Journal of the Operations Research Society of Japan
Vol. 60, No. 2, April 2017, pp. 156–177


# SECURITY GAMES TAKING ACCOUNT OF INVASION ROUTES AND ATTRITION

Ryusuke Hohzaki
*National Defense Academy*

Ginjiro Sakai
*Japan Ministry of Defense*

(Received February 22, 2016; Revised December 2, 2016)

*Abstract* This paper deals with security games which would be found around our lives. In a facility represented by a network, several types of invaders/attackers conflict with security guards/defenders who have also several security teams. The attacker chooses an invasion path to move along. He incurs some attrition by the conflict on arcs but surviving attackers give damage to the facility on his invasion route while the defender tries to minimize the damage by intercepting the attacker by a limited number of guards. The defender takes a randomized plan with respect to the adoption of each security team and the deployment of guards. Since the attacker know the defender's randomized plan before his decision making, the security problem is modeled by a Stackelberg game with the superiority of the attacker on information acquisition to the defender. There has been no research on the security game with multiple types of players modeled on a network, which explicitly takes account attrition on players. By some numerical examples, we investigate the best configuration of staff numbers in security teams and some characteristics of optimal defense to mitigate the damage caused by the attackers.

**Keywords**: Game theory, security game, network, attrition, quadratic programming, linear programming

## 1. Introduction

This paper deals with security games which would be found around our lives. In a facility represented by a network, several types of invaders/attackers conflict with security guards/defenders who have also several security teams. The attacker chooses an invasion path to move along. He incurs some attrition by the conflict on arcs but surviving attackers give damage to the facility on his invasion route while the defender tries to minimize the damage by intercepting the attacker by a limited number of guards. The defender takes a randomized plan with respect to the adoption of each security team and the deployment of guards. Since the attacker know the defender's randomized plan before his decision making, the security problem is modeled by a Stackelberg game with the superiority of the attacker on information acquisition to the defender. There has been no research on the security game with multiple types of players modeled on a network, which explicitly takes account attrition on players. In the security game, we investigate the best configuration of staff numbers in security teams and the characteristics of optimal defense to mitigate the damage caused by the attackers.

After the September 11 in 2001, the U.S. policy of Homeland Security Act (2002) affects other countries security policy because a chain of terrors sequentially occurred in several advanced countries. The U.S. policy is defined as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur". Some countries are going to adopt the acts by replacing their country names with "the U.S.". In academia, applications

of Operations Research (OR) to the homeland security have been developed these days [13].

Not concerning with the prevalence, OR researchers have studied security problems lieing in our lives from the past. Chaiken and Larson [6] surveyed 68 published papers on efficient activities of urban emergency services such as the police, fire fighting and ambulance, in respect to (1) determining the number of units to have on duty, (2) locating the units, (3) designing their response areas or patrol areas, (4) relocating units, and (5) planning preventive-patrol patterns for police cars. Olson and Wright [28] categorized the occurrences of incidents in a high-crime area in Chicago and proposed a patrol policy to maximize the expected number of occasions a police unit encounters per unit time in street blocks by a Markov chain model. The authors commented that the application of search theory, which Koopman [25] founded, was effective but the model had to take account of regional properties and geographic characteristics in the local area for effective patrol policies.

If we regard security game as a competition between a security team and its opponent, the security game is categorized in the field of attack-and-defense game. The attack-and-defense game originates from an old-fashioned OR application called *Blotto game* [41]. In the game, Colonel Blotto and his opponent dispatch their platoons to capture some forts and the result of the game or how many forts he occupies depends on two competitors' allocation strategies of their platoons or their resources on hand.

They recently make use of the attack-and-defense game, in which two players compete with each other for some valuable targets, to model their security games, as follows. Scaparra and Church [35] analyzed a Stackelberg game, in which a leader fortifies some facilities and then a follower attacks them after observing the fortification. Hausken [11, 12] considered another type of attack-and-defense game. An attacker or a defender decides how much to invest in attacking or defending some targets aligned in parallel, series or others. As Scaparra and Church did, Yang et al. [42] studied a Stackelberg game, in which a leader decides which targets he defends under the constraint of the limited number of defended targets.

Basilico et al. [3] took a model similar to Olson and Wright's model. A defender is a patrolling person in a geographic region. While sequentially observing the defender's position, an attacker is going to invade the region and decides to attack or not targets on the nodes he reaches, worrying about an arrest by the defender coming there during attacking the target. In the model of Baykal-Gursoy et al. [4], a patrolling defender tries to mitigate the damage an attacker causes to targets placed on several nodes on a network. Garnaev et al. [10] considered the same security game on a network but modeled the problem by a Bayesian game assuming two types of attackers. Shieh et al. [36] focused a cooperation of multiple defenders in their Stackelberg security game. Fang et al. [7] consider a attack-and-defense game with moving targets. They applied their method to a ferryboat protection problem to protect refugee supply lines.

Some analyzed attack-and-defense games in specific domains of telecommunication networks, electric power grids, road networks and railway networks, such as Kodialam and Lakshman [24], Salmeron et al. [34], Bell et al. [5] and Perea and Puerto [30], respectively.

The following researches considered security games at airports. They are trendy and remarkable because their proposed methodologies are embedded into real operations.Paruchuri et al. [29] explained their algorithm for an equilibrium of their security game, which was embedded in the solver, named DOBSS (Decomposed optimal Bayesian Stackelberg solver), installed in security system ARMOR (Assistant for randomized monitoring over routes) for Los Angeles International Airport (LAX). Their model is a Stackelberg game in which an attacker gets a part of information about a defender. The ARMOR supports security staffs

to set up vehicular checkpoints and canine patrolling plans. Pita et al. [31, 32] also describes the ARMOR system. Pita et al. [33] discussed a deviation from optimal behavior of the attacker caused by the attacker's bounded rationality and limited observation in the Stackelberg security game, aiming at the LAX protection. Jain et al. [22] explicated IRIS system in the United State. The Federal Air Marshal Service (FAMS) has deployed the IRIS in a pilot program to randomize the schedules of air marshals on international flights by game theory. The U.S. has other real systems of public transportation with applications of game theory. The U.S. Transportation Security Administration tested GUARDS (Game-theoretic unpredictable and randomly deployed security) system to deploy security staffs at more than 400 airports. PROTECT (Port resilience operational/tactical enforcement to combat terrorism) is another pilot system, which the U.S. Coast Guard adopted to protect the port functions against terrors as a game-theoretical planning system. Tambe [38] describes the functions of these real systems and explains their game-theoretical methodologies installed in these systems.

Some researchers use security games to contribute to effective border patrols. Agmon et al. [1] considered a Stackelberg game of multiple robot patrol around a closed area with the existence of an adversary attempting to penetrate into the area. The penetrator gets the security information of the robots in advance and the payoff of the game is the detection probability of the penetrator. Agmon et al. [2] extended their previous research by changing the contents of security information. Vanek et al. [40] also discussed a two-person zero-sum security game with patrollers and penetrators. They shows the effectiveness of their optimal penetration strategy in sea area with active pirates.

As Agmon et al. did, Morita et al. [27] and Hohzaki et al. [17] aimed at a contribution to the automation of security. In the first paper, they explicitly represented a security space by a network and proposed a resilient patrol planning under the situation that a security robot has some options of patrol route and an invader has some invasion routes in a facility. The second paper extended the first by proposing a new routing method for the best invasion on a dynamic network involving time passage and applying the method to a robust air defense against unknown aerial invaders in the air area above Tokyo in Japan.

The problems on the dynamic network are a little different from those on classical stationary networks such as the shortest path problem. When we consider the security network, the problem tends to become dynamic problems including the passage of time. In the concrete, the criterion of the problem is calculated differently depending on time even if a security team passes along the same route. They have to consider time space as well as geographic space in those problems. Recently in Japan, several occurrences of natural disasters stimulate researchers to develop evacuation planning systems and analyses on traffic congestion in the emergency by the medium of the dynamic network of Ford and Fulkerson [9], such as Takizawa et al. [37]. The dynamic network concept is also necessary for security games on networks.

Fare inspection in transit systems shows us other good approaches to the security in public transportation systems. In some urban transit systems, passengers are physically able to enter platforms without purchasing tickets, which is illegal though. To deter the fare evasion, inspection teams patrol to check ticket possession on the transit system or at the exits of the transit stations. Jiang et al. [23] and Yin et al. [43] discussed an optimal patrol strategy of inspection teams by a two-person zero-sum Stackelberg game on a dynamic network with timetable of transit vehicles. The authors applied their method to LA Metro in Los Angeles.

The modeling of the security game by differential game of Isaacs [19] is very rare. Fe-

ichtinger [8] adopt the model for a security game between a continuously moving thief and the police.

Many researches on the security game discussed the security in comparatively small and closed areas like public facilities. Some researchers deal with an effective allocation of security resource in larger areas like urban residential areas and metropolitan areas. For such security games, Tsai et al. [39] and Iwashita et al. [21] devised feasible computational algorithms for equilibrium points.

Hohzaki and Chiba [15], Hohzaki and Higashio [16], and Hohzaki and Sunaga [18] noted some attrition through a collision between an attacker and a defender, and embedded attrition models in their security games. The authors developed various models with the attrition which obey the linear law and the square law of Lanchester's attrition model [26].

Among papers cited above, the followings consider networks as security spaces to make the models realistic: [35], [11], [12], [3], [4], [10], [34], [5], [30], [1], [2], [40], [27], [17], [9], [37], [23], [43], [8], [39], [21], [15], [16] and [18]. Among these researches, just [15], [16] and [18] explicitly take account of attrition on players, which would occur through the conflict between attackers and defenders. However they were modeled in the context of interception of attackers. They did not consider multiple types of attackers nor any damage as a criterion of the security problem but single-type attackers and the number of surviving attackers at a destination.

To evolve the security games further for reality, we mentioned just an idea about a security game with multiple types of invaders and several teams of security guards under damage criterion and showed the availability of mathematical programming for optimal security plans in an explanatory article [14]. In this paper, we furthermore construct two additional security models and develop detailed theories about four security games with multiple types of invaders and multiple security teams. We also propose some methodologies to derive optimal security plans by linear programming and quadratic programming formulations and clarify an optimal deployment of security guards, an optimal configuration of security teams and the sensitivity of parameters by some computational analyses. According to the advice of Olson and Wright [28], we express a security space by a network and consider invasion routes in the concrete. While trying to investigate adequate payoff functions for a realistic security policy, we adopt several models of the Stackelberg security game with the superiority of the invader to the security team with respect to information acquisition. There has been no research on the security game with multiple types of players defined on a network, which explicitly takes account some attrition on players.

In Section 2, we describe a basic model of our game. In Section 3, we formulate the game into a quadratic programming problem to derive an equilibrium point. After then, in Sections 4 and 5, we modify the basic model to make it more realistic and propose two improved models. We take an example of airport security and analyze an effective security plan from the viewpoint of cost-performance in Section 6. There we investigate the best configuration of staff numbers in security teams and some characteristics of optimal defense to mitigate the damage caused by the attackers.

## 2. A Basic Model of Security Game

We consider a security game in a facility, in which an invader/attacker tries to invade the facility and give as much damage as possible and a security/defender desires to mitigate it. There are some types of attackers. Taking an airport as an example, we can think of criminals, smugglers, terrorists and others. Intelligent attackers would gather information

about the security in advance to aim at the weakest point of the security. In our model, we consider a Stackelberg security game with multiple teams of attackers.

(A1) A security space consists of a network $G(\boldsymbol{N}, \boldsymbol{E})$ with a node set $\boldsymbol{N}$ and an arc set $\boldsymbol{E}$. There are two players, an attacker/invader and a defender/security.

(A2) There are several types of attackers, a set of which is denoted by $\boldsymbol{H}$. The attacker of a type $h \in \boldsymbol{H}$ invades the facility network with an initial number $R_0^h$ of his members and goes to his destination node. On the way to the destination, he makes some damage of damage rate $d_e^h$ per attacker just after going through an arc $e$. A pure strategy of the $h$-type attacker is to choose a path among a set of invasion routes $\Omega^h$.

(A3) The defender has several security teams, a set of which is denoted by $\boldsymbol{S}$. A team $s \in \boldsymbol{S}$ has an initial number $B_0^s$ of guards to deploy on arcs for the defense of the facility against the attacker. A pure strategy of the defender is to make a deployment plan of $B_0^s$ on arcs and how often he applies each security team $s$, $g(s)$. On the frequency $g(s)$, the defender has an upper bound $U(s)$, which satisfies $\sum_{s\in S} U(s) \geq 1$, as a financial constraint on the team $s$.

The defender gets the statistics about the occurrence of incidents by the attackers in the past and estimates a distribution of the attacker's type by $\{f(h), h \in \boldsymbol{H}\}$, where $f(h)$ is the occurrence probability of type $h$ in an incident.

(A4) Both the attacker and the defender incur some attrition through a conflict between them on an arc and the conflict continues by the annihilation of a player. The attrition obeys a linear model. When $x$ members of the attacker and $y$ guards combat on arc $e \in \boldsymbol{E}$, the residual number of attackers is given by the following expression, depending on the attacker's type $h$ and the security's team $s$:

$$\max\{0,\ x - \gamma_e^{hs} y\}. \tag{1}$$

Coefficient $\gamma_e^{hs}$ is called the power ratio of the defender's power against the attacker's power.

(A5) Through the past observation on the security deployment, the attacker knows the deployment plan of each security team $s \in \boldsymbol{S}$ and the frequency $g(s)$ of defender's taking $s$. However he does not certainly know the defender's deployment plan just on the date he attacks the facility.

(A6) Both players are interested in how much damage the attacker makes, which is the payoff of the game. The attacker wants to maximize it and the defender desires to minimize it.

We can think of several different damage situations depending on the attacker type, which are taken account of in Assumption (A2). At an airport, smugglers would make profit just after leaving the airport terminal. At the same time, the security side incurs some damage by letting them out because their contrabands could have negative effects on the society. We would properly assume that the smugglers give some damage just at the exit of the facility or their destinations without any damage on the way to there. If the attackers are terrorists, they would try to make as much damage as possible while moving on the way to their destinations. Here we assume a zero-sum payoff, which means that the profit of the attacker is the loss of the defender and vice versa. As assumed in Assumption (A3), the security side has several teams as a preparation for estimated risks. A different team has a different number of guards with different equipments and a different strength against the attacker.

From now we formulate our security game into a Stackelberg game and derive an equilibrium of the game. Before that, let us clarify the attrition model given by the expression

(1).

This expression is called the Lanchester linear model, which prescribes an attrition law between two competitors $A$ and $B$. Lanchester [26] derived differential equations which theoretically describe attrition dynamics of two competitors under a specific combat situation. A solution of the equations shows us a linear relationship between two sides' attrition, as follows.

$$X_0 - X = \gamma(Y_0 - Y), \tag{2}$$

where $X_0$ and $X$ are an initial number and a present number of competitor $A$, respectively, and $Y_0$ and $Y$ an initial number and a present number of competitor $B$. Coefficient $\gamma$ is called the power ratio or the exchange ratio of $B$'s power against $A$'s one and thought to be kept constant during the combat. If the combat continues until an exhaustion of competitor $B$ ($Y = 0$) or $A$ ($X = 0$), the number of remaining $A$ or remaining $B$ is given by

$$X = \max\{0, X_0 - \gamma Y_0\}, \quad Y = \max\left\{0, Y_0 - \frac{1}{\gamma}X_0\right\}. \tag{3}$$

From the basics of the attrition, we have the following lemmas in terms of the survival number of player A marching along a path, which was already proved by Hohzaki and Chiba [15].

**Lemma 2.1** ([15]). *A path $l$ from a starting node to a destination node consists of arcs $\{e_1, e_2, \cdots, e_m\}$. Assuming that each arc $e_j$ has its power ratio $\gamma_{e_j}$ and the deployment of $y_{e_j}$ defenders, the attacker with its initial number $X_0$ survives $k$ interceptions by the defender and would has his survived number*

$$X_k = \max\left\{0,\ X_0 - \sum_{j=1}^{k} \gamma_{e_j} y_{e_j}\right\} \tag{4}$$

*just after passing through the $k$-th arc $e_k$.*

From the next section, we are going to formulate our problem into a Stackelberg game and derive its equilibrium.

## 3. Formulation and Equilibrium

Let us first define players' strategies. We denote a mixed strategy of type $h \in \boldsymbol{H}$ of attacker by $\pi_h = \{\pi_h(l), l \in \Omega^h\}$, where $\pi_h(l)$ is the probability of choosing a path $l$, and all types of mixed strategies by $\pi \equiv \{\pi_h, h \in \boldsymbol{H}\}$. The feasible regions of $\pi_h$ and $\pi$ are

$$\Pi_h \equiv \{\{\pi_h(l), l \in \Omega^h\} | \sum_{l \in \Omega^h} \pi_h(l) = 1,\ \pi_h(l) \geq 0,\ l \in \Omega^h\} \tag{5}$$

and $\Pi \equiv \prod_{h \in H} \Pi_h$, respectively. The defender decides a deployment plan $\boldsymbol{y}^s = \{y_e^s, e \in \boldsymbol{E}\}$ of the security team $s$ by the number of guards $y_e^s$ on arc $e$ and the probability of taking the team $s$, $g(s)$, on the relevant day. $\boldsymbol{y}^s$ has to satisfy conditions: $\sum_{e \in E} y_e^s \leq B_0^s$ and $y_e^s \geq 0$ ($e \in \boldsymbol{E}$) although we can replace the first inequality with an equation if the security is allowed to waste its staffs. The mixed strategy $g(s)$ has its feasibility conditions: $\sum_{s \in S} g(s) = 1$ and $0 \leq g(s) \leq U(s)$ ($s \in \boldsymbol{S}$).

Using the notations defined above, let us derive the payoff of the game. For a pure strategy $l$ of the $h$-type attacker and a team-$s$ security deployment $\boldsymbol{y}^s$, the payoff is given by

$$P_{hs}^1(l, \boldsymbol{y}^s) = \sum_{e \in E_l} d_e^h \max\left\{0,\ R_0^h - \sum_{e' \in E_l^e} \gamma_{e'}^{hs} y_{e'}^s\right\},$$

taking account of the total attrition on the way to the destination and Equation (4). $E_l$ is a set of arcs on the path $l$ and $E_l^e$ is a set of arcs from the start node through an arc $e$ along the path $l$. From the derivation, we calculate the expectation of the game value by a defender mixed strategy $g(s)$ and further by a mixed strategy of the $h$-type attacker, $\pi_h$, as follows.

$$\begin{aligned} P_h^1(l,(g,\boldsymbol{y})) &= \sum_{s\in S} g(s) P_{hs}^1(l,\boldsymbol{y}^s) = \sum_{s\in S} g(s) \sum_{e\in E_l} d_e^h \max\left\{0,\ R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right\}, \\ P_h^1(\pi_h,(g,\boldsymbol{y})) &= \sum_{l\in\Omega^h} \pi_h(l) P_h^1(l,(g,\boldsymbol{y})) \\ &= \sum_{l\in\Omega^h} \pi_h(l) \sum_{s\in S} g(s) \sum_{e\in E_l} d_e^h \max\left\{0,\ R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right\} \end{aligned} \tag{6}$$

Since the attacker observes the security strategy $\{(g(s),\boldsymbol{y}^s), s\in \boldsymbol{S}\}$, the $h$-type attacker maximizes the expected value of the game or $\max_{\pi_h} P_h^1(\pi_h,(g,\boldsymbol{y}))$ with respect to $\pi_h$. Anticipating the rational behavior of the attacker, the defender is going to minimize the expectation of the maximized value,

$$\begin{aligned} &\sum_{h\in H} f(h) \max_{\pi_h} P_h^1(\pi_h,(g,\boldsymbol{y})) \\ &= \max_{\pi\in\Pi} \sum_{h\in H} f(h) \sum_{l\in\Omega^h} \pi_h(l) \sum_{s\in S} g(s) \sum_{e\in E_l} d_e^h \max\left\{0,\ R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right\}, \end{aligned}$$

by changing his strategy $\{(g(s),\boldsymbol{y}^s), s\in \boldsymbol{S}\}$.

From the discussion above, the optimization problem on the security side is to find an optimal strategy $(g,\boldsymbol{y})$ of minimax-optimizing the following expected payoff:

$$P^1(\pi,(g,\boldsymbol{y})) = \sum_{h\in H} f(h) \sum_{l\in\Omega^h} \pi_h(l) \sum_{s\in S} g(s) \sum_{e\in E_l} d_e^h \max\left\{0,\ R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right\}. \tag{7}$$

The problem is a Stackelberg game with a leader of taking $\{(g(s),\boldsymbol{y}^s), s\in \boldsymbol{S}\}$ and a follower of choosing $\pi$. An optimal defender strategy $(g^*,\boldsymbol{y}^*)$ is derived from the minimax optimization of the expression (7) and an optimal attacker's strategy $\pi_h^*$ of each type $h\in \boldsymbol{H}$ is given by maximizing the function $P_h^1(\pi_h,(g^*,\boldsymbol{y}^*))$ knowing the optimal defender strategy.

From the feasible conditions of $\pi_h$ in Equation (5), the maximization of $P^1(\pi,(g,\boldsymbol{y}))$ is transformed in

$$\begin{aligned} &\max_{\pi\in\Pi} \sum_{h\in H} f(h) \sum_{l\in\Omega^h} \pi_h(l) \sum_{s\in S} g(s) \sum_{e\in E_l} d_e^h \max\left\{0,\ R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right\} \\ &= \sum_{h\in H} f(h) \max_{l\in\Omega^h} \sum_{s\in S} g(s) \sum_{e\in E_l} d_e^h \max\left\{0,\ R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right\}. \end{aligned} \tag{8}$$

Therefore, the minimax-optimization problem becomes

$$\min_{g,y}\max_{\pi\in\Pi} P^1(\pi,(g,\boldsymbol{y})) = \min_{g,y}\sum_{h\in H} f(h)\max_{l\in\Omega^h}\sum_{s\in S} g(s)\sum_{e\in E_l}\max\left\{0,\ d_e^h\left(R_0^h - \sum_{e'\in E_l^e}\gamma_{e'}^{hs}y_{e'}^s\right)\right\}. \tag{9}$$

To derive an optimal defender strategy, we introduce a variable $\mu_h$, which finally coincides with the maximized value of $\max_{l\in\Omega^h}$, or its set $\mu\equiv\{\mu_h, h\in\boldsymbol{H}\}$ and a variable $\eta_{le}^{hs}$, which bears $\max\{0,\cdot\}$, or its set $\eta\equiv\{\eta_{le}^{hs}, e\in\boldsymbol{E}_l, l\in\Omega^h, h\in\boldsymbol{H}, s\in\boldsymbol{S}\}$ in the problem (9), and have a final formulation of quadratic programming problem:

$$\begin{aligned}
(F_S^1)\quad & \min_{g,y,\mu,\eta}\ \sum_{h\in H} f(h)\mu_h \\
s.t.\quad & \mu_h \geq \sum_{s\in S} g(s)\sum_{e\in E_l}\eta_{le}^{hs},\ l\in\Omega^h,\ h\in\boldsymbol{H}, \\
& \eta_{le}^{hs} \geq d_e^h\left(R_0^h - \sum_{e'\in E_l^e}\gamma_{e'}^{hs}y_{e'}^s\right),\ e\in E_l,\ s\in\boldsymbol{S},\ l\in\Omega^h,\ h\in\boldsymbol{H}, \\
& \eta_{le}^{hs}\geq 0,\ e\in E_l,\ s\in\boldsymbol{S},\ l\in\Omega^h,\ h\in\boldsymbol{H}, \\
& \sum_{e\in E} y_e^s \leq B_0^s,\ s\in\boldsymbol{S}, \\
& y_e^s\geq 0,\ e\in\boldsymbol{E},\ s\in\boldsymbol{S}, \\
& \sum_{s\in S} g(s) = 1, \\
& 0\leq g(s)\leq U(s),\ s\in\boldsymbol{S}.
\end{aligned}$$

Knowing the optimal defender strategy $g^*$ and $\boldsymbol{y}^*$, an optimal attacker strategy $\pi_h^*$ is given by solving

$$\max_{\pi_h} P_h^1(\pi_h,(g^*,\boldsymbol{y}^*)) = \max_{\pi_h\in\Pi_h}\sum_{l\in\Omega^h}\pi_h(l)\sum_{s\in S} g^*(s)\sum_{e\in E_l} d_e^h\max\left\{0,\ R_0^h - \sum_{e'\in E_l^e}\gamma_{e'}^{hs}y_{e'}^{*s}\right\}.$$

As seen from the transformation (8), the optimal strategy is evidently a choice of some path $l$ of achieving $\max_{l\in\Omega^h}$ or any mixed strategy consisting of those paths.

Hereafter we sometimes use some notations with no superscript and no subscript as their sets, without any notice, like $\boldsymbol{d}$, for example, which indicates a set $\{d_e^h, e\in\boldsymbol{E}, h\in\boldsymbol{H}\}$.

## 4. A Model with an Attacker's Strong Motive of Invasion

Here we improve the previous model, in which the defender could underestimate an attacker's strong motive of invasion in the security network. In the case that the defender is strong enough to annihilate the attacker on any invasion route, the previous model shows us zero payoff and the attacker has no motive of invasion in the facility, in theory. In practice, however, some invaders, especially terrorists, try to make an invasion even if they are thought to never reach their destinations and never survive at all. Some invaders have too strong motive of invasion to give up intruding in the network even by the estimation of his annihilation. Such invaders are eager to make the number of their surviving members

larger even if it is expected to be negative, and to take a chance on a little probability of penetrating the security net.

Here we take the strong motive of invasion into account and consider a naive number of the number of initial attackers minus the number of wasted attackers as a payoff function, which could be negative as well as positive. We would achieve our modeling by changing the payoff function of the $h$-type attacker from Equation (6) to the following:

$$P_h^2(\pi_h,(g,\boldsymbol{y}))=\sum_{l\in\Omega^h}\pi_h(l)\sum_{s\in S}g(s)\sum_{e\in E_l}d_e^h\left(R_0^h-\sum_{e'\in E_l^e}\gamma_{e'}^{hs}y_{e'}^s\right).$$

If the defender is aware of the attacker's strong motive of invasion, the payoff of the defender is changed from Equation (7) to

$$\begin{aligned}P^2(\pi,(g,\boldsymbol{y})) &= \sum_{h\in H}f(h)P_h^2(\pi_h,(g,\boldsymbol{y}))\\ &= \sum_{h\in H}f(h)\sum_{l\in\Omega^h}\pi_h(l)\sum_{s\in S}g(s)\sum_{e\in E_l}d_e^h\left(R_0^h-\sum_{e'\in E_l^e}\gamma_{e'}^{hs}y_{e'}^s\right).\end{aligned}$$

In the similar way to the transformation (8) and (9), we carry out its minimax optimization of the expected payoff as follows.

$$\begin{aligned}&\min_{g,y}\max_{\pi\in\Pi}P^2(\pi,(g,\boldsymbol{y}))=\min_{g,y}\sum_{h\in H}f(h)\max_{l\in\Omega^h}\sum_{s\in S}g(s)\sum_{e\in E_l}d_e^h\left(R_0^h-\sum_{e'\in E_l^e}\gamma_{e'}^{hs}y_{e'}^s\right)\\ &=\min_{g,y}\sum_{h\in H}f(h)\max_{l\in\Omega^h}\sum_{e\in E_l}d_e^h\left(R_0^h-\sum_{s\in S}\sum_{e'\in E_l^e}\gamma_{e'}^{hs}g(s)y_{e'}^s\right)\end{aligned}\tag{10}$$

Let us introduce a new variable $z_e^s\equiv g(s)y_e^s$ into the formulation. From the feasible conditions of $g(s)$: $\sum_{s\in S}g(s)=1$ and $0\le g(s)\le U(s)$, and those of $\boldsymbol{y}^s$: $\sum_{e\in E}y_e^s=B_0^s$ and $y_e^s\ge 0$, we generate the feasible conditions of $z_e^s$. From $\sum_{e\in E}z_e^s=g(s)B_0^s$, we have $g(s)=\sum_{e\in E}z_e^s/B_0^s$ and then $\sum_{e\in E}z_e^s/B_0^s\le U(s)$ and $1=\sum_s g(s)=\sum_s(\sum_{e\in E}z_e^s/B_0^s)$. With an additional condition of nonnegativity, we have the following feasible conditions on $z_e^s$.

$$\sum_{s\in S}\frac{1}{B_0^s}\sum_{e\in E}z_e^s=1,\quad \frac{1}{B_0^s}\sum_{e\in E}z_e^s\le U(s),\quad z_e^s\ge 0.\tag{11}$$

Because of $y_e^s=z_e^s/g(s)=B_0^s z_e^s/\sum_{e'\in E}z_{e'}^s$, we can inversely construct $g(s)$ and $\boldsymbol{y}^s$ from $z_e^s$ by the following expressions.

$$g(s)=\frac{1}{B_0^s}\sum_{e\in E}z_e^s,\quad y_e^s=B_0^s\frac{z_e^s}{\sum_{e'\in E}z_{e'}^s}.\tag{12}$$

Using $\boldsymbol{z}=\{z_e^s,\ e\in\boldsymbol{E},s\in\boldsymbol{S}\}$, we have a linear programming formulation from the problem

(10).

$$
\begin{aligned}
(F_S^2) \quad & \min_{z,\mu} \sum_{h\in H} f(h)\mu_h \\
s.t. \quad & \mu_h \geq \sum_{e\in E_l} d_e^h \left( R_0^h - \sum_{s\in S} \sum_{e'\in E_l^e} \gamma_{e'}^{hs} z_{e'}^s \right),\ l \in \Omega^h,\ h \in \boldsymbol{H}, \qquad (13)\\
& \sum_{s\in S} \frac{1}{B_0^s} \sum_{e\in E} z_e^s = 1, \\
& \frac{1}{B_0^s} \sum_{e\in E} z_e^s \leq U(s),\ s \in \boldsymbol{S}, \\
& z_e^s \geq 0,\ e \in \boldsymbol{E},\ s \in \boldsymbol{S}.
\end{aligned}
$$

After deriving an optimal solution $z_e^{*s}$ from the problem $(F_S^2)$, we calculate an optimal strategy of the defender, $g^*(s)$ and $y_e^{*s}$, by the expressions (12).

## 5. A Model with the Change of Damage Rate

By the model in Section 4, we incorporate the attacker's strong motivation of invasion, as we often see in terrors at public facilities such as airports, theaters, public transit stations and others. However we find a shortcoming in the modified model, as follows. By a security strategy $(g(s), \boldsymbol{y}^s)$, we estimate the number of the $h$-type surviving attackers just after leaving an arc $e$ on a path $l$ by

$$
V_{le}^h \equiv \sum_{s\in S} g(s) \left( R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right) \qquad (14)
$$

and the damage there by $d_e^h V_{le}^h$. A solution of problem $(F_S^2)$ makes the security to deploy more guards at the place with larger damage rate $d_e^h$ and larger power ratio because such a deployment efficiently decreases the damage even though the number $V_{le}^h$ is negative. Let us imagine that the security forces make $V_{le}^h$ negative on an arc $e$ with larger $d_e^h$ but $V_{le'}^h$ positive on the other arc $e'$ with smaller $d_{e'}^h$. If the security team $s$ additionally increases its number $B_0^s$, the solution of $(F_S^2)$ could bring more guards on the arc $e$ to accelerate the negativity of $V_{le}^h$ while keeping the number of guards deployed on the arc $e'$ unchanged. In practice, however, the security would judge that the guards on the arc $e$ are strong enough because of $V_{le}^h < 0$ and put or redeploy some excess staffs on the arc $e'$ with positive $V_{le'}^h$ to reinforce there. The fact gives us an idea that we should change the damage rate depending on whether $V_{le}^h$ is positive or negative. Generally, we'd better use larger rate $d_e^h$ if $V_{le}^h$ is positive but smaller rate $\underline{d_e^h}$ if negative. In this model, we evaluate the damage on the arc $e$ by

$$
\max \left\{ d_e^h \left( R_0^h - \sum_{s\in S} \sum_{e'\in E_l^e} \gamma_{e'}^{hs} g(s) y_{e'}^s \right),\ \underline{d_e^h} \left( R_0^h - \sum_{s\in S} \sum_{e'\in E_l^e} \gamma_{e'}^{hs} g(s) y_{e'}^s \right) \right\}. \qquad (15)
$$

In the result, we define the following expected payoff

$$P^3(\pi,(g,\boldsymbol{y})) = \sum_{h\in H} f(h) \sum_{l\in\Omega^h} \pi_h(l) \sum_{e\in E_l} \max\left\{ d_e^h \left( R_0^h - \sum_{s\in S} \sum_{e'\in E_l^e} \gamma_{e'}^{hs} g(s) y_{e'}^s \right), \underline{d_e^h} \left( R_0^h - \sum_{s\in S} \sum_{e'\in E_l^e} \gamma_{e'}^{hs} g(s) y_{e'}^s \right) \right\}$$

by a security mixed strategy $(g,\boldsymbol{y})$ and an invader mixed strategy $\pi$.

We can accomplish the minimax optimization of the expected payoff by replacement of $z_e^s \equiv g(s)y_e^s$ for $(g,\boldsymbol{y})$ in the same way as the formulation $(F_S^2)$ in Section 4, as follows.

$$\begin{aligned}
(F_S^3) \quad & \min_{z,\mu,\eta} \sum_{h\in H} f(h)\mu_h \\
s.t. \quad & \mu_h \geq \sum_{e\in E_l} \eta_{le}^h,\ l\in\Omega^h,\ h\in \boldsymbol{H}, \\
& \eta_{le}^h \geq d_e^h \left( R_0^h - \sum_{s\in S} \sum_{e'\in E_l^e} \gamma_{e'}^{hs} z_{e'}^s \right),\ e\in E_l,\ l\in\Omega^h,\ h\in\boldsymbol{H}, \\
& \eta_{le}^h \geq \underline{d_e^h} \left( R_0^h - \sum_{s\in S} \sum_{e'\in E_l^e} \gamma_{e'}^{hs} z_{e'}^s \right),\ e\in E_l,\ l\in\Omega^h,\ h\in\boldsymbol{H}, \\
& \sum_{s\in S} \frac{1}{B_0^s} \sum_{e\in E} z_e^s = 1, \\
& \frac{1}{B_0^s} \sum_{e\in E} z_e^s \leq U(s),\ s\in S, \\
& z_e^s \geq 0,\ e\in \boldsymbol{E},\ s\in S.
\end{aligned}$$

After deriving optimal variables $\boldsymbol{z}^*$ from the linear programming problem $(F_S^3)$, we construct an optimal security strategy $(g^*,\boldsymbol{y}^*)$ by Equations (12).

Recalling that the equation (14) is the number of remaining $h$-type attackers averaged up over the security teams $\boldsymbol{S}$, we have another evaluation depending on not the expected number $V_{le}^h$ but the rude survival number established for a specific security team $s$, that is,

$$V_{le}^{hs} \equiv R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s.$$

In this case, the resultant expected payoff is given by

$$P^4(\pi,(g,\boldsymbol{y})) = \sum_{h\in H} f(h) \sum_{l\in\Omega^h} \pi_h(l) \sum_{s\in S} g(s) \sum_{e\in E_l} \max\left\{ d_e^h \left( R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right), \underline{d_e^h} \left( R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right) \right\}.$$

In the same way as the derivation of formulation $(F_S^1)$ from the expected payoff $P^1(\pi,(g,\boldsymbol{y}))$, we have the following quadratic programming problem.

$$
\begin{aligned}
(F_S^4) \quad & \min_{g,y,\mu,\eta} \sum_{h\in H} f(h)\mu_h \\
s.t. \quad & \mu_h \geq \sum_{s\in S} g(s) \sum_{e\in E_l} \eta_{le}^{hs},\ l\in\Omega^h,\ h\in \boldsymbol{H}, \\
& \eta_{le}^{hs} \geq d_e^h \left( R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right),\ e\in E_l,\ s\in \boldsymbol{S},\ l\in\Omega^h,\ h\in\boldsymbol{H}, \\
& \eta_{le}^{hs} \geq \underline{d_e^h} \left( R_0^h - \sum_{e'\in E_l^e} \gamma_{e'}^{hs} y_{e'}^s \right),\ e\in E_l,\ s\in \boldsymbol{S},\ l\in\Omega^h,\ h\in\boldsymbol{H}, \\
& \sum_{e\in E} y_e^s \leq B_0^s,\ s\in\boldsymbol{S}, \\
& y_e^s \geq 0,\ e\in\boldsymbol{E},\ s\in\boldsymbol{S}, \\
& \sum_{s\in S} g(s) = 1, \\
& 0\leq g(s)\leq U(s),\ s\in\boldsymbol{S}.
\end{aligned}
$$

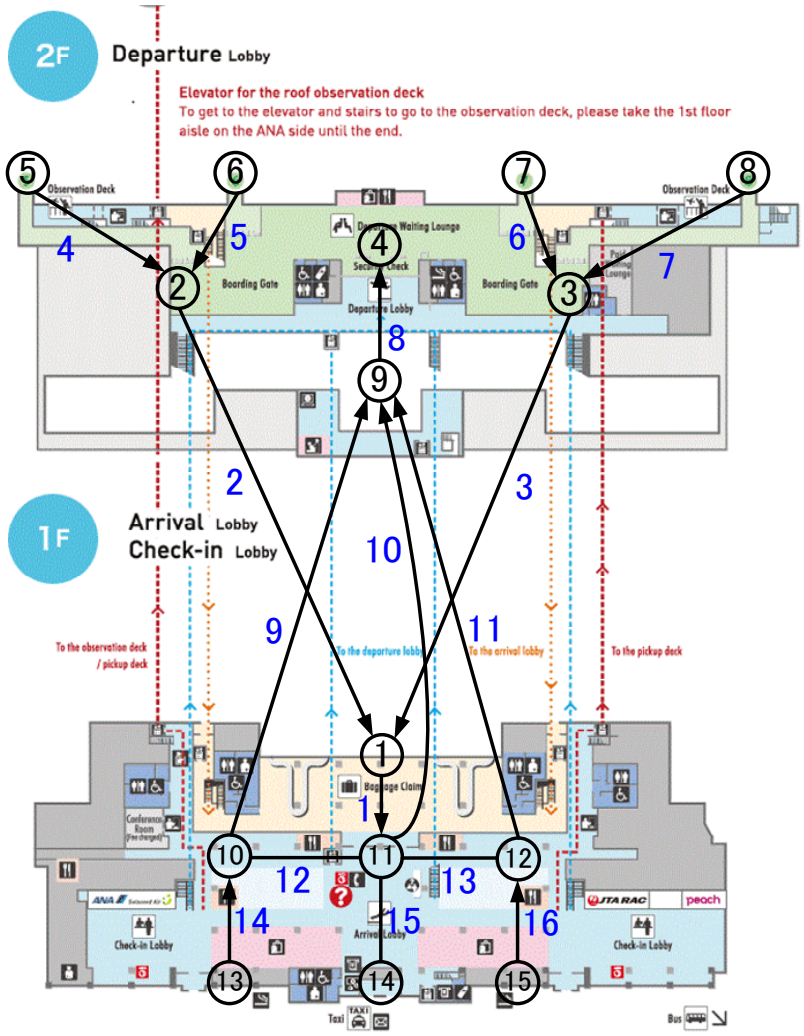
## 6. Numerical Examples

Here we take a security problem against smugglers and terrorists in an airport terminal and analyze an effective security plan within a fixed budget of security by formulation $(F_S^3)$ in Section 5. Let us describe our scenario setting:

(1) Security space and invasion routes: We take Ishigaki airport [20], which is shown by the floor plan of Figure 1, as a security space. The space is a network with 15 nodes and 16 undirected arcs. Some arcs have arrows which indicate the direction the attacker goes through there. An attacker of type $h=1$ is smugglers, who get off an airplane and go from boarding gates (Node 5, 6, 7, 8) through baggage claim (Node 1) to the airport central exit (Node 14). An attacker of type $h=2$ is terrorists. They try to make as much damage as possible while they enter terminal entrances (Node 13, 14, 15) the first floor, go up the second floor and finally lock others out of the departure waiting lounge (Node 4). The smugglers have 4 options of routes from boarding gates to the central exit. The terrorists have 9 invasion routes from the entrances to the departure waiting lounge. Table 1 shows their invasion routes in detail.

(2) Attackers and their damage rates: A set of attacker types is $\boldsymbol{H}=\{1,2\}$ and the appearance probability of them is assumed to be $f(1)=0.8$ and $f(2)=0.2$. Table 2 shows damage rates, $d_e^h$ and $\underline{d_e^h}$. The $h=1$-type attacker has $R_0^1=5$ smugglers and they have damage rate $d_e^1=10$ only after leaving the airport terminal. The $h=2$-type attacker is a terrorist group of $R_0^2=10$ members and they make damage on the way to their destination node 4, especially large damage in the arrival lobby ($d_e^2=15$), and the departure lobby and departure waiting lounge ($d_e^2=8$).
For negative expected number of surviving attackers, the damage rates $\underline{d_e^h}$ is set to be $\underline{d_e^1}=2$ at the exit for the smuggler, and $\underline{d_e^2}=1.5$ near the departure lobby and the departure waiting lounge, and $\underline{d_e^2}=3$ around the arrival lobby for the terrorists.

(3) Security: The defender has two teams of securities, $\boldsymbol{S}=\{1,2\}$. Security $s=1$ is a




*) Copyright is reserved to Ishigaki Air Terminal Co., Ltd.

Figure 1: A network of airport terminal

normal team, who handles venial accidents happened often in daily life at the airport. Security $s = 2$ is a special team, which is trained to handle serious accidents and incidents including terrorism. The security team $s = 2$ has an upper bound $U(2) = 0.3$ but the normal team has no upper bound or $U(1) = 1$.

(4) Power ratios: Table 3 shows the setting of $\gamma_e^{hs}$. The security team $s = 1$ has an ordinary capability of intercepting smugglers and its largest power ratio is $\gamma_e^{11} = 0.8$ for the baggage claim. But the team has little ability to defend the facility against terrorists because of its low ratios $\gamma_e^{21} = 0.1 \sim 0.3$. The security team $s = 2$ is deployed mainly against the terrorists. Its power ratio against the terrorists is high to be $\gamma_e^{22} = 1.6$ for closed spaces such as the passageway between the departure lobby and the departure waiting lounge but low to be $\gamma_e^{22} = 0.8$ for open spaces around the arrival lobby. Generally, the power ratio of the security $s = 2$ is about 2 to 3 times as large as that of the security $s = 1$ against the smugglers and about 5 to 10 times against the terrorists because of their equipment.

Here we analyze an optimal allocation of $B_0^1$ and $B_0^2$ under a limited security cost. Let us assume that the security $s = 2$ costs double as the security $s = 1$. Because $g(s)$ is the

Table 1: Invasion routes ($\Omega^1$ and $\Omega^2$)

| type | route # | nodes in the route | type | route # | nodes in the route |
|---|---|---|---|---|---|
| | 1 | 5,2,1,11,14 | | 1 | 13,10,9,4 |
| h=1 | 2 | 6,2,1,11,14 | | 2 | 13,10,11,9,4 |
| | 3 | 7,3,1,11,14 | | 3 | 13,10,11,12,9,4 |
| | 4 | 8,3,1,11,14 | h=2 | 4 | 14,11,9,4 |
| | | | | 5 | 14,11,10,9,4 |
| | | | | 6 | 14,11,12,9,4 |
| | | | | 7 | 15,12,9,4 |
| | | | | 8 | 15,12,11,9,4 |
| | | | | 9 | 15,12,11,10,9,4 |

Table 2: Damage rates ($d_e^h$ and $\underline{d_e^h}$)

| | h \ e | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $d_e^h$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 10 | 10 | 10 |
| | 2 | 15 | 10 | 10 | 5 | 5 | 5 | 5 | 8 | 8 | 8 | 8 | 15 | 15 | 15 | 15 | 15 |
| $\underline{d_e^h}$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| | 2 | 3 | 2 | 2 | 1 | 1 | 1 | 1 | 1.5 | 1.5 | 1.5 | 1.5 | 3 | 3 | 3 | 3 | 3 |

deployment frequency or adoption probability of security team $s$, $C \equiv g(1)B_0^1 + 2g(2)B_0^2$ indicates the mean security cost with a measure of the number of guard $s = 1$. While fixing the security cost $C$, we change $B_0^1$ to $1, 2, \cdots, C$ to investigate the expected damage (the game value) and optimal deployments of the security. Since the security $s = 2$ has rather larger effectiveness $\gamma_e^{hs}$ compared to $s = 1$, an optimal deployment frequency of $s = 2$ is $g(2) = 0.3$ in all cases. Therefore, $B_0^2$ is determined by $(C - 0.7 \times B_0^1)/(2 \times 0.3)$ for varying $B_0^1$.

We first analyze an optimal security deployment in the case of $C = 40$ and would verify the existence of the best configuration of staff numbers in security teams $s = 1$ and 2, or the best mix of $B_0^1$ and $B_0^2$. Our second analysis is about the best configuration of $B_0^1$ and $B_0^2$ for varying security cost $C$. In the last analysis, we figure out the effects of damage rates and power ratios on optimal security deployments. We use notation $(i, j)$ as an alternate of an arc $e$ with its terminal nodes $i$ and $j$.

### 6.1. Optimal deployment of guards for cost $C = 40$ (Example 1)

Figure 2 shows the change of the game values for $B_0^1$ and Figure 3 does the change of optimal deployment of security $s = 1$ and $s = 2$ with no curve for no deployment. First let us take

Table 3: Power ratios ($\gamma_e^{hs}$)

| (h,s) \ e | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (1,1) | 0.8 | 0.5 | 0.5 | 0 | 0 | 0 | 0 | 1 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 |
| (1,2) | 1 | 1 | 1.2 | 0 | 0 | 0 | 0 | 2 | 0.8 | 0.8 | 0.8 | 0.6 | 0.6 | 0.6 | 0.6 | 0.6 |
| (2,1) | 0.2 | 0.2 | 0.2 | 0 | 0 | 0 | 0 | 0.3 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 |
| (2,2) | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1.6 | 1 | 1 | 1 | 0.8 | 0.8 | 0.8 | 0.8 | 0.8 |

a look at Figure 2. The game value gradually decreases during $1 \leq B_0^1 \leq 4$ and reaches its minimum 46.5 at $B_0^1 = 4$. After the point, it increases in a monotonic manner and ends with a quick upturn to its maximum 78.3 at $B_0^1 = 40$ of no $s = 2$ security guards. The upturn teaches us the necessity of two security teams for a rational security of the airport terminal.

As for the security deployment, all of $s = 1$ security guards are positioned on arc $1 = (1, 11)$ but $s = 2$ guards are on arcs $12 = (10, 11)$, $13 = (11, 12)$, $14 = (13, 10)$, $15 = (14, 11)$ and $16 = (15, 12)$. The first and second arcs, 12 and 13, have the same number of guards deployed and the other three arcs also have the same number of deployment. However the former deployment and the latter one have different changing directions between their increasing and decreasing. The former increases for $B_0^1$ larger than 4 but decrease for $B_0^1 \geq 34$. The latter decreases for $B_0^1 \geq 4$ and becomes zero at $B_0^1 = 34$. Let us analyze these characteristics of equilibria in detail, noting that the effectiveness of each security team $s$ depends on not only the power ratio $\gamma_e^{hs}$ but also the total number $B_0^s$ and the deployment frequency $g(s)$.

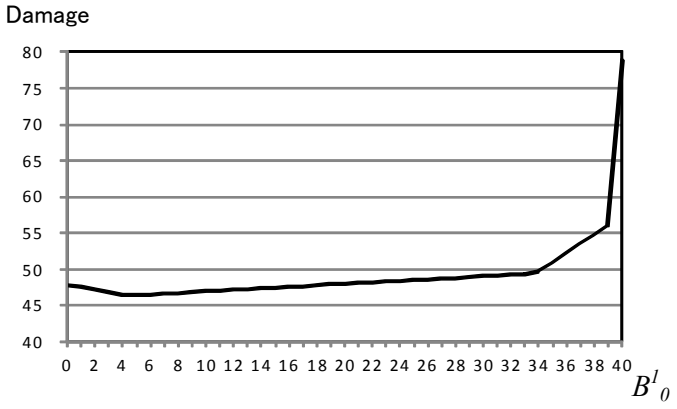



Figure 2: The expected damage for $B_0^1$

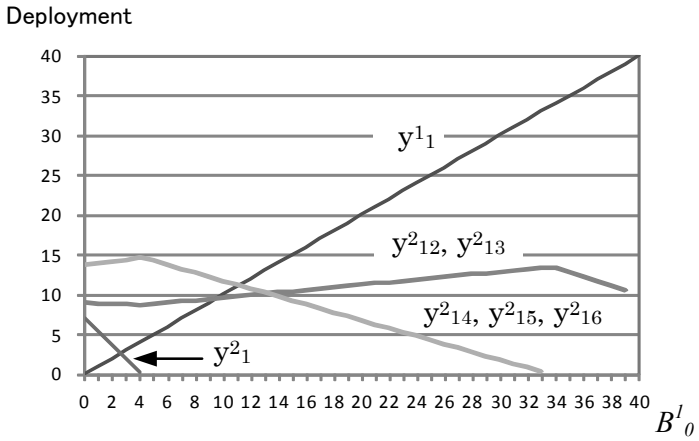



Figure 3: Optimal deployment of guards for $B_0^1$

(1) Case of $B_0^1 \leq 4$:
The security team $s = 2$ is so efficient that it is used up to the upper bound of frequency $g(s) = U(s) = 0.3$ and the security team $s = 1$ is applied with the frequency $g(s) = 0.7$.

Since $s = 1$ guards are effective against the smugglers ($h = 1$), all members of $B_0^1$ are deployed to intercept the smugglers, as $y_1^1$ shows. They are concentrated on arc $1 = (1, 11)$ between the baggage claim and the arrival lobby, which has the highest ratio $\gamma_1^{11} = 0.8$, because the smugglers give damage after leaving the terminal and all their routes pass through the baggage claim.

The terrorists ($h = 2$) give more damage to the facility than the smugglers ($h = 1$) but their incident probability $f(2) = 0.2$ is one-fourth as much as that of the smugglers. Therefore, the smugglers have more influence on the average damage than the terrorists. Therefore, in the case of small $B_0^1$, as $y_1^2$ shows, the security team $s = 2$ supports the $s = 1$ team to inspect the smugglers on arc $1 = (1, 11)$ by a portion of $B_0^2$. As $B_0^1$ increases, the support of the $s = 2$ security, $y_1^2$, becomes weaker on arc 1 and it is cut off at $B_0^1 = 4$. For $B_0^1$ larger than 4, the $s = 1$ team is used to inspect the smugglers and the $s = 2$ team is to intercept the terrorists. The usage of each security team is specialized to handle a respective type of attacker.

Besides the subsidiary inspection mission against the smugglers on arc $1 = (1, 11)$ stated above, the security team $s = 2$ has a main mission to intercept the terrorists on arcs $12 = (10, 11)$, $13 = (11, 12)$, $14 = (13, 10)$, $15 = (14, 11)$ and $16 = (15, 12)$. In the case of $B_0^1 \leq 4$, $y_{15}^2$ becomes larger because arc 15 is a key arc to cover the movement of both the smugglers and the terrorists. Against the terrorists, $y_e^2$ on arcs $e = 14$ and $e = 16$ at entrance also increases. Corresponding to the increase, the deployment on arcs 12 and 13 is depressed a little.

As seen above, the security resources are concentrated on the arc $1 = (1, 11)$ because of its high effectiveness against the smuggler $h = 1$. This security strategy makes $\mu_1$ in problem $(F_S^3)$ nonpositive, which indicates a perfect interdiction of the smugglers on all their routes.

By the discussion so far, we summarize the characteristics of optimal security plan as follows. Security $s = 1$ concentrates his guards near the baggage claim to manage the interdiction of the smugglers, that is, the concentration of deployment of $s = 1$ guards at the baggage claim. Security $s = 2$ defends mainly the arrival lobby and entrances against the terrorists. The most effective allocation of guards is given by $B_0^1 = 4$ and $B_0^2 = 62$.

As for the game value, security $s = 1$ has a little more effective interdiction against the smugglers than security $s = 2$ because of its higher upper bound $g(1) = 0.7$. That is why the expected damage slightly decreases as $B_0^1$ becomes larger and reaches its minimum 46.5 at $B_0^1 = 4$.

(2) Case of $4 < B_0^1 < 34$:

The frequency of deployment $g(1) = 0.7$ still works for security $s = 1$, which is a main defender on arc 1 against the smugglers. Compared with the first case, a security plan changes a little bit for the terrorist interception. The numbers of $s = 2$ guards $y_e^2$ deployed on two groups of arcs 12 and 13, and arcs 14, 15 and 16 show different changes. As $B_0^1$ becomes larger and the number of $s = 2$ guards becomes smaller, the deployment on the former arcs is getting stronger but that on the latter arcs weaker. Only the former deployment is sustained for $B_0^1$ larger than 34.

We might explain the change of the deployment against the terrorists, as follows. Considering the terrorists cause damage everywhere on the way to their destination, the security has to wear them out as quickly as possible after their invasion on arcs with large damage rate $d_e^h$. Arc $8 = (9, 4)$ has the largest power ratio 1.6, and arcs $9 = (10, 9)$, $10 = (11, 9)$ and $11 = (12, 9)$ have the second largest one 1.0. But they are not so im-

portant as arcs $e = 12, 13, 14, 15, 16$ with large damage rates $d_e^2 = 15$ for the security deployment to lower the damage by the terrorists. The five arcs are located in the arrival lobby and are important for the earlier interception of the terrorists. Among the arcs, the first two arcs 12 and 13 are involved in four invasion routes and occupy a good position for interception. By these reasons, the $s = 2$ security deployment is more focused on the first two arcs as $B_0^1(B_0^2)$ is getting larger(smaller).

We explain the change of the game value as follows. As seen above, the increment of $B_0^1$ is used just against the smugglers and its effective rate per $s = 1$ guard is steady. On the other hand, the decrement of $B_0^2$ drives the $s = 2$ security deployment to change from on five arcs to on two arcs, as explained above, and the rate of the damage increment by the terrorists per $s = 2$ guard, which is given by $\mu_2$ in problem $(F_S^3)$, overcomes the first effective rate of the $s = 1$ security. As a result, the damage increases as $B_0^1$ becomes larger.

(3) Case of $34 \leq B_0^1$:

In this case, the $s = 2$ guards are positioned only on arcs 12 and 13, and the number of deployed guards becomes smaller according to the decrease of $B_0^2$. The increase of $B_0^1$ does not change the concentration strategy of $B_0^1$ guards on arc 1 to handle the smugglers because the $s = 1$ team has no effect on the interception of the terrorists.

The $s = 2$ guards is not enough to intercept the terrorists in terms of their number $B_0^2$ and their usage frequency $g(2) = 0.3$, and then the damage rate increases more than the previous case of $4 < B_0^1 < 34$. In the extreme case of $B_0^1 = C = 20$ of using no $s = 2$ guard, the security loses any control on the terrorist and the damage jumps up to 78.8.

Let us summarize the characteristics of optimal security strategies. The security team $s = 1$ is deployed just against the smuggler in all cases because of no effect on the terrorists. The security can effectively control the invasion of the smugglers by the interception on any arc with large power ratio on their routes. The security team $s = 2$ complements the $s = 1$ team for the defense against the smugglers in the case of smaller $B_0^1$ but it is specialized for the defense against the terrorists in the case of larger $B_0^1$. For an optimal deployment, the $s = 2$ security deliberate on the damage rate of the terrorists, the power ratio and the quick interception at earlier time against the terrorists. In the case of large $B_0^1$, security $s = 1$ focuses on the defense against the smugglers without any care of the terrorists because of its small appearance frequency $f(2) = 0.2$. An effective security by two teams lies in the specialization that each team of guards is focused on its effective defense against one type of invaders taking account of its power ratio and damage rate of arcs on invaders' routes, and interception time.

We investigate optimal defense policies in other cases of security cost $C$ from 5 through 75 and make sure of optimal security strategies as in the case $C = 40$ and the existence of the best configuration of staff numbers in two security teams.

### 6.2. The minimum damage and the best security configuration for security cost

Figure 4 and 5 show the change of the minimum damage and the optimal allocation of $B_0^1$ for varying security cost $C$ from 5 through 75. A maximum allocation of $B_0^1$ is equal to $C$, which is indicated by a diagonal in Figure 5. From these figures, we can figure out the best configuration of the numbers of guards in two security teams.

The curve of the minimum damage monotonically decreases approximately separated by two regions with different decreasing rates. The deployment of the security team $s = 2$ is focused on arcs 12 and 13 in the case of small security cost, but in the case of large cost, the deployment of additional guards is expanded up to arcs 14, 15 and 16 of having lower

effectiveness of interception, as shown in Example 1. Therefore, the decreasing rate of the damage hebetates in the case of high security cost.

The larger the security cost becomes, more guards are allocated to the team $s = 2$ in the best configuration because the $s = 2$ guards are more effective against both types of attackers than the $s = 1$ guard. The tendency is restricted by the upper bound $U(2) = 0.3$ and the cost. Anyway, in the case of $C = 5$, an optimal security consists of just the $s = 1$ guards.

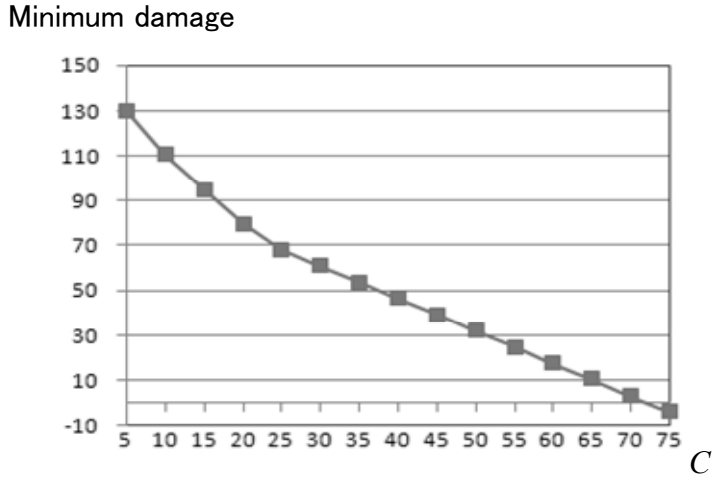



Figure 4: Minimum damage for security cost

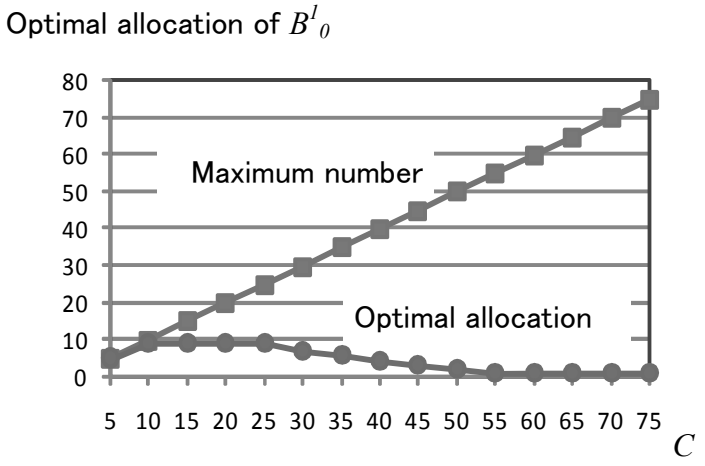



Figure 5: Optimal allocation of $B_0^1$ for security cost

### 6.3. Effects of damage rates and power ratios on rational security strategy

Here we evaluate the effects of damage rates $d_{15}^2$ and $\overline{d_{15}^2}$ on optimal security strategy. We also do an analysis on power ratio $\gamma_{15}^{22}$. A basic case is $B_0^1 = 30$ and $B_0^2 = 31.7$ with security cost $C = 40$ with the same other parameters as set in the beginning of Section 6. First let us review that in the basic case, the expected damage is 49.1 and the optimal security deployment is given by $y_1^1 = 30$, $y_{12}^2 = y_{13}^2 = 13.0$ and $y_{14}^2 = y_{15}^2 = y_{16}^2 = 1.9$.

(1) Effects of the damage rates of arc 15

Here we change damage rates $d_{15}^2$ and $\underline{d_{15}^2}$ to 20 and 5 from their original numbers 15 and 3, respectively, under the situation that the central arrival lobby is more crowded and more dangerous to terrors. In this case, the expected damage increases to 51.3 and the optimal deployment of $s = 2$ security changes to $y_{12}^2 = y_{13}^2 = 13.5$, $y_{14}^2 = y_{16}^2 = 0.2$ and $y_{15}^2 = 4.3$ remaining the $s = 1$ security deployment $y_1^1 = 30$ unchanged.
Against the clever terrorists who try to attack weaker points of security or damageable points of facility, the security enforces the arc $15 = (14, 11)$ by increasing the deployment there.

(2) Effects of the power ratio of arc 15
Here we increase power ratio $\gamma_{15}^{22}$ to 1.2 from its original number 0.8 assuming that the central arrival lobby is so a closer area that the defensive efforts would be more effective that other lobbies. In this case, the expected damage decreases to 48.6 and the original optimal deployment changes a little bit to $y_{12}^2 = y_{13}^2 = 12.9$, $y_{14}^2 = y_{16}^2 = 2.3$ and $y_{15}^2 = 1.5$ with no change of $y_1^1$.
The security side wants to increase the number of guards on arc 15 because of higher effectiveness of defense there on the attrition of the terrorists. However the terrorists hesitate to go through the arc and tend to take his way to other arcs. Due to the rational estimation on the terrorist behavior, the security practically decreases $y_{15}^2$ while increasing $y_{14}^2$ and $y_{16}^2$ on complementary arcs 14 and 15. The more effectiveness of defense on arcs makes the security put less defensive efforts there but more efforts in other places in order to construct a faultless defense against every invasion route in a complementary manner.

## 7. Conclusions

This paper deals with a security game model with invaders and security teams. In this model, a geographical space is represented by a network and then we can explicitly take account of invasion routes for several types of invaders. At the same time, we can definitely specify a deployment of guards belonging to multiple security teams on the network. Furthermore, we incorporate attrition occurred on players in our model. We adopt a Stackelberg game, which has been often taken in many researches on the security game with one player's superiority on information acquisition. There was no paper on such a security game model in the past. As our zero-sum payoff of the game, we try several functions to adjust to practical situations. We apply our model to a small-size but actual airport protection and notice some realistic properties of optimal security plans and recognize a lesson that there exist an optimal combination of multiple security systems and an optimal allocation of guards among the systems. If the security team is thought to be a preparation for rarely-happened incidents, an analyst is in charge of verifying the cost-performance of security to a decision maker of organizing the team. We showed some analyses on the cost-performance by some examples.

Because we use many parameters in this model, we first have to evaluate and set proper values on the parameters for realistic security systems. When we consider a security system larger than our example in this paper, the security network would be too complicated to set invasion routes manually and we would need an algorithm to make the routes automatically by graph-network theory. We mentioned a trial to improve the payoff function above. A nonzero-sum payoff would be more flexible than ours. But for the nonzero-sum game, it would be more difficult to derive equilibrium points, as many papers showed. The comments described above could be our future topics and our model has many points to be improved

further. Anyway, the most important necessity to upgrade the applicability of our model to practical security is an incorporation of time space such as the traveling time of invaders and the deployment time of guards. It would be comparatively easy on our proposed network, we think.

## References


[1] N. Agmon, S. Kraus, and G.A. Kaminka: Multi-robot perimeter patrol in adversarial settings. *IEEE International Conference on Robotics and Automation*, (2008), 2339–2345.

[2] N. Agmon, V. Sadov, G.A. Kaminka, and S. Kraus: The impact of adversarial knowledge on adversarial planning in perimeter patrol. *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multi-Agent Systems*, **1** (2008), 55–62.

[3] N. Basilico, N. Gatti, and F. Amigoni: Patrolling security games: Definition and algorithms for solving large instances with single patroller and single intruder. *Artificial Intelligence*, **284** (2012), 78–123.

[4] M. Baykal-Gursoy, Z. Duan, H.V. Poor, and A. Garnaev: Infrastructure security game. *European Journal of Operational Research*, **239** (2014), 469–478.

[5] M. Bell, U. Kanturska, J. Schmocker, and A. Fonzone: Attacker-defender models and road network vulnerability. *Philosophical Transactions of the Royal Society*, **366** (2008), 1893–1906.

[6] J.M. Chaiken and R.C. Larson: Methods for allocating urban emergency units: A survey. *Management Science*, **19** (1971), 110–130.

[7] F. Fang, A.X. Jiang, and M. Tambe: Optimal patrol strategy for protecting moving targets with multiple mobile resources. *Proceedings of the 2013 International Conference on Autonomous Agents and Multi-Agent Systems*, (2013), 957–964.

[8] G. Feichtinger: A differential games solution to a model of competition between a thief and the police. *Management Science*, **29** (1983), 686–699.

[9] L.R. Ford and D.R. Fulkerson: *Flows in Networks* (Princeton University Press, Princeton, 1962), 142–151.

[10] A. Garnaev, M. Baykal-Gursoy, and H.V. Poor: Incorporating attack-type uncertainty into network protection. *IEEE Transactions on Information Forensics and Security*, **9** (2014), 1278–1287.

[11] K. Hausken: Defense and attack of complex and dependent systems. *Reliability Engineering and System Safety*, **95** (2010), 29–42.

[12] K. Hausken: Protecting complex infrastructures against multiple strategic attackers. *International Journal of Systems Science*, **42** (2011), 11–29.

[13] J. Herrmann (ed.): *Handbook of Operations Research for Homeland Security* (Springer Science & Business Media, 2012).

[14] R. Hohzaki: On several models of security games taking accout of networks. *Communications of the Operations Research Society of Japan*, **61** (2016), 226–233 (in Japanese).

[15] R. Hohzaki and T. Chiba: An attrition game on an acyclic network. *Journal of the Operational Research Society*, **66** (2015), 979–992.

[16] R. Hohzaki and T. Higashio: An attrition game on a network ruled by Lanchester's square law. *Journal of the Operational Research Society*, **67** (2016), 691–707.

[17] R. Hohzaki, S. Morita, and Y. Terashima: A patrol problem in a building by search theory. *Proceedings of 2013 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, (2013), 104–111.

[18] R. Hohzaki and K. Sunaga: Attrition game models with asymmetric information on a network. *Journal of the Operations Research Society of Japan*, **59** (2016), 195–217.

[19] R. Isaacs: *Differential Games* (John Wiley & Son, New York, 1965), 336–337.

[20] Ishigaki airport: Homepage, `http://www.ishigaki-airport.co.jp/facility.html`.

[21] H. Iwashita, K. Ohori, and H. Anai: Optimization of security resource based on game theory. *Abstracts of the 2015 Fall National Conference of Operations Research Society of Japan*, (2015), 4–5 (in Japanese).

[22] M. Jain, J. Tsai, J. Pita, C. Kiekintveld, S. Rathi, M. Tambe, and F. Ordonez: Software assistants for randomized patrol planning for the LAX airport police and the federal air marshal service. *Interfaces*, **40** (2010), 267-290.

[23] A.X. Jiang, Z. Yin, M.P. Johnson, M. Tambe, C. Kiekintveld, K. Leyton-Brown, and T. Sandholm: Towards optimal patrol strategies for fare inspection in transit systems. *Proceedings of AAAI Spring Symposium: Game Theory for Security, Sustainability, and Health*, (2012).

[24] M. Kodialam and T.V. Lakshman: Detecting network intrusions via sampling: A game theoretical approach. *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications (IEEE INFOCOM)*, **3** (2003), 1880–1889.

[25] B.O. Koopman: Search and screening. Operations Evaluation Group, Office of the Chief on Naval Operations, Navy Department (1946).

[26] F.W. Lanchester: *Aircraft in Warfare: The Dawn of the Fourth Arm* (Constable and Company Lt., London, 1916).

[27] S. Morita, R. Hohzaki, and Y. Hatakeyama: A patrol routing problem using mathematical programming. *Transactions on Mathematical Modeling and its Applications of the Information Processing Society of Japan*, **4** (2011), 19–35 (in Japanese).

[28] D.G. Olson and G.P. Wright: Models for allocating police preventive patrol effort. *Operational Research Quarterly*, **26** (1975), 703–715.

[29] P. Paruchuri, J.P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus: Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games. *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multi-Agent Systems*, **2** (2008), 895-902.

[30] F. Perea and J. Puerto: Revisiting a game theoretic framework for the robust railway network design against intentional attacks. *European Journal of Operational Research*, **226** (2013), 286–292.

[31] J. Pita, M. Jain, J. Marecki, F. Ordonez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus: Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport. *Proceedings of the 7th International Joint Conference on Autonomous Agents and Multi-Agent Systems*, (2008), 125–132.

[32] J. Pita, M. Jain, F. Ordonez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus: Using game theory for Los Angeles airport security. *AI Magazine*, **30** (2009), 43–57.

[33] J. Pita, M. Jain, M. Tambe, F. Ordenez, and S. Kraus: Robust solutions to Stackelberg games: Addressing bounded rationality and limited observations in human cognition.

*Artificial Intelligence*, **174** (2010), 1142–1171.

[34] J. Salmeron, R.K. Wood, and R. Baldick: Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems*, **19** (2004), 905–912.

[35] M.P. Scaparra and R.L. Church: A bilevel mixed integer program for critical infrastructure protection planning. *Computers & Operations Research*, **35** (2008), 1905–1923.

[36] E. Shieh, M. Jain, A.X. Jiang, and M. Tambe: Efficiently solving joint activity based security games. *Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence*, (2013), 346–352.

[37] A. Takizawa, M. Inoue, and N. Katoh: An emergency evacuation planning model using the universally quickest flow. *The Review of Socionetwork Strategies*, **6** (2012), 15–28.

[38] M. Tambe: *Security and Game Theory-Algorithms, Deployed Systems, Lessons Learned* (Cambridge University Press, New York, 2012).

[39] J. Tsai, Z. Yin, J.Y. Kwak, D. Kempe, C. Kiekintveld, and M. Tambe: Urban security: Game-theoretic resource allocation in networked physical domains. *Proceedings of the 24th AAAI Conference on Artificial Intelligence*, (2010), 881–886.

[40] O. Vanek, B. Bosansky, M. Jakob, and M. Pechoucek: Transiting areas patrolled by a mobile adversary. *2010 IEEE Symposium on Computational Intelligence and Games (CIG)*, (2010), 9–16.

[41] A.R. Washburn: TPZS applications: Blotto games. *Wiley Encyclopedia of Operations Research and Management Science*, **7** (John Wiley & Sons, 2011), 5504–5511.

[42] R. Yang, C. Kiekintveld, F. Ordonez, M. Tambe, and R. John: Improving resource allocation strategies against human adversaries in security games: An extended study. *Artificial Intelligence*, **195** (2013), 440–469.

[43] Z. Yin, A.X. Jiang, M. Tambe, C. Kiekintveld, K. Leyton-Brown, T. Sandholm, and J.P. Sullivan: TRUSTS: Scheduling randomized patrols for fare inspection in transit systems using game theory. *AI Magazine*, **33** (2012), 59–72.

Ryusuke Hohzaki
Department of Computer Science
National Defense Academy
1-10-20 Hashirimizu
Yokosuka 239-8686, Japan
E-mail: hozaki@nda.ac.jp