An Ambiguity Aversion Framework of Security Games under Ambiguities

Wenjun Ma[1], **Xudong Luo**[2], **and Weiru Liu**[1]
[1]School of Electronics, Electrical Engineering and Computer Science,
Queen's University Belfast, Belfast, UK, BT7 1NN
$\{w.ma, w.liu\}$@qub.ac.uk
[2] Institute of Logic and Cognition, Sun Yat-sen University, Guangzhou, China, 510275
luoxd3@mail.sysu.edu.cn

Abstract

Security is a critical concern around the world. Since resources for security are always limited, lots of interest have arisen in using game theory to handle security resource allocation problems. However, most of the existing work does not address adequately how a defender chooses his optimal strategy in a game with absent, inaccurate, uncertain, and even ambiguous strategy profiles' payoffs. To address this issue, we propose a general framework of security games under ambiguities based on Dempster-Shafer theory and the ambiguity aversion principle of minimax regret. Then, we reveal some properties of this framework. Also, we present two methods to reduce the influence of complete ignorance. Our investigation shows that this new framework is better in handling security resource allocation problems under ambiguities.

1 Introduction

Nowadays, protecting people and critical assets against potential attacks has become a critical problem for public security around the world [Tambe, 2011]. It is impossible to provide surveillance on all the targets of security. Thus, it is an increasing concern about how to allocate security resources. Essentially, addressing this concern requires a strategy of allocating security sources (e.g., security team or defender) based on the understanding of how terrorists (the attacker) usually plan and act according to their knowledge of security capabilities. In the literature, most of the existing work deals with this problem in Stackelberg's game framework (a specific kind of game in game theory) [Pita *et al.*, 2009; Tambe, 2011]. That is, a defender commits to a strategy first and an attacker makes his decision based on the defender's commitment. The typical solution concept in these games is Strong Stackelberg Equilibrium (SSE), which concentrates on determining the defender's optimal mixed strategy based on two assumptions: (i) the attacker knows this strategy and responds optimally; and (ii) both players have point-valued payoffs for each *pure strategy profile* (a complete list of pure strategies, one for each player in the game).

However, in real life, a human attacker usually acts on partial information of a defender's strategies and the attacker's rationality is bounded [Tambe, 2011; Yang *et al.*, 2012]. Moreover, Korzhyk *et al.* [2011] suggests that the Nash Equilibrium (NE) strategy should be applied instead of SSE when a defender is unclear about an attacker's knowledge of surveillance. Furthermore, the assumption of point-valued payoffs is also unrealistic because the payoff of each pure strategy profile, which is based on experts analysis, historical data, and airport managers' judgements, is often ambiguous because of time pressure, lack of data, random events, reliability of information sources, and so on. In particular, the payoff of a pure strategy profile often has to face two types of ambiguity: (i) the value of a payoff is ambiguous: (a) absent, (b) interval-valued, and (c) of multiple possibilities; (ii) the strategy profile that relates to a given payoff is ambiguous.

Let us consider a scenario in an airport area, which covers the following five targets: Shopping Area (SA), Prayer Room (PR), Special Location (SL), VIP Lounges (VL), and Hotel (H). Now an airport manager tries to assign a security team to cover one of these five targets, and an attacker will choose one to assault. So, there are two consequences for the interaction: the security team succeeds in protecting a target or the attacker succeeds in assaulting a target. And the payoffs of an interaction for the defender might be ambiguous. (i) The value of payoff is ambiguous: (a) *absent*: because the special location in an airport is unique, it is hard to estimate the value, such as the Butterfly Garden in Singapore Changi Airport; (b) *interval-valued*: the payoff of protecting a shopping area mainly depends on the amounts of customers, which is indeterministic in a period; and (c) *ambiguity lottery*: for instance, the prayer room, after knowing that the assessment expert is a religionist, the airport manager would not completely trust the expert's suggestion, e.g., a reliability of 80%. Thus, the manager is uncertain about the payoff of Prayer Room with 20%. (ii) The pure strategy profile that relates to a given payoff is ambiguous: suppose the more people a location may have, the higher the payoff. Since the hotel usually is close to the VIP lounge, it may be easier to estimate roughly a combined total number of people in both places, but it is difficult to estimate a total number of people in each place. So, sometimes the manager does not know the payoff of these two targets separately. Given these two types of ambiguity, our task in this paper is to determine the defender's optimal strategy.

More specifically, based on Dempster-Shafer (D-S) theory

[Shafer, 1976], we first use the ambiguity aversion principle of minimax regret [Ma *et al.*, 2013] to obtain the preference degree of a given player for the subsets of pure strategy profiles. Then, we consider the distance of each subset of profiles' preference degree to the worst preference degree to set the relative payoffs of this player. Thus, according to whether some payoffs are absent, we introduce two methods to calculate mass values, which indicate the possibilities of a subset of pure strategy profiles containing the best outcome for the given player. Moreover, we deploy the idea behind the ambiguity aversion principle of minimax regret to obtain the player's belief degree of a belief interval for each pure strategy profile. Finally, from the belief degrees of each player, we can derive the defender's optimal strategy directly.

This paper advances the state of the art on the topic of security resources allocation in the following aspects. (i) We identify two types of ambiguity in security resources allocation: ambiguous payoffs and ambiguous strategy profile. (ii) We propose an ambiguity aversion framework to determine the optimal strategy for a defender in security games under ambiguities. (iii) Our framework can consider the correctness of point-value security game models under ambiguities. (iv) We show the relationship between the payoffs boundary and the risk attitude of a player in security games under ambiguities. And (v) we present two methods to reduce complete ignorance in security games under ambiguities.

The rest of this paper is organized as follows. Section 2 recaps D-S theory and relevant definitions. Section 3 formally defines security games under ambiguities. Section 4 develops an ambiguity aversion framework to handle security games under ambiguities. Sections 5 discusses some properties of our framework. Section 6 handles the influence of complete ignorance. Section 7 discusses the related work. Finally, Section 8 concludes the paper with future work.

2 Preliminaries

This section recaps a decision method based on D-S theory [Shafer, 1976], which extends the probability theory as follow.

Definition 1. *Let Θ be a set of exhaustive and mutually exclusive elements, called a frame of discernment (or simply a frame). Function $m: 2^{\Theta} \rightarrow [0,1]$ is a mass function if $m(\emptyset) = 0$ and $\sum_{A \subseteq \Theta} m(A) = 1$. With respect to m, belief function (Bel) and plausibility function (Pl) are defined as follows:*

$$Bel(A) = \sum_{B \subseteq A} m(B), \tag{1}$$

$$Pl(A) = \sum_{B \cap A \neq \phi} m(B). \tag{2}$$

The following is a normalized version of the generalized Hartley measure for nonspecificity [Dubois and Prade, 1985].

Definition 2. *Let m be a mass function over a frame of discernment Θ and $|A|$ be the cardinality of set A. Then the ambiguity degree of m, denoted as $\delta : m \rightarrow [0,1]$, is given by:*

$$\delta = \frac{\sum_{A \subseteq \Theta} m(A) \log_2 |A|}{\log_2 |\Theta|}. \tag{3}$$

Hence, we can define an ambiguity decision problem, which is a 4-tuple (C, S, U, M) as follow:

- $C = \{c_1, \ldots, c_n\}$ is the set of all choices, such as all possible actions;
- $S = \{s_1, \ldots, s_m\}$ is the set of consequences caused by these choices;
- $F = \{f_c \mid c \in C, \forall s \in S, f_c(s) \in \Re\}$, i.e., the utility of consequence $s \in S$ that is caused by selecting choice $c \in C$ is $f_c(s) \in \Re$ (a real number set);
- $M = \{m_c \mid c \in C\}$, i.e., the decision maker's uncertainty about the utility that choice c could cause (due to multiple possible consequences) is represented by mass function m_c over the frame of discernment $\Theta = \{h_1, \ldots, h_n\}$, where $h_i \in \Re$ and for any $f_c(s)$, $f_c(s) \in \Theta$.

Thus, the point-valued expected utility function [Von Neumann and Morgenstern, 1944] can be extended to an expected utility interval [Strat, 1990]:

Definition 3. *For choice c_1 specified by mass function m_{c_1} over $\Theta = \{h_1, ..., h_n\}$, its expected utility interval is $EUI(c_1) = [\underline{E}(c_1), \overline{E}(c_1)]$, where*

$$\underline{E}(c_1) = \sum_{A \subseteq \Theta} m_{c_1}(A) \min\{h_i \mid h_i \in A\}, \tag{4}$$

$$\overline{E}(c_1) = \sum_{A \subseteq \Theta} m_{c_1}(A) \max\{h_i \mid h_i \in A\}. \tag{5}$$

The following is a decision rule for expected utility intervals, i.e., the ambiguity aversion principle of minimax regret, which is presented in [Ma *et al.*, 2013]:

Definition 4. *Let m be a mass function over $\Theta = \{h_1, ..., h_n\}$, $EUI(x) = [\underline{E}(x), \overline{E}(x)]$ be the expected utility interval of choice $x \in C$, and $\delta(x)$ be the ambiguity degree of m_x. Then the ambiguity-aversion maximum regret of choice c_i against choice c_j, denoted as $\Re_{c_i}^{c_j} \in \Re$, is given by:*

$$\Re_{c_i}^{c_j} = \varepsilon(c_j) - \underline{E}(c_i), \tag{6}$$

where $\varepsilon(c_j) = \overline{E}(c_j) - \delta(c_j)(\overline{E}(c_j) - \underline{E}(c_j))$. And the strict preference ordering $\succ$ over these two choices c_i and c_j is defined as follow:

$$c_i \succ c_j \Leftrightarrow \Re_{c_i}^{c_j} < \Re_{c_j}^{c_i}. \tag{7}$$

This ordering states that choice c_i is strictly preferred than c_j, if the ambiguity-aversion maximum regret of c_i is smaller than that of c_j. Also, it is easy to prove that $\underline{E}(c) \leq \varepsilon(c) \leq \overline{E}(c)$, and $\varepsilon(c)$ means that for the reason of ambiguity aversion, the decision maker will reduce his upper expected utility (but still not lower than $\underline{E}(c)$) for a given choice based on the ambiguity degree δ of m_c.

Moreover, we can prove easily that with the binary relation $\sim$ (i.e., $x \sim y$ if $x \not\succ y$ and $y \not\succ x$), we can compare any two choices properly. Finally, in game theory, the problem of selecting the optimal strategy for a given player with respect to the strategies selected by other players can be considered as a

decision problem for selecting the best choice under the condition that the strategies (choices) of other players are given. So, when the payoff functions in game theory are represented by mass functions, we can find the optimal strategy by Definitions 3 and 4.

3 Security Games under Ambiguities

This section defines security games under ambiguities.[1]

Based on the airport scenario in Section 1, we can construct a payoff matrix of a security game as shown in Table 1, in which the defender is the row player and the attacker is the column player. Moreover, their payoffs are listed in the cells as "a; b", where a for the defender's payoff and b for the attacker's. Consider the second row in Table 1. When the pure strategy profile is (*PR*, *SA*),[2] which means the defender fails to protect *SA*, the payoff of the defender is negative (e.g., $[-7,-3]$) and that of the attacker is positive (e.g., 5). Since the evaluation of the shopping area is inaccurate for the defender, an interval value is used for his payoffs (e.g., $[-7,-3]$). Similarly, when the profile is (*PR*, *PR*), the defender succeeded in protecting the prayer room. As the evaluation of the prayer room is based on an expert's suggestion, $m(c) = 0.8$ means the reliability for the expert's evaluation c is 80% and $m(d) = 0.2$ means the expert's suggestion is unreliable for the defender with 20%. Moreover, when the profile is (*PR*, *SL*), $null$ means that the defender is completely unknown for the value he might lose if he fails to protect the special location. Finally, the defender cannot distinguish the payoffs of (*PR*, *VL*) and (*PR*, *H*), but just knows that the payoff of these two compound strategy profiles is -8. Formally, we have:

Definition 5. *A security game under ambiguities, denoted as G, is a 6-tuple of $(N, A, \Psi, \Theta, M, U)$, where:*

- $N = \{1, 2\}$ *is the set of players, where* 1 *stands for the defender and* 2 *stands for the attacker.*
- $A = \{A_i \mid i = 1, 2\}$*, where A_i is the finite set of all pure strategies of player i.*[3]
- $\Psi = \{(a_k, b_l) \mid a_k \in A_1 \wedge b_l \in A_2\}$ *is the set of all pure strategy profiles.*
- $\Theta = \{\Theta_i \mid \Theta_i = \Theta_i^+ \cup \Theta_i^-, i = 1, 2\}$*, where Θ_i^+ is a finite positive number set and Θ_i^- is a finite negative number set.*
- $M = \{m_{i,X} \mid i = 1, 2,\ X \subseteq \Psi\}$*, where $m_{i,X}$ is the mass function over a frame of discernment Θ_i^+ or Θ_i^-.*
- $U = \{u_i(X) \mid i = 1, 2,\ X \subseteq \Psi\}$*, where $u_i(X)$ is the payoff function $u_i : 2^\Psi \to M$.*

Moreover, for any $X \subseteq \Psi \wedge |X| > 1$, if $\exists u_i(Y)_{Y \subset X} \wedge m_{i,Y}(B) > 0 \wedge B \subset \Theta_i^+$ or $B \subset \Theta_i^-$, then $m_{i,X}(\Theta_i^-) = 1$.

[1] In this paper, we only consider simple security games that face one type of attacker in order to discover more intrinsic characteristics of security games under ambiguities.

[2] The defender's strategy is *PR* (covering the Prayer Room) and the attacker's strategy is SA (attacking the Shopping Area).

[3] Assigning a security team covering a specific place can be regards as a pure strategy in the security game.

Table 1: Airport security game
Here a=$\{-8, -7\}$, b=$\{-9, \ldots, 0\}$, c=$\{5, 6\}$, d=$\{0, \ldots, 9\}$.

	SA	PR	SL	VL | H
SA	$[2, 6]$; -7	$\{m(a) = 0.8,$ $m(b) = 0.2\}$; 3	$null$; 2	-8; 7
PR	*[-7,-3]; 5*	*{m(c)=0.8, m(d)=0.2}; -5*	$null$; 2	*-8; 7*
SL	$[-7, -3]$; 5	$\{m(a) = 0.8,$ $m(b) = 0.2\}$; 3	$null$; -4	-8; 7
VL	$[-7, -3]$; 5	$\{m(a) = 0.8,$ $m(b) = 0.2\}$; 3	$null$; 2	{(VL,VL);(H,H)}:7; -9
H	$[-7, -3]$; 5	$\{m(a) = 0.8,$ $m(b) = 0.2\}$; 3	$null$; 2	{(VL,H);(H,VL)}:-8; 7

The same as traditional game theory, for each player his mixed strategy set is denoted as Δ_i, in which a probability is assigned to each of his pure strategy. By this definition, we can distinguish two types of ambiguity in security games. (i) The value of a payoff is ambiguous: (a) *absent*: for $u_i(X)$, we have $|X| = 1 \wedge \forall u_i(Y)_{X \subseteq Y}$, $m_{i,Y}(\Theta_i^+) = 1$ or $m_{i,Y}(\Theta_i^-) = 1$; (b) *interval value*: for $u_i(X)$, we have $m_{i,X}(B) = 1$, where $B = \{h_i, \ldots, h_j\} \wedge B \subset \Theta$; and (c) *ambiguity lottery*: for $u_i(X)$, $\exists B \subset \Theta_i$ such that $m_{i,X}(B) > 0 \wedge |B| > 1$. And (ii) the pure strategy profile that relates to a given payoff is ambiguous: for $u_i(X)$, we have $|X| > 1 \wedge m_{i,X}(\Theta_i^-) \neq 1$. Moreover, the value of payoff is not ambiguous if the payoff is: (i) a *point value*: for $u_i(X)$, we have $m(\{B\}) = 1$, where $B \subseteq \Theta_i \wedge |B| = 1$; or (ii) *risk*: for $u_i(X)$, if $m(B) > 0$, then $B \subseteq \Theta_i \wedge |B| = 1$. Finally, the profile that relates to a given payoff is not ambiguous if for $u_i(X)$, we have $|X| = 1$.

Clearly, for any $u_i(X)$, $X \subseteq \Psi$ and $|X| = 1$, if we have $h_i \in \Theta_i$ and $m(\{h_i\}) = 1$, then the payoff of each pure strategy profile is a point value, which means that the security game under ambiguities is reduced to a traditional security game. Moreover, the definition assumes that there are imprecise probabilities [Shafer, 1976] for the payoffs of the subsets of profiles. This is consistent with our intuition that the possible payoff values in a given security game are often finite and discrete. For example, if the payoffs are actually money, then the number of payoffs is finite and their differences will not be less than 0.01. Hence, in order to consider the payoffs of compound profiles, the payoff function is defined on the set of all pure strategy profiles subsets. Finally, the last sentence in Definition 5 means the possible subsets of strategy profiles that do not appear in the payoff matrix of a game (e.g., Table 1) have no influence on the outcome of this game.

Finally, we take the second row in Table 1 about the airport scenario in Section 1 as an example to discuss some insights of these two types of ambiguity. (i) The value of a payoff is ambiguous. (a) An absent payoff means there are no appropriate values to represent a situation, i.e., he only knows the result of the pure strategy profile is successful or not. Thus, we can distinguish two types of absent payoff: positive absent payoff ($m(\{\Theta_i^+\}) = 1$) and negative absent payoff ($m(\{\Theta_i^-\}) = 1$). In Table 1, when the profile is (*PR*, *SL*), it satisfies this situation and $m_{1,\{(PR,SL)\}}(\{\Theta_i^-\}) = 1$. (b) For interval-valued payoffs, the complete ignorance of player i for the interval-valued payoff $[x_s, x_t]$ of the payoff function $u_i(X)$ can be represented by $m_{i,X}(\{x_s, \ldots, x_t\}) = 1$.

Table 2: Airport security game
Here a=$\{-8, -7\}$, b=$\{-9, \ldots, 0\}$, c=$\{5, 6\}$, d=$\{0, \ldots, 9\}$.

	SA	PR	SL	VL | H
SA	$m(\{2, \ldots, 6\}) = 1;\ m'(\{-7\}) = 1$	$m(a) = 0.8, m(b) = 0.2;\ m'(\{3\}) = 1$	$m(b) = 1;\ m'(\{2\}) = 1$	$m(\{-8\}) = 1;\ m'(\{7\}) = 1$
PR	$m(\{-7, \ldots, -3\});\ m'(\{5\}) = 1$	$m(c) = 0.8, m(d) = 0.2;\ m'(\{-5\}) = 1$	$m(b) = 1;\ m'(\{2\}) = 1$	$m(\{-8\}) = 1;\ m'(\{7\}) = 1$
SL	$m(\{-7, \ldots, -3\}) = 1;\ m'(\{5\}) = 1$	$m(a) = 0.8, m(b) = 0.2;\ m'(\{3\}) = 1$	$m(d) = 1;\ m'(\{-4\}) = 1$	$m(\{-8\}) = 1;\ m'(\{7\}) = 1$
VL	$m(\{-7, \ldots, -3\}) = 1;\ m'(\{5\}) = 1$	$m(a) = 0.8, m(b) = 0.2;\ m'(\{3\}) = 1$	$m(b) = 1;\ m'(\{2\}) = 1$	$m_{\{(VL,VL);(H,H)\}}(\{7\}) = 1;$ $m'_{\{(VL,VL);(H,H)\}}(\{-9\}) = 1$
H	$m(\{-7, \ldots, -3\}) = 1;\ m'(\{5\}) = 1$	$m(a) = 0.8, m(b) = 0.2;\ m'(\{3\}) = 1$	$m(d) = 1;\ m'(\{2\}) = 1$	$m_{\{(VL,H);(H,VL)\}}(\{-8\}) = 1;$ $m'_{\{(VL,H);(H,VL)\}}(\{7\}) = 1$

It means that player i only knows that the payoff that he can gain could be any value in-between x_s and x_t, but cannot be sure which value it is. Then, by Equations (4) and (5), we can obtain the corresponding expected payoff interval as follow:

$$EUI_i(X) = [x_s \times 1, x_t \times 1] = [x_s, x_t]. \quad (8)$$

That is, the expected payoff interval is the same as the interval-valued payoff itself. Thus, in Table 1, when the pure strategy profile is (*PR*, *SA*), it satisfies this situation and $m_{1,\{(PR,SA)\}}(\{-7, \ldots, -3\}) = 1$. (c) Ambiguity lottery means that multiple discrete situations are possible with (a generalization of) the probability of each situation being known. In Table 1, when the profile is (*PR*, *PR*), it satisfies this situation. And (ii) the pure strategy profile that relates to a given payoff is ambiguous: it means some strategies of players are closely related and so the combined value is applied in this situation. In Table 1, profiles (*PR*, *VL*) and (*PR*, *H*) satisfy this situation and $m_{1,\{(PR,VL),(PR,H)\}}(\{-8\}) = 1$. Thus, we can represent the payoff matrix in Table 1 by mass functions as shown in Table 2 without changing its meaning.

4 Ambiguity Aversion Framework

This section discusses how to handle a security game under ambiguities. To handle such a game, we first transform all the five types of payoff values (i.e., absent, interval-valued, ambiguity lottery, point-valued, and risk) into point values for all subsets of pure strategy profiles. Then, we handle the payoffs of compound strategy profiles by finding the point value for each pure strategy profile. Finally, the defender's optimal strategy can be obtained by well established methods (e.g., [Pita *et al.*, 2009; Tambe, 2011; Yang *et al.*, 2012]).

The basic assumptions of our framework are as follow:

A1: Each player i will consider the relative expected payoff of the subsets of profiles.

A2: Each player will maximize his expected payoffs relative to his subjective priorities.

A3: The worst expected outcome of negative absent payoff is worse than any other types of payoffs.

Intuitively, A1 means that if a player believes he will not obtain the expected payoff that is lower than the worst payoff in the game, he only needs to consider how well the given strategy performs compared with the worst one. A2 is a rational player assumption. A3 means that for the reason of caution, the players think that there exists a chance that the negative absent payoff turns out to be the worst outcome in the game.

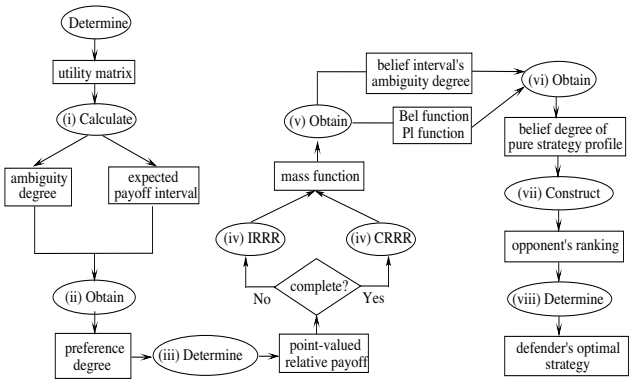

Figure 1: Procedure of our ambiguity aversion method

As a consequence of these assumptions, we can deploy the ambiguity aversion method, as shown in Figure 1, to obtain the point value for all pure strategy profiles as follow.

(i) Calculate the expected payoff intervals and ambiguity degree of X_r for a given player i.

As we can represent all types of payoffs by mass functions in security games under ambiguities, we can calculate the expected payoff intervals for the defender by Equations (4) and (5), and the ambiguity degree by Equation (3) directly.

(ii) Obtain preference degree $\nu_i(X_r)$ for player i.

Definition 6. *Let $EUI_i(X_r) = [\underline{E}_i(X_r), \overline{E}_i(X_r)]$ be an interval-valued expected payoff of profile subset X_r for player i, and $\delta_i(X_r)$ be the ambiguity degree of m_{i,X_r}, then the preference degree of X_r is given by:*

$$\nu_i(X_r) = \frac{2\underline{E}_i(X_r) + (1 - \delta_i(X_r))(\overline{E}_i(X_r) - \underline{E}_i(X_r))}{2}. \quad (9)$$

Actually, since the preference degree of $\nu_i(X_r)$ is a kind of pointed value expected utility, it is reasonable to assume that $\nu_i(X_r) \in [\underline{E}_i(X_r), \overline{E}_i(X_r)]$. Thus, with this assumption, it is easy to prove that Definition 6 is a unique one that satisfies the properties in Definition 4. Moreover, Ma *et al.* [2013] proved that the preference ordering induced by this definition is equivalent to that in Definition 4.

In the security game as shown in Table 1, suppose $\Theta_1 = \{-9, -8, \ldots, 0, 1, \ldots, 9\}$. According to Definition 5, we can express all types of ambiguities in Table 1 by mass functions. Thus, by Equation (9), the defender's preference degrees can be obtained as shown in Table 3.[4]

[4]Here we consider the payoff value of the defender first. Later

Table 3: Preference degree for the defender

	SA	PR	SL	VL | H
SA	3.2	−6.74	−9	−8
PR	−5.8	5.46	−9	−8
SL	−5.8	−6.74	0	−8
VL	−5.8	−6.74	−9	{(VL,VL);(H,H)}:7
H	−5.8	−6.74	−9	{(VL,H);(H,VL)}:−8

Table 4: Point-valued relative payoffs for the defender

	SA	PR	SL	VL | H
SA	12.2	2.26	0	1
PR	3.2	14.46	0	1
SL	3.2	2.26	9	1
VL	3.2	2.26	0	{(VL,VL);(H,H)}:16
H	3.2	2.26	0	{(VL,H);(H,VL)}:1

Table 5: Mass function for the defender

m({(SA,SA)})=0.15,	m({(SA,PR)})=0.03,	m({(SA,VL),(SA,H)})=0.01,
m({(PR,SA)})=0.04,	m({(PR,PR)})=0.18,	m({(PR,VL),(PR,H)})=0.01,
m({(SL,SA)})=0.04,	m({(SL,PR)})=0.03,	m({(SL,VL),(SL,H)})=0.01,
m({(VL,SA)})=0.04,	m({(VL,PR)})=0.03,	m({(H,VL),(VL,H)})=0.01,
m({(H,SA)})=0.04,	m({(H,PR)})=0.03,	m({(VL,VL),(H,H)})=0.19,
m({(SL,SL)})=0.11,	and m(Ψ)=0.05.	

Table 6: Belief interval $[Bel, Pl]$ for defender

	SA	PR	SL	VL	H
SA	[0.15,0.2]	[0.03,0.08]	[0,0.05]	[0,0.06]	[0,0.06]
PR	[0.04,0.09]	[0.18,0.23]	[0,0.05]	[0,0.06]	[0,0.06]
SL	[0.04,0.09]	[0.03,0.08]	[0.11,0.16]	[0,0.06]	[0,0.06]
VL	[0.04,0.09]	[0.03,0.08]	[0,0.05]	[0,0.24]	[0,0.06]
H	[0.04,0.09]	[0.03,0.08]	[0,0.05]	[0,0.06]	[0,0.24]

(iii) Determine player i's relative payoff $d_i(X_r)$ between the given preference degree and the worst one in a game.

First, the worst preference degree can be defined as follow:

Definition 7. *For a security game under ambiguities, a preference degree is the worst preference degree, denoted as $\nu_i^w(X_k)$ (w means the worst one), of player i if and only if*

$$\forall X_r \subset \Psi \wedge U_i(X_r) \neq \emptyset,\ \nu_i^w(X_k) \leq \nu_i(X_r).$$

Thus, we can formally define the relative payoff as follow:

Definition 8. *Let $\nu_i^w(X_k)$ be the worst preference degree of player i, then the relative payoff, denoted as $d_i(X_r)$, for the subset of pure strategy profiles X_r is:*

$$d_i(X_r) = \nu_i(X_r) - \nu_i^w(X_k). \tag{10}$$

Clearly, we have $d_i(X_r) \geq 0$. The motivation of this step is to transform all the payoff values into positive numbers in order to obtain the mass values in the next step. For the airport security game in Table 1, by Equation (10), we can obtain the defender's point-valued relative payoffs as shown in Table 4.

(iv) Derive the mass function from $d_i(X_r)$ for player i.

Since a belief interval can be used to express the belief degree and uncertainty of each pure strategy profile for a given player, we need a method to assign a mass value to each subset of pure strategy profiles. In fact, the mass value based on $d_i(X_r)$ represents the possibility that a subset of pure strategy profiles contains the most favorable outcome that player i would like to have. Thus, we present the following two theorems (which are the variants of the comparison rules in [Ma *et al.*, 2012], and so we omit their similar proofs here for the sake of space):

Theorem 1. *For a given security game with absent payoffs, let $X_r \subset \Psi$ be one of n elements such that $d_i(X_r) \neq 0$ with relative payoff a_j, then the mass function over Ψ of profiles subset X_r for player i is:*

$$m_i(X_r) = \frac{a_j}{\sum_{k=1}^{n} a_k + \sqrt{n}},\ (k = 1, 2, \ldots, n). \tag{11}$$

Moreover, the uncertainty for the whole game for player i is

$$m_i(\Psi) = \frac{\sqrt{n}}{(\sum_{k=1}^{n} a_k + \sqrt{n})},\ (k = 1, 2, \ldots, n). \tag{12}$$

on we will discuss the attacker's .

Theorem 2. *For a given security game without any absent payoff, let $X_r \subset \Psi$ be one of n elements such that $d_i(X_r) \neq 0$ with relative payoff a_j, then the mass function over Ψ of profiles subset X_r for player i is:*

$$m_i(X_r) = \frac{a_j}{\sum_{k=1}^{n} a_k},\ (k = 1, 2, \ldots, n). \tag{13}$$

Intuitively, in a game without absent payoffs, there is some evidence for all the payoff evaluations. So, the value of the worst preference degree is based on some evidence. However, for an absent payoff where a player has absolutely no idea about the value, it means that the result of the worst preference degree is completely obtained by the subjective judgement about the boundary of the payoff values. So, the player has some kind of uncertainty about the result of the absent payoff (whether it turns out to be worse than the lower bound of the values). Hence, the player has to express his uncertainty in this situation to depict his preference of the strategies. So, we deploy Theorems 1 and 2 to derive the mass function.

For the airport security game in Table 1, by Theorems 1 and 2, we can obtain the mass function for the defender in Table 5 from the relative payoffs as shown in Table 4.

(v) Obtain the belief interval by Definition 1 for player i.

For the airport security game in Table 1, we can obtain the belief interval for the defender as shown in Table 6 by Definition 1 from the mass function shown in Table 5.

(vi) Obtain the point-valued belief degree based on the belief interval for player i.

Definition 9. *Let $m_i(X_r)$ be the mass value of the profiles subset X_r for player i and $m_i(\Psi)$ be the mass value of Ψ, which both induce belief function $Bel_i(y)$ and plausibility function $Pl_i(y)$ over Ψ. Let $\delta_i(y)$ be the ambiguity degree of the belief interval ($y = \{(a_j, a_{-j})\} \subset X_t$), then its point-valued belief degree is given by*

$$\eta_i(y) = \frac{2Bel_i(y) + (1 - \delta_i(y))(Pl_i(y) - Bel_i(y))}{2}, \tag{14}$$

where

$$\delta_i(y) = \frac{\sum\limits_{y \bigcap B \neq \emptyset} m_i(B) \log_2 |B|}{\log_2 |\Psi|}. \tag{15}$$

Table 7: Norm form for airport security game

	SA	PR	SL	VL	H
SA	0.17; 0.01	0.05; 0.05	0.02; 0.05	0.03; 0.04	0.03; 0.04
PR	0.06; 0.06	0.2; 0.018	0.02; 0.05	0.03; 0.04	0.03; 0.04
SL	0.06; 0.06	0.05; 0.05	0.13; 0.02	0.03; 0.04	0.03; 0.04
VL	0.06; 0.06	0.05; 0.05	0.02; 0.05	0.11; 0	0.03; 0.04
H	0.06; 0.06	0.05; 0.05	0.02; 0.05	0.03; 0.04	0.11; 0

(vii) Construct the point-valued belief degree of player i's adversaries by repeating steps (i) to (vi).

For the airport security game in Table 1, repeat steps (i) to (vi) for the attacker. Then by Definition 9 and the belief interval for the defender shown in Table 6, we can obtain the traditional security game as shown in Table 7.[5]

(viii) Use some well established methods in security games to determine the optimal mixed strategy of the defender.

For the airport security game in Table 1, by Table 7 and the idea in [Korzhyk *et al.*, 2011], we can obtain the optimal mixed strategy of the defender is $(\frac{5}{13}/SA, \frac{4}{13}/PR, \frac{4}{13}/SL)$.

5 Properties

This section reveals two properties of our framework. One is about the correctness of point-value game models under ambiguities and the other is about the risk attitude of the defender.

As we pointed out in Section 1, most existing researches of security games assume that all players have point-valued payoffs for each pure strategy profile. However, in real-life security allocation problems, since the experts or data analysts have to estimate a complex security system that involves a large number of uncontrollable and unpredictable factors, it is very reasonable to assume that there exist some deviations for the point-valued estimations of payoffs. So, the manager will ask the question: under which condition, the defender's optimal strategy obtained from the point-valued payoffs is the same if the estimation has a range of deviation? Since the defender's optimal strategy is determined by the set of SSE or NE, we can answer this question by the following theorem:

Theorem 3. *Let a_{s_l} be the payoffs of each pure strategy profile s_l in a traditional security game $G=(N, A, \Psi, \Theta, M, U)$ for player i, $[b_{s_l}, c_{s_l}]$ ($b_{s_l} \cdot c_{s_l} > 0 \wedge a_{s_l} \in [b_{s_l}, c_{s_l}]$) be the interval payoffs of each profile in $G' = (N, A, \Psi, \Theta', M', U')$, if for any two payoffs a_{s_k}, a_{s_r} in G, we have $a_{s_k} - b_{s_k} = a_{s_r} - b_{s_r}$, $c_{s_k} - b_{s_k} = c_{s_r} - b_{s_r}$, and $|\Theta'^{+}| = |\Theta'^{-}|$, then these two games G and G' have the same set of SSE (and NE).*

Proof. As we use the belief degree in Definition 9 to determine the optimal strategy for the defender in our framework, according to [Weibull, 1996] and the concept of SSE [Korzhyk *et al.*, 2011], we only need to prove that a_{s_l} and the belief degree, $\eta_i(s_l)$, of $[b_{s_l}, c_{s_l}]$ satisfy an equation $\eta_i(s_l) = ka_{s_l} + l$, where $k > 0 \wedge k, l \in \Re$ ($\Re$ is a set of real numbers). It can be easily proved in our framework. So, games G and G' have the same set of NE and SSE. □

[5]Due to page limit, we do not present each step of the attacker's payoffs value in this paper.

Now, we turn to the second property about the player's risk attitude. Actually, the preference degree in Definition 6 can be presented by $\nu_i(X_r) = \alpha \underline{E}_i(X_r) + (1-\alpha)\overline{E}_i(X_r)$, where $\alpha = \frac{(1+\delta_i(X_r))}{2}$. Similarly to Hurwicz's criterion [Jaffray and Jeleva, 2007], this definition ascribes a value, which is a weighted sum of its worst and best expected payoffs of the subset of pure strategy profiles X_r. Thus, α can be interpreted as a degree of pessimism. That is, a risk seeking (optimism) player will assign a lower value to α than a risk averse (pessimism) player for the same expected payoffs intervals. So, a risk seeking player will obtain a higher preference degree than a risk averse player for the same expected payoff intervals. Hence, by Definition 2, we find that the ambiguity degree is determined by mass function m and frame Θ. Furthermore, as the mass function will not change for a given set of pure strategy profiles and the boundary of Θ is based on the manger's subjective judgement, we can show that a player's risk attitude can be influenced by the boundary of Θ:

Theorem 4. *Let m be a mass function on frame $\Theta_i = \{h_1, \ldots, h_n\}$, $\nu_i(X)$ be the preference degree that obtained from m, m' be a mass function on $\Theta'_i = \{k_1, \ldots, k_m\}$. If $\Theta'_i \supset \Theta_i$ and $m'(X) = m(X)$, $X \subset \Theta_i$ then $\nu'_i(X) > \nu_i(X)$.*

Proof. Because $m'(X) = m(X)$, $X \subset \Theta_i$, and $\Theta'_i \supset \Theta_i$, by Definition 2, we have $\delta'_i(X_r) < \delta_i(X_r)$. Hence, by $m'(X) = m(X)$ and Equations (4) and (5), we have $EUI_i = EUI'_i$. Thus, by Equation (9), we have $\nu'_i(X) > \nu_i(X)$. □

Intuitively, Theorem 4 means that for an expected payoff interval, the more risk seeking the defender is, the wider the range he will consider for the possible payoffs values of the whole game. For example, when considering value of the real estates, the manager may not worry too much about an error within a range of one thousand dollars for the price of a house, since one thousand is a very small value for a house. The defender will then be more risk seeking to determine the point value estimation for a house. However, when considering the daily revenue of shops, the manager might be more cautious to consider an error within the range of one thousand. So, this theorem means that the manager should not over-estimate the possible payoff values in a security game under ambiguities if he wants to be cautious when estimating the value of each pure strategy profile. Simply, the players' risk attitude will influence the point-valued belief degree and eventually the solution of a security game under ambiguities.

6 Reduce Influence of Complete Ignorance

In a security game, it is very important to reduce the effect of complete ignorance for the strategy profile selection. For example, in an airport, if the defender is unsure about the value of the security targets and chooses a wrong strategy for patrolling, then the attacker will take advantage and make a successful assault, which is unacceptable for public security. Moreover, in our framework, the complete ignorance for the strategy profile selection of player i is determined by $m_i(\Psi)$, where Ψ is the set of all pure strategy profiles. We now provide two methods to reduce the complete ignorance in a security game as shown in the following theorem:

Theorem 5. *In security game $G = (N, A, \Psi, \Theta, M, U)$, let $d_i(X_r)$ be the relative payoffs of game G, $m_i(\Psi)$ be the uncertainty of the whole game (complete ignorance) that defined in Theorem 1. Then:*

(i) For game $G' = (N, A, \Psi, \Theta, M', U')$, if $d'_i(X_r) > d_i(X_r)$, and $\forall d_i(X_s) = 0$, $d'_i(X_s) = d_i(X_s)$, then $m'_i(\Psi) < m_i(\Psi)$.

(ii) For game $G'' = (N, A \cup B, \Psi \cup \Phi, \Theta, M \cup M'', U \cup U'')$, if $G = (N, A, \Psi, \Theta, M, U)$, $d_i(X_r) \in [t, 2t]$, where $t > \frac{\sum d_i(X_r)}{2n}$, then $m''_i(\Psi \cup \Phi) < m_i(\Psi)$.

Proof. We can prove (i) and (ii) together. By Theorem 1 and $\forall d_i(X_s) = 0$, $d'_i(X_s) = d_i(X_s)$, we have

$$m_i(\Psi) - m'_i(\Psi) = \frac{\sqrt{n}}{(\sum_{j=1}^{n} a_j + \sqrt{n})} - \frac{\sqrt{n}}{(\sum_{j=1}^{n} a'_j + \sqrt{n})},$$

where a_j is the value of the relative payoff $d_i(X_r)$ such that $a_j > 0$, a'_j is the value of the relative payoff $d'_i(X_r)$ such that $a'_j > 0$, and n is the number of element a_j or a'_j. Clearly, by $d'_i(X_r) > d_i(X_r)$, we have $a'_j > a_j$. Thus, item (i) holds.

Moreover, in G'', when the number of relative payoffs in Δ is 1, we have:

$$\frac{\sqrt{n}}{(\sum_{j=1}^{n} a_i + \sqrt{n})} > \frac{\sqrt{n}}{(2nt + \sqrt{n})} > \frac{\sqrt{n+1}}{(2nt + t + \sqrt{n+1})}.$$

So, in this case, item (ii) holds. When the number of relative payoffs in Δ is $k - 1$, item (ii) also holds. Then, when the number of relative payoffs in Δ is k (assume the sum of $k - 1$ relative payoffs in Φ is b, the newly added one's relative payoff is c), we have $\sum_{j=1}^{n} a_j + b + c < 2t(n + k - 1) + 2t$ because the relative payoffs in Φ belongs to $[t, 2t]$. Then:

$$\frac{\sqrt{n+k-1}}{(\sum_{j=1}^{n} a_i + b + \sqrt{n+1})} > \frac{\sqrt{n+k}}{(2nt + b + c + \sqrt{n+k})}.$$

So, when the number of relative payoffs in Δ is k, item (ii) holds as well. Therefore, item (ii) holds no matter how many relative payoff values in Φ. □

Actually, Theorem 5 tells us that there are two methods for reducing the effects of complete ignorance for strategy selection in a security game under ambiguities: (i) to increase the importance degrees of some security targets (apparently, we cannot increase that of an absent payoff one); and (ii) to consider more security targets before selecting a strategy when the importance degrees of all security targets are not too high. These are consistent with our intuition. In fact, if the values of some security targets are high enough, then the defender will not hesitate to assign a random patrolling to cover those targets. On the other hand, if all security targets are not so important, the defender can consider more targets or make the absent payoff target more specific. For example, when the payoff of a shopping area is unknown, the defender can consider carefully that the payoff of which shop is unknown and how to evaluate other shops. In this way, he can reduce the effect of complete ignorance for his optimal strategy selection.

7 Related Work

Recently, there have been lots of interest in studying the games under ambiguity. Eichberger and Kelsey [2011] show that ambiguity preferences will cause players to pursue strategies with high payoffs of equilibrium and ambiguity-aversion can make the strategies with low payoffs of equilibrium less attractive. Similarly, Giuseppe and Maria [2012] investigate the difference among equilibria with respect to various attitudes toward ambiguity, and show that different types of contingent ambiguity will affect equilibrium behavior. And Bade [2011] proposes a game-theoretic framework that studies the effect of ambiguity aversion on equilibrium outcomes based on the relaxation of randomized strategies. However, none of these models provides a method to handle the two types of ambiguity, which our model did.

The problem of modeling uncertainty has become a key challenge in the realm of security. Kiekintveld *et al.* [2010] introduce an infinite Bayesian Stackelberg game method to model uncertain distribution of payoffs. Yang *et al.* [2012] consider the bounded rationality of human adversaries and use prospect theory [Kahneman and Tversky, 1979] and quantal response equilibrium to obtain the defender's optimal strategy. Korzhyk *et al.* [2011] consider the uncertainty of the attacker's surveillance capability and suggest that the defender should select the NE strategy in this situation. However, none of them has considered the ambiguities in security games. Instead, our paper has fully considered this issue.

8 Conclusions and Future Work

This paper proposed an ambiguity aversion framework for security games under ambiguities. Moreover, we reveal two properties of our framework about the correctness of point-value security game models under ambiguities and player's risk attitude in our ambiguous games. In addition, we propose two methods to reduce the effects of complete ignorance in security games under ambiguities. There are many possible extensions to our work. Perhaps the most interesting one is the psychological experimental study of our ambiguity aversion framework. Another tempting avenue for evaluating our framework is to show that under ambiguity, selecting the defender's optimal strategy by our framework is better than a random point-valued game matrix. Hence, we can also consider the effect of regret and ambiguity aversion for constructing the equilibrium and selecting the defender's optimal strategy. Finally, We will consider the event reasoning framework developed in the CSIT project [Ma *et al.*, 2009; 2010; Miller *et al.*, 2010] as a testbed to fully evaluate the usefulness of our model.

Acknowledgments

We would like to thank anonymous reviewers for insightful comments which helped us significantly to improve this paper. This work has been supported by the EPSRC projects EP/G034303/1; EP/H049606/1 (the CSIT project); Bairen plan of Sun Yat-sen University; National Natural Science Foundation of China (No. 61173019); major projects of the Ministry of Education, China (No. 10JZD0006).

References

[Bade, 2011] Sophie Bade. Ambiguous act equilibria. *Games and Economic Behavior*, 71(2):246–260, 2011.

[Dubois and Prade, 1985] Didier Dubois and Henri Prade. A note on measures of specificity for fuzzy sets. *International Journal of General Systems*, 10(4):279–283, 1985.

[Eichberger and Kelsey, 2011] Jürgen Eichberger and David Kelsey. Are the treasures of game theory ambiguous? *Economic Theory*, 48(2-3):313–339, 2011.

[Giuseppe and Maria, 2012] De Marco Giuseppe and Romaniello Maria. Beliefs correspondences and equilibria in ambiguous games. *International Journal of Intelligent Systems*, 27(2):86–102, 2012.

[Jaffray and Jeleva, 2007] Jean-Yves Jaffray and Meglena Jeleva. Information processing under imprecise risk with the hurwicz criterion. In *Proceedings of the Fifth International Symposium on Imprecise Probability: Theories and Applications*, pages 233–242, 2007.

[Kahneman and Tversky, 1979] Daniel Kahneman and Amos Tversky. Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2):263–291, 1979.

[Kiekintveld *et al.*, 2010] Christopher Kiekintveld, Janusz Marecki, and Milind Tambe. Approximation methods for infinite Bayesian Stackelberg games: Modeling distributional payoff uncertainty. In *Proceedings of 10th International Conference on Autonomous Agents and Multiagent Systems*, pages 1005–1012, 2010.

[Korzhyk *et al.*, 2011] Dmytro Korzhyk, Zhengyu Yin, Christopher Kiekintveld, Vincent Conitzer, and Milind Tambe. Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. *Journal of Artificial Intelligence Research*, 41(2):297–327, 2011.

[Ma *et al.*, 2009] Jianbing Ma, Weiru Liu, Paul Miller, and WeiQi Yan. Event composition with imperfect information for bus surveillance. In *Proceedings of the Sixth IEEE International Conference on Advanced Video and Signal Based Surveillance*, pages 382–387, 2009.

[Ma *et al.*, 2010] Jianbing Ma, Weiru Liu, and Paul Miller. Event modelling and reasoning with uncertain information for distributed sensor networks. In *Proceedings of Scalable Uncertainty Management - 4th International Conference*, pages 236–249, 2010.

[Ma *et al.*, 2012] Wenjun Ma, Xudong Luo, and Wei Xiong. A novel D-S theory based AHP decision apparatus under subjective factor disturbances. In *AI 2012: Advances in Artificial Intelligence, LNCS*, volume 7691, pages 863–877, 2012.

[Ma *et al.*, 2013] Wenjun Ma, Wei Xiong, and Xudong Luo. A model for decision making with missing, imprecise, and uncertain evaluations of multiple criteria. *International Journal of Intelligent Systems*, 28(2):152–184, 2013.

[Miller *et al.*, 2010] Paul Miller, Weiru Liu, Chris Fowler, Huiyu Zhou, Jiali Shen, Jianbing Ma, Jianguo Zhang, WeiQi Yan, Kieran McLaughlin, and Sakir Sezer. Intelligent sensor information system for public transport - to safely go... In *Proceedings of the Seventh IEEE International Conference on Advanced Video and Signal Based Surveillance*, pages 533–538, 2010.

[Pita *et al.*, 2009] James Pita, Manish Jain, Fernando Ordóñez, Christopher Portway, Milind Tambe, Craig Western, Praveen Paruchuri, and Sarit Kraus. Using game theory for Los Angeles airport security. *AI Magazine*, 30(1):43–57, 2009.

[Shafer, 1976] Glenn Shafer. *A Mathematical Theory of Evidence*. Limited paperback editions. Princeton University Press, 1976.

[Strat, 1990] Thomas M. Strat. Decision analysis using belief functions. *International Journal of Approximate Reasoning*, 4(56):391 – 417, 1990.

[Tambe, 2011] Milind Tambe. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*. Cambridge University Press, Cambridge, 2011.

[Von Neumann and Morgenstern, 1944] John Von Neumann and Oskar Morgenstern. *Theory of Games and Economic Behavior*. Princeton University Press, 1944.

[Weibull, 1996] Jörgen Weibull. *Evolutionary Game Theory*. MIT Press, Cambridge, Massachusetts, 1996.

[Yang *et al.*, 2012] Rong Yang, Christopher Kiekintveld, Fernando Ordóñez, Milind Tambe, and Richard John. Improving resource allocation strategies against human adversaries in security games: An extended study. *Artificial Intelligence*, DOI: 10.1016/j.artint.2012.11.004, 2012.