	0.4	0.3	0.1	0.2

The outcome for each player when the attacker attacks to each *Pipeline Segment* in case one are presented in Table A2.

Table A2, payoffs in case one of illustrated case study

Case 1													
	POD	POC	POS	U_a^1	U_a^2	U_a^3	U_a^4	U_d^1	U_d^2	U_d^3	U_d^4	U_a^{Total}	U_d^{Total}
1	0%	0%	0%	32.00	6.00	21.00	29.00	-26.00	-26.00	-26.00	-26.00	22.50	-26.00
2	0%	10%	10%	34.70	9.60	20.70	27.90	-27.80	-28.30	-28.60	-28.40	24.41	-28.15
3	0%	10%	10%	32.00	9.60	20.70	27.90	-25.10	-25.60	-25.90	-25.70	23.33	-25.45
4	0%	20%	20%	32.60	9.60	22.20	29.40	-24.20	-25.20	-25.80	-25.40	24.02	-24.90
5	0%	10%	10%	32.00	6.90	21.60	29.70	-25.10	-25.60	-25.90	-25.70	22.97	-25.45
6	0%	20%	20%	31.80	7.20	19.80	26.20	-24.20	-25.20	-25.80	-25.40	22.10	-24.90
7	0%	20%	20%	35.80	9.60	20.60	27.80	-28.20	-29.20	-29.80	-29.40	24.82	-28.90
8	0%	10%	10%	37.40	9.60	23.40	30.60	-29.60	-30.10	-30.40	-30.20	26.30	-29.95
9	0%	0%	0%	35.00	9.00	23.00	34.00	-29.00	-29.00	-29.00	-29.00	25.80	-29.00

Table A3 shows the player's payoff in case of attack to each *Pipeline Segment* in case 2.

Table A3, payoffs in case two of illustrated case study

Case 2													
	POD	POC	POS	U_a^1	U_a^2	U_a^3	U_a^4	U_d^1	U_d^2	U_d^3	U_d^4	U_a^{Total}	U_d^{Total}
1	0%	0%	0%	32.00	6.00	21.00	29.00	-26.00	-26.00	-26.00	-26.00	22.50	-26.00
2	0%	20%	20%	29.40	7.20	17.40	23.80	-22.60	-23.60	-24.20	-23.80	20.42	-23.30
3	0%	10%	10%	32.00	9.60	20.70	27.90	-25.10	-25.60	-25.90	-25.70	23.33	-25.45
4	0%	20%	20%	32.60	9.60	22.20	29.40	-24.20	-25.20	-25.80	-25.40	24.02	-24.90
5	40%	10%	46%	14.00	-0.66	9.36	14.22	-7.46	-9.76	-11.14	-10.22	9.18	-9.07
6	30%	10%	37%	22.28	3.12	13.68	18.72	-15.02	-16.87	-17.98	-17.24	14.96	-16.32
7	50%	10%	55%	14.45	0.15	7.65	11.70	-7.55	-10.30	-11.95	-10.85	8.93	-9.48
8	40%	10%	46%	17.24	0.96	10.44	14.76	-10.16	-12.46	-13.84	-12.92	11.18	-11.77
9	0%	10%	10%	30.20	6.90	19.80	29.70	-24.20	-24.70	-25.00	-24.80	22.07	-24.55

References

Aguirre, and Taboada. 2012. 'An Evolutionary Game Theory Approach for Intelligent Patrolling', *Procedia Computer Science*, 12: 140-45.

Alpern, Steve, Thomas Lidbetter, Alec Morton, and Katerina Papadaki. 2016. 'Patrolling a Pipeline'.

Alpern, Steve, Alec Morton, and Katerina Papadaki. 2011. 'Patrolling games', *Operations Research*, 59: 1246-57.

API780, American Petroleum Institute. 2012. "Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries." In *Recommended Practice*. Washington, DC: American Petroleum Institute.

Bajpai, S., A. Sachdeva, and J. P. Gupta. 2010. 'Security risk assessment: applying the concepts of fuzzy logic', *J Hazard Mater*, 173: 258-64.

Basilico, Gatti, and Amigoni. 2012. 'Patrolling security games: Definition and algorithms for solving large instances with single patroller and single intruder', *Artificial Intelligence*, 184-185: 78-123.

Bier, and Azaiez. 2009. *Game theoretic risk analysis of security threats* (Springer: New York, USA).

Bo An, Shieh, Yang, Tambe, Baldwin, DiRenzo, Maule, and Meyer. 2012. "PROTECT - A Deployed Game-Theoretic System for Strategic Security Allocation for the United States Coast Guard." In *AI Magazine*. USA: Association for the Advancement of Artificial Intelligence.

CCPS, (Center for chemical Process Safety). 2008. *Guidelines for chemical transportation safety, security, and risk management* (America Institute of Chemical Engineers, John Wiley & Sons: New York, USA).

———. 2010. *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites* (America Institute of Chemical Engineers, John Wiley & Sons: New York, USA).

Fang, Fei, Thanh H Nguyen, Rob Pickles, Wai Y Lam, Gopalasamy R Clements, Bo An, Amandeep Singh, Milind Tambe, and Andrew Lemieux. 2016. "Deploying PAWS: Field optimization of the protection assistant for wildlife security." In *Proceedings of the Twenty-Eighth Innovative Applications of Artificial Intelligence Conference*.

Feng, Qilin, Hao Cai, Zhilong Chen, Xudong Zhao, and Yicun Chen. 2016. 'Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks', *Journal of loss prevention in the process industries*, 43: 614-28.

Gatti. 2008. "Game Theoretical Insights in Strategic Patrolling." In *18th europian conference on Artificial Intelligence*, edited by Malik Ghallab, Constantine D. Spyropoolos, Nikos Fakotakis and Nikos Avouris.

McKelvey, and Palfrey. 1995. 'Quantal Response Equilibria for Normal Form Games', *Games and Economic Behavior*, 10: 6-38.

———. 1998. 'Quantal Response Equilibria for Extensive Form Games', *Experimental Economics*, 1: 9-41.

Moore, David A. 2013. 'Security Risk Assessment Methodology for the petroleum and petrochemical industries', *Journal of loss prevention in the process industries*, 26: 1685-89.

Owen. 2013. *The Boundaries of Security 2013.pdf* (Future Fibre Technologies Pty Ltd).

Papadaki, Katerina, Steve Alpern, Thomas Lidbetter, and Alec Morton. 2016. 'Patrolling a Border', *Operations Research*, 0: null.

Pita, Jain, Marecki, Ordóñez, Portway, Tambe, Western, Paruchuri, and Kraus. 2008. "Deployed ARMOR Protection: The Application of a Game Theoretic Model for Security at the Los Angeles International Airport." In *Autonomous Agents and Multiagent Systems (AAMAS 2008)*. Estoril, Portugal: International Foundation for Autonomous Agents and Multiagent systems.

Pita, Tambe, Kiekintveld, Cullen, and Steigerwald. 2011. "GUARDS: Game-Theoretic Security Allocation on a National Scale." In *Autonomous Agents and Multiagent Systems (AAMAS 2011)*. Taipei, Taiwan: International Foundation for Autonomous Agents and Multiagent Systems.

Reniers, and Dullaert. 2011. 'TePiTri: A screening method for assessing terrorist-related pipeline transport risks', *Security Journal*, 25: 173-86.

Reniers, Herdewel, and Wybo. 2013. 'A Threat Assessment Review Planning (TARP) decision flowchart for complex industrial areas', *Journal of loss prevention in the process industries*, 26: 1662-69.

Rezazadeh, Talarico, Reniers, Cozzani, and Zhang. 2016. "Applying game theory for securing oil and gas pipelines." In. Process Safety and Environmental Protection.

Srivastava, and Gupta. 2010. 'New methodologies for security risk assessment of oil and gas industry', *Process Safety and Environmental Protection*, 88: 407-12.

Talarico, Reniers, Sörensen, and Springael. 2015. 'MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries', *Reliability Engineering & System Safety*, 138: 105-14.

Talarico, Sorensen, Reniers, and Springael. 2015. 'pipeline securiry.' in Hakim, Albert and Shiftan (eds.), *Securing Transportation Systems* (John Wiley & sons, Inc.).

Tambe. 2012. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned* (Cambridge University Press: United States of America).

Tsai, Rathi, Kiekintveld, Ordóñez, and Tambe. 2009. "ATool for Strategic Security Allocation in Transportation Networks." In *Autonomous Agents and Multiagent Systems (AAMAS 2009)*. Budapest, Hungary: International Foundation for Autonomous Agents and Multiagent systems.

Yin, Jiang, Tambe, Kiekintveld, Leyton-Brown, Sandholm, and Sullivan. 2012. 'TRUSTS: Scheduling Randomized Patrols for Fare Inspection in Transit Systems using Game Theory', *Association for the Advancement of Artificial Intelligence*.

Zhang, L., and G. Reniers. 2016. 'A Game-Theoretical Model to Improve Process Plant Protection from Terrorist Attacks', *Risk Analysis*.