aerospace

MDPI

Article

An Agent-Based Empirical Game Theory Approach for Airport Security Patrols

Stef Janssen *,†, **Diogo Matias** † and **Alexei Sharpanskykh**

Air Transport And Operations Group, Delft University of Technology, Kluyverweg 1, 2629HS Delft, The Netherlands; diogo.pomatias@gmail.com (D.M.); O.A.Sharpanskykh@tudelft.nl (A.S.)

* Correspondence: s.a.m.janssen@tudelft.nl

† These authors contributed equally to this work.

Received: 12 December 2019; Accepted: 10 January 2020; Published: 18 January 2020

Abstract: Airports are attractive targets for terrorists, as they are designed to accommodate and process large amounts of people, resulting in a high concentration of potential victims. A popular method to mitigate the risk of terrorist attacks is through security patrols, but resources are often limited. Game theory is commonly used as a methodology to find optimal patrol routes for security agents such that security risks are minimized. However, game-theoretic models suffer from payoff uncertainty and often rely solely on expert assessment to estimate game payoffs. Experts cannot incorporate all aspects of a terrorist attack in their assessment. For instance, attacker behavior, which contributes to the game payoff rewards, is hard to estimate precisely. To address this shortcoming, we proposed a novel empirical game theory approach in which payoffs are estimated using agent-based modeling. Using this approach, we simulated different attacker and defender strategies in an agent-based model to estimate game-theoretic payoffs, while a security game was used to find optimal security patrols. We performed a case study at a regional airport, and show that the optimal security patrol is non-deterministic and gives special emphasis to high-impact areas, such as the security checkpoint. The found security patrol routes are an improvement over previously found security strategies of the same case study.

Keywords: agent-based modeling; patrolling games; security game; airport security; empirical game theory

1. Introduction

Ever since the attacks on the World Trade Center, 11 September 2001, airports have significantly enhanced security operations, procedures, and checks. However, not only has security improved, but also terrorists have adapted their way of acting. The START database for terrorism attacks shows that many incidents related to aviation have occurred in recent years [1]. The Brussels and Atattürk Airport attacks (2016) are two prime examples of this. They illustrate a recent terrorist threat where publicly accessible areas of airports are the target of attack. Protecting these targets, where many people move freely, is a challenging task for security agencies because attackers do not have to face passenger or carry-on luggage checks. Additionally, limited security resources make it extremely difficult to track a terrorist in a crowded scene.

Airport security patrols are an effective method to defend against these types of attacks. However, security resources are often scarce, preventing full coverage of all targets at all times. Security patrol routes, therefore, must be intelligently deployed by taking into account differences in the importance of targets, different attack threats, and potential uncertainty over the types, capabilities, knowledge, and preferences of attackers faced.

Game-theoretic analysis has emerged as a powerful tool to provide optimal decisions in the security domain. Game theory provides a mathematical framework to study interactions between strategic and self-interested agents who maximize the effectiveness of their actions. This makes it is appropriate to model adversarial reasoning for security resource allocation and scheduling problems [2].

One application of game theory is in the domain of security resource allocation and scheduling, included in a research area known as security games. These have shown to be successful in solving real-world security problems in which security officers deploy limited resources to protect important infrastructures against human adversaries [3–7]. A security game is a two-player game between a defender and an attacker. The defender wants to allocate her (the attacker is, following convention, referred to as “he” and the defender as “she”) limited resources to defend critical targets, while the attacker seeks his most favorable target to attack. Each player has a set of available actions associated with a particular payoff (also known as utility), based on the outcome of the corresponding choices within the game. Payoffs are the reward and penalties to both the defender and the attacker in a successful or an unsuccessful attack.

Commonly, game-theoretic models rely only on expert knowledge to estimate payoff values. However, these are hard to estimate, since uncertainty is intrinsic to real-world security domains. It is, therefore, difficult for a security expert to properly estimate payoff values for different defender–attacker interactions. Moreover, exclusive reliance on human expert assessment can be expensive, prone to human biases and restrictive [8].

Agent-based modeling and simulation is a promising technique to address this challenge of estimating payoffs. Agent-based models consist of a set of autonomous and intelligent agents who can perceive their environment and interact in the environment to solve problems, achieve goals or execute tasks. Agent-based models are particularly suitable to represent socio-technical systems, such as airports [9]. Considering an airport terminal environment, it allows the specification of different agents, such as airport operational employees, passengers, security officers, and an attacker agent, who are able to perceive all processes happening around them and interact with each other to achieve their individual goals.

Through simulations, it is possible to identify emergent patterns and relations that are not explicitly coded in the model. One example of an emergent property is the vulnerable areas in an airport terminal where an attack can lead to many casualties. The identification of these vulnerable areas is of crucial importance as it indicates patrol areas where security should be reinforced.

The goal of this work is to improve the payoff matrices in security games, by using agent-based model results to define them. Although many security studies have focused on either agent-based modeling [10,11], or security games [3,12], combining both approaches to improve security-game payoffs has not been addressed. To this end, we investigate a scenario in which an attacker aims to detonate an improvised explosive device (IED) on a publicly accessible area of a regional airport, while security agents execute patrol routes in the airport terminal. We use an agent-based model to determine the number of casualties of a terrorist attack and use these results to specify payoffs in a security game. This security game is then used to determine the patrol route of security officers that minimizes the expected number of casualties in a terrorist attack.

This paper is organized as follows. In Section 2, we discuss relevant related work, and in Section 3 an overview of the case study is provided. Then, Section 4 provides an overview of our novel methodology, while Section 5 explains the proposed model in detail. The discussion of the simulations results is presented in Section 6, and, lastly, Section 7 concludes this paper.

2. Related Work

This section provides an overview of relevant work in the domain of airport security, security games and agent-based modeling.

2.1. Airport Security

Airport security is driven by rules and guidelines defined by different organizations. For instance, the European Union has formalized airport regulations in its laws [13,14], the United States has the Aviation and Transportation Security Act [15], and the ICAO provides a security manual [16]. These rules and regulations form the basis for the implementation of the different security measures at airport terminals.

One of the most important measures that are implemented at airport terminals are security checkpoints [17,18]. At security checkpoints, dangerous items are confiscated from passengers to reduce the risk of a terrorist attack involving aircraft. This is done using a combination of random checks (i.e., explosive trace detection), and targeted searches based on sensor readings (i.e., walk through metal detector). This combination of random checks and targeted searches makes it difficult for attackers to predict and therefore sabotage the security checkpoint.

These security checkpoints, however, lead to large groups of passengers accumulating in queues in the open airport areas. These queues have recently become targets of terrorists, such as the Brussels and Atattürk Airport bomb attacks. They have the potential for a high number of casualties and are accessible without going through the security checkpoint.

Regardless of the location of the security checkpoint, these soft targets in front of security checkpoints remain an issue for airports. They have therefore turned to security officers that patrol around the airport to identify and arrest potential terrorists. Security patrols are an effective method to defend against terrorist attacks, but they cannot fully cover all targets at all times. We, therefore, turn to security games to design effective random patrol routes to reduce the risk of a terrorist attack as much as possible.

2.2. Security Games

Security games have emerged as an important research domain in multi-agent systems. Over recent years, game-theoretic models have been deployed in many real-world applications: canine-patrol and vehicle checkpoints at the Los Angeles International Airport [3], allocation of US Federal Air Marshals to international flights [5], US Coast Guard patrol boats [6], and many others [4,7].

Security games are often formulated as a Stackelberg game. A Stackelberg Security Game assumes a leader (defender) and a follower (attacker). The defender must protect a set of targets as well as possible, using limited resources. The attacker aims to maximize the impact of its attack. In these games, it is assumed that the defender first commits to a (possibly randomized) security policy, while a strategic attacker uses surveillance to learn and create beliefs about the defender's strategy. After careful planning, the attacker selfishly optimizes its payoff, considering the policy chosen by the defender. The outcome of such a game is an equilibrium: a combination of strategies in which both players' strategies are best responses to each other, i.e., cannot improve their payoff by changing their strategy.

A strategy can be of two types: pure strategies or mixed strategies. A pure strategy of an agent is one of the agent's actions, which is selected with certainty. A mixed strategy is a probability distribution over the set of actions. A mixed strategy allows for randomization which is critical in security domains as it avoids the vulnerability that comes with predictability associated with human-designed schedules. Humans are unable to produce a completely random set of events, leading to potentially predictable patterns that may be explored by an intelligent attacker [19].

Relevant to this work are papers that focus on security scheduling and allocation to prevent the attacker from exploiting a particular gap in the defender's patrol. One relevant application was introduced by Pita et al. [3], who computed optimal schedules that randomized road security checkpoints and terminal canine patrols. In that work, Pita et al. specify the patrolling problem as a Bayesian Stackelberg game, allowing the agent to appropriately weigh the different actions in randomization, as well as uncertainty over adversary types. However, that work did not explicitly consider spatio-temporal aspects, assuming that the attacker chooses a target to attack and is automatically at that location, without considering the time it takes to reach it. Moreover, the attacker agent could only be arrested at a target, while in real-world scenarios he can also be caught in his path from the airport entrance towards his target.

Furthermore, Prakash et al. [20] employed an empirical game theory approach. This empirical approach uses a simulation engine to model the domain area and then uses this to specify game payoffs. This methodology is similar to the one proposed in this paper, but instead of using agent-based modeling to estimate the game payoff values, the authors use standard event-based simulation models for the same purpose. Agent-based modeling is capable of characterizing socio-technical systems, including the representation of agents' behavior and interactions which is impossible using the methodology of Prakash et al. Furthermore, their work focused on the domain of cybercrime, which has several differences from the airport security domain. There is a growing body of theoretical work in the field of empirical game theory, of which the work of Wellman et al. [21] and more recently the work of Tuyls et al. [22] are examples. Despite being important theoretical contributions, these do not consider human behavior and interactions and are not specific for security problems.

Other notable work is in the area of spatio-temporal security games, also known as patrol planning games. Generally, these games are played on graphs where targets are nodes and a patrol strategy is a vector consisting of defender's positions at each point in time. This approach captures the spatial evolution over time, i.e., correlates one position at time t to another position at time $t+1$. Applications range from robotic patrols [23] to green security games [24], and protection of major infrastructures such as airports [6,25]. Fang et al. [26] focuses on protecting mobile targets, which results in a continuous set of strategies for the agents. Motivated by the domain of ferry protection, Xu et al. [27] developed a model to solve spatio-temporal games with weighted moving targets.

A recent relevant work in the domain of spatio-temporal game theory was introduced by Zhang et al. [28]. Zhang focuses on finding optimal randomize patrol strategies in a chemical cluster. In that work, potential targets are represented as nodes of a patrolling graph. The security surveys different areas by traveling in the graph and staying a certain amount of time at each node when patrolling that target. The main contribution of Zhang's work is that an optimal patrol schedule does not correspond to a randomized fixed patrolling strategy (fixed set of different positions over time), but rather to a set of transition probabilities between nodes of the patrolling graph. In other words, their patrol schedule represents the probability that the defender performs a certain movement. Due to these advantages, we will use the work of Zhang et al. as a basis for our case study.

Despite being a field with many real-world successful deployments, security games also face multiple challenges. Those include bounded rationality [29,30], uncertainty arising due to human dynamic behavior [31,32], and learning in security games, with a special emphasis on reinforcement learning to identify the best defender strategy against an adaptive opponent who is able to observe defender's behavior, learn and adapt to best respond to it [33]. To partially overcome these limitations, we use agent-based modeling to define payoffs in security games.

2.3. Agent-Based Modeling

Agent-based modeling is one of the most prominent approaches to study the performance of complex adaptive multi-agent systems [34]. Complexity can be interpreted as non-linear interactions between agents (or agents with the environment), leading to unexpected emergence patterns. Agent-based modeling provides a bottom-up approach to build socio-technical systems with autonomous and intelligent agents who can perceive their environment and interact in the environment. Using agent-based models, multiple scales of analysis and multiple types of adaption and learning mechanisms can be incorporated, which is not straightforward with other modeling techniques. Additionally, it can be used to explicitly represent spatio-temporal elements of agents and the environment, which allows for a better representation of dynamic and uncertain systems.

Noteworthy work in the aviation sector includes the work of Weiss et al. [10], who developed an agent-based model for airport defense, and the work of Cheng et al. [35] who created an agent-based model to evaluate the effect of group dynamics on passenger flow during an evacuation in an airport terminal. Moreover, Janssen et al. [9] introduced a novel agent-based methodology combined with Monte Carlo simulations for security risk assessment. In that work, security agents aimed to detect forbidden items in passenger's luggage while being under constant time pressure.

A recent relevant work in the domain of agent-based modeling was proposed by Janssen et al. [11]. The authors developed an agent-based model to study the relationship between security and efficiency in a regional airport terminal. It focuses on a scenario where an attacker aims to detonate an IED in a publicly accessible area of a regional airport while considering efficiency indicators such as queuing time for passengers, among others. This work offers a promising methodology to investigate airport security and efficiency. We use the work of Janssen et al. in our case study, as described below.

3. Case Study

This section describes the system, operational context, and scenarios under study. We study a scenario in a regional airport terminal, where a security officer patrols around four identified targets: an entrance area, two check-in areas, and a checkpoint area. We focus on a threat scenario in which a bomb attack in the publicly accessible areas of our regional airport terminal occurs. Based on this threat, 20 attacking scenarios are modeled varying in the period of 25 min with a 5 min increment per scenario (e.g., an attacker entering the airport within the first five minutes, . . .). For each attack time interval, the attacker selects one of the four identified targets to attack. That period was chosen to enclose all the attacks that may happen within the first 30 min since the attacker takes time to move from the airport entrance to the selected target.

Figure 1 illustrates the airport open publicly accessible area analyzed in this case study. The focus of our study is on airport terminal patrols, which includes processes such as check-in, facility visits, security checkpoint operations, queuing, gate processes, movement of passengers between these operations, and movement of security officers around the airport terminal. Using our empirical game theory methodology, as described below, we aim to determine the most effective patrolling route for a security officer in the airport terminal.

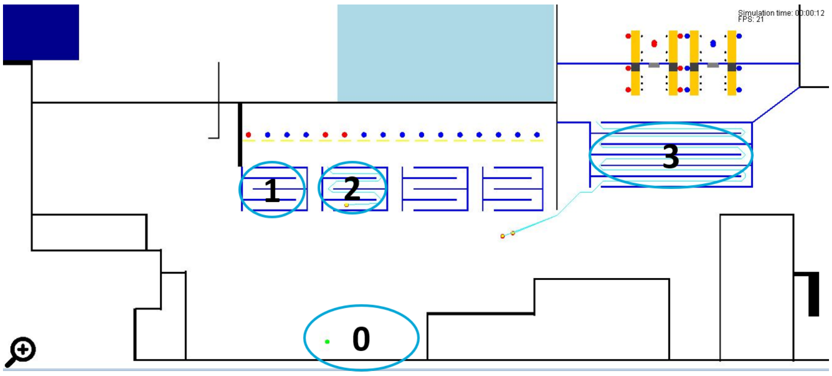

Figure 1. Airport layout of the open publicly accessible areas considered in this case study, with indicators for different targets. 0: Entrance area, 1 and 2: Check-in areas, 3: Security checkpoint area. For the full airport layout, refer to [11].

4. Methodology

The main aim of our work is to decrease uncertainty in game-theoretic payoff structures by estimating them using agent-based simulation results. There is a significant need to address uncertainty in both players' rewards, since key domain features like attacker behavior, which contribute to these rewards, are hard to estimate exactly by experts alone. Hence, this methodology improves on the game-theoretic payoff structures which often rely only on expert assessment. To accomplish this goal, we propose the following methodology, graphically shown in Figure 2.

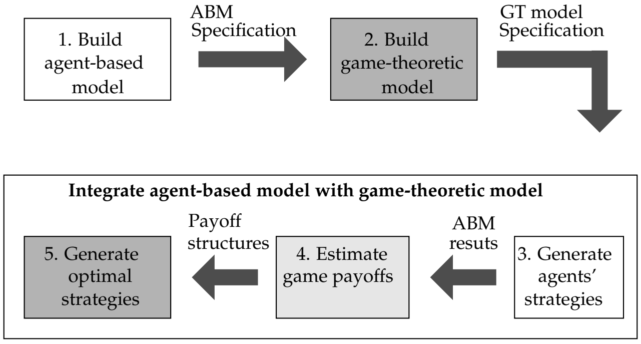
1. Build agent-based model
ABM Specification
2. Build game-theoretic model
GT model Specification
Integrate agent-based model with game-theoretic model
5. Generate optimal strategies
Payoff structures
4. Estimate game payoffs
ABM resuts
3. Generate agents' strategies

Figure 2. Step by step methodology followed in this work. Note: ABM refers to agent-based modeling and GT refers to game theory. Dark gray boxes correspond to the GT model (Step 2 and 5). White boxes correspond to the agent-based model (Step 1 and 3). The light gray box represent the interaction between the agent-based model results and the game-theoretic payoff function.

First, we define the agent-based model. Every agent-based model requires the definition and modeling of three key entities: agents, their environment and interactions between agents and agents with the environment. In this work, we extend the model of Janssen et al. work [11]. This model was chosen as a starting point since most airport terminal processes along with the strategic, tactical and operational behavior of passengers, defenders, and an attacker was modeled.

An initial evaluation of the agent-based model was performed to analyze how the airport system behaves in different scenarios. This helped to gain knowledge of critical areas with the highest agglomeration of passengers where an attack could have hazardous effects in terms of impact (human casualties). Those were deemed as potential targets. Using this information, 20 different threat scenarios (see Section 3) were modeled for the IED threat. The outcomes of the agent-based model simulations will later be used to specify game-theoretic payoffs.

The specification of a game-theoretic model consists of the definition of the players involved in the game, specification of the mathematical model constraints and assumptions, and the solution concept to find an equilibrium solution for both players. In this paper, we follow the model of Zhang et al. work [28]. Zhang defines a game-theoretic model aiming to select random, but strategic security patrols in a chemical cluster. This model is used, as it is a spatio-temporal game, where the set of actions available for each agent takes into consideration both spatial and temporal conditions. This is a crucial requirement in security domains since a terrorist attack can happen anytime and anywhere.

Security patrols should also be spatio-temporal, rather than only spatial, since the security officer can only detect an attacker if he is both in observation range and there is a time overlap between the attacker intrusion and the security patrol. Furthermore, this allows security officers to take different actions at distinct points in time, rather than following a predefined optimal fixed patrolling strategy. This is a great advantage as it enables better patrol randomization. The model assumes perfect rational players, i.e., reward maximizers whose strategies are best responses to each other.

The next step is to integrate both methods, which forms the core of our methodology. This step starts by generating the agent's strategies that will be simulated in the agent-based model and how they are translated to the player's set of actions in the game framework. These actions in our model consist of security patrols in the airport terminal for the defender, as well as attacks at distinct times and targets for the attacker. Each attacker–defender strategy pair is modeled and simulated in the agent-based model so that payoffs for each combination of actions are generated.

Once all attacker and defender strategy combinations are simulated, the agent-based model outcome is computed. This output is defined as the average number of human casualties after an IED attack. This is then used as an input to define payoffs for the players in the game. The key contribution of this paper is embedded in this step, where game-theoretic payoff matrices are enhanced with data generated by an agent-based model capable of simulating real-world events, rather than relying only on expert assessment. In this way, more objective and more robust payoff structures are incorporated in security games.

The last step of the integration process consists of solving the game (i.e., finding an equilibrium) and generating optimal strategies for both players. These results indicate the set of actions that should be taken at each time step by both players. Moreover, the optimal payoff values are computed. The proposed methodology ends with the evaluation of the optimal solution. This is done by simulating the (probabilistic) optimal defender–attacker strategy pair in the agent-based model. The resulting agent-based model metrics are gathered and used as input to compute the payoff values for both players. These are compared to the ones obtained initially after solving the game to confirm that the game-theoretic solution strategies are optimal.

5. Models

This section describes the agent-based model, the game-theoretic model and the integration of the two models. This corresponds to the first four steps of the methodology.

5.1. Agent-Based Model

The agent-based model environment consists of a regional airport terminal including physical objects (wall and desks), an IED (defined by its location, number of particles and mass), terminal areas (check-in, checkpoint, queuing, gate, facility and entrance area) and flights [11]. The outline of the terminal building is shown in Figure 1. Agents cannot obtain complete, accurate, up-to-date information about the environment's state, because it is limited by their observation range. Hence, the environment is partially accessible.

The agent architecture has three different layers: Strategic Layer, Tactical Layer and Operational Layer. In each layer, there are different modules responsible for the execution of specific actions. The Operational Layer comprises a perception module that is responsible for the agent's observation and an actuation module that executes actions and communications between agents. The Tactical Layer consists of a belief module that maintains beliefs based on observations, actions, and internal states. This layer is also responsible for the navigation and activity accomplishment. Lastly, the Strategic Layer is responsible for a higher-level belief and for generating a plan: an ordered sequence of activities to be carried out by the agent.

All passengers, security agents, operational employees, and the terrorist attacker are represented by agents. Below the main characteristics of these agents are summarized. A full description of this model can be found in [11].

5.1.1. Operational Employee

Operational employees communicate a wait request to passengers when they are in their observation range. These waiting requests can be communicated to passengers completing check-in or checkpoint activities.

5.1.2. Passenger

Passengers are described by airport arrival time, level of disorientation, the suitability of their luggage, whether they checked-in already, and if they are a facility visitor. For now, it suffices to state that the level of disorientation refers to how confused the passenger arrives in the airport, while suitability of luggage attributes how well the luggage of the passenger fits with their appearance. These properties are associated with real numbers and are important indicators used in the SPOT program of the TSA [36]. In that procedure, security officers assign points to passengers to evaluate their danger to the airport: if the points accredited to a certain passenger surpasses a threshold, a secondary screening is performed. Passengers can complete different activities, namely: check-in, checkpoint, facility and gate activity.

5.1.3. Attacker

The attacker is a human agent like any other passenger and hence shares the same characteristics. However, he has one unique goal: to cause as many human casualties at the airport as possible. To achieve this objective, the attacker agent carries an IED that he intends to detonate. This activity consists of three phases: target selection, movement to target and execution of the attack.

This paper extends the model of Janssen et al. by modeling different attacking scenarios based on an IED threat. Thus, in the first phase, the target selection is deterministic, meaning that the attacker has already selected a target to attack (from the set of 4 available options) before entering the airport. This approach implements a common assumption in security games where the attacker is assumed to have identified a breach/weakness in the security schedule through long term observation. Therefore, the attacker already knows when and where to execute his attack. In the second phase, the attacker moves from the airport entrance to the target. On his way, he might be observed by a security officer resulting in one of two events. With a probability p_{arrest}, the attacker is arrested and is not able to execute the attack, and with a probability of $1 - p_{arrest}$ he detonates the IED on the spot. Alternatively, the attacker is not observed and continues moving towards the target, where the last phase starts. Once he reached that area, the attacker detonates the IED.

5.1.4. Security Patrolling Agent

A security patrolling agent can observe physical objects, passengers, and attackers in her observation radius and line of vision. The security patrolling agent has a set of strategies corresponding to patrols around the airport which she follows.

During a patrol, the security officer randomly chooses an agent within her observation range, to evaluate whether it is an attacker or not. This evaluation lasts for a certain period and is performed according to the SPOT program described previously. When the points assigned to the observed agent exceed a specific threshold, the security officer will try to arrest the agent. If the agent is a passenger, the passenger is arrested and they both leave the airport. On the other hand, if the agent is an attacker, the security agent may arrest the attacker with a probability of p_{arrest}. If the security agent successfully arrests the attacker, the IED is not detonated. Alternatively, the attacker detonates the IED on the spot.

5.2. *Game-Theoretic Model*

We explain the spatio-temporal game of Zhang et al. [28], by describing the different components of the game. The game of Zhang et al. is a graph game, so we first translate the airport terminal layout to a graph. Based on this graph, we then specify the patrolling graph. This patrolling graph describes the possible actions and strategies of the defender.

Then, the time discretization scheme, the players in the game, and their set of actions and rewards are discussed. Finally, the solution concept is explained, along with the method to find equilibrium solutions. This section explains the theoretical basis of the game, while Section 5.3 later specifies how we applied this to our case study.

5.2.1. Airport Graph

The airport terminal is described by a graph $G(V, E)$ where $|V|$ represents the number of vertices and $|E|$ the number of edges, shown in Figure 3. Targets are modeled as vertices whereas the path between those is modeled as edges. Two important parameters are considered: time to move between targets and time to patrol a target. The time to move between targets (i.e., edge length) is constrained by the airport layout, whereas a target patrolling time is determined by the target importance for security purposes. Targets where a higher density of passengers is expected need to be patrolled more thoroughly.

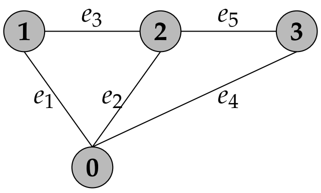

Figure 3. The graph model $G(V, E)$ of the airport terminal. The targets correspond to the targets as shown in Figure 1.

5.2.2. Patrolling Graph

Based on the airport graphic model, a patrolling graph $G_p(V_p, E_p)$ is generated. A basic example of such a graph is graphically illustrated in Figure 4. In this figure, we show two reference strategies for the security agent. In both cases, the security agent starts her patrol at T_0 at time 0. At this moment, she has two possible choices: either to move to T_3 (blue arrow) or stay at T_0 (red arrow). If the defender chose to move to T_3, then she only has one option available: patrol T_3 for two time units. On the other hand, if the defender stayed in T_0 previously, her choices are confined to moving to T_1, and then staying there for one time unit. Finally, the security agent terminates either patrol strategy by moving to T_0 at time 3. These are just two representative examples of defender's strategies to illustrate the definition of a strategy, but there are many more possible strategies in this example.

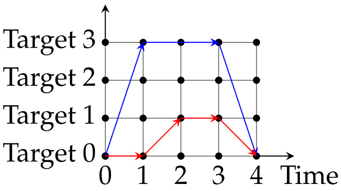

Figure 4. Two example strategies in a reduced version of the patrolling graph of the game. The actual patrolling graph contains nodes with corresponding times up to 1000 s.

A node in G_p is defined by a tuple (t, i), where $t \in [0, t_{max}]$ specifies the time and $i \in 0, 1, \ldots, |V| - 1$ represents a node in the airport graph $G(V, E)$. An edge from node (t_1, i_1) to (t_2, i_2) represents an action of the security agent where she moves from i_1 at time t_1 and arrives at i_2 at time t_2. A deterministic patrol strategy is a sequence of edges denoted as $e_p^1, \ldots, e_p^N$, where $e_p^i \in E_p$ is a patrolling edge, and N refers to the length of the patrolling graph, i.e., to the last patrolling edge. These patrolling graph edges have to comply to three requirements: (i) the in-degree of the start node of e_p^1 is zero; (ii) the out-degree of the end node of e_p^N is zero; (iii) e_p^i and e_p^{i+1} are connected, which means that the end node of e_p^i is the start node of e_p^{i+1}.

5.2.3. Time Discretization

The time dimension is discretized into equal time slices with the length of each time slice representing a second, with a total of t_{max} times. It is assumed that the security patrolling time and traveling time can only start at integer values of the time axis. The attacker can only start his attack at the beginning of each time slice as well. An attack lasts for a different amount of time depending on the target since the attacker takes different time from the airport entrance towards the target. Using this discretization scheme, it is possible to list all attacker strategies.

5.2.4. Players

The model considers a two-player game between a security agent (defender/leader) and a terrorist (attacker/follower), where both players are assumed to be perfectly rational. Consequently, both players are payoff maximizers. It is assumed that the attacker can gather information about the security patrol by long term observation, and the game is, therefore, a Stackelberg game.

5.2.5. Strategies

The strategies for both the defender and the attacker are introduced below.

Defender

At each node of the patrolling graph G_p, the defender can choose to examine that target or move to an adjacent node. These choices are described as edges in G_p. In this way, we define the security agent's strategy s_d as a set of probabilities of transitions between nodes in the patrolling graph G_p.

$$s_d = \prod_{(v_i,v_j)\in E_p} c_{v_i-v_j} \tag{1}$$

where $c_{v_i-v_j}$ specifies the probability of transition between node $v_i \in V_p$ to node $v_j \in V_p$, and $\prod$ represents the Cartesian product of all edges in G_p (i.e., all $(v_i, v_j) \in E_p$).

Attacker

An attacker's pure strategy s_a is defined by a target to attack and a time to start the attack.

$$s_a = (t, i) \tag{2}$$

where $t \in [0, \ldots, t_{max}]$ represents the attack start time and $i \in \{T_0, \ldots, T_3\}$ denotes the airport target. Furthermore, the attacker is constrained to attack only one target, i.e., play a pure strategy.

5.2.6. Payoff

Payoffs are provided after every transition between nodes. Equation (3) gives an example of the defender payoff function.

$$U_d = R_1 \times c_1 + \ldots + R_N \times c_N \tag{3}$$

Each element R_i contains the payoff value associated with a particular transition between nodes c_i in the patrolling graph. The specific definition of these variables in our case study will be explained in Section 5.3.2.

R_N and c_N denote the payoff value associated with the last transition between nodes. This may lead to transitions between nodes that do not produce any outcome in the agent-based model. In this case, the payoff value associated with those transitions is assumed to be zero for both agents.

The reward value is defined based on a particular outcome arising from the agent-based model: the average number of human casualties for each transition between nodes of the patrolling graph G_p. Section 6 elaborates further on the reward structure outlined in this paper. The game is defined as a zero-sum game, hence the attacker reward $U_a = -U_d$.

5.2.7. Solution Concept

To find an equilibrium solution, the model employs the concept of Stackelberg equilibrium $(s_d^*, s_a^*) = (\vec{c}^*, (t^*, i^*))$ that meet the following constraints:

$$(t^*, i^*) = argmax_{(t,i)\in S_a} u_a(\vec{c}, (t, i)) \tag{4}$$

$$\vec{c}^* = argmax_{\vec{c}\in S_d} u_d(\vec{c}, (t^*, i^*)) \tag{5}$$

As in all Stackelberg Security games, the defender (leader) first commits to a patrolling strategy $\vec{c}$, while the attacker (follower) can observe the defender's strategy and acts optimally according to it (Equation (4)). The security officer can also determine the attacker's optimal solution, hence she choose her strategy optimally as well (Equation (5)). Since the player's reward functions are linear polynomials of $\vec{c}$, a multiple linear programming algorithm can be used to compute the Stackelberg equilibrium solution.

In the first step, u_a and u_d are initialized for each attacker strategy. Then, a linear programming algorithm can be formulated, as shown below.

- Objective Function:

$$Max_{\vec{c} \in S_d} u_d(t^{\#}, i^{\#}, \vec{c}) \tag{6}$$

- Constraints:

$$\sum_{in \in \{s \in V_p | (s, V_p) \in E_p\}} c_{in - V_p} = \sum_{out \in \{e \in V_p | (V_p, e) \in E_p\}} c_{V_p - out} \tag{7}$$

$$\sum_{out \in \{e \in V_p | (root, e) \in E_p\}} c_{root - out} = 1 \tag{8}$$

$$u_a(t^{\#}, i^{\#}) \geq \alpha + u_a(t, i), \forall (t, i) \in S_a \tag{9}$$

$$u_a = -u_d \tag{10}$$

where *in*, *s*, *e*, *out* and *root* refer to nodes of the patrolling graph G_p, α is a small positive number and $S_a(S_d)$ is the strategy set of the attacker (defender). The *root* nodes represents a target where the security officer starts her patrol shift. Constraint 7 illustrates a property of probabilities c_{s-e} that for each intermediate node (node with both income and outcome edges) of G_p the sum of all income probabilities must equal the sum of all outcome probabilities. Constraint 8 describes a second property of probabilities c_{s-e} that the sum of probabilities going out from the root node equals 1. This means that the defender starts at the root node and must perform an action on what to do next. Constraint 9 assumes that the attacker strategy $u_a(t^{\#}, i^{\#})$ is the attacker optimal strategy. Moreover, α ensures that this model does not rely on the "breaking-tie" assumption, but it is still optimal. The breaking-tie concept assumes that when the follower (attacker) is indifferent on payoffs by playing different pure strategies, he will play the strategy that is preferable for the leader (defender). Lastly, constraint 10 defines a zero-sum game. The Stackelberg equilibrium is found by getting the arguments $(\vec{c}, (t, i))$ for which Equation (6) is maximum.

5.3. Integration of Agent-Based Results as Game-Theoretic Payoffs

Our integration of agent-based modeling and game theory is accomplished in three sequential steps. First, both the security and attacker strategies are generated, followed by the specification of game payoffs using agent-based model results. The last step consists of generating the optimal strategies for both players.

5.3.1. Generate Agents' Strategies

The first step of the integration module starts with the generation of the defender and attacker strategies. We discuss each of them individually below.

Defender Strategy

Given the chosen time discretization of 1 s, the set of strategies for the security agent is defined as follows. The airport entrance hall is regarded as the root node from where each patrol starts and ends. Following the airport layout (see Section 3), the security agent can only move to adjacent nodes.

Once the security agent reaches a certain target, she stays there for a given period (patrolling time) which differs from target to target. The reasoning behind this choice was to distinguish between targets that are more security-critical to the airport. For example, a successful attack in an area with a higher density of people can lead to more human casualties, thus that target should be better monitored. The patrol times as used in this work are shown in Table 1. These are based on initial experiments with the agent-based model and expert input. To include uncertainty related to disruption on security patrols, the time spent at the targets is according to a Normal distribution. When the patrolling time has passed, the agent must move to another adjacent node.

Table 1. Patrolling time for each target in seconds. Normal distributions are characterized by their mean (first parameter) and the standard deviation (second parameter).

T_0	T_1&T_2	T_3
$\mathcal{N}(60, 30)$	$\mathcal{N}(240, 30)$	$\mathcal{N}(360, 30)$

Using the layout of the airport graph (see Section 3), and the patrolling times of Table 1, we generated all possible deterministic patrolling strategies that can be executed within 1000 s. By performing a brute force search, we identified a total of 66 different patrol strategies that fit these criteria. This corresponds to a total of 596 different patrolling graph edges (movements).

Attacker Strategy

We considered 20 actions for the attacker. These actions have a five-minute interval uncertainty, for a period of 25 min for each of the identified targets ($T_0, \ldots, T_3$). The attacker agent may be caught in his path towards the target, even if both the security agent and the terrorist agent are not in the same area, but the latter is within the observation range of the former. This is a closer representation of reality than the standard game-theoretic formulation, as security officers can observe further than just their current target. This ensures that more realism is included than would be possible in the game-theoretic formulation alone.

5.3.2. Specify Payoffs Using Agent-Based Results

After generating the set of strategies for both agents, the next step is to specify the payoffs based on the agent-based model outcomes obtained from the previous step. As mentioned above, we focus on the average number of human casualties.

The number of casualties is estimated as follows. For each attacker and defender strategy, a consequence function that assesses the number of human fatalities is calculated for the simulated threat scenario. This function is used to determine the consequences for a simulation run of our agent-based model. Monte Carlo simulations are executed to evaluate the average number of casualties based on a set of N simulation runs. This average number of casualties corresponds to the conditional risk R_c, as defined in the work of Janssen et al. [11].

Following the generic payoff function specified in Section 5.2, first, we define $\vec{R}$ as the average number of casualties for each transition between nodes. F_i refers to the average number of casualties obtained when the defender performs the movement corresponding to the probability that the defender performs move i, denoted as c_i. Equation (11) shows the used payoff function.

$$U^{d}_{target,time} = -(\mathrm{F}_1 \times c_1 + \ldots + \mathrm{F}_{596} \times c_{596}) \tag{11}$$

The final game-theoretic model consists of 11,920 payoff values generated from the combination of 20 different attacker options and 596 security patrolling movements.

The above payoff function uses different F values for each attacker strategy combination. Therefore, 20 different payoff functions were defined $U_{0,0}, \ldots, U_{3,4}$ for each player. The target index varies from 0 (T_0) to 3 (T_3). The time index varies from 0 (attack enters the airport within the first 5 min) to 4 (attack enters the airport between the 20 to 25 min). Moreover, the defender's reward has a negative sing to penalize her for each human fatality. We assumed a zero-sum game; thus, the attacker reward has the opposite value of the defender.

5.3.3. Verification of Optimal Strategies

In the last step of our methodology, we generate the optimal attacker and defender strategy using the generated payoff values. These optimal strategies are simulated in the agent-based model and the outcomes of this simulation are compared to the ones obtained with the initial simulation assessment. The results are expected to be similar to positively verify the optimal game-theoretic solution. It is important to note that this does step does not correspond to validation. Validation of the strategy can be done using real-life tests, but is known to be difficult in practice [37,38].

6. Experiments and Results

Experiments performed with the above model are described in this section. First, the agent-based model experimental setup and results are described. Then, game-theoretic results are shown. Both the game-theoretic rewards are detailed along with the Stackelberg game solution for a generated security probabilistic patrol route and a fixed patrol route. Finally, the optimal strategies obtained for a probabilistic patrol route are subjected to evaluation.

6.1. Experimental Setup

The agent-based model contains a set of parameters in the experiments, of which the important ones are shown in Table 2. Apart from the number of simulations runs N, the parameters in this table were calibrated by Janssen et al. [11]. Additional parameter values of the model may be found in that work as well. It is important to note that all flights are defined with the same departure time, as commonly happens at regional airports. The model was implemented in the AATOM simulator, a Java-based open-source agent-based airport terminal operations simulator [39].

Table 2. Agent-based model parameters.

Parameter	Value
Simulation parameters	
Simulation runs	500
Airport and flight parameters	
Flight departure time	7200 s
Number of flights	3
Number of open checkpoint lanes	2
Number of open check-in desks	3
Agents parameters	
Proportion passengers check-in	0.5
Check-in time	*Norm(60,6)* s
Checkpoint time	*Norm(45,4.5)* s
Observation radius	10 m
Security arrest probability	0.8

The number of simulations required to obtain a proper estimate of the distribution of the model output was determined based on the coefficient of variation. Figure 5 shows the coefficient of variation for two different attacker–defender strategy pairs. It shows that the coefficient of variation tends to stabilize between 300 and 400 simulations. Consequently, the number of simulations N was set to be 500 to ensure a proper estimation of the model output for all attacker–defender strategy pairs.

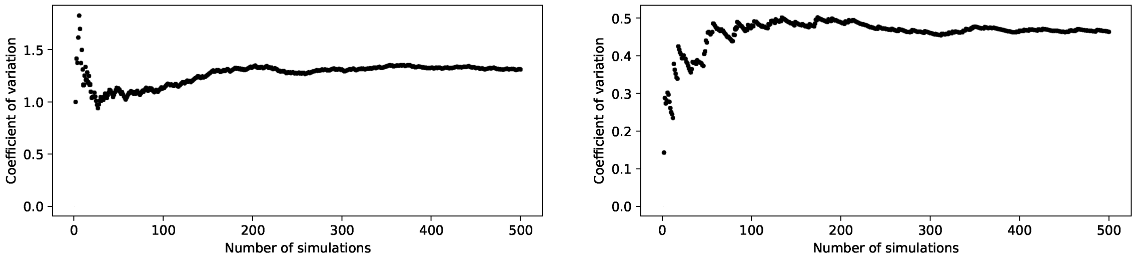

Figure 5. Coefficient of variability varying with the number of simulation runs.

6.2. *Agent-Based Model Results*

Table 3 shows a selected subset agent-based results associated with a particular defender transition between two nodes of G_p (i.e., a movement) and an attacker strategy (target, time).

Table 3. Illustrative example of agent-based outcomes. Cas. denotes the average number of casualties. Eff. represents the efficiency of the patrol for each movement, which is defined as the percentage of simulation runs in which the defender successfully arrested the attacker.

Start Node	**End Node**	**Att. Strategy**	**Cas.**	**Eff. (%)**
(Time (s), Target)	**(Time (s), Target)**	**(Target,Time (min))**		
(0, T_0)	(6, T_2)	$(T_0; 0–5)$	4.27	0
(6, T_2)	(246, T_2)	$(T_0; 0–5)$	2.194	21.72
(1933, T_3)	(1964, T_0)	$(T_0; 0–5)$	-	-
(0, T_0)	(31, T_3)	$(T_3; 0–5)$	0	100
(0, T_0)	(31, T_3)	$(T_0; 20–25)$	-	-
(1582, T_3)	(1942, T_3)	$(T_3; 20–25)$	11.615	7.69

From the agent-based model simulation, two scenarios can occur. First, for a particular defender movement and attack strategy, an interaction between both agents occurs. This interaction may be a successful attack or a successful arrest. However, it may also happen that for a particular defender movement and attack strategy, no interaction between both agents occurs. The later happens since the time of the defender movement does not coincide with the attack interval. For instance, movement $(1933, T_3)$ to $(1964, T_0)$ will not lead to a defender–attacker interaction when the attacker attacks T_0 within the first five minutes. Later in the game formulation, these cases will have a zero payoff value associated. The reasoning behind this choice was to assign a neutral payoff value for both players in the cases where they did not interact.

6.3. *Game-Theoretic Results*

Based on the results of Section 6.2, we describe the game-theoretic solution, focusing on rewards and strategies for each player.

6.3.1. Stackelberg Game Solution

Figure 6 shows a graphical representation of the Stackelberg Equilibrium solution of the game. The black lines symbolize the defender's optimal patrolling strategy, i.e., the non-zero probabilities for each of the actions of the defender. Each line segment has an associated number representing the probability that the defender will take that action, which is not shown in the figure. For instance, at time 0, the defender will move to check-in area (T_2) with a probability of 0.129. Alternatively, the defender also has an option to stay at the airport entrance (T_0) for 60 s with a probability of 0.871.

An interesting result of the generated strategy is that T_1 is not patrolled at all. This target is covered by patrolling T_2, which is close to T_1. The area around T_1 is in the observation radius of the defender when she is in T_2. Furthermore, T_2 is a more central target, and can, therefore, be reached faster from the other targets.

The attacker's best response strategy is to attack the checkpoint area (T_3), entering the airport at a time between ten to 15 min, illustrated in Figure 6 as a red line. Please note that the red line only covers T_3 for visualization simplicity. In reality, the attacker always enters the airport through T_0 and takes some time to arrive at the target.

Table 4 shows the agent-based model results associated with the patrol movements corresponding to the optimal patrol strategy. Only the patrol movements that lead to a defender–attacker interaction are shown. It is important to note that there is one movement for which the period does not coincide with the attacker entering time of 10 to 15 min. This occurs since the attacker takes time to reach his target destination in a crowded airport. All other movements that are part of the optimal strategy, but are not present in Table 4, are those where there was no interaction between both players. The payoff associated with those movements is set to zero.

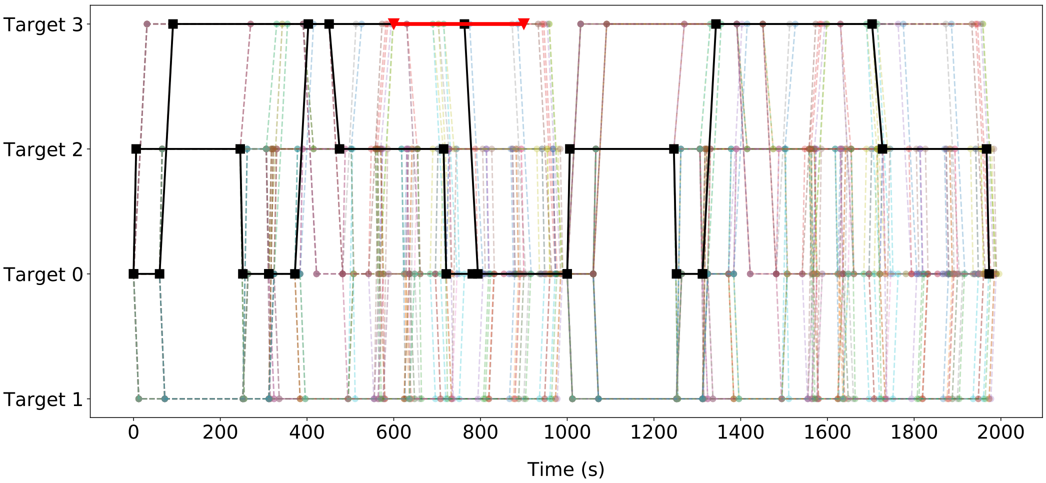

Figure 6. The optimal patrolling strategy over time and the attacker's best response. The black lines symbolize the defender's optimal (probabilistic) patrolling strategy. Each line segment (each movement) has an associated number representing the probability that the defender will do that movement. The red line illustrates the attacker's best response strategy. Please note that the red line only covers T_3 for the sake of visualization simplicity. In reality, the attacker enters the airport through its entrance (T_0) and takes some time to arrive at the target destination. Lastly, the remaining colors with lower opacity represent all possible movements that may have been chosen by the security officer.

When the probability value and expected number of casualties associated with each movement (as outlined in Table 4) are introduced in Equation (11), the optimal reward values for the defender and attacker are obtained.

$$\begin{aligned} U^{d}_{3,2} = -(&2.286 \times 0.129 + 1.540 \times 0.129 + 6.083 \times 0.129 \\ &+ 1.427 \times 0.871 + 2.284 \times 0.871 + 5.430 \times 0.871 \\ &+ 10.789 \times 1) = -20.03 \end{aligned}$$

The attacker reward is the negation of the defender's reward, i.e., $U^{a}_{3,2} = 20.03$. Figure 7 shows every attacker's reward value associated with each attacker's strategy against the defender optimal (probabilistic) patrolling strategy. These are computed similarly as the one illustrated in the equation above.

These results show that attacking the security checkpoint (T_3) between 5 and 20 min yields the highest reward for the attacker when compared to attacking other targets within the same time frame. This may be explained as follows. Passengers arriving in previous time intervals finished their check-in activity and are going towards the security checkpoint, leading to a higher density of people around that area. Thus, if the attack is successful, its impact would be large. This is not the case for all the other targets since there are passengers who did the check-in online and go straight to the T_3 which results in a lower concentration of passengers around those areas. Moreover, an attack within the first five minutes has a lower consequence since fewer people are at the airport terminal. The airport gets more crowded as time gets closer to the flight departure time.

It is also worth noticing that an attack on targets T_0, T_1 and T_2, at the latest time interval yields higher rewards for the attacker when compared to other periods. This is the case, as the number of people entering the airport considerably increases during that time interval which results in a higher concentration of people in those areas. This increase results from the fact that as time passes by, it gets closer to the flight departure time and therefore more people start entering the airport. As mentioned earlier, the latter increases the chances and consequences of a successful attack.

Table 4. Agent-based results associated with the movements of the defender that are part of the optimal patrol strategy.

Start Node	End Node	Prob.	Cas.	Eff. (%)
(Time (s), Target)	(Time (s), Target)			
(403, T_3)	(763, T_3)	0.129	2.286	72.67
(763, T_3)	(794, T_0)	0.129	1.540	78.94
(794, T_0)	(1000, T_0)	0.129	6.083	41.35
(475, T_2)	(715, T_0)	0.871	1.427	70.68
(721, T_0)	(781, T_0)	0.871	2.284	72.59
(781, T_0)	(1000, T_0)	0.871	5.430	47.70
(1006, T_2)	(1246, T_2)	1	10.789	0

By comparing the results of Figures 6 and 7, the defender's optimal strategy choice may be justified as follows. From Figure 7 it can be observed that the attacker reward by attacking T_3 while entering the airport between five to ten minutes yields the second-highest value. Therefore, the defender favors the patrol of that area during the corresponding period. The latter observation may be the reason the defender's optimal strategy does not contain additional movements that patrol the optimal attack target at the optimal attack time (between 10 to 15 min).

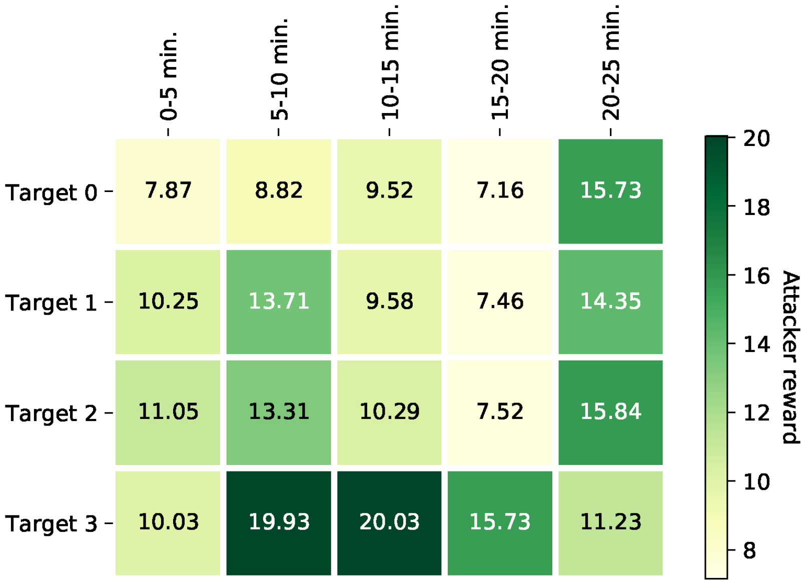

Figure 7. Attacker reward values for each attacking strategy, when the defender performs the optimal patrol illustrated in Figure 6.

However, the optimal defender strategy does not coincide with the attacker target for the entire attack time interval. Specifically, the defender choice after leaving T_3 is to go either to T_2 or T_0, and, eventually, staying there until a new patrol starts. These results can be explained by the fact that the attacker, in his path to T_3, may be detected by the defender if she is either at check-in area 2 (T_2) or the airport entrance (T_0).

These results show that the optimal security patrol gives special emphasis to high-impact areas, such as the security checkpoint, to reduce the total security risk. This is an improvement over the more simplistic strategies as shown in the work of Janssen et al. [11].

6.3.2. Deterministic Patrolling Strategy

In the current patrolling practice, the security officer may follow a deterministic patrolling strategy. In a deterministic patrolling strategy, the probability that an action is taken is constrained to be either 0 or 1, rather than a probabilistic value between 0 and 1. To investigate this scenario, we follow the same procedure illustrated in Section 6.3.1, but with the aforementioned constraint where the decision variables are either 0 or 1. Figure 8 illustrates the optimal strategy for both agents. The red line represents the attacker's optimal strategy, while the black line denotes the defender's best response. It is interesting to observe that for a fixed patrolling strategy, the attacker's best response remains to be T_3, but changes the attacking time interval to a time range between five to ten minutes. This result shows that attacking T_3 during the time interval between five and ten minutes yields a high payoff for the attacker. Therefore, it reinforces the defender's patrol choice of covering that target during that time interval in the probabilistic patrol strategy, as discussed in Section 6.3.1.

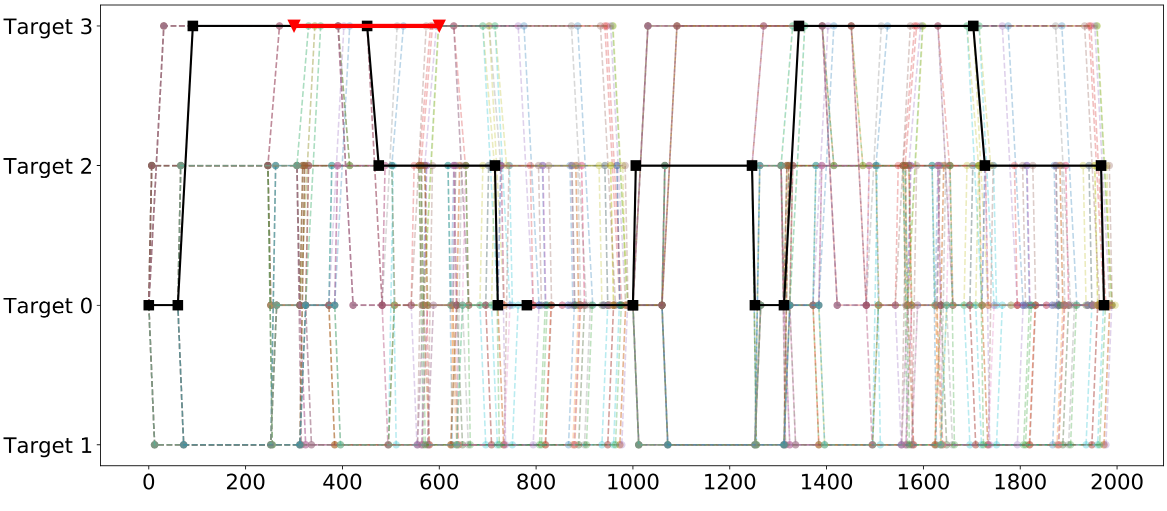

Figure 8. The deterministic optimal patrolling strategy over time and the attacker's best response. The black lines symbolize the defender's optimal patrolling strategy. The probability associated with each movement is 1.

Results, as shown in Figure 8, show that if the defender would follow the fixed patrolling route and the attacker plays his best response rewards for the defender and the attacker are −21.417 and 21.417 respectively. This shows that by randomizing over different movements at different times, the defender can generate strategies that are effective against a potential terrorist attack. These conclusions can help airport managers design security procedures.

6.4. Verification

Finally, the last step of our methodology is to simulate the optimal game-theoretic defender–attacker strategy pair in the agent-based model and compare the results with the ones resulting from the initial agent-based simulations. In this step, we can verify if the obtained solutions from the game-theoretic model are still valid in the agent-based model.

To do this, we simulated the optimal probabilistic defender patrolling strategy in the agent-based model. A total of 2000 simulations were executed. We simulate the obtained defender strategy against all attacker strategies (i.e., all target-time combinations). Figure 9 represents the average number of casualties per attacked target per time when the defender performs her optimal probabilistic patrol strategy. Please note that Figure 9 is different from Figure 7 as the prior represents the optimal reward value. This is a function of the average number of casualties and the probability of executing the optimal movements.

From Figure 9 it can be noted that the number of casualties when the attacker attacks T_0 is lower than at other targets. The airport entrance is a target where people do not agglomerate as intensively as they do at the check-in areas (T_1 and T_2) and the checkpoint (T_3). Furthermore, the highest patrol efficiencies occur at the optimal attack target (T_3). This reinforces the choice of the defender's optimal strategy since it achieves a higher arrest rate against the optimal attacker target.

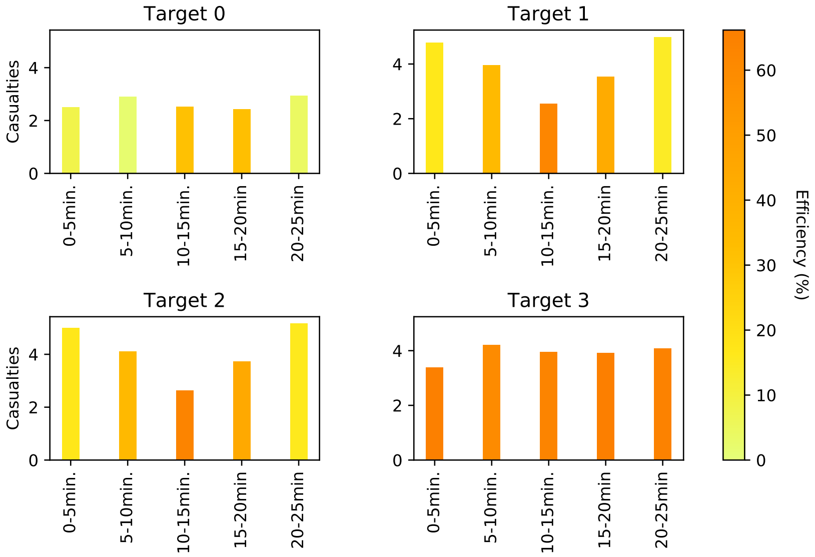

Figure 9. The number of casualties per attacking strategy against the optimal defender's strategy.

To understand the variability in the number of casualties in each simulation run, a boxplot of the results in Figure 10 was generated. This figure shows that the number of casualties in T_0 is lower than those on the other targets, while T_3 yields higher casualty values on average. This is because the passenger density at the airport entrance is smaller than the check-in areas, which is smaller than the security checkpoint. T_3 also yields the highest number of casualties that occurred in one simulation. This is a striking result because it indicates that a successful attack leading to a higher number of human fatalities may happen in reality, even if the security is executing the optimal patrol strategy. Therefore, it can be concluded that despite the optimal security strategy having higher patrol arrest rates at T_3, the potential consequences of a successful attack there are highest.

Finally, Table 5 shows the new agent-based model results associated with the patrol movements corresponding to the optimal probabilistic patrol strategy. Therefore, if the probability value and casualty value associated with each movement (in Table 5) are introduced in Equation (11), it is possible to compute the defender and attacker optimal reward values.

$$\begin{aligned} U^d_{3,2} = -(&2.667 \times 0.129 + 1.976 \times 0.129 + 5.602 \times 0.129 \\ &+ 1.413 \times 0.871 + 2.096 \times 0.871 + 6.721 \times 0.871 \\ &+ 9 \times 1) = -19.22 \end{aligned}$$

The attacker reward is the opposite of the defender's reward, i.e., $U^a_{3,2} = 19.22$. If we compare these values with the one achieved by the game-theoretic model ($-20.030/20.030$) we conclude that the payoffs are close, which verifies the proposed strategy.

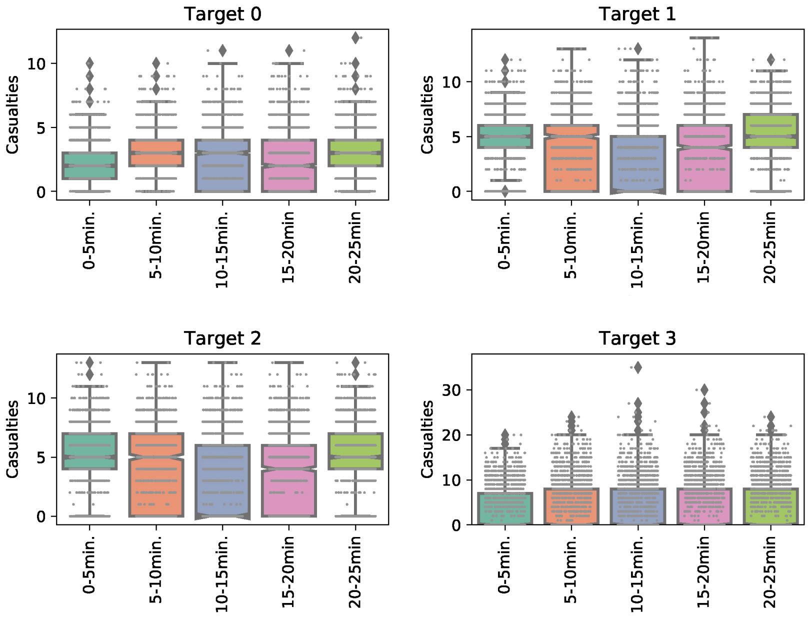

Figure 10. Number of casualties per target per time in each simulation run. Please note that the axis scales are different among targets. Two outliers (40 and 56 casualties), at T_3 between 20 and 25 min, were omitted from the figure to enhance readability.

Table 5. Empirical results for the optimal patrolling strategy in the verification step. All other movement probabilities are zero.

Start Node	End Node	Prob.	Cas.	Eff. (%)
(Time (s), Target)	(Time (s), Target)			
(403, T_3)	(763, T_3)	0.129	2.667	73.56
(763, T_3)	(794, T_0)	0.129	1.976	76.12
(794, T_0)	(1000, T_0)	0.129	5.602	43.08
(475, T_2)	(715, T_0)	0.871	1.413	71.26
(721, T_0)	(781, T_0)	0.871	2.096	82.61
(781, T_0)	(1000, T_0)	0.871	6.721	53.19
(1006, T_2)	(1246, T_2)	1	9	0

7. Conclusions and Future Work

This paper introduced a novel methodology to improve game-theoretic solutions by specifying payoff values based on the outcomes of an agent-based model. These payoff values are often defined by relying on expert assessment alone, which can be prone to errors and human biases. Our empirical game theory methodology improves current game-theoretic formulations by relying on data generated by a realistic agent-based model.

The methodology was applied to a case study in a regional airport terminal for an improvised explosive device threat. Results show that by strategically randomizing patrol routes, higher expected rewards for the security officer are achieved. This leads to a reduced number of expected casualties in an improvised explosive device attack. Furthermore, it was found that by allowing the defender to make probabilistic decisions at different time points, a higher reward is obtained when compared to a fixed optimal patrolling strategy. This supports the results of Zhang et al. [28]. Results further show that the optimal security patrol gives special emphasis to high-impact areas, such as the security checkpoint, to reduce the total security risk. This is an improvement over the more simplistic strategies as shown in the work of Janssen et al. [11].

This work can be extended in several directions. First, different strategies with less restrictive constraints may be investigated to understand if better rewards can be achieved. For instance, time spent at each target may be varied more to understand the influence of that parameter on the current model. Secondly, research on human behavior can be included to incorporate more complex behavior in the agent-based model. For instance, cultural backgrounds and motivations of attackers may be modeled to obtain more accurate results. In addition, the game model can also be improved to incorporate different human rationality models [29]. Lastly, uncertainty related to potential patrol disruptions may also be further investigated to improve the current game-theoretic model [32]. Finally, the proposed methodology can be applied to different infrastructures such as hospitals, schools, and banks.

Author Contributions: Methodology, D.M. and S.J.; software, S.J.; formal analysis, D.M.; writing—original draft preparation, D.M. and S.J.; writing—review and editing, A.S.; supervision, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. National Consortium for the Study of Terrorism and Responses to Terrorism (START). The Global Terrorism Database (GTD) [Data File]. 2018. Available online: https://www.start.umd.edu/gtd (accessed on 14 January 2020).
2. Tambe, M. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*; Cambridge University Press: Cambridge, UK, 2011.
3. Pita, J.; Jain, M.; Marecki, J.; Ordóñez, F.; Portway, C.; Tambe, M.; Western, C.; Paruchuri, P.; Kraus, S. Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport. In Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems: Industrial Track. International Foundation for Autonomous Agents and Multiagent Systems, Estoril, Portugal, 12–16 May 2008; pp. 125–132.
4. Pita, J.; Tambe, M.; Kiekintveld, C.; Cullen, S.; Steigerwald, E. GUARDS—Innovative application of game theory for national airport security. In Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence, Barcelona, Spain, 19–22 July 2011.
5. Tsai, J.; Rathi, S.; Kiekintveld, C.; Ordonez, F.; Tambe, M. IRIS-a tool for strategic security allocation in transportation networks. *AAMAS (Ind. Track)* **2009**, 37–44. [CrossRef]
6. Shieh, E.; An, B.; Yang, R.; Tambe, M.; Baldwin, C.; DiRenzo, J.; Maule, B.; Meyer, G. Protect: A deployed game theoretic system to protect the ports of the united states. In Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems-Volume 1. International Foundation for Autonomous Agents and Multiagent Systems, Valencia, Spain, 4–8 June 2012; pp. 13–20.
7. Yin, Z.; Jiang, A.X.; Tambe, M.; Kiekintveld, C.; Leyton-Brown, K.; Sandholm, T.; Sullivan, J.P. TRUSTS: Scheduling randomized patrols for fare inspection in transit systems using game theory. *AI Mag.* **2012**, *33*, 59–59. [CrossRef]
8. Heinrich, J.; Silver, D. Deep reinforcement learning from self-play in imperfect-information games. *arXiv* **2016**, arXiv:1603.01121.
9. Janssen, S.; Sharpanskykh, A. Agent-based modelling for security risk assessment. In Proceedings of the International Conference on Practical Applications of Agents and Multi-Agent Systems, Porto, Portugal, 21–23 June 2017; pp. 132–143.
10. Weiss, W.E. Dynamic security: An agent-based model for airport defense. In Proceedings of the 2008 Winter Simulation Conference, Miami, FL, USA, 7–10 December 2008; pp. 1320–1325.
11. Janssen, S.; Sharpanskykh, A.; Curran, R. Agent-based modelling and analysis of security and efficiency in airport terminals. *Transp. Res. Part C Emerg. Technol.* **2019**, *100*, 142–160. [CrossRef]

12. Jain, M.; Conitzer, V.; Tambe, M. Security scheduling for real-world networks. In Proceedings of the 2013 International Conference on Autonomous Agents and Multi-Agent Systems. International Foundation for Autonomous Agents and Multiagent Systems, St. Paul, MN, USA, 6–10 May 2013; pp. 215–222.
13. Council of European Union. Council Regulation (EU) no 300/2008. 2008. Available online: http://data.europa.eu/eli/reg/2008/300/oj (accessed on 14 January 2020).
14. Council of European Union. Council Regulation (EU) no 1998/2015. 2008. Available online: http://data.europa.eu/eli/reg_impl/2015/1998/oj (accessed on 14 January 2020).
15. 107th Congress. Aviation and Transportation Security Act. 2001. Available online: https://www.gpo.gov/fdsys/pkg/PLAW-107publ71/pdf/PLAW-107publ71.pdf (accessed on 14 January 2020).
16. ICAO. *Aviation Security Manual (Doc 8973—Restricted)*; ICAO: Montreal, QC, Canada, 2017.
17. Kirschenbaum, A.A. The social foundations of airport security. *J. Air Transp. Manag.* **2015**, *48*, 34–41. [CrossRef]
18. Washington, A. *All-Hazards Risk and Resilience: Prioritizing Critical Infrastructures Using the RAMCAP Plus [hoch] SM Approach*; ASME: New York, NY, USA, 2009.
19. Wagenaar, W.A. Generation of random sequences by human subjects: A critical survey of literature. *Psychol. Bull.* **1972**, *77*, 65. [CrossRef]
20. Prakash, A.; Wellman, M.P. Empirical game-theoretic analysis for moving target defense. In Proceedings of the Second ACM Workshop on Moving Target Defense, Denver, CO, USA, 12 October 2015; pp. 57–65.
21. Wellman, M.P. Methods for empirical game-theoretic analysis. In Proceedings of the AAAI, Boston, MA, USA, 16–20 July 2006; pp. 1552–1556.
22. Tuyls, K.; Perolat, J.; Lanctot, M.; Leibo, J.Z.; Graepel, T. A generalised method for empirical game theoretic analysis. In Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems. International Foundation for Autonomous Agents and Multiagent Systems, Stockholm, Sweden, 10–15 July 2018; pp. 77–85.
23. Basilico, N.; Gatti, N.; Amigoni, F. Patrolling security games: Definition and algorithms for solving large instances with single patroller and single intruder. *Artif. Intell.* **2012**, *184*, 78–123. [CrossRef]
24. Xu, H.; Ford, B.; Fang, F.; Dilkina, B.; Plumptre, A.; Tambe, M.; Driciru, M.; Wanyama, F.; Rwetsiba, A.; Nsubaga, M.; et al. Optimal patrol planning for green security games with black-box attackers. In *International Conference on Decision and Game Theory for Security*; Springer: Cham, Switzerland, 2017; pp. 458–477.
25. Vorobeychik, Y.; An, B.; Tambe, M. Adversarial patrolling games. In Proceedings of the 2012 AAAI Spring Symposium Series, Palo Alto, CA, USA, 26–28 March 2012.
26. Fang, F.; Jiang, A.X.; Tambe, M. Optimal patrol strategy for protecting moving targets with multiple mobile resources. In Proceedings of the 2013 International Conference on Autonomous Agents and Multi-Agent Systems. International Foundation for Autonomous Agents and Multiagent Systems, St. Paul, MN, USA, 6–10 May 2013; pp. 957–964.
27. Xu, H.; Fang, F.; Jiang, A.X.; Conitzer, V.; Dughmi, S.; Tambe, M. Solving zero-sum security games in discretized spatio-temporal domains. In Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence, Québec City, QC, Canada, 27–31 July 2014.
28. Zhang, L.; Reniers, G.; Chen, B.; Qiu, X. CCP game: A game theoretical model for improving the scheduling of chemical cluster patrolling. *Reliab. Eng. Syst. Saf.* **2018**. [CrossRef]
29. Kar, D.; Fang, F.; Delle Fave, F.; Sintov, N.; Tambe, M. A game of thrones: When human behavior models compete in repeated stackelberg security games. In Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems. International Foundation for Autonomous Agents and Multiagent Systems, Istanbul, Turkey, 4–8 May 2015; pp. 1381–1390.
30. Nguyen, T.H.; Yang, R.; Azaria, A.; Kraus, S.; Tambe, M. Analyzing the effectiveness of adversary modeling in security games. In Proceedings of the Twenty-Seventh AAAI Conference on Artificial Intelligence, Bellevue, WA, USA, 14–18 July 2013.
31. Kiekintveld, C.; Islam, T.; Kreinovich, V. Security games with interval uncertainty. In Proceedings of the 2013 International Conference on Autonomous Agents and Multi-Agent Systems. International Foundation for Autonomous Agents and Multiagent Systems, St. Paul, MN, USA, 6–10 May 2013; pp. 231–238.

32. Nguyen, T.H.; Jiang, A.X.; Tambe, M. Stop the compartmentalization: Unified robust algorithms for handling uncertainties in security games. In Proceedings of the 2014 International Conference on Autonomous Agents and Multi-Agent Systems. International Foundation for Autonomous Agents and Multiagent Systems, Paris, France, 5–9 May 2014; pp. 317–324.
33. Klima, R.; Tuyls, K.; Oliehoek, F.A. Model-Based Reinforcement Learning under Periodical Observability. In Proceedings of the 2018 AAAI Spring Symposium Series, Stanford, CA, USA, 26–28 March 2018.
34. Bonabeau, E. Agent-based modeling: Methods and techniques for simulating human systems. *Proc. Natl. Acad. Sci. USA* **2002**, *99*, 7280–7287. [CrossRef] [PubMed]
35. Cheng, L.; Reddy, V.; Fookes, C.; Yarlagadda, P.K. Impact of passenger group dynamics on an airport evacuation process using an agent-based model. In Proceedings of the 2014 International Conference on Computational Science and Computational Intelligence, Las Vegas, NV, USA, 10–13 March 2014; Volume 2, pp. 161–167.
36. US Government Accountability Office (GAO). *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*; US Government Accountability Office (GAO): Washington, DC, USA, 2013.
37. Ford, B. Real-World Evaluation and Deployment of Wildlife Crime Prediction Models. Ph.D. Thesis, University of Southern California, Los Angeles, CA, USA, 2017.
38. Gholami, S.; Ford, B.; Fang, F.; Plumptre, A.; Tambe, M.; Driciru, M.; Wanyama, F.; Rwetsiba, A.; Nsubaga, M.; Mabonga, J. Taking it for a test drive: A hybrid spatio-temporal model for wildlife poaching prediction evaluated through a controlled field test. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*; Springer: Cham, Switzerland, 2017; pp. 292–304.
39. Janssen, S.; Sharpanskykh, A.; Curran, R.; Langendoen, K. AATOM: An Agent-based Airport Terminal Operations Model Simulator. In Proceedings of the 51st Computer Simulation Conference, SummerSim 2019, Berlin, Germany, 22–24 July 2019.