Ma, W., Liu, W., Mcareavey, K., Luo, X., Jiang, Y., Zhan, J., & Chen, Z. (2020). A decision support framework for security resource allocation under ambiguity. *International Journal of Intelligent Systems*, 36(1), 5-52. <https://doi.org/10.1002/int.22288>

Peer reviewed version

Link to published version (if available):
[10.1002/int.22288](https://doi.org/10.1002/int.22288)

[Link to publication record in Explore Bristol Research](#)
PDF-document

This is the author accepted manuscript (AAM). The final published version (version of record) is available online via Wiley at <https://onlinelibrary.wiley.com/doi/full/10.1002/int.22288?af=R> . Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available:
<http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/>

A Decision Support Framework for Security Resource Allocation under Ambiguity

Wenjun Ma¹, Weiru Liu², Kevin McAreevey², Xudong Luo^{3‡}, Yuncheng Jiang^{1¶},
Jieyu Zhan¹, and Zhenzhou Chen¹

¹Guangzhou Key Laboratory of Big Data and Intelligent Education, School of Computer Science,
South China Normal University, Guangzhou, China.

²School of Computer Science, Electrical and Electronic Engineering, and Engineering Maths,
University of Bristol, Bristol, UK.

³Guangxi Key Lab of Multi-Source Information Mining & Security, Faculty of Computer Science and
Information Technology, Guangxi Normal University, Guilin, China.

ABSTRACT

There has been increasing interest in using Stackelberg game (known as a security game) to allocate limited security resources against different attacker types with a specific probability distribution. However, real problems of this kind often face ambiguous information such as imprecise, unreliable and absent payoffs, and ambiguous assignments of these payoffs. To this end, based on decision theory and the Dempster-Shafer theory of evidence, this paper proposes a novel framework that can handle these common types of ambiguity. More specifically, this paper deploys the underlying principles of existing rules from decision theory, as a way to characterise different attitudes to ambiguity, during the transformation of ambiguous payoffs into point-valued payoffs. Hence, our framework holds some good properties: (i) it subsumes traditional security games without ambiguous payoffs, (ii) a uniform margin of error will not affect the results, and (iii) the influence of complete ignorance can be minimised. Also, our framework is evaluated by using nine different transformation rules, under various conditions and constraints, against 73,000 randomly generated games (a first comprehensive empirical evaluation to date). The evaluation reveals the benefits of each transformation rule and confirms that different rules can model individuals' different attitudes to ambiguity.

Keywords: decision making under uncertainty, game theory, security game, public security, D-S theory, ambiguity.

1. INTRODUCTION

Since today the public security issue is so crucial^{1,2}, it is very significant to decide how to allocate limited security resources for the success of security operations globally^{3,4,5,6}. Most existing studies address this issue using a special type of (Bayesian) Stackelberg game, known as a security game with two players (a defender and an attacker). In a security game, the defender selects a strategy that can maximise their payoff. Usually, this strategy is a *mixed strategy*, which means a probability distribution over a player's set of pure strategies. Thus, a solution to a security game is the defender's *optimal mixed strategy*, which maximises their payoff. Finding such a strategy is generally understood as a randomised patrol scheduling

[‡]The corresponding Author e-mail: luoxd@mailbox.gxnu.edu.cn.

[¶]The corresponding Author e-mail: ycjiang@scnu.edu.cn

problem, where the mixed strategy specifies the amount of resources that should be dedicated to defending each security target. On the other hand, the attacker can observe the defender's mixed strategy and accordingly take a pure strategy (*i.e.*, to attack a target) that maximises their own payoff.* Therefore, the purpose of finding the defender's optimal mixed strategy is to provide the defender with a schedule that can influence the attacker's choice such that the defender's payoff is maximised.

The typical concept of solution to security games is Strong Stackelberg Equilibrium (SSE), which is based on three assumptions as follows:

- S1:** The attacker can observe the defender's strategy commitment and respond it optimally.
- S2:** The defender can precisely execute their optimal mixed strategy.
- S3:** Each player has a point-valued (precise) payoff for each pure strategy profile.

There has been much interest in the security field over the applicability of the SSE for real-world security resource allocation^{7,8}. However, in reality these assumptions may be unrealistic.

Thus, this paper relaxes assumption **S3** to handle uncertainly valued utility. A common argument in the literature is that payoff are pervaded with uncertainty because they are inferred from imperfect information (*e.g.*, unreliable expert analyses and incomplete historical data). It is worth noting that the Bayesian Stackelberg model already provides some handling of uncertainty over payoffs. Intuitively, if the decision makers are unsure about the motivation/preferences of the attacker, then they can model this as different payoff matrices against different attacker types, where the likelihood of each attacker type is based on *a priori* probability distribution^{9,10,11,12}. This type of uncertainty is commonly termed risk¹³, only applicable when objective or subjective probabilities are available. However, there is a growing interest in addressing other forms of uncertainty over payoff^{14,15,16,17,18}. For example, another important form of uncertainty related to **S3**, which the Bayesian Stackelberg model cannot handles, is ambiguity¹³. Ambiguity here refers to situations of insufficient information to precisely assign point-valued payoff to every pure strategy profile, or to justify a probability distribution over point-valued payoffs. One notable framework that handles a specific form of ambiguity is the interval security game (ISG) model^{15,17,19}, which represents ambiguous payoff as intervals of point-valued payoffs. However, ambiguity is a much broader issue than is addressed by the ISG model, and the ISG model cannot handle many other forms of ambiguity.

In this paper, two broad classes of ambiguity are identified:

- **Ambiguous payoff**, which cannot be represented by a point-value or a probability distribution over point-values, such as:
 - **Imprecise payoff**, represented as a interval of point-valued payoffs.
 - **Unreliable payoff**, represented as a point-valued or an interval-valued payoff with a reliability degree.
 - **absent payoff**, represented as an undefined payoff, required when no other payoffs are appropriate.
- **Ambiguous payoff assignments**: several pure strategy profiles in a similar situation where it is difficult to assign a unique payoff to each profile.

Notice that interval-valued payoffs are a special case of uncertainty this paper concerns, but this paper also considers other intuitive forms of uncertainty which cannot be handled by the ISG model nor the standard Bayesian Stackelberg game.

For example, suppose there are five security targets in an airport: a shopping area (**SA**), a prayer room (**PR**), a special location (**SL**), a VIP lounge (**VL**), and a hotel (**H**). A security team defends these targets, while the attacker chooses a target to attack. The defender's payoff of taking a strategy against the attacker's choice of a strategy could be affected by ambiguity.

*Depending on context, "the attacker" (resp. "the defender") means "the attacker in a game" in the general case or "the attacker in the game" for a specific game.

First, ambiguous payoff could exist: (i) interval-valued payoffs are assigned to **SA** because of an imprecise estimation of the number of shoppers; (ii) unreliable payoffs are assigned to **PR** because the security team does not fully trust the expert's judgement of this target—in this case the point-valued payoff provided by the expert has a reliability of 80%; and (iii) absent payoffs are assigned to **SL** because it is hard to estimate a meaningful value. Second, ambiguity exists over the assignment of payoffs for some targets. Specifically, the payoffs for **VL** and **H** are proportional to the number of people at these locations but since **H** is in close proximity to **VL**, it is easier to estimate the combined total number of people than to separately estimate the total number of people at each target. In other words, the security team cannot distinguish between **VL** and **H** and so just assigns an overall payoff to these targets.

In this paper, our objective is to advise a security team on the best allocation of security resources via determining the team's optimal mixed strategy from an ambiguous security game. More specifically, this paper designs a general ambiguity-tolerant security game in which the Dempster-Shafer (D-S) theory of evidence^{20,21,22,23} is used to represent and reason with all these different forms of ambiguity. The main task of this novel model is to transform these ambiguous payoffs into point-valued payoffs (and hence a traditional security game), given different attitudes to ambiguity inspired by decision theory, so our framework is also suitable for traditional security games.

Specifically, this paper first models each type of ambiguous payoff as a *mass function* in D-S theory and then apply one of several alternative transformations to these mass functions as a way of interpreting these ambiguous payoffs as point-valued ones. Here different transformation rules reflect different rationales of individuals, so that our framework can adapt to different security requirements. For instance, the Γ -maximin rule²⁴ is based on the principle of minimum acceptable expected payoff and thus can reflect a pessimistic attitude to ambiguity (*i.e.*, players only consider the worst possible point-valued payoff modelled by the mass function). Conversely, the maximax rule is based on the principle of maximum acceptable expected payoff and thus can reflect an optimistic attitude to ambiguity. This paper also uses the ambiguity-aversion principle of minimax regret^{25,26} to construct our own transformation rule.

Moreover, this paper conducts a series of experiments to evaluate our framework, with respect to various aspects, especially the sensitivity of choosing different transformation rules. Specifically, this paper compares nine different transformation rules regarding the defender's resulting optimal mixed strategy and corresponding payoff. Also, this paper systematically evaluates each rule by generating 1,000 random games representing ground-truth values under various constraints. Each ground-truth game is then randomly extended to 8 different types of ambiguous security games (based on 8 different constraints), providing a total of 8,000 different ambiguous security games. Each ambiguous security game is then solved with 9 different instantiations of our framework while the ground-truth game is solved directly, providing us with $1,000 + (8,000 \times 9) = 73,000$ traditional security games and optimal strategies for comparison.

This paper advances the state-of-the-art on the topic of security resource allocation in the following aspects: (i) Two types of ambiguity are identified in security resource allocation problems (*i.e.*, ambiguous payoff and ambiguous payoff assignments). (ii) A general ambiguity-tolerant method is proposed to find the defender's optimal mixed strategy for an ambiguous security game. (iii) We propose a new transformation rule for ambiguous payoffs based on the ambiguity-aversion principle of minimax regret. (iv) A number of theoretical properties are proved, including that our framework subsumes traditional security games, a uniform margin of error does not affect the result, and the influence of complete ignorance is minimised. (v) Our framework is implemented and then evaluated against 9 different rules for transforming ambiguous payoffs into point-valued payoffs, with a total of 73,000 random games generated under various constraints. And (vi) it confirms that there are benefits with each rule, depending on the type of ambiguity that exists.

The rest of the paper is organised as follows. Section 2 recaps security games and D-S theory. Section 3 defines ambiguous security games and relevant concepts. Section 4

presents our general framework for solving ambiguous security games. Section 5 discusses the instantiations of our framework using a new transformation rule and some other alternative rules. Section 6 experimentally evaluate our framework. Section 7 discusses related work. Finally, Section 8 concludes the paper with future work.

2. PRELIMINARIES

This section will recap security games and D-S theory.

2.1. Security Games

Stackelberg games²⁷ are a well-known game involving two players: a leader and a follower. Each player has a set of pure strategies, where a pure strategy specifies an action to execute in any state. Payoffs are defined for each player over the set of pure strategy profiles, which is the product of the leader's set of pure strategies and the follower's set of pure strategies. Bayesian Stackelberg games²⁷ then generalise this model by introducing a probability distributions over the set of types for each player, while payoffs are again defined for all the possible combinations of player types over the set of pure strategy profiles.

Security games^{3,4,5} are a special type of Bayesian Stackelberg game with only one type of leader (defender) but still many possible types of the follower (attacker). Moreover, it assumes that for each pure strategy profile, either the defender or the attacker wins and the other loses. However, importantly these games are unnecessarily zero-sum. This assumption is motivated by the security domain where, for example, a security team may have a high payoff for successfully preventing a terrorist attack, but there may still be some propaganda value associated with a failed attack for a terrorist group. In addition, a common simplification in security games is the assumption of a set of security *targets* where the pure strategies for the defender and attacker correspond to defending or attacking these targets, respectively. Intuitively, it means that if the attacker succeeds in attacking a target then the attacker (resp. defender) will have the same payoff regardless of the pure strategy chosen by the defender (*i.e.*, if the defender fails then their strategy is irrelevant). The definition of a security game in this paper does not need this assumption, but the assumption can simplify examples throughout this paper. That is, payoffs are defined based on whether a target is defended or not.

Definition 1. A traditional security game is a 6-tuple $(N, T, \mathbf{p}, A, \Psi, U)$, where:

- (i) $N = \{d, a\}$ is the set of players, where d is the defender and a is the attacker;
- (ii) $T = \{t_1, \dots, t_n\}$ is a nonempty finite set of n possible attacker types;
- (iii) $\mathbf{p}$ is a probability function over T ;
- (iv) $A = \{A_i \mid i \in N\}$, where A_i is a finite set of pure strategies for player i ;
- (v) $\Psi = A_d \times A_a$ is the set of pure strategy profiles; and
- (vi) $U = \{u_i^t \mid t \in T, i \in N\}$ is the set of payoff functions, where $u_i^t : \Psi \rightarrow \mathbb{R}$ is a payoff function for player i and attacker type t over Ψ .

As mentioned in Section 1, an important concept in game theory is a mixed strategy Δ_i for a player i , *i.e.*, a probability distribution over the set of the player's pure strategies. While there are many interpretations to mixed strategies²⁷, a popular one is that a player commits to a pure strategy in a randomised manner. For example, if a player has two pure strategies s_1 and s_2 , then a mixed strategy $\{\Delta(s_1) = \frac{1}{2}, \Delta(s_2) = \frac{1}{2}\}$ implies that the player uses a fair coin flip to decide whether to commit to s_1 or s_2 . In security games dealing with security patrol scheduling, the common interpretation is that a mixed strategy for the defender represents the proportion of resources that should be dedicated to each security target when generating

	s_3	s_4
s_1	1; 1	3; 0
s_2	0; 0	2; 1

Table I. Example game for comparing SSE and NE. Each cell is two players' payoff for a strategy profile (*e.g.*, for strategy profile (s_1, s_4) , the row player's payoff is 3 and the column player's is 0).

a randomised patrol schedule. Given a mixed strategy profile (Δ_d, Δ_a) and an attacker type t , the payoff value for player i is given by:

$$u_i^t(\Delta_d, \Delta_a) = \sum_{s_d \in A_d} \sum_{s_a \in A_a} \Delta_d(s_d) \Delta_a(s_a) u_i^t(s_d, s_a). \quad (1)$$

Similarly, the overall payoff regarding all the attacker types is given by:

$$u_i(\Delta_d, \Delta_a) = \sum_{t \in T} p(t) u_i^t(\Delta_d, \Delta_a). \quad (2)$$

These types of probability-weighted payoffs are referred to as *expected payoffs*.

Ultimately, our goal is to find the optimal pure or mixed strategy for the defender. The most common concepts of solution to games are SSE and NE (Nash Equilibrium). The major difference between them in the context of security games is as follows:[†]

SSE: It assumes that the defender first commits to a mixed strategy, and then the attacker can observe the defender's commitment and accordingly commits to a pure strategy based on this observation.

NE: It assumes that both players commit to mixed strategies simultaneously (*i.e.*, that the attacker cannot observe the defender's commitment).

The underlying assumption of SSE is that the defender surely commits to a mixed strategy that maximises their expected payoff and the attacker surely commits to a pure strategy that maximises their own expected payoff according to the defender's commitment. In addition, if there is more than one pure strategy for the attacker that maximises their expected payoff with respect to the defender's commitment, then it is assumed that the attacker surely commits to a pure strategy that can result in the maximum expected payoff for the defender (otherwise the optimal solution is not well defined). Conversely, the underlying assumption of NE is that each player definitely selects a mixed strategy that ensures their expected payoff is not less than any other mixed strategy, while considering their opponent's expected commitment.

Example 1 (NE). Consider the game in Table I. In the NE solution concept, both players select their mixed strategies simultaneously. In this case, although neither player can observe the action of the other player, it assumes that both players can correctly forecast their opponent's strategy and then play a best response based on this forecast. This is common knowledge to both players. For example, assume the column player selects pure strategy s_3 as their equilibrium strategy. In this case, the row player's expected payoff is:

$$u_{row}(\Delta_{row}, s_3) = p \times 1 + (1 - p) \times 0 = p$$

for any mixed strategy $\{\Delta_{row}(s_1) = p, \Delta_{row}(s_2) = 1 - p\}$, where $0 \leq p \leq 1$. Thus, if the column player selects pure strategy s_3 , then pure strategy s_1 (*i.e.*, the mixed strategy Δ_{row} where $p = 1$) can maximise the row player's expected payoff. In other words, pure strategy

[†]These differences do not necessary apply for other types of games.

s_1 is the row player's best response to the column player's pure strategy s_3 . In this case, no player can obtain a higher expected payoff by changing their own strategy, which means that (s_1, s_3) is an NE.

In fact, the equilibrium can be obtained by using a best response function $RE_i(\Delta_{i'})$ for a player i , where $\Delta_{i'}$ is a mixed strategy selected by their opponent i' as an equilibrium strategy. Assume the column player selects a mixed strategy $\{\Delta_{col}(s_3) = q, \Delta_{col}(s_4) = 1 - q\}$ as their equilibrium strategy, where $0 \leq q \leq 1$. In this case, the row player's expected payoff can be calculated as follows:

$$u_{row}(\Delta_{row}, \Delta_{col}) = p \times q \times 1 + p \times (1 - q) \times 3 + (1 - p) \times q \times 0 + (1 - p) \times (1 - q) \times 2$$

for any mixed strategy $\{\Delta_{row}(s_1) = p, \Delta_{row}(s_2) = 1 - p\}$, where $0 \leq p \leq 1$. Thus, for any mixed strategy Δ_{col} of the column player, the best response for the row player is $RE_{row}(\Delta_{col}) = s_1$. Assume the row player selects a mixed strategy $\{\Delta_{row}(s_1) = p, \Delta_{row}(s_2) = 1 - p\}$ as their equilibrium strategy, where $0 \leq p \leq 1$. In this case, the column player's expected payoff can be calculated as follows:

$$u_{col}(\Delta_{row}, \Delta_{col}) = p \times q \times 1 + p \times (1 - q) \times 0 + (1 - p) \times q \times 0 + (1 - p) \times (1 - q) \times 1$$

for any mixed strategy $\Delta_{col} = \{\Delta_{col}(s_3) = q, \Delta_{col}(s_4) = 1 - q\}$, where $0 \leq q \leq 1$. Thus, for any mixed strategy Δ_{row} of the row player, the best response, $RE_{col}(\Delta_{row})$, for the column player is s_3 if $p > \frac{1}{2}$, Δ_{col} for any $q \in [0, 1]$ if $p = \frac{1}{2}$, and s_4 if $p < \frac{1}{2}$. If the best responses for the row player and the column player are considered, it can be seen that only one situation satisfies both. That is, the row player definitely selects pure strategy s_1 in response to any strategy of the column player, while the column player definitely selects pure strategy s_3 in response to the row player selecting s_1 . So, (s_1, s_3) is an NE (the only NE in this example). $\square$

Example 2 (SSE). For the game in Table I, in the term of SSE solution, the row player selects their mixed strategy first, then the column player observes the mixed strategy and accordingly selects their best response to the strategy the row player actually takes rather than a forecast. Assume the row player selects a mixed strategy $\{\Delta_{row}(s_1) = p, \Delta_{row}(s_2) = 1 - p\}$, where $0 \leq p \leq 1$. In this case, we have:

(i) When $p > \frac{1}{2}$, the column player selects $RE_{col}(\Delta_{row}) = s_3$ and the row player's expected payoff is $u_{col}(\Delta_{row}, s_3) = p \times 1 + (1 - p) \times 0 = p$.

(ii) When $p = \frac{1}{2}$, the column player selects $RE_{col}(\Delta_{row}) \in \{s_3, s_4\}$. However, the SSE assumes that the column player will break ties in the row player's favour (i.e., by selecting s_4) meaning that the row player's expected payoff is $u_{col}(\Delta_{row}, s_4) = \frac{1}{2} \times 3 + \frac{1}{2} \times 2 = 2.5$.

(iii) When $p < \frac{1}{2}$, the column player selects $RE_{col}(\Delta_{row}) = s_4$ and the row player's expected payoff is $u_{col}(\Delta_{row}, s_4) = p \times 3 + (1 - p) \times 2 = 2 - p$.

Therefore, (Δ_{row}, s_4) such that $\Delta_{row}(s_1) = \frac{1}{2}$ and $\Delta_{row}(s_2) = \frac{1}{2}$ is an SSE. $\square$

In the term of NE solution, the equilibrium is obtained by a forecast of each player's strategy since both players select their strategies simultaneously. However, applying using the SSE into security games, the equilibrium is obtained by the attacker's observation of the defender's strategy since the defender acts first and the attacker can observe the defender's strategy. As shown in Examples 1 and 2, these assumptions may result in different equilibria for the same game.

2.2. Dempster-Shafer Theory of Evidence

For handling various types of ambiguity that are common in real-world security resource allocation problems, a mathematical framework is needed. Dempster-Shafer (D-S) theory of

260 evidence²² have been chosen for this purpose because, as seen in later sections, this framework
 261 enables the defender to handle all types of ambiguity this paper has identified coherently. The
 262 fundamental definition in D-S theory is as follows:

263 **Definition 2.** Let Θ be a set of exhaustive and mutually exclusive elements, called a frame
 264 of discernment (or frame). A function $m : 2^\Theta \rightarrow [0, 1]$ is called a mass function over Θ if
 265 $m(\emptyset) = 0$ and $\sum_{A \subseteq \Theta} m(A) = 1$. A set $A \subseteq \Theta$ such that $m(A) > 0$ is called a focal element
 266 of m . A mass function m is called a simple mass function if there exists at most one $A \subset \Theta$
 267 such that A is a focal element of m . A belief function and a plausibility function for m ,
 268 denoted as Bel_m and Pl_m , are defined as:

$$269 \quad \text{Bel}_m(A) = \sum_{B \subseteq A} m(B), \quad (3)$$

$$270 \quad \text{Pl}_m(A) = \sum_{A \cap B \neq \emptyset} m(B). \quad (4)$$

271

272 D-S theory is commonly recognised as a generalisation of probability theory, but they are
 273 significant different: in the D-S theory normalised values are assigned to subsets of a given set
 274 (a frame of discernment), while in probability theory normalised values are assigned to single
 275 elements of a given set (a set of states).

276 **Example 3.** Suppose Alice lost her phone, but she just knows in the library, or the
 277 bedroom or the calssroom. By D-S theory, this can be modelled as a mass distribution:
 278 $m(\{\text{library}, \text{bedroom}, \text{classroom}\}) = 1$ and for any $A \subset \{\text{library}, \text{bedroom}, \text{classroom}\}$, $m(A) =$
 279 0 . This mass distribution exactly reflects that Alice is only certain her phone is in one of
 280 these three location but has no further information. In probability theory, on the other hand,
 281 this must be modelled by a probability distribution p such that $p(\text{library}) + p(\text{bedroom}) +$
 282 $p(\text{classroom}) = 1$. Since Alice is ignorant about the exact location, the probability distribution
 283 must apply the principle of insufficient reason²⁸ such that $p(\text{library}) = p(\text{bedroom}) =$
 284 $p(\text{classroom}) = \frac{1}{3}$. Thus, the treatment of ignorance in probability theory is less intuitive
 285 than that in D-S theory, because D-S theory does not assume that her phone is equally
 286 possible in each location. In D-S theory, information such as $\text{Bel}_m(\{\text{classroom}\}) = 0$ and
 287 $\text{Pl}_m(\{\text{classroom}\}) = 1$ can be expressed, (i.e., that Alice does not have any degree certainty
 288 about her phone is in the classroom but believes it is plausible that this is the case).

289 This gap between the belief and the plausibility values for a given set represents the
 290 degree of uncertainty over this set based on the available evidence. In this sense, D-S theory
 291 is particularly useful for reasoning in the presence of ignorance, impreciseness, and other
 292 ambiguities. Moreover, probability functions are a special case of mass functions since mass
 293 functions and belief functions do not need to satisfy additivity. In fact, if $\forall A \subseteq \Theta$ such that
 294 $|A| \neq 1$, $m(A) = 0$, then m is a probability function.

295 Finally, since evidence may be incompletely reliable in reality, a *discount factor* for a
 296 mass function was introduced by²². Formally, we have:

297 **Definition 3.** Let m be a mass function over Θ and $\tau \in [0, 1]$ be a discount factor. Then a
 298 discounted mass function for m with respect to τ is defined as:

$$299 \quad m^{(\tau)}(A) = \begin{cases} (1 - \tau)m(A) & \text{if } A \subset \Theta, \\ \tau + (1 - \tau)m(A) & \text{if } A = \Theta. \end{cases} \quad (5)$$

300 When $\tau = 0$, the evidence is completely reliable and when $\tau = 1$ the evidence is completely
 301 unreliable. Essentially, some of the masses assigned to some subsets are discounted and then
 302 allocated to the frame (representing complete ignorance).

303 **Example 4.** Bob believes that Alice lost her phone in the classroom amongst three locations:
 304 library, bedroom, and classroom. This is modelled by a mass distribution m over a frame

305 $\{\text{library}, \text{bedroom}, \text{classroom}\}$ such that $\mathbf{m}(\{\text{classroom}\}) = 1$. However, Bob is not considered
 306 to be a completely reliable source since he sometimes makes things up, so his evidence should
 307 be discounted. For example, if Bob is considered to be 80% reliable, then with a discounted
 308 factor $\tau = 1 - 0.8 = 0.2$, a discounted mass function $\mathbf{m}^{(0.2)}$ can be constructed from $\mathbf{m}$ such
 309 that

$$\begin{aligned}
 310 \quad & \mathbf{m}^{(0.2)}(\{\text{classroom}\}) \\
 311 \quad &= (1 - 0.2) \times \mathbf{m}(\{\text{classroom}\}) \\
 312 \quad &= (1 - 0.2) \times 1 \\
 313 \quad &= 0.8, \\
 314 \quad & \mathbf{m}^{(0.2)}(\{\text{library}, \text{bedroom}, \text{classroom}\}) \\
 315 \quad &= 0.2 + (1 - 0.2)\mathbf{m}(\{\text{library}, \text{bedroom}, \text{classroom}\}) \\
 316 \quad &= 0.2 + (1 - 0.2) \times 0 \\
 317 \quad &= 0.2.
 \end{aligned}$$

318 This ability to deal with reliability is another advantage of D-S theory over other
 319 uncertainty theories such as probability theory.

320 A payoff mass function can be interpreted in numerous ways. The notion of an expected
 321 payoff interval introduced²⁹ is an important one.

322 **Definition 4.** Let $\mathbf{m}$ be a payoff mass function over Θ . Then an interval $\text{EUI}(\mathbf{m}) =$
 323 $[\underline{\mathbf{E}}(\mathbf{m}), \bar{\mathbf{E}}(\mathbf{m})]$, called the expected payoff interval for $\mathbf{m}$, is defined as:

$$324 \quad \underline{\mathbf{E}}(\mathbf{m}) = \sum_{A \subseteq \Theta} \mathbf{m}(A) \min A, \quad (6)$$

$$325 \quad \bar{\mathbf{E}}(\mathbf{m}) = \sum_{A \subseteq \Theta} \mathbf{m}(A) \max A. \quad (7)$$

326 Thus payoff mass functions can be used to represent ambiguous payoffs.

327 **Example 5.** In the airport scenario in Section 1, let pure strategy set $X = \{(\mathbf{PR}, \mathbf{PR})\}$,
 328 and the defender's payoff mass distribution $\{\mathbf{m}_{d,X}^{t_1}(\{5, 6\}) = 0.8, \mathbf{m}_{d,X}^{t_1}(\Theta^+) = 0.2\}$. Then the
 329 defender's expected payoff interval is $[\underline{\mathbf{E}}(\mathbf{m}_{d,X}^{t_1}), \bar{\mathbf{E}}(\mathbf{m}_{d,X}^{t_1})]$, where:

$$\begin{aligned}
 330 \quad & \underline{\mathbf{E}}(\mathbf{m}_{d,X}^{t_1}) = (0.8 \cdot 5) + (0.2 \cdot 0) = 4, \\
 331 \quad & \bar{\mathbf{E}}(\mathbf{m}_{d,X}^{t_1}) = (0.8 \cdot 6) + (0.2 \cdot 9) = 6.6.
 \end{aligned}$$

332 Now we turn to a mass function's ambiguity degree^{25,26}:

333 **Definition 5.** Let $\mathbf{m}$ be a mass function over Θ . Then a function $\delta_{\mathbf{m}} : 2^\Theta \rightarrow [0, 1]$, called
 334 an ambiguity degree with respect to $\mathbf{m}$, is defined as:

$$335 \quad \delta_{\mathbf{m}}(A) = \frac{\sum_{A \cap B \neq \emptyset} \mathbf{m}(B) \log_2 |B|}{\log_2 |\Theta|}. \quad (8)$$

336 **Example 6.** Given the mass function $\mathbf{m}^{(0.2)}$ from Example 4, we have:

$$\begin{aligned}
 337 \quad \delta_{\mathbf{m}^{(0.2)}}(\Theta) &= \frac{(\mathbf{m}^{(0.2)}(\{\text{car}\}) \log_2 |\{\text{car}\}|) + (\mathbf{m}^{(0.2)}(\Theta) \log_2 |\Theta|)}{\log_2 |\Theta|} \\
 338 &= \frac{(0.8 \times \log_2 1) + (0.2 \times \log_2 3)}{\log_2 3} \\
 339 &= 0.2.
 \end{aligned}$$

Class	Subclass	Description
C1 Ambiguous utility	C1a <i>Interval-valued</i> payoff	When a payoff value is imprecise
	C1b <i>Unreliable</i> payoff	When there is a reliability degree associated with a point/interval-valued payoff
	C1c <i>Absent</i> payoff	When a payoff is unknown or when no payoff is appropriate
C2 Ambiguous utility assignments		When some pure strategy profiles are closely related.

Table II. Classifications of ambiguity in security games.

The definition of $\delta_m(\Theta)$ is a normalised version of the generalised Hartley measure for non-specificity³⁰. Since $\log_2 |\Theta|$ is the same divisor for the ambiguity degree of any mass function over a frame of discernment Θ , it does not change the ordering from the generalised Hartley measure. Thus, the revised definition also satisfies additivity, subadditivity, normalization, symmetry, and branching³¹. Also, it can guarantee $\forall A \subseteq \Theta, \delta_m(A) \in [0, 1]$.

Using this ambiguity degree, along with the belief interval from Definition 2,^{25,26} define the notion of a point-valued belief degree as follows:

Definition 6. Let m be a mass function over Θ . Then a function $\eta_m : 2^\Theta \rightarrow [0, 1]$, called a point-valued belief degree with respect to m , is defined as:

$$\eta_m(A) = \frac{2\text{Bel}_m(A) + (1 - \delta_m(A))(\text{Pl}_m(A) - \text{Bel}_m(A))}{2}. \quad (9)$$

In the above definition, this ambiguity degree is used as a factor when determining point-valued belief degrees because smaller subsets are preferred because these subsets are less ambiguous.

Example 7. Given the mass function $m^{(0.2)}$ in Example 4, if $A = \{\text{classroom}\}$, we have:

$$\begin{aligned} \eta_{m^{(0.2)}}(A) &= \frac{2\text{Bel}_{m^{(0.2)}}(A) + (1 - \delta_{m^{(0.2)}}(A))(\text{Pl}_{m^{(0.2)}}(A) - \text{Bel}_{m^{(0.2)}}(A))}{2} \\ &= \frac{2(0.8) + (1 - 0.2)(1 - 0.8)}{2} \\ &= 0.88. \end{aligned}$$

3. MODELLING AMBIGUITY IN SECURITY GAMES

In Section 1, the major types of ambiguity in security games are identified and further clarified in Table II. This section will handle the four types of ambiguity **C1a**, **C1b**, **C1c** and **C2** in a single framework. In real security games, it is common for some or all of these classes of ambiguity to coexist.

Example 8. In the airport scenario, there are five security targets: **SA**, **PR**, **SL**, **VL**, and **H**. For each target, there are two possible states: defended or undefended. If a defended target is attacked, then the defender wins and the attacker loses. If an undefended target is attacked, then the attacker wins and the defender loses. payoffs for each player and each state have been obtained as shown in Table III(a). These can be directly translated into an standard security game as shown in Table III(b). Unfortunately, some of these payoffs are ambiguous. In most cases, each cell is a pair of payoffs for a singleton (unambiguous) set of pure strategy profiles. For example, the defender's payoff for the singleton set of pure strategy profiles $\{(\mathbf{PR}, \mathbf{SA})\}$ is the interval $[-7, -3]$. Unfortunately, some payoff are also ambiguous. For example, it assigns the defender's undefended payoff for the set of targets $\{\mathbf{VL}, \mathbf{H}\}$ to the ambiguous set of pure strategy profiles $\{(\mathbf{SA}, \mathbf{VL}), (\mathbf{SA}, \mathbf{H})\}$ because these

(a) Ambiguous payoffs obtained through knowledge acquisition.

Target(s)	Defended		Undefended	
	Defender	Attacker	Defender	Attacker
{SA}	[2, 6]	-7	[-7, -3]	5
{PR}	$\langle [5, 6], 0.8 \rangle$	-5	$\langle [-8, -7], 0.8 \rangle$	3
{SL}	null	-4	null	2
{VL, H}	7	-9	-8	7

(b) Full ambiguous payoff matrix where the defender is the row player and the attacker is the column player.

	SA	PR	SL	VL, H
SA	[2, 6]; -7	$\langle [-8, -7], 0.8 \rangle$; 3	null; 2	$\{(\text{SA}, \text{VL}), (\text{SA}, \text{H})\} \mapsto -8; 7$
PR	[-7, -3]; 5	$\langle [5, 6], 0.8 \rangle$; -5	null; 2	$\{(\text{PR}, \text{VL}), (\text{PR}, \text{H})\} \mapsto -8; 7$
SL	[-7, -3]; 5	$\langle [-8, -7], 0.8 \rangle$; 3	null; -4	$\{(\text{SL}, \text{VL}), (\text{SL}, \text{H})\} \mapsto -8; 7$
VL	[-7, -3]; 5	$\langle [-8, -7], 0.8 \rangle$; 3	null; 2	$\{(\text{VL}, \text{VL}), (\text{H}, \text{H})\} \mapsto 7; -9$
H	[-7, -3]; 5	$\langle [-8, -7], 0.8 \rangle$; 3	null; 2	$\{(\text{VL}, \text{H}), (\text{H}, \text{VL})\} \mapsto -8; 7$

Table III. Ambiguous security game for the airport scenario.

correspond to the pure strategy profiles in which **VL** and **H** are attacked when undefended. On the other hand, it assigns the defender's payoff for the set of targets $\{\text{VL}, \text{H}\}$ to the ambiguous set of pure strategy profiles $\{(\text{VL}, \text{VL}), (\text{H}, \text{H})\}$ because these correspond to the pure strategy profiles in which **VL** and **H** are attacked when defended.

In order to handle each type of ambiguity in a unified framework, it first needs to interpret them in the same mathematical theory. Thus, D-S theory is deployed to provide a formal definition of an ambiguous security game as follows:

Definition 7. An ambiguous security game is an 8-tuple $(N, T, \mathbf{p}, A, \Psi, \Theta, M, U)$, where:

- (i) $N, T, \mathbf{p}, A$ and Ψ are as in traditional security games (refer to Definition 1);
- (ii) $\Theta = \{\Theta_i^+ \mid i \in N\} \cup \{\Theta_i^- \mid i \in N\}$, where Θ_i^+ and Θ_i^- are finite positive and negative number sets, which means all possible positive payoffs and negative payoffs for player i , respectively;
- (iii) $M = \{M_i \mid M_i = M_i^+ \cup M_i^-, i \in N\}$, where M_i^+ and M_i^- are sets of payoff mass functions over Θ_i^+ and Θ_i^- , respectively, for player i ; and
- (iv) $U = \{u_i^t \mid t \in T, i \in N\}$ is the set of payoff functions, where $u_i^t : [\Psi]^t \rightarrow M_i$ is a payoff function for player i and attacker of type t over a partition $[\Psi]^t$ of Ψ for t .[‡]

To avoid repetition of notations, some notations are defined, which will be referred to for the rest of this paper. Let $i \in N$ be a player. Let $t \in T$ be a type of attacker. Let $X \in [\Psi]^t$ be a set of pure strategy profiles for t . Let $u_i^t(X) = m_{i,X}^t$ be a payoff mass function for X with respect to i and t over $\Theta_i^\circ \in \{\Theta_i^+, \Theta_i^-\}$.

In general, simple payoff mass functions (see Section 2.2) are sufficient for modelling most intuitive types of ambiguous payoff, (e.g., **C1a**, **C1b**, and **C1c** all correspond to simple payoff mass functions). Also, the focal elements of payoff mass functions in our framework always are consecutive sets of point-valued payoffs. However, it does not impose any restrictions on the types of payoff mass functions that can be used to model ambiguous payoffs and thus our framework can handle arbitrary payoff mass functions. With regards to ambiguous payoff

[‡]Let $S_1, \dots, S_n \subseteq S$ and $[S] = \{S_1, \dots, S_n\}$ be a set of sets representing a partition of S such that: (i) $\emptyset \notin [S]$; (ii) $S_1 \cup \dots \cup S_n = S$; and (iii) $\forall S_i, S_j \in [S]$ such that $S_i \neq S_j, S_i \cap S_j = \emptyset$.

assignments, the meaning of the partition $[\Psi]^t$ is that payoffs should only be assigned to distinct subsets of Ψ for a given attacker type t . Namely, no two subsets of Ψ should consider the same pure strategy profile in a single payoff assignment for t . This restriction ensures that the ambiguous security games do not encounter inconsistent payoff assignments. However, the superscript in $[\Psi]^t$ means that it allows different partitions of Ψ for different attacker types.[§]

Clearly, the fundamental differences between ambiguous security games (see Definition 7) and traditional ones (see Definition 1) relate to their payoff functions $u_i^t : [\Psi]^t \rightarrow M_i$ and $u_i^t : \Psi \rightarrow \mathbb{R}$. These definitions highlight two important differences. Firstly, each payoff function is defined as a mapping to a set of payoff mass functions rather than the set of real numbers. Secondly, payoffs are assigned to subsets of the set of pure strategy profiles rather than to elements in the set of pure strategy profiles, *i.e.*, $X \in [\Psi]^t$ rather than $\psi \in \Psi$.

Evidently, the payoff functions require us to interpret all payoffs as payoff mass functions. For interval-valued payoff, the ignorance of player i over interval $[x, y]$ can be represented by a payoff mass function $m_{i,X}^t$ such that $m_{i,X}^t(\{x, \dots, y\}) = 1$. This indicates that the player knows the payoff is in-between x and y , but cannot determine the precise payoff. A unreliable payoff can then be represented as discounted payoff mass functions. For example, if interval $[x, y]$ has a reliability of 80%, then this can be represented by the discounted payoff mass function $m_{i,X}^{t,(0.2)}$.

An assumption of security games is that, for any pure strategy profile, either the defender *wins* and the attacker *loses* (in case that they choose the same target) or the attacker *wins* and the defender *loses* (in case that they choose the different targets). Thus, regardless of whether a suitable payoff is actually assigned, the result of any pure strategy profile for a player is always either positive or negative. Therefore, although the absent payoff indicates a payoff is unknown or no payoff is appropriate, the defender still knows at least it is positive or negative payoff by considering the strategy selected by each player. Thus, there are two types of absent payoffs: positive absent payoffs and negative absent payoffs. Since positive payoffs for player i are defined over Θ_i^+ and negative payoffs are defined over Θ_i^- , it follows that positive absent payoffs can be represented by a payoff mass function $m_{i,X}^t$ such that $m_{i,X}^t(\Theta_i^+) = 1$ and negative absent payoffs can be represented by $m_{i,X}^t$ such that $m_{i,X}^t(\Theta_i^-) = 1$.

In summary, by Definition 7, the ambiguity types **C1a**, **C1b**, **C1c**, and **C2** can be model by the ambiguous security game as shown by the following proposition.

Proposition 1. *An ambiguous security game can model the ambiguity types **C1a**, **C1b**, **C1c**, and **C2**.*

Proof

An ambiguous security game is affected by a given class of ambiguity if there exists a player i , an attacker type t , a set of pure strategy profiles $X \in [\Psi]^t$ and payoff mass function $m_{i,X}^t$ for X with respect to i and t over Θ_i° , where

C1a: $m_{i,X}^t(B)=1$ such that $B \subset \Theta_i^\circ$ and $\forall x \in \Theta_i^\circ$, if $\min B \leq x \leq \max B$, then $x \in B$;

C1b: $m_{i,X}^t(\Theta_i^\circ) = \tau$ and $\exists B \subset \Theta_i^\circ$ such that $m_{i,X}^t(B) = 1 - \tau$, where $0 < \tau < 1$ is a discount factor;

C1c: $m_{i,X}^t(\Theta_i^\circ) = 1$; and

C2: $|X| > 1$. □

Example 9. *In the airport scenario, an ambiguous security game can be constructed, where $T = \{t_1\}$, $p(t_1) = 1$, $A_d = A_a = \{SA, PR, SL, VL, H\}$, $\Theta_d^- = \Theta_a^- = \{-9, \dots, 0\}$,*

[§]In other words, given two attacker types t_1 and t_2 such that $t_1 \neq t_2$, the payoffs for t_1 may be affected by **C2** while the payoffs for t_2 may not.

	SA	PR	SL	VL, H
SA	$\{m(\{2, \dots, 6\}) = 1\};$ $\{m(\{-7\}) = 1\}$	$\{m(\{-8, -7\}) = 0.8,$ $m(\Theta^-) = 0.2\};$ $\{m(\{3\}) = 1\}$	$\{m(\Theta^-) = 1\};$ $\{m(\{2\}) = 1\}$	$\{(\mathbf{SA}, \mathbf{VL}), (\mathbf{SA}, \mathbf{H})\}$ $\mapsto \{m(\{-8\}) = 1\};$ $m(\{7\}) = 1\}$
PR	$\{m(\{-7, \dots, -3\}) = 1\};$ $\{m(\{5\}) = 1\}$	$\{m(\{5, 6\}) = 0.8,$ $m(\Theta^+) = 0.2\};$ $\{m(\{-5\}) = 1\}$	$\{m(\Theta^-) = 1\};$ $\{m(\{2\}) = 1\}$	$\{(\mathbf{PR}, \mathbf{VL}), (\mathbf{PR}, \mathbf{H})\}$ $\mapsto \{m(\{-8\}) = 1\};$ $\{m(\{7\}) = 1\}$
SL	$\{m(\{-7, \dots, -3\}) = 1\};$ $\{m(\{5\}) = 1\}$	$\{m(\{-8, -7\}) = 0.8,$ $m(\Theta^-) = 0.2\};$ $\{m(\{3\}) = 1\}$	$\{m(\Theta^+) = 1\};$ $\{m(\{-4\}) = 1\}$	$\{(\mathbf{SL}, \mathbf{VL}), (\mathbf{SL}, \mathbf{H})\}$ $\mapsto \{m(\{-8\}) = 1\};$ $\{m(\{7\}) = 1\}$
VL	$\{m(\{-7, \dots, -3\}) = 1\};$ $\{m(\{5\}) = 1\}$	$\{m(\{-8, -7\}) = 0.8,$ $m(\Theta^-) = 0.2\};$ $\{m(\{3\}) = 1\}$	$\{m(\Theta^-) = 1\};$ $\{m(\{2\}) = 1\}$	$\{(\mathbf{VL}, \mathbf{VL}), (\mathbf{H}, \mathbf{H})\}$ $\mapsto \{m(\{7\}) = 1\};$ $\{m(\{-9\}) = 1\}$
H	$\{m(\{-7, \dots, -3\}) = 1\};$ $\{m(\{5\}) = 1\}$	$\{m(\{-8, -7\}) = 0.8,$ $m(\Theta^-) = 0.2\};$ $\{m(\{3\}) = 1\}$	$\{m(\Theta^-) = 1\};$ $\{m(\{2\}) = 1\}$	$\{(\mathbf{VL}, \mathbf{H}), (\mathbf{H}, \mathbf{VL})\}$ $\mapsto \{m(\{-8\}) = 1\};$ $\{m(\{7\}) = 1\}$

Table IV. Matrix of payoff mass function pair $\{u_d^{t_1}(X); u_a^{t_1}(X)\}$.

442 $\Theta_d^+ = \Theta_a^+ = \{0, \dots, 9\}$, and $U = \{u_d^{t_1}, u_a^{t_1}\}$ such that $u_d^{t_1}$ and $u_a^{t_1}$ are as shown in Table IV.
 443 Firstly, the defender's payoff for pure strategy profile $(\mathbf{PR}, \mathbf{SA})$ demonstrates ambiguity
 444 type **C1a**. Secondly, the defender's payoff for pure strategy profile $(\mathbf{PR}, \mathbf{PR})$ demonstrates
 445 **C1b**. Thirdly, the defender's payoff for pure strategy profile $(\mathbf{PR}, \mathbf{SL})$ demonstrates **C1c**.
 446 Finally, the payoffs for pure strategy profiles $(\mathbf{PR}, \mathbf{VL})$ and $(\mathbf{PR}, \mathbf{H})$ demonstrates **C2**.
 447 With regards to partition $[\Psi]^t$, if sets $\{(\mathbf{PR}, \mathbf{VL}), (\mathbf{PR}, \mathbf{H})\}$ and $\{(\mathbf{PR}, \mathbf{VL}), (\mathbf{PR}, \mathbf{SL})\}$
 448 both are assigned payoffs, then our judgements may be inconsistent since pure strategy profile
 449 $(\mathbf{PR}, \mathbf{VL})$ is included in both sets. More specifically, $\{(\mathbf{PR}, \mathbf{VL}), (\mathbf{PR}, \mathbf{H})\}$ means that the
 450 defender cannot distinguish between the payoffs for $(\mathbf{PR}, \mathbf{VL})$ and $(\mathbf{PR}, \mathbf{H})$ but the defender
 451 can do from $(\mathbf{PR}, \mathbf{SL})$. On the other hand, $\{(\mathbf{PR}, \mathbf{VL}), (\mathbf{PR}, \mathbf{SL})\}$ means that the defender
 452 cannot distinguish the payoffs for $(\mathbf{PR}, \mathbf{VL})$ and $(\mathbf{PR}, \mathbf{SL})$ but the defender can do from
 453 $(\mathbf{PR}, \mathbf{H})$. In addition, partition $[\Psi]^t$ must satisfy that $\forall X \in [\Psi]^t$, either the defender wins
 454 and the attacker loses for each $\psi \in X$ or the attacker wins and the defender loses for each
 455 $\psi \in X$. For example, $\{(\mathbf{VL}, \mathbf{VL}), (\mathbf{PR}, \mathbf{H})\}$ is an invalid element in a partition because the
 456 defender wins in $(\mathbf{VL}, \mathbf{VL})$ and thus requires a positive payoff, while the defender loses in
 457 $(\mathbf{PR}, \mathbf{H})$ and thus requires a negative payoff.

458 **Proposition 2.** Ambiguous security games can model traditional ones.

459 *Proof*

460 An ambiguous security game models a traditional security game if, for each player $i \in N$, each
 461 attacker type $t \in T$, each set of pure strategy profiles $X \in [\Psi]^t$, and each payoff mass function
 462 $m_{i,X}^t$ over Θ_i° , we have that $|X| = 1$ and $\exists h \in \Theta_i^\circ$ such that $m_{i,X}^t(\{h\}) = 1$. In this case, since
 463 h is a real number, it is possible to interpret $m_{i,X}^t$ such that h is the point-valued payoff of X .
 464 By the assumption that $X = \{\psi\}$ for some pure strategy profile $\psi \in \Psi$, it is also possible to
 465 interpret h as the point-valued payoff for ψ . $\square$

4. GENERAL FRAMEWORK FOR AMBIGUOUS SECURITY GAMES

466 This section will present a general ambiguity-tolerant framework for handling ambiguous
 467 security games. Specifically, this paper transforms these ambiguous security games into
 468 traditional ones so that some well established methods^{5,32,33} can be used for deriving the
 469 optimal allocation strategy for the defender. More specifically, this section first introduces the
 470 notion of a projected point-valued payoff function which transforms the ambiguous payoffs of
 471 types **C1a**, **C1b**, and **C1c** into point values for sets of pure strategy profiles. Then ambiguous
 472 payoff assignments **C2** and complete ignorance (caused by **C1c**) are handled by constructing

a mass distribution for each player using these new point values. Finally, a traditional payoff matrix is determined from these new mass distributions.

4.1. Framework Definition

In order to use our general ambiguity-tolerant framework to solve ambiguous security games, three basic assumptions should be adopted:

- A1:** Each player considers the payoff for a subset of pure strategy profiles in relation to the payoffs for other subsets of pure strategy profiles.
- A2:** Each player maximises their expected payoffs relative to their subjective priorities.
- A3:** A negative absent payoff is not preferred to any other payoff.

Namely, **A1** states that if a player believes they cannot get an expected payoff lower than the worst payoff in the game, they only need to consider how well the given set of pure strategy profiles perform against the worst performing set of pure strategy profiles. **A2** means the player is rational. **A3** means that, to encourage caution, players regards the negative absent payoff as the worst possible payoff in the game.

A fundamental component in our framework is the notion of a projected point-valued payoff function. This function is used to transform a set of payoffs, represented as payoff mass functions, into a set of point payoffs. Formally, we have:

Definition 8. Let M be a set of payoff mass functions. Then a function $\text{Proj} : M \rightarrow \mathbb{R}$ is called a projected point-valued payoff function if $\forall \mathbf{m}_1, \mathbf{m}_2 \in M$, if it satisfies:

- (i) **Boundary:** $\text{Proj}(\mathbf{m}_1) \in \text{EUI}(\mathbf{m}_1)$,
 - (ii) **Preference:** if $\text{Proj}(\mathbf{m}_1) \geq \text{Proj}(\mathbf{m}_2)$ then $\mathbf{m}_1$ is at least as preferable as $\mathbf{m}_2$,
- where $\text{Proj}(\mathbf{m}_1)$ is interpreted as an expected point-valued payoff with respect to $\mathbf{m}_1$.

We have that if $\exists h \in \Theta$ such that $\mathbf{m}(\{h\}) = 1$ then $\text{EUI}(\mathbf{m}) = [h, h]$ and thus $\text{Proj}(\mathbf{m}) = h$ since the **Boundary** condition requires that $\text{Proj}(\mathbf{m}) \in \text{EUI}(\mathbf{m})$. With regards to assumption **A3**, if our model can support the modelling of complete ignorance, then a projected point-valued payoff function satisfying the following optional property is needed:

- (iii) **Conservative Estimation:** $\text{Proj}(\mathbf{m}) = \min \Theta$ if Θ is the frame of $\mathbf{m}$ and $\mathbf{m}(\Theta) = 1$.

Note that if an ambiguous security game does not contain absent payoffs, then this property is not required from the projected point-valued payoff function.

Our framework must be instantiated with a particular projected point-valued payoff function before it can be applied to an ambiguous security game. For an instantiated Proj function, it is also desirable that the lower and upper bounds of each expected payoff interval are interpreted in a uniform way (*i.e.*, using the same coefficient):

- (iv) **Uniform Convex Combination:** $\text{Proj}(\mathbf{m}) = \alpha \underline{\text{E}}(\mathbf{m}) + (1 - \alpha) \bar{\text{E}}(\mathbf{m})$ ($\alpha \in [0, 1]$).

There are actually numerous projected point-valued payoff functions can be proposed. For example, $\text{Proj}(\mathbf{m}) = \underline{\text{E}}(\mathbf{m})$ is the worst-case (*pessimistic* attitude toward ambiguity) projected point-valued payoff function, while $\text{Proj}(\mathbf{m}) = \bar{\text{E}}(\mathbf{m})$ is the best-case (*optimistic* attitude toward ambiguity) one. In order to explore the importance of this function in our framework, Section 5 will propose one based on the ambiguity-aversion principle of minimax regret^{25,26}, while some other possibilities inspired by different rules in the literature on decision theory^{34,24,35,36} will be considered as well. Finally, Section 6 will experimentally evaluate these functions in order to understand the advantages of each when applied to an ambiguous security game. However, for the remainder of this section, this paper will assume that such a function exists.

The **Preference** property reveals the essence of the value obtained by a projected point-valued payoff function. Specifically, this value is an interpretation of an ambiguous payoff,

which reflects a player's preference over the corresponding subset of pure strategy profiles. Hence, **Preference** implies that such a function identifies a preference ordering over strategies. Formally, we have:

Definition 9. A total order over $[\Psi]^t$, denoted $\succeq_{i,\text{Proj}}^t$ and called a **Proj** ordering for i and t , is defined as:

$$X_1 \succeq_{i,\text{Proj}}^t X_2 \Leftrightarrow \text{Proj}(\mathbf{m}_{i,X_1}^t) \geq \text{Proj}(\mathbf{m}_{i,X_2}^t). \quad (10)$$

Moreover, $X_1 \sim_{i,\text{Proj}}^t X_2$ if $X_1 \succeq_{i,\text{Proj}}^t X_2$ and $X_2 \succeq_{i,\text{Proj}}^t X_1$. Also, $X_1 \succ_{i,\text{Proj}}^t X_2$ if $X_1 \succeq_{i,\text{Proj}}^t X_2$ and $X_2 \not\succeq_{i,\text{Proj}}^t X_1$. Thus, X_1 and X_2 are equally preferred if $X_1 \sim_{i,\text{Proj}}^t X_2$ and X_1 is strictly preferred to X_2 if $X_1 \succ_{i,\text{Proj}}^t X_2$.

Using a projected point-valued payoff function, each ambiguous payoff in an ambiguous security game can be interpreted as a point-value. As such, it allows us to compare sets of pure strategy profiles with respect to their ambiguous payoffs. Moreover, two concepts related to projected point-valued payoff functions can also be defined: (i) the worst (*i.e.*, the lowest) projected point-valued utility for a player in an ambiguous security game, and (ii) the relative payoff which describes the distance between the projected point-valued payoff of a set of pure strategy profiles for a player and type of attacker with respect to the worst projected point-valued payoff for that player. Formally, we have:

Definition 10. A projected point-valued payoff $\text{Proj}(\mathbf{m}_{i,X^w}^{t^w})$ with respect to $t^w \in T$ and $X^w \in [\Psi]^{t^w}$ is called the worst **Proj** projected one for i if and only if

$$\forall t \in T, \forall X \in [\Psi]^t, \text{Proj}(\mathbf{m}_{i,X^w}^{t^w}) \leq \text{Proj}(\mathbf{m}_{i,X}^t). \quad (11)$$

Definition 11. For i and t , a relative payoff function $\mathbf{d}_i^t : [\Psi]^t \rightarrow \mathbb{R}$ is defined as:

$$\mathbf{d}_i^t(X) = \text{Proj}(\mathbf{m}_{i,X}^t) - \text{Proj}(\mathbf{m}_{i,X^w}^{t^w}). \quad (12)$$

Clearly, it is always the case that $\mathbf{d}_i^t(X) \geq 0$. Note that, since **Proj** is fixed for an ambiguous security game, for simplicity it will be omitted from subsequent notation.

If there are no absent payoffs or ambiguous payoff assignments, then after every $\mathbf{m}_{i,X}^t$ is projected into a point-valued utility using **Proj**, an ambiguous game becomes a traditional security game and thus the solution concept of the traditional one can be applied. However, when either absent payoffs or ambiguous payoff assignments appear, additional steps need to be taken to handle such ambiguity.

The value of $\text{Proj}(\mathbf{m}_{i,X}^t)$ indicates reward or penalty when X is played. When X has an absent payoff (**C1c**), the value of $\text{Proj}(\mathbf{m}_{i,X}^t)$ for X may be far from the real value. So, instead of *guessing* a point-valued payoff projected in this case, this problem is shifted to the set of pure strategy profiles Ψ by using $\text{Proj}(\mathbf{m}_{i,X'}^t)$ (or more precisely $\mathbf{d}_i^t(X')$) to work out what these values imply in terms of relative *preference* of their respective sets of profiles X .[¶] To determine the relative preference of each pure strategy $\psi \in \Psi$, first a mass function $\mathbf{m}$ over $T \times \Psi$ is constructed (*i.e.*, formulas (13) and (14)), and then the relative preference (an actual value) for each ψ is obtained after transforming and manipulating this $\mathbf{m}$ in a number of steps (see Definitions 5-13). Similarly when there are ambiguous payoff assignments (**C2**), the same method can be used to define a mass function $\mathbf{m}$ over $T \times \Psi$ (see Definition 12) and again generate a relative preference for every ψ (see Definitions 5-13).

Definition 12. A function $\mathbf{m}_i : 2^{T \times \Psi} \rightarrow [0, 1]$ is a mass function for i over $T \times \Psi$.

[¶]Here, we want to derive a value for each $\psi \in \Psi$ which could be interpreted as a mirror image of a point-valued payoff for ψ , had this value existed.

(i) **Absent payoffs:** If there exists $t_k \in T$ and $X_k \in [\Psi]^{t_k}$ such that $\mathbf{m}_{i,X_k}^{t_k}(\Theta_i^\circ) = 1$, then $\mathbf{m}_i$ for a pure strategy profiles subset X of an attacker type t is defined as:

$$\mathbf{m}_i(\{t\} \times X) = \frac{\mathbf{d}_i^t(X)}{\sum_{t_k \in T} \sum_{X_k \in [\Psi]^{t_k}} \mathbf{d}_i^{t_k}(X_k) + \sqrt{n}}, \quad (13)$$

where $n = \sum_{t_k \in T} |\{X_k \mid X_k \in [\Psi]^{t_k} \wedge \mathbf{d}_i^{t_k}(X_k) \neq 0\}|$. Moreover, $\mathbf{m}_i(T \times \Psi)$ is defined for the mass value of the frame $T \times \Psi$ as:

$$\mathbf{m}_i(T \times \Psi) = \frac{\sqrt{n}}{\sum_{t_k \in T} \sum_{X_k \in [\Psi]^{t_k}} \mathbf{d}_i^{t_k}(X_k) + \sqrt{n}}. \quad (14)$$

(ii) **No absent payoffs:** If there does not exist $t_k \in T$ and $X_k \in [\Psi]^{t_k}$ such that $\mathbf{m}_{i,X_k}^{t_k}(\Theta_i^\circ) = 1$, then $\mathbf{m}_i$ for a pure strategy profiles subset X of an attacker type t is defined as:

$$\mathbf{m}_i(\{t\} \times X) = \frac{\mathbf{d}_i^t(X)}{\sum_{t_k \in T} \sum_{X_k \in [\Psi]^{t_k}} \mathbf{d}_i^{t_k}(X_k)}. \quad (15)$$

Formulas (13)-(15) are game-theoretical variants of the comparison rules from our another paper³⁷. Intuitively, in a game without absent payoffs, there is some evidence for all the payoffs. Therefore, the worst projected point-valued payoff is based on some evidence. However, given an absent payoff where a player is completely ignorant, the worst projected point-valued payoff must be obtained by a subjective judgement on the boundary of the payoffs. In other words, there is some degree of uncertainty over the result of an absent payoff (*e.g.*, the payoff might be worse than the lower bound of the values). Hence, the player still needs to express their uncertainty in this situation in order to model their preference over the set of pure strategy profiles. Definition 12 is applied in order to derive a mass function for each player in this way.

To begin making use of these new mass functions for deriving traditional payoffs, first the ambiguity degree of each mass function for each player i over $T \times \Psi$ obtained by Definition 5 will be considered. Then by the ambiguity degree of each mass function in Definition 12, along with the belief interval (see Definition 2), the point-valued belief degree for each player i over $T \times \Psi$ can be obtained by Definition 6.

Finally, given a player i , attacker type set T , the set of all pure strategy profiles Ψ , and the mass function $\mathbf{m}_i$ for i over a joint frame $T \times \Psi$, by Definition 2 the belief interval $[\text{Bel}_{\mathbf{m}_i}(\{t\} \times X), \text{Pl}_{\mathbf{m}_i}(\{t\} \times X)]$ for any attacker type $t \in T$ and any set of pure strategy profiles $X \in [\Psi]^t$ can be obtained. Next, by Definition 5, the ambiguity degree for $\{t\} \times X$ can be obtained. By Definition 6, then the point-valued belief degree for $\{t\} \times X$ can be obtained. This point-valued belief degree actually allows us to derive the traditional point-valued payoff for each pure strategy profile directly:

Definition 13. A function $\text{Tr}_i^t : \Psi \rightarrow [0, 1]$ is a traditional payoff for i and t if

$$\text{Tr}_i^t(\psi) = \eta_{\mathbf{m}_i}(\{t\} \times \{\psi\}). \quad (16)$$

At this point a traditional security game is obtained and thus some well-established methods can be employed for finding the defender's optimal mixed strategy.

4.2. Framework Procedure

This section will present the procedure for finding the defender's optimal mixed strategy for an ambiguous security game. This procedure starts with initial information describing the

Figure 1. Framework procedure for handling ambiguous security games.

win/lose payoffs for sets of targets with respect to each player and each type of attacker as well as a probability distribution over the set of attacker types (*e.g.*, Table III(a)). This information may include imprecise, unreliable or absent payoffs, and ambiguous payoff assignments (*e.g.*, Table III(b)). The procedure must then translate all the payoffs into payoff mass functions for sets of pure strategy profiles (*e.g.*, Table IV). This information now constitutes an ambiguous security game and represents the basic input for our framework. Table V summarises our notations.

Figure 1 shows the complete procedure, where:

Step 1: For each player $i \in N$, each attacker type $t \in T$, and each set of pure strategy profiles $X \in [\Psi]^t$, obtain projected point-valued payoff $\text{Proj}(m_{i,X}^t)$ as described in Definition 8.

Step 2: For each player $i \in N$, each attacker type $t \in T$, and each set of pure strategy profiles $X \in [\Psi]^t$, determine relative payoff $d_i^t(X)$ between the projected point-valued

Notation	Description
N	Set of players
$i \in N$	Player
T	Set of attacker types
$t \in T$	Attacker type
Ψ	Set of all pure strategy profiles
$\psi = (s_d, s_a) \in \Psi$	Pure strategy profile
$[\Psi]^t$	Partition of Ψ for t
$X \in [\Psi]^t$	Set of pure strategy profiles
Θ_i^+ (resp. Θ_i^-)	Set of positive (resp. negative) point-valued payoffs for i
$\mathbf{m}_{i,X}^t$	payoff mass function over $\Theta_i^\circ \in \{\Theta_i^+, \Theta_i^-\}$ for X with respect to i and t
$\text{Proj}(\mathbf{m}_{i,X}^t)$	Projected point-valued payoff of $\mathbf{m}_{i,X}^t$
$\sum_{t^w} \text{Proj}$	Proj transformation rule with respect to i and t
$\text{Proj}(\mathbf{m}_{i,X^w})$	Worst projected point-valued payoff for i
$\mathbf{d}_i^t(X)$	Relative payoff of X with respect to i and t
$\mathbf{m}_i$	Mass function over $T \times \Psi$ for i
$\text{Bel}_{\mathbf{m}_i}(\{t\} \times X)$	Belief of $\{t\} \times X$ with respect to $\mathbf{m}_i$
$\text{Pl}_{\mathbf{m}_i}(\{t\} \times X)$	Plausibility of $\{t\} \times X$ with respect to $\mathbf{m}_i$
$\delta_{\mathbf{m}_i}(\{t\} \times X)$	Ambiguity degree of $\{t\} \times X$ with respect to $\mathbf{m}_i$
$\eta_{\mathbf{m}_i}(\{t\} \times X)$	point-valued belief degree of $\{t\} \times X$ with respect to $\mathbf{m}_i$
$\text{Tr}_i^t(\psi)$	Traditional point-valued payoff for ψ with respect to i and t

Table V. Summary of notation for the general ambiguity-tolerant framework.

609 payoff $\text{Proj}(\mathbf{m}_{i,X}^t)$ and the worst projected point-valued payoff $\text{Proj}(\mathbf{m}_{i,X^w}^{t^w})$ for i by
 610 Definitions 10 and 11.

611 **Step 3:** For each player $i \in N$, construct mass function $\mathbf{m}_i$ by using formulas (13) and (14)
 612 if the game has absent payoffs or formula (15), otherwise.

613 **Step 4:** For each player $i \in N$, each attacker type $t \in T$, and each pure strategy profile $\psi \in \Psi$,
 614 obtain traditional point-valued payoff $\text{Tr}_i^t(\psi) = \eta_{\mathbf{m}_i}(\{t\} \times \{\psi\})$ from mass function $\mathbf{m}_i$
 615 by Definitions 6 and 13, *i.e.*, using belief interval $[\text{Bel}_{\mathbf{m}_i}(\{t\} \times \{\psi\}), \text{Pl}_{\mathbf{m}_i}(\{t\} \times \{\psi\})]$
 616 from Definition 2 and ambiguity degree $\delta_{\mathbf{m}_i}(\{t\} \times \{\psi\})$ from Definition 5.

617 **Step 5:** Use an existing SSE solver of security games to find the optimal mixed strategy for
 618 the defender.

619 In Step 1, a security team can select different projected point-valued payoff functions for
 620 their specific application with ambiguous information. For example, if some loss is unaffordable
 621 (*e.g.*, the loss of life), they may consider the worst case outcome with respect to ambiguous
 622 information and accordingly adopt the minimum acceptable expected payoff. This reflects
 623 a pessimistic attitude to ambiguity, comparable to the Γ -maximin approach²⁴. On the other
 624 hand, if a security team prefers to minimise regret, then they may adopt the ambiguity-aversion
 625 principle of minimax regret^{25,26}. If a security team thinks that all the possible payoffs should be
 626 equally considered (a principle of indifference), they may adopt the Transferable Belief Model
 627 (TBM)³⁵. Step 2 is to transform all the payoffs into positive numbers in order to obtain the
 628 mass values in the following step. This is justified by assumption **A1**: each player considers
 629 the relative expected payoff for the subset of pure strategy profiles. As to Step 3, a method is
 630 needed to assign a mass value to each subset of pure strategy profiles. In fact, the mass value
 631 based on $\mathbf{d}_i^t(X)$ represents the possibility that a subset of pure strategy profiles contains the
 632 most favorable outcome which can be achieved by the player i .

633 4.3. Framework Properties

634 This subsection will examine properties of our ambiguity-tolerant framework. First the effect
 635 of applying our framework to a traditional security game is considered:

Theorem 1 (Subsumption of traditional security games). *SSE and NE of a traditional security game is the same by using our framework or the traditional one.*

Proof

By Definition 7 and Proposition 2, the payoff function in a traditional security game $u_i^t : \Psi \rightarrow \mathbb{R}$ can be rewritten as $u_i^t : [\Psi]^t \rightarrow M$, where for each player $i \in N$, each attacker type $t \in T$, and each set of pure strategy profiles $X \in [\Psi]^t$, we have that $|X| = 1$ and $m_{i,X}^t(\{k_j\}) = 1$ such that $k_j \in \Theta_i$. Consequently, the projected point-valued payoff $\text{Proj}(u_i^t(X)) = k_j$ is obtained, where $u_i^t(X) = m_{i,X}^t$ and $\text{EUI}(m_{i,X}^t) = [k_j, k_j]$, since the **Boundary** property requires that $\text{Proj}(m_{i,X}^t) \in \text{EUI}(m_{i,X}^t)$.

Suppose the worst Proj projected point-valued payoff for a player is d . Since there is no any absent payoff in a traditional security game, formula (15) can be applied to obtain the mass function for each player i as follows:

$$m_i(\{t\} \times X) = \frac{k_j - d}{\sum_{i=1}^n (k_i - d)}.$$

As a result, by Definition 2, formulas (8) and (9), the point-valued belief degree of X with respect to t can be obtained as follows:

$$\eta_{m_i}(\{t\} \times X) = \frac{k_j - d}{\sum_{i=1}^n (k_i - d)}.$$

Thus, for the defender, there exists a positive real number $\frac{1}{\sum_{i=1}^n (k_i - d)}$ and a real number $-\frac{d}{\sum_{i=1}^n (k_i - d)}$ with respect to each type of attacker such that

$$\eta_{m_i}(\{t\} \times X) = \frac{1}{\sum_{i=1}^n (k_i - d)} \text{Proj}(u_i^t(X)) - \frac{d}{\sum_{i=1}^n (k_i - d)}$$

for all singleton sets of pure strategy profiles $X \in [\Psi]^t$. Then the Harsanyi Transformation³⁸ can be applied to convert the game into a traditional security game. According to the Weibull's proof³⁹, it is easily to prove the two games $G_1 = (N, A, u)$ and $G_2 = (N, A, \eta)$ have the same best response correspondences and dominance relations between strategies. So the set of NE is invariant.

Finally, it just needs to prove that our framework does not change the magnitude relation of the payoffs for traditional security games. That is, for a pure strategy profile $(s_d, \text{RE}(s_1))$ (s_1 is a pure strategy of the defender and $\text{RE}_1(s_1)$ is a response strategy of the attacker to s_1), for any $k_i \in \mathbb{R}^+$, $b_i \in \mathbb{R}$, and player $i \in N$, we have:

- (i) If $\text{Proj}(u_d^t(\{(s_1, \text{RE}_1(s_1))\})) \geq \text{Proj}(u_d^t(\{(s_j, \text{RE}_1(s_j))\}))$ for all other pure strategies s_j of the defender, then

$$k_d \text{Proj}(u_d^t(\{(s_1, \text{RE}_1(s_1))\})) + b_d \geq k_d \text{Proj}(u_d^t(\{(s_j, \text{RE}_1(s_j))\})) + b_d.$$

Thus, the defender still plays a best-response.

- (ii) If $\text{Proj}(u_a^t(\{(s_1, \text{RE}_1(s_1))\})) \geq \text{Proj}(u_a^t(\{(s_1, \text{RE}_j(s_1))\}))$ for all other response strategies $\text{RE}_j(s_1)$ of the attacker, then

$$k_a \text{Proj}(u_a^t(\{(s_1, \text{RE}_1(s_1))\})) + b_a \geq k_a \text{Proj}(u_a^t(\{(s_1, \text{RE}_j(s_1))\})) + b_a.$$

Thus, the attacker still plays a best-response.

- (iii) If $\text{Proj}(u_d^t(\{(s_1, \text{RE}_1(s_1))\})) \geq \text{Proj}(u_d^t(\{(s_1, \tau(s_1))\}))$, where $\tau(s_1)$ is a pure strategy from the set of attacker best-responses to s_1 , then

$$k_d \text{Proj}(u_d^t(\{(s_1, \text{RE}_1(s_1))\})) + b_d \geq k_d \text{Proj}(u_d^t(\{(s_1, \tau(s_1))\})) + b_d.$$

Thus, the attacker still breaks ties optimally for the defender.

676 According to SSE⁴⁰, $\frac{1}{\sum_{i=1}^n (k_i - d)} > 0$, and $-\frac{d}{\sum_{i=1}^n (k_i - d)} \in \mathbb{R}$, the set of SSE is invariant with
 677 respect to these transformations. $\square$

678 Theorem 1 ensures that when applying our framework to a traditional security game, the
 679 same optimal mixed strategy for the defender can be found as the game solved directly. So our
 680 framework is also applicable to traditional security games. Further, if an ambiguous security
 681 game does not involve **C1c** and **C2**, then this theorem implies that the projected point-valued
 682 payoffs constitute traditional payoffs. Thus, in this case, it is unnecessary to execute Steps 2-4
 683 of our framework and this is indicated by the dotted line in Figure 1. However, to simplify our
 684 discussions, in the rest of this paper it assumes that these steps are always executed.

685 As pointed out in Section 1, most existing studies on security games assume that all the
 686 players have a point-valued payoff for each pure strategy profile. However, in reality, experts
 687 or data analysers must estimate these values in complex domains involving large numbers of
 688 uncontrollable and unpredictable factors. Thus, it is reasonable to assume that the real values
 689 are within a certain some range. A security team may then ask the question: under what
 690 condition does the defender's optimal mixed strategy remain the same if the point-valued
 691 payoffs have a range of deviation?

692 This question can be answered by the following theorem:

693 **Theorem 2** (Uniform margin of error). *Let $G_1 = (N, T, \mathbf{p}, A, \Psi, \Theta_1, M_1, U_p 1)$ be a*
 694 *traditional security game,^{||} and $a_{i,\psi}^t$ be the point-valued payoff in G_1 for a pure strategy*
 695 *profile ψ of player i and attacker type t . Let $G_2 = (N, T, \mathbf{p}, A, \Psi, \Theta_2, M_2, U_2)$ be an*
 696 *ambiguous security game and $[b_{i,\psi}^t, c_{i,\psi}^t]$ be the interval-valued payoff in G_2 for a pure strategy*
 697 *profile ψ of a player i against attacker type t such that $a_{i,\psi}^t \in [b_{i,\psi}^t, c_{i,\psi}^t]$ and $b_{i,\psi}^t, c_{i,\psi}^t > 0$. If,*
 698 *for any two payoffs a_{i,ψ_1}^t and a_{i,ψ_2}^t in G_1 and any two payoffs $[b_{i,\psi_1}^t, c_{i,\psi_1}^t]$ and $[b_{i,\psi_2}^t, c_{i,\psi_2}^t]$*
 699 *in G_2 , $a_{i,\psi_1}^t - b_{i,\psi_1}^t = a_{i,\psi_2}^t - b_{i,\psi_2}^t$ and $c_{i,\psi_1}^t - b_{i,\psi_1}^t = c_{i,\psi_2}^t - b_{i,\psi_2}^t$, then G_1 and G_2 have the*
 700 *same set of SSE and NE if the projected point-valued payoff function for G_2 satisfies the*
 701 **Uniform Convex Combination** property.

702 *Proof*

703 In our framework the belief degree (see Definition 6) is used to determine the optimal
 704 strategy for the defender. According to the Weibull's proof³⁹, Theorem 1, and SSE⁴⁰,
 705 it only needs to prove that $a_{i,\psi}^t \in G_1$ and the belief degree $\eta_{m_i}(\{t\} \times \{\psi\}) \in G_2$ satisfy
 706 $\eta_{m_i}(\{t\} \times \{\psi\}) = ka_{i,\psi}^t + z$, where $k, z \in \mathbb{R}$ and $k > 0$. For game G_2 , each pure strategy
 707 profile ψ , each player i , and each attacker type t , we have $\text{EUI}(m_{i,\{\psi\}}^t) = [b_{i,\psi}^t, c_{i,\psi}^t]$. Since
 708 the projected point-valued payoff function for G_2 satisfies the property of **Uniform Convex**
 709 **Combination**, we have $\text{Proj}(m_{i,\{\psi\}}^t) = \alpha b_{i,\psi}^t + (1 - \alpha)c_{i,\psi}^t$, where $\alpha \in [0, 1]$. Also, for any
 710 two payoffs a_{i,ψ_1}^t and a_{i,ψ_2}^t in G_1 and any two payoffs $[b_{i,\psi_1}^t, c_{i,\psi_1}^t]$ and $[b_{i,\psi_2}^t, c_{i,\psi_2}^t]$ in G_2 , we
 711 assume $a_{i,\psi_1}^t - b_{i,\psi_1}^t = a_{i,\psi_2}^t - b_{i,\psi_2}^t = l$ and $c_{i,\psi_1}^t - b_{i,\psi_1}^t = c_{i,\psi_2}^t - b_{i,\psi_2}^t = h$. Thus, we have:

$$712 \quad \text{Proj}(m_{i,\{\psi\}}^t) = a_{i,\psi}^t - (a_{i,\psi}^t - b_{i,\psi}^t) + (1 - \alpha)(c_{i,\psi}^t - b_{i,\psi}^t) = a_{i,\psi}^t - l + (1 - \alpha)h.$$

713 Suppose the worst case projected point-valued payoff for a player is d . Since there does not
 714 exist any absent payoff in game G_2 , by formula (15), we have:

$$715 \quad m_i(\{t\} \times \{\psi\}) = \frac{a_{i,\psi}^t - l + (1 - \alpha)h - d}{\sum_{\psi \in \Psi} (a_{i,\psi}^t - l + (1 - \alpha)h - d)}.$$

716 Let $k = \frac{1}{\sum_{\psi \in \Psi} (a_{i,\psi}^t - l + (1 - \alpha)h - d)}$ and $z = \frac{(1 - \alpha)h - l - d}{\sum_{\psi \in \Psi} (a_{i,\psi}^t - l + (1 - \alpha)h - d)}$. Then by Definition 6, we have

717 $\eta_{m_i}(\{t\} \times \{\psi\}) = ka_{i,\psi}^t + z$. Thus, G_1 and G_2 have the same SSE and NE. $\square$

^{||}Here, without loss of generality, Definition 7 is used to represent a traditional security game.

In a security game, it is important to reduce the effect of complete ignorance over the strategy profile selection. For example, in an airport, if the defender is completely ignorant about the payoffs associated with some security target, then likely this will affect their choice of patrolling strategy. If their choice is less than optimal, then this ignorance may be exploited by the attacker, resulting in a lower expected payoff for the defender. In our framework, complete ignorance over the strategy profile selection of a player i is determined by $\mathbf{m}_i(T \times \Psi)$, where Ψ is the set of all pure strategy profiles. In the following theorem, two methods are provided for reducing the effect of complete ignorance in a security game:

Theorem 3 (Reduced influence of complete ignorance). *Let $G_1 = (N, T, \mathbf{p}, A, \Psi, \Theta, M_1, U_1)$, G_2 , and G_3 be three ambiguous security games with absent payoffs, $\mathbf{d}_i^{t,j}(X_r)$ be the relative payoff in G_j ($j = 1, 2, 3$) for the set of pure strategy profile X_r with respect to player i and attacker type t , and let $\mathbf{m}_i^j(T \times \Psi)$ be the uncertainty (complete ignorance) over the game G_j . Then*

(i) *if $G_2 = (N, T, \mathbf{p}, A, \Psi, \Theta, M_2, U_2)$ such that $\mathbf{d}_i^{t,2}(X_r) > \mathbf{d}_i^{t,1}(X_r)$ and $\forall i \in N, t \in T, X_s \in [\Psi]^t$ such that $\mathbf{d}_i^{t,1}(X_s) = 0$, we have $\mathbf{d}_i^{t,2}(X_s) = \mathbf{d}_i^{t,1}(X_s)$, then $\mathbf{m}_i^2(T \times \Psi) < \mathbf{m}_i^1(T \times \Psi)$.*

(ii) *if $G_3 = (N, T, \mathbf{p}, A \cup B, \Psi \cup \Phi, \Theta, M_1 \cup M_3, U_1 \cup U_3)$ such that $\mathbf{d}_i^{t,1}(X_r) \in [t, 2t]$ where $t > \frac{\sum \mathbf{d}_i^{t,1}(X_r)}{2n}$, then $\mathbf{m}_i^3(T \times (\Psi \cup \Phi)) < \mathbf{m}_i^1(T \times \Psi)$.*

Proof

By assumption **A3**, the Proj projected point-valued payoff functions for G_1 , G_2 , and G_3 must satisfy the **Conservative Estimation** property where, for some payoff mass function $\mathbf{m}$, $\text{Proj}(\mathbf{m}) = \min \Theta$ if Θ is the frame of $\mathbf{m}$ and $\mathbf{m}(\Theta) = 1$. Item (i) and (ii) can be proved together. By Definition 12 and the assumption that $\forall i \in N, t \in T, X_s \in [\Psi]^t$ such that $\mathbf{d}_i^{t,1}(X_s) = 0$, we have $\mathbf{d}_i^{t,2}(X_s) = \mathbf{d}_i^{t,1}(X_s)$, the following holds:

$$\mathbf{m}_i^1(T \times \Psi) - \mathbf{m}_i^2(T \times \Psi) = \frac{\sqrt{n}}{(\sum_{j=1}^n a_j + \sqrt{n})} - \frac{\sqrt{n}}{(\sum_{k=1}^n a_k + \sqrt{n})},$$

where a_j is the value of the relative payoff $\mathbf{d}_i^{t,1}(X_r)$ such that $a_j > 0$, a_k is the value of the relative payoff $\mathbf{d}_i^{t,2}(X_r)$ such that $a_k > 0$, and n is the number of possible a_j elements. By assumption $\mathbf{d}_i^{t,2}(X_r) > \mathbf{d}_i^{t,1}(X_r)$, we have $a_k > a_j$. Thus, item (i) holds.

Moreover, item (ii) can be proved by induction the number of relative payoffs in G_3 with respect to Φ as follows:

Basis: When the number of relative payoffs in G_3 with respect to Φ 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.

Induction step: For each $k - 1 \geq 1$, assume item (ii) holds for $t = k - 1$ and show that it holds for $t = k$. Moreover, when the number of relative payoffs with respect to Φ is k , we have $\sum_{j=1}^n a_j + b + c < 2t(n + k - 1) + 2t$, where b is the sum of $k - 1$ relative payoffs with respect to Φ and c is the additional relative payoff, since the relative payoffs with respect to Φ belong to $[t, 2t]$. Then we have

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

So, when the number of relative payoffs with respect to Φ is k , item (ii) holds also. Thus, it holds regardless of the number of relative payoff with respect to Φ . $\square$

Actually, the above theorem shows two methods for reducing the effects of complete ignorance on strategy selection in ambiguous security games: (i) by increasing the payoffs associated with some security targets (those assigned an absent payoff cannot be increased); and (ii) by considering more security targets before selecting a strategy when the value evaluation of all security targets are not excessively high. These methods are consistent with our intuition. For example, if the value of some security targets is high enough, then the defender should not hesitate to assign a random patrol to cover these targets. On the other hand, if the value of no security target is high enough, then the defender can consider more targets or make the absent payoff target more specific. In the airport scenario, when the payoff of a shopping area is unknown, the defender can carefully consider that the payoff of which shop is unknown and how to evaluate other shops. In this way, they can reduce the effect of complete ignorance for their optimal strategy selection. Hence, by the following lemma, it shows that the preference about the strategy profiles is reflected by the security teams choice of a projected point-valued payoff function.

Lemma 1. *Let G be an ambiguous security game without $C2$ (i.e., ambiguous payoff assignments). For any two pure strategy profiles ψ_1 and ψ_2 in a G , if $\text{Proj}(\mathbf{m}_{i,\{\psi_1\}}^t) > \text{Proj}(\mathbf{m}_{i,\{\psi_2\}}^t)$, then $\eta_{\mathbf{m}_i}(\{t\} \times \{\psi_1\}) > \eta_{\mathbf{m}_i}(\{t\} \times \{\psi_2\})$, meaning that player i prefers ψ_1 to ψ_2 given attacker type t .*

Proof

Suppose $\text{Proj}(\mathbf{m}_{i,\{\psi_1\}}^t) > \text{Proj}(\mathbf{m}_{i,\{\psi_2\}}^t)$. Then by formula (12), we have

$$\mathbf{d}_i^t(\{\psi_1\}) > \mathbf{d}_i^t(\{\psi_2\}).$$

By Definitions 2 and 12, for any $\psi \in \Psi$, it only needs to consider $\mathbf{m}_i(\{t\} \times \{\psi\})$ and $\mathbf{m}_i(T \times \Psi)$ to obtain the belief interval of ψ since G does not have ambiguous payoff assignments. When absent payoffs exist in G , by Definitions 2 and 12 and formula (8), we have:

$$\begin{aligned}
 \mathbf{m}_i(\{t\} \times \{\psi_1\}) &= \text{Bel}_{\mathbf{m}_i}(\{t\} \times \{\psi_1\}) > \mathbf{m}_i(\{t\} \times \{\psi_2\}) = \text{Bel}_{\mathbf{m}_i}(\{t\} \times \{\psi_2\}), \\
 \text{Pl}_{\mathbf{m}_i}(\{t\} \times \{\psi_1\}) &= \mathbf{m}_i(\{t\} \times \{\psi_1\}) + \mathbf{m}_i(T \times \Psi) > \\
 \text{Pl}_{\mathbf{m}_i}(\{t\} \times \{\psi_2\}) &= \mathbf{m}_i(\{t\} \times \{\psi_2\}) + \mathbf{m}_i(T \times \Psi), \\
 \delta_{\mathbf{m}_i}(\{t\} \times \{\psi_1\}) &= \mathbf{m}_i(\{t\} \times \Psi) = \delta_{\mathbf{m}_i}(\{t\} \times \{\psi_2\}).
 \end{aligned}$$

Thus, by formula (9), we have $\eta_{\mathbf{m}_i}(\{t\} \times \{\psi_1\}) > \eta_{\mathbf{m}_i}(\{t\} \times \{\psi_2\})$. If there does not exist any absent payoff in G , then by Definition 12, we have:

$$\begin{aligned}
 \mathbf{m}_i(\{t\} \times \{\psi_1\}) &= \text{Bel}_{\mathbf{m}_i}(\{t\} \times \{\psi_1\}) = \text{Pl}_{\mathbf{m}_i}(\{t\} \times \{\psi_1\}) > \\
 \mathbf{m}_i(\{t\} \times \{\psi_2\}) &= \text{Bel}_{\mathbf{m}_i}(\{t\} \times \{\psi_2\}) = \text{Pl}_{\mathbf{m}_i}(\{t\} \times \{\psi_2\}), \\
 \delta_{\mathbf{m}_i}(\{t\} \times \{\psi_1\}) &= \delta_{\mathbf{m}_i}(\{t\} \times \{\psi_2\}) = 0.
 \end{aligned}$$

Thus, by formula (9), we have $\eta_{\mathbf{m}_i}(\{t\} \times \{\psi_1\}) > \eta_{\mathbf{m}_i}(\{t\} \times \{\psi_2\})$. □

Given an ambiguous security game without ambiguous payoff assignments, it follows from Lemma 1 that the ordering over the set of pure strategy profiles with respect to their traditional payoffs is equivalent to the ordering over this set with respect to the projected point-valued payoffs associated with each singleton set of pure strategy profiles. Thus, Lemma 1 highlights the importance of the projected point-valued payoff function in relation to the final result.

5. AMBIGUITY-AVERSION TRANSFORMATION RULE

This section will present a new projected point-valued payoff function to instantiate our general framework for ambiguous security games, and discuss some alternative rules.

5.1. A New Projected point-valued payoff Function

To take this concept further, the ambiguity-aversion maximum regret^{25,26} can be redefined in the context of ambiguous security games as follows:

Definition 14. A function $R_i^t : [\Psi]^t \times [\Psi]^t \rightarrow \mathbb{R}$, called an ambiguity-aversion maximum regret function with respect to i and t , is defined as:

$$R_i^t(X_f, X_g) = \varepsilon(\mathbf{m}_{i,X_g}^t) - \underline{E}(\mathbf{m}_{i,X_f}^t), \quad (17)$$

where $\varepsilon(\mathbf{m}_{i,X_g}^t) = \bar{E}(\mathbf{m}_{i,X_g}^t) - \delta_{\mathbf{m}_{i,X_g}^t}(\Theta_i^\circ)(\bar{E}(\mathbf{m}_{i,X_g}^t) - \underline{E}(\mathbf{m}_{i,X_g}^t))$. A total order over $[\Psi]^t$, denoted as $\succeq_{R_i^t}$ and called an ambiguity-aversion maximum regret ordering with respect to i and t , is defined as:

$$X_f \succeq_{R_i^t} X_g \Leftrightarrow R_i^t(X_f, X_g) \leq R_i^t(X_g, X_f). \quad (18)$$

Moreover, $X_f \sim_{R_i^t} X_g$ if $X_f \succeq_{R_i^t} X_g$ and $X_g \succeq_{R_i^t} X_f$. Also, $X_f \succ_{R_i^t} X_g$ if $X_f \succeq_{R_i^t} X_g$ and $X_g \not\succeq_{R_i^t} X_f$. That is, X_f is equally preferred to X_g if $X_f \sim_{R_i^t} X_g$ and X_f is strictly preferred to X_g if $X_f \succ_{R_i^t} X_g$.

This ordering states that a set of pure strategy profiles X_f is strictly preferred to X_g if the ambiguity-aversion maximum regret for X_f is lower than that of X_g . This idea can also be applied to a projected point-valued payoff function. Formally, we have:

Definition 15. Let $\mathbf{m}$ be a payoff mass function. Then the ambiguity-aversion minimax regret function is defined as:

$$\text{AAMR}(\mathbf{m}) = \frac{2\underline{E}(\mathbf{m}) + (1 - \delta_{\mathbf{m}}(\Theta))(\bar{E}(\mathbf{m}) - \underline{E}(\mathbf{m}))}{2}. \quad (19)$$

So, AAMR is an instantiation of the Proj function in Definition 8.

Example 10. For the airport scenario, we have

$$\text{AAMR}(\mathbf{m}_{d,\{(PR,PR)\}}^{t_1}) = \frac{2 \times 4 + (1 - \frac{0.8 \times \log_2 2 + 0.2 \times \log_2 10}{\log_2 10})(6.6 - 4)}{2} = 4.72693.$$

From this projected point-valued payoff function, a transformation rule $\succeq_{i,\text{AAMR}}^t$ can be defined for a player i and attacker type t . Hence, the following proposition shows this rule can induce the ambiguity-aversion maximum regret ordering $\succeq_{R_i^t}$ (see Definition 14) as follows:

Proposition 3. Given a player i , an attacker type t , and sets of pure strategy profiles $X_f, X_g \in [\Psi]^t$, $X_f \succeq_{R_i^t} X_g \Leftrightarrow X_f \succeq_{i,\text{AAMR}}^t X_g$.

Proof

By Definitions 14 and 15, we have:

$$\begin{aligned} X_f \succeq_{R_i^t} X_g &\Leftrightarrow R_i^t(X_f, X_g) \leq R_i^t(X_g, X_f) \\ &\Leftrightarrow \varepsilon(\mathbf{m}_{i,X_g}^t) - \underline{E}(\mathbf{m}_{i,X_f}^t) \leq \varepsilon(\mathbf{m}_{i,X_f}^t) - \underline{E}(\mathbf{m}_{i,X_g}^t) \\ &\Leftrightarrow \bar{E}(\mathbf{m}_{i,X_g}^t) - \delta_{\mathbf{m}_{i,X_g}^t}(\Theta_i^\circ)(\bar{E}(\mathbf{m}_{i,X_g}^t) - \underline{E}(\mathbf{m}_{i,X_g}^t)) - \underline{E}(\mathbf{m}_{i,X_f}^t) \\ &\leq \bar{E}(\mathbf{m}_{i,X_f}^t) - \delta_{\mathbf{m}_{i,X_f}^t}(\Theta_i^\circ)(\bar{E}(\mathbf{m}_{i,X_f}^t) - \underline{E}(\mathbf{m}_{i,X_f}^t)) - \underline{E}(\mathbf{m}_{i,X_g}^t) \\ &\quad \frac{2\underline{E}(\mathbf{m}_{i,X_f}^t) + (1 - \delta_{\mathbf{m}_{i,X_f}^t}(\Theta_i^\circ))(\bar{E}(\mathbf{m}_{i,X_f}^t) - \underline{E}(\mathbf{m}_{i,X_f}^t))}{2} \\ &\geq \frac{2\underline{E}(\mathbf{m}_{i,X_g}^t) + (1 - \delta_{\mathbf{m}_{i,X_g}^t}(\Theta_i^\circ))(\bar{E}(\mathbf{m}_{i,X_g}^t) - \underline{E}(\mathbf{m}_{i,X_g}^t))}{2} \\ &\Leftrightarrow \text{AAMR}(\mathbf{m}_{i,X_f}^t) \geq \text{AAMR}(\mathbf{m}_{i,X_g}^t) \\ &\Leftrightarrow X_f \succeq_{i,\text{AAMR}}^t X_g. \end{aligned}$$

834

□

835 Clearly, it can easily prove that the ambiguity-aversion minimax regret function satisfies
 836 the required properties of a projected point-valued payoff function (*i.e.*, **Boundary** and
 837 **Preference**). Moreover, using the **Boundary** property, the uniqueness of Definition 15 for
 838 the ambiguity-aversion maximum regret ordering $\succeq_{R_i^t}$ by Definition 14 can be proved as follows:

839 **Proposition 4.** *Given a payoff mass function $\mathbf{m}$ over Θ , Definition 15 is the unique linear*
 840 *function $f(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) = a(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) + b$ (where a and b are real numbers), which*
 841 *satisfies assumption $f(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) \in [\underline{\mathbf{E}}(\mathbf{m}), \bar{\mathbf{E}}(\mathbf{m})]$.*

842 *Proof*

843 By the assumption and Definition 14, we have

844 (i) $2a\underline{\mathbf{E}}(\mathbf{m}) + a(1 - \delta_{\mathbf{m}}(\Theta))(\bar{\mathbf{E}}(\mathbf{m}) - \underline{\mathbf{E}}(\mathbf{m})) + b \geq \underline{\mathbf{E}}(\mathbf{m})$, and

845 (ii) $2a\underline{\mathbf{E}}(\mathbf{m}) + a(1 - \delta_{\mathbf{m}}(\Theta))(\bar{\mathbf{E}}(\mathbf{m}) - \underline{\mathbf{E}}(\mathbf{m})) + b \leq \bar{\mathbf{E}}(\mathbf{m})$.

846 If $b > 0$ and $a \geq \frac{1}{2}$, when $\underline{\mathbf{E}}(\mathbf{m}) = \bar{\mathbf{E}}(\mathbf{m}) > 0$, we have $f(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) \geq \bar{\mathbf{E}}(\mathbf{m})$. It violates item
 847 (ii). If $b > 0$ and $a < \frac{1}{2}$, when $\delta_{\mathbf{m}}(\Theta) = 1$, $\underline{\mathbf{E}}(\mathbf{m}) > \frac{b}{1-2a}$, we have $f(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) \leq \underline{\mathbf{E}}(\mathbf{m})$. It
 848 violates item (i). If $b < 0$ and $a \geq \frac{1}{2}$, when $\underline{\mathbf{E}}(\mathbf{m}) = \bar{\mathbf{E}}(\mathbf{m}) > \frac{-b}{2a-1}$, we have $f(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) \geq$
 849 $\bar{\mathbf{E}}(\mathbf{m})$. It violate item (ii). If $b < 0$ and $a < \frac{1}{2}$, when $\delta_{\mathbf{m}}(\Theta) = 1$, we have $f(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) \leq$
 850 $\underline{\mathbf{E}}(\mathbf{m})$. It violate item (i). Thus, $b = 0$. Hence, if $b = 0$ and $a > \frac{1}{2}$, when $\underline{\mathbf{E}}(\mathbf{m}) = \bar{\mathbf{E}}(\mathbf{m})$, we have
 851 $f(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) \geq \bar{\mathbf{E}}(\mathbf{m})$. It violate item (ii). If $b = 0$ and $a < \frac{1}{2}$, when $\delta_{\mathbf{m}}(\Theta) = 1$, we have
 852 $f(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) \leq \underline{\mathbf{E}}(\mathbf{m})$. It violate item (i). Thus, $a = \frac{1}{2}$. Thus, only Definition 15 satisfies
 853 our assumption that $f(\varepsilon(\mathbf{m}) + \underline{\mathbf{E}}(\mathbf{m})) \in [\underline{\mathbf{E}}(\mathbf{m}), \bar{\mathbf{E}}(\mathbf{m})]$. □

854 In fact, by Propositions 3 and 4, Definition 15 is the unique linear function definition that
 855 satisfies the preference ordering in Definition 14. One advantage of applying the ambiguity-
 856 aversion minimax regret function in Definition 15 is that it can characterise the *player's*
 857 *attitude to risk*. Actually, this projected point-valued payoff function can be defined for a
 858 payoff mass function $\mathbf{m}$ over Θ as $\text{AAMR}(\mathbf{m}) = \alpha\underline{\mathbf{E}}(\mathbf{m}) + (1 - \alpha)\bar{\mathbf{E}}(\mathbf{m})$, where $\alpha = \frac{1+\delta_{\mathbf{m}}(\Theta)}{2}$.
 859 This definition demonstrates that the ambiguity-aversion minimax regret function is a special
 860 case of the Hurwicz criterion³⁴, since it assigns a value to a subset of pure strategy profiles X
 861 as a weighted sum of the worst and best expected payoffs of X . However, it has two advantages
 862 over the Hurwicz criterion: (i) with the Hurwicz criterion, the value of α is commonly based
 863 on a subjective judgement, whereas the ambiguity-aversion minimax regret function provides
 864 a method to specify this value; and (ii) with the Hurwicz criterion, the value of α is fixed for
 865 each player, whereas the ambiguity-aversion minimax regret function allows this value to vary
 866 between all payoff mass functions in an ambiguous security game. Given this relationship,
 867 the α in Definition 15 can be interpreted as a degree of pessimism. That is, a risk-seeking
 868 (optimistic) player assigns a lower value to α while a risk-averse (pessimistic) player assigns
 869 a higher value to α . In other words, given the same expected payoff intervals, a risk-seeking
 870 player can obtain a higher projected point-valued payoff than a risk-averse player. Hence, as
 871 the mass function does not change for a given set of pure strategy profiles and the boundary of
 872 Θ is based on a subjective judgement, it shows that a player's attitude to risk can be influenced
 873 by the boundary of Θ :

874 **Proposition 5.** *Let $\mathbf{m}_1$ and $\mathbf{m}_2$ be payoff mass functions over Θ_1 and over Θ_2 , respectively.*
 875 *If $\Theta_2 \supset \Theta_1 \supset Z$ and $\mathbf{m}_2(Z) = \mathbf{m}_1(Z)$ then $\text{AAMR}(\mathbf{m}_2) > \text{AAMR}(\mathbf{m}_1)$.*

876 *Proof*

877 Because $\mathbf{m}_2(Z) = \mathbf{m}_1(Z)$, $Z \subset \Theta_1$, and $\Theta_2 \supset \Theta_1$, by Definition 5, we have $\delta_{\mathbf{m}_2}(\Theta_2) < \delta_{\mathbf{m}_1}(\Theta_1)$.
 878 Hence, by $\mathbf{m}_2(Z) = \mathbf{m}_1(Z)$ and formulas (6) and (7), we have $\text{EUI}(\mathbf{m}_1) = \text{EUI}(\mathbf{m}_2)$. Thus, by
 879 formula (19), we have $\text{AAMR}(\mathbf{m}_2) > \text{AAMR}(\mathbf{m}_1)$. □

	SA	PR	SL	VL, H
SA	2.602	-7.473	-9	$\{(\mathbf{SA}, \mathbf{VL}); (\mathbf{SA}, \mathbf{H})\}$: -8
PR	-6.398	4.727	-9	$\{(\mathbf{PR}, \mathbf{VL}); (\mathbf{PR}, \mathbf{H})\}$: -8
SL	-6.398	-7.473	0	$\{(\mathbf{SL}, \mathbf{VL}); (\mathbf{SL}, \mathbf{H})\}$: -8
VL	-6.398	-7.473	-9	$\{(\mathbf{VL}, \mathbf{VL}); (\mathbf{H}, \mathbf{H})\}$: 7
H	-6.398	-7.473	-9	$\{(\mathbf{VL}, \mathbf{H}); (\mathbf{H}, \mathbf{VL})\}$: -8

Table VI. (Step 1) Projected point-valued payoffs for the defender.

	SA	PR	SL	VL, H
SA	11.602	1.527	0	$\{(\mathbf{SA}, \mathbf{VL}); (\mathbf{SA}, \mathbf{H})\}$: 1
PR	2.602	13.727	0	$\{(\mathbf{PR}, \mathbf{VL}); (\mathbf{PR}, \mathbf{H})\}$: 1
SL	2.602	1.527	9	$\{(\mathbf{SL}, \mathbf{VL}); (\mathbf{SL}, \mathbf{H})\}$: 1
VL	2.602	1.527	0	$\{(\mathbf{VL}, \mathbf{VL}); (\mathbf{H}, \mathbf{H})\}$: 16
H	2.602	1.527	0	$\{(\mathbf{VL}, \mathbf{H}); (\mathbf{H}, \mathbf{VL})\}$: 1

Table VII. (Step 2) Relative payoffs for the defender.

$A \subseteq T \times \Psi$	$m_d(A)$	$A \subseteq T \times \Psi$	$m_d(A)$
$\{(t_1, (\mathbf{SA}, \mathbf{SA}))\}$	0.155	$\{t_1\} \times \{(\mathbf{SA}, \mathbf{VL}), (\mathbf{SA}, \mathbf{H})\}$	0.013
$\{(t_1, (\mathbf{PR}, \mathbf{SA}))\}$	0.035	$\{t_1\} \times \{(\mathbf{PR}, \mathbf{VL}), (\mathbf{PR}, \mathbf{H})\}$	0.013
$\{(t_1, (\mathbf{SL}, \mathbf{SA}))\}$	0.035	$\{t_1\} \times \{(\mathbf{SL}, \mathbf{VL}), (\mathbf{SL}, \mathbf{H})\}$	0.013
$\{(t_1, (\mathbf{VL}, \mathbf{SA}))\}$	0.035	$\{t_1\} \times \{(\mathbf{H}, \mathbf{VL}), (\mathbf{VL}, \mathbf{H})\}$	0.013
$\{(t_1, (\mathbf{H}, \mathbf{SA}))\}$	0.035	$\{t_1\} \times \{(\mathbf{VL}, \mathbf{VL}), (\mathbf{H}, \mathbf{H})\}$	0.214
$\{(t_1, (\mathbf{SL}, \mathbf{SL}))\}$	0.12	$\{t_1\} \times \Psi$	0.053
$\{(t_1, (\mathbf{SA}, \mathbf{PR}))\}$	0.02		
$\{(t_1, (\mathbf{PR}, \mathbf{PR}))\}$	0.183		
$\{(t_1, (\mathbf{SL}, \mathbf{PR}))\}$	0.02		
$\{(t_1, (\mathbf{VL}, \mathbf{PR}))\}$	0.02		
$\{(t_1, (\mathbf{H}, \mathbf{PR}))\}$	0.02		

Table VIII. (Step 3) Mass distribution for the defender m_d .

Intuitively, the above proposition means that the more risk-seeking the defender is, the wider the range of values they consider from the set of possible payoffs of the whole game. For example, when considering the value of the real estate, a security team may not worry too much about an error regarding the price of a property within a range of one thousand dollars, since one thousand dollars is tiny compared to the total price. The team may then be more risk-seeking when determining the point-valued estimation of a property. However, when considering the daily revenue of a shop, the team might be more cautious when handling an error within the range of one thousand dollars. In other words, if a security team wishes to pursue a cautious approach, this proposition means that they should not over-estimate the possible payoffs in an ambiguous security game when estimating the value of each pure strategy profile. So, the players risk attitude can influence the point-valued belief degree and the eventual solution strategy for an ambiguous security game.

5.2. Scenario

Given this new projected point-valued payoff function, the applicability of our framework on the airport scenario introduced in Section 1 can be illustrated.

Example 11 (Step 1). *Given the ambiguous payoff matrix in Table IV, itp can find that the payoff mass function payoff of the defender assigned to the set of pure strategy profiles $\{(\mathbf{PR}, \mathbf{PR})\}$ is $\{m_{d, \{(\mathbf{PR}, \mathbf{PR})\}}^{t_1}(\{5, 6\}) = 0.8, m_{d, \{(\mathbf{PR}, \mathbf{PR})\}}^{t_1}(\Theta_d^+) = 0.2\}$. When applying the ambiguity-aversion minimax regret function to this payoff mass function, we have:*

$$\text{AAMR}(m_{d, \{(\mathbf{PR}, \mathbf{PR})\}}^{t_1}) = \frac{2 \times 4 + (1 - \frac{0.8 \times \log_2 2 + 0.2 \times \log_2 10}{\log_2 10})(6.6 - 4)}{2} = 4.727.$$

After applying this to all the sets of pure strategy profiles in partition $[\Psi]^{t_1}$, the ambiguity-aversion minimax regret matrix of the defender is obtained as shown in Table VI.

Example 12 (Step 2). *Given the ambiguity-aversion minimax regret function matrix for the defender from Table VI, it can find that the worst projected point-valued payoff for this*

(a) Belief intervals.

	SA	PR	SL	VL	H
SA	[0.155, 0.208]	[0.020, 0.074]	[0, 0.053]	[0, 0.067]	[0, 0.067]
PR	[0.035, 0.088]	[0.183, 0.237]	[0, 0.053]	[0, 0.067]	[0, 0.067]
SL	[0.035, 0.088]	[0.020, 0.074]	[0.12, 0.174]	[0, 0.067]	[0, 0.067]
VL	[0.035, 0.088]	[0.020, 0.074]	[0, 0.053]	[0, 0.267]	[0, 0.067]
H	[0.035, 0.088]	[0.020, 0.074]	[0, 0.053]	[0, 0.067]	[0, 0.267]

(b) Ambiguity degrees.

	SA	PR	SL	VL	H
SA	0.053	0.053	0.053	0.056	0.056
PR	0.053	0.053	0.053	0.056	0.056
SL	0.053	0.053	0.053	0.056	0.056
VL	0.053	0.053	0.053	0.1	0.056
H	0.053	0.053	0.053	0.056	0.1

(c) point-valued belief degrees, equivalent to traditional payoffs.

	SA	PR	SL	VL	H
SA	0.18	0.046	0.025	0.032	0.032
PR	0.06	0.209	0.025	0.032	0.032
SL	0.06	0.046	0.146	0.032	0.032
VL	0.06	0.046	0.025	0.12	0.032
H	0.06	0.046	0.025	0.032	0.12

Table IX. (Step 4) Information derived from the defender's mass function m_d .

matrix is -9 . Then the relative payoff of the defender for the set of pure strategy profiles $\{(\mathbf{PR}, \mathbf{PR})\}$ can be obtained as follows:

$$d_d^{t_1}(\{(\mathbf{PR}, \mathbf{PR})\}) = 4.727 - (-9) = 13.727.$$

After this is applied to all sets of pure strategy profiles in the partition $[\Psi]^{t_1}$, the relative payoff matrix for the defender is obtained as shown in Table VII.

Example 13 (Step 3). The defender could have absent payoffs, e.g., see Tables III(a), III(b) and IV. Thus, the mass function for the defender over frame $T \times \Psi$ is defined using formulas (13) and (14). So, given the relative payoff matrix for the defender in Table VII, the mass value for $\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}$ can be obtained as follows:

$$m_d(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}) = \frac{13.727}{70.845 + \sqrt{16}} = 0.183.$$

After this is applied to all sets of pure strategy profiles in $[\Psi]^{t_1} \cup \{\Psi\}$, the mass distribution for the defender m_d is obtained as shown in Table VIII.

Example 14 (Step 4). Given the mass distribution for the defender from Table VIII, it can find the belief and plausibility values for set $\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}$ as follows:

$$\begin{aligned} \text{Bel}_{m_d}(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}) &= m_d(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}) = 0.183, \\ \text{Pl}_{m_d}(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}) &= m_d(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}) + m_d(\{t_1\} \times \Psi) = 0.183 + 0.053 = 0.236, \end{aligned}$$

where $[\text{Bel}_{m_d}(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}), \text{Pl}_{m_d}(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\})]$ is the belief interval for $\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}$. After this is applied to all elements in the product set $T \times \Psi$, the belief interval for each element is obtained as shown in Table IX(a). Then the ambiguity degree values for $\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}$ can be obtained as follows:

$$\delta_{m_d}(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}) = \frac{0.183 \times \log_2 1 + 0.053 \times \log_2 25}{\log_2 25} = 0.053.$$

After this is applied to all elements in the product set $T \times \Psi$, the ambiguity degree for each element is obtained as shown in Table IX(b).

Given the belief interval matrix of the defender in Table IX(a) and the ambiguity degree matrix for the defender in Table IX(b), the point-valued belief degree for $\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}$

	SA	PR	SL	VL	H
SA	0.18; 0.009	0.046; 0.054	0.025; 0.049	0.032; 0.035	0.032; 0.035
PR	0.06; 0.063	0.209; 0.018	0.025; 0.049	0.032; 0.035	0.032; 0.035
SL	0.06; 0.063	0.046; 0.054	0.146; 0.022	0.032; 0.035	0.032; 0.035
VL	0.06; 0.063	0.046; 0.054	0.025; 0.049	0.12; 0	0.032; 0.035
H	0.06; 0.063	0.046; 0.054	0.025; 0.049	0.032; 0.035	0.12; 0

Table X. (Step 5) Traditional security game.

Principle	Attitude	Notation	Definition	Requirements
Minimum Acceptable EU ²⁴	Pessimistic	MinA(m)	$\underline{E}(m)$	–
Maximum Acceptable EU	Optimistic	MaxA(m)	$\bar{E}(m)$	–
Hurwicz Weighted EU ³⁴	Weighted (pessimistic/optimistic)	Hurwicz(m)	$\alpha \underline{E}(m) + (1 - \alpha) \bar{E}(m)$	$\alpha \in [0, 1]$
TBM ³⁵	Indifference	TBM(m)	$\sum_{h \in \Theta} h \sum_{A \subseteq \Theta \text{ s.t. } h \in A} \frac{m(A)}{ A }$	–
OWA ³⁶	Weighted (outcomes)	OWA(m)	$\sum_{A \subseteq \Theta} m(A) \sum_{j=1}^{ A } w_j h_j$	$w_j \in [0, 1], \sum_{j=1}^{ A } w_j = 1$ and h_j is the j -th highest value in A

Table XI. Projected point-valued payoff function instantiations.

929 can be found as follows:

$$930 \quad \eta_{m_d}(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\}) = \frac{2 \times 0.183 + (1 - 0.053) \times (0.237 - 0.183)}{2} = 0.209.$$

931 After the point-valued belief degree is applied to all the elements in $T \times \Psi$, the point-valued
 932 belief degree for each element is obtained as shown in Table IX(c). Then the traditional point-
 933 valued payoff with respect to the attacker type t_1 for the pure strategy profile $(\mathbf{PR}, \mathbf{PR})$ can
 934 be obtained directly, i.e., $\text{Tr}_d^{t_1}((\mathbf{PR}, \mathbf{PR})) = \eta_{m_d}(\{t_1\} \times \{(\mathbf{PR}, \mathbf{PR})\})$.

935 **Example 15** (Step 5). After obtaining the traditional point-valued payoffs with respect to
 936 attacker type t_1 for all pure strategy profiles in Ψ , it can repeat steps 1-4 for the attacker
 937 and obtain the traditional point-valued payoffs for the game as shown in Table X. If the SSE
 938 solution concept⁴⁰ is applied for security games, the optimal mixed strategy of the defender
 939 can be obtained as follows:

$$940 \quad \Delta_d(\mathbf{SA}) = 0.389, \Delta_d(\mathbf{PR}) = 0.333, \Delta_d(\mathbf{SL}) = 0.278.$$

941 5.3. Alternative Transformation Rules

942 In reality, it may be desirable to adopt alternative attitudes to ambiguity when instantiating
 943 our framework (see Table XI for an outline). Thus, this subsection will discuss various attitudes
 944 inspired by well-known methods on decision making under ambiguity, and explain how to use
 945 the intuitions of these decision rules to define projected point-valued payoff functions and the
 946 corresponding transformation rules.

947 When being applied to an ambiguous security game, the MinA function prefers a set of pure
 948 strategy profiles achieving a lower expected payoff. So it is a pessimistic method concerning the
 949 worst case outcome, meaning that a player may lose the chance for high payoff gains. Instead,
 950 the MaxA function reflects an optimistic attitude to ambiguity. So when being applied to an
 951 ambiguous security game, it results in a set of pure strategy profiles maximising the achievable

upper expected payoff. The **Hurwicz** function is a compromise between **MinA** and **MaxA**, by assigning a weight α to balances optimism and pessimism. Each player can individually set α for unlikely they would change their attitude to ambiguity during a single game.

The first three projected point-valued payoff functions are based on the expected payoff interval, reflecting the decision maker's attitude to the expected payoff interval directly. However, some different projected point-valued payoff functions can be considered. The **TBM** function translates a belief function to a probability and then uses Bayesian decision theory for decision making. The method distinguishes the credal level from the pignistic level. Thus, beliefs are represented and updated on the first level, and belief functions are transformed to probabilities at the pignistic level using the principle of insufficient-reason. In fact, this decision rule reflects the player's attitude to ambiguity of each possible outcome of a mass function via the principle of indifference²⁸: each possible outcome is equally plausible. This attitude can be modeled via a **TBM**-style EU. Finally, the **OWA** function obtains point-valued payoffs also based on a player's ambiguity attitude to evaluate the expected payoff for a responsible decision maker. As to the **Hurwicz** function, this paper assumes that a player does not change their attitude to ambiguity during a single game. Thus, there exists only one weighting vector for any subset of values $A \subseteq \Theta$.

Importantly, although all the projected point-valued payoff functions can be used in Step 1 of our framework, some of them still cannot handle absent payoffs, meaning that a player is completely ignorant about the payoffs. This paper interprets this as complete ignorance over the whole frame and construct a mass function for each player as that in Definition 12, but the negative absent payoffs must be zero. By Definitions 10 and 11, this restriction satisfies our assumption **A3** (*i.e.*, a negative absent payoff should not be greater than any other payoff). However, with some projected point-valued payoff functions, the negative absent payoffs do not necessarily correspond to the worst projected point-valued payoff. If so, the projected point-valued payoff functions does not satisfy this restriction and thus they cannot be applied to ambiguous security games with absent payoffs. Nevertheless, these projected point-valued payoff functions can be applied if the ambiguous security game does not contain absent payoffs. In this way, they can handle the remaining types of ambiguity **C1a**, **C1b**, and **C2** in our framework.

For the five projected point-valued payoff functions presented in this section, the following three ones are compatible (in our framework) with absent payoffs: (i) Minimum Acceptable EU function; (ii) Hurwicz function when $\alpha = 1$; and (iii) OWA function when the minimum element of a frame has weight $w = 1$.

6. EXPERIMENTAL EVALUATION

We have used Java to implement our framework,^{**} including an implementation of the DOBSS⁴¹ mixed-integer linear program (MILP) for the **ibm ilog cplex optimization studio** 12.6.^{††} The input of security games supported by our system (called SEGUA) include simplified payoff matrices and standard ones, such as those in Tables III(a) and III(b). To evaluate a variety of properties of our framework, our experiments have opted to use randomly generated ambiguous security games represented as simplified payoff matrices. Our evaluation experiments are done on a desktop computer with an Intel Xeon E5-2620 2GHz CPU and 16GB of RAM running Microsoft Windows 7 Enterprise 64-bit.

6.1. Experiment Setting

For a traditional security game G and an ambiguous one $\tilde{G}$, let $\text{EU}(G, \Delta_d, s_a)$ be the defender's expected payoff from G when the defender takes a mixed strategy Δ_d and the attacker

^{**}The software is online at <https://github.com/kevinmcareavey/segua>.

^{††}<http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/>

997 takes a pure strategy s_a , $\text{OMS}_d(G)$ be the optimal mixed strategy of the defender in G .
 998 Let $\text{OPS}_a(G, \Delta_d)$ be the optimal pure strategy of the attacker in G when the defender takes
 999 a mixed strategy Δ_d , and $\text{SeGUA}_{\text{Proj}}(\tilde{G})$ be the traditional security game found by applying
 1000 the **Proj** instantiation of our framework on $\tilde{G}$.

1001 Our experiments aim to examine the effect of different transformation rules on the
 1002 expected payoff of the defender's optimal mixed strategy. So the experiments start with a
 1003 randomly generated traditional security game G (called a ground-truth game), and then
 1004 randomly extend G to an ambiguous one $\tilde{G}$. The defender's maximum expected payoff
 1005 in these experiments is defined as $\text{EU}(G, \Delta_d, s_a)$ (where $\Delta_d = \text{OMS}_d(\text{SeGUA}_{\text{Proj}}(\tilde{G}))$ and
 1006 $s_a = \text{OPS}_a(G, \Delta_d)$), representing the *true* expected payoff resulted from G if the defender
 1007 takes Δ_d and the attacker takes s_a . That is, the defender chooses a strategy based on an
 1008 ambiguous view of world $\text{SeGUA}_{\text{Proj}}(\tilde{G})$, while the attacker does based on an exact view of
 1009 world G but the knowledge of the defender's strategy commitment. However, the defender's
 1010 expected payoff is from the true state of world G rather than what they "believe" to be the
 1011 true state of world $\text{SeGUA}_{\text{Proj}}(\tilde{G})$. So the defender's mixed strategy Δ_d may or may not be
 1012 their optimal mixed strategy in G , even though it is their optimal mixed strategy regarding
 1013 $\text{SeGUA}_{\text{Proj}}(\tilde{G})$.

1014 As summarised in Table II, our framework can handle four types of ambiguity, *i.e.*, **C1a**,
 1015 **C1b**, **C1c**, and **C2**. This evaluation focuses on **C1a** (imprecise payoff) and **C1b** (unreliable
 1016 payoff), but consider neither **C1c** nor **C2** (because this type of ambiguity is handled in the
 1017 same way by every instantiation of our framework).

1018 In total the experiments examine the following nine different instantiations of our
 1019 framework: (i) AAMR; (ii) MaxA; (iii) Hurwicz ($\alpha = 0.2$); (iv) Hurwicz ($\alpha = 0.4$); (v) TBM
 1020 ($\alpha = 0.5$); (vi) Hurwicz ($\alpha = 0.6$); (vii) Hurwicz ($\alpha = 0.8$); (viii) MinA; and (ix) OWA (linear
 1021 weighting). It is worth recalling that given a payoff mass function $\mathbf{m}$, $\text{Hurwicz}(\mathbf{m}) = \text{MaxA}(\mathbf{m})$ if
 1022 $\alpha = 0$, and $\text{Hurwicz}(\mathbf{m}) = \text{MinA}(\mathbf{m})$ if $\alpha = 1$. Moreover, $\text{Hurwicz}(\mathbf{m}) = \text{TBM}(\mathbf{m})$ if $\alpha = 0.5$ and
 1023 $\forall S \subseteq \Theta$ such that $\mathbf{m}(S) > 1$ then S is an interval set of payoffs. Thus, $\text{Hurwicz}(\mathbf{m}) = \text{TBM}(\mathbf{m})$
 1024 if $\alpha = 0.5$ since ambiguous payoffs where non-zero masses are assigned to non-interval sets
 1025 of payoffs (*e.g.*, a mass function $\mathbf{m}$ such that $\mathbf{m}(\{2, 7, 9\}) = 1$) does not be consider in this
 1026 case. Finally, since there are so many possible weightings which could be used by OWA, this
 1027 evaluation simply assigns higher weights to higher payoffs. Specifically, given a set of payoffs
 1028 $S \subseteq \Theta$ such that $n = |S|$ and $\vec{S} = (h_1, \dots, h_n)$ is the ascending ordering of S , the weight of the
 1029 i -th element in $\vec{S}$ is defined as $w_i = \frac{2i}{n(n+1)}$. For example, the weights of payoffs 5, 6, 7, and 8
 1030 are 0.1, 0.2, 0.3, and 0.4, respectively.

1031 In the remainder of this section, the experiments will randomly generate each ground-
 1032 truth traditional security game G with: (i) pure strategy sets $A_d = A_a = \{s_1, \dots, s_n\}$ for
 1033 some random $n \in \{2, \dots, 9\}$; (ii) a set of attacker types $T = \{t_1, \dots, t_m\}$ for some random
 1034 $m \in \{2, \dots, 9\}$, where the probability distribution $\mathbf{p}$ over T is randomly assigned and $\forall t_i \in$
 1035 $T, \mathbf{p}(t_i) > 0$; (iii) fixed negative and positive frames for each player defined as $\Theta_d^- = \Theta_a^- =$
 1036 $\{-100, \dots, 0\}$ and $\Theta_d^+ = \Theta_a^+ = \{0, \dots, 100\}$; and (iv) random negative and positive payoffs
 1037 selected from these respective frames.

1038 6.2. Imprecise payoffs

1039 Let A_a be a singleton set of targets and u_i^+ (resp. u_i^-) be a positive (resp. negative) point-
 1040 valued payoff for A_a with respect to a player $i \in N$ and an attacker type $t \in T$. Then we can
 1041 determine the maximum values which can be used to extend all ground-truth payoffs for A_a
 1042 and t into valid interval payoffs as follows:

$$\begin{aligned} 1043 \quad \sigma_{\max}^{dec} &= \min\{|\min \Theta_i^\circ - u_i^\circ| \mid \circ \in \{+, -\}, i \in N\}, \\ 1044 \quad \sigma_{\max}^{inc} &= \min\{|\max \Theta_i^\circ - u_i^\circ| \mid \circ \in \{+, -\}, i \in N\}. \end{aligned}$$

1045 Given some random $\sigma^{dec} \in \{0, \dots, \sigma_{\max}^{dec}\}$ and $\sigma^{inc} \in \{0, \dots, \sigma_{\max}^{inc}\}$, a random positive (resp.
 1046 negative) interval-valued payoff for A_a and each $i \in N$ with respect to t can be defined as

1047 $[u_i^+ - \sigma^{dec}, u_i^+ + \sigma^{inc}]$ (resp. $[u_i^- - \sigma^{dec}, u_i^- + \sigma^{inc}]$). In other words, the same σ^{dec} and σ^{inc}
 1048 values have been used to extend all four payoffs associated with A_a and t . Thus, $\sigma_{\max}^{dec}$ and
 1049 $\sigma_{\max}^{inc}$ represent the maximum values which can be used to increase the size of all interval-valued
 1050 payoffs associated with A_a and t while ensuring that these new intervals remain within their
 1051 respective frames.

1052 To analyse the effect of each transformation rule on an ambiguous security game with
 1053 interval-valued payoffs, our experiments put the following constraints:

- 1054 **I1**: No constraints on σ^{dec} or σ^{inc} ;
- 1055 **I2**: $\sigma^{dec} = 0$ and $\sigma^{inc} > 0$;
- 1056 **I3**: $\sigma^{inc} > \sigma^{dec}$;
- 1057 **I4**: $\sigma^{dec} > \sigma^{inc}$; and
- 1058 **I5**: $\sigma^{dec} > 0$ and $\sigma^{inc} = 0$.

1059 Intuitively, **I1** requires that each new interval is valid in the frame and contains the original
 1060 ground-truth payoff. **I2** and **I5** require that the ground-truth payoff are, respectively, the
 1061 minimum and maximum values in the new interval. **I3** and **I4** provide a relaxation of **I2** and
 1062 **I5** in that they only require the ground-truth payoff to be closer to, respectively, the minimum
 1063 and maximum values in the new interval.

1064 Figures 2–6 show the results for each constraint with respect to 1000 randomly generated
 1065 ground-truth games G .^{‡‡} For each constraint, an ambiguous security game $\tilde{G}$ is generated. For
 1066 each ambiguous security game and each instantiation of our framework, a traditional security
 1067 game $\text{SeGUA}_{\text{Proj}}(\tilde{G})$ is generated. Then the traditional one is solved to find the defender's
 1068 optimal mixed strategy $\Delta_d = \text{OMS}_d(\text{SeGUA}_{\text{Proj}}(\tilde{G}))$, determine the attacker's optimal pure
 1069 strategy $s_a = \text{OPS}_a(G, \Delta_d)$, and calculate the defender's true maximum expected payoff
 1070 $\text{EU}(G, \Delta_d, s_a)$ from the ground-truth game. Finally, each instantiation with respect to their
 1071 corresponding maximum expected payoffs is ranked. Each graph then shows the number
 1072 of samples found at each rank, for each framework instantiation, where the highest rank
 1073 corresponds to those samples where the maximum expected payoff was the same when solving
 1074 the ambiguous game as when solving the ground-truth game directly. In other words, the
 1075 highest rank corresponds to those samples where the defender chooses a mixed strategy based
 1076 on $\text{SeGUA}_{\text{Proj}}(\tilde{G})$, which is optimal with respect to G (*i.e.*, where the defender achieves the
 1077 true maximum expected payoff whether they have an ambiguous or exact view of the world).

1078 Since in constraint **I2** (resp. **I5**), transformation rule MaxA (resp. MinA) ensures the
 1079 projected point-valued payoffs are exactly the ground-truth payoffs, it is not surprising that in
 1080 constraint **I2** (resp. **I5**), instantiation MaxA (resp. MinA) results in the true maximum expected
 1081 payoff of the defender in all the samples. The relationship between these instantiations and
 1082 Hurwicz also helps to explain why the results from the Hurwicz become worse as α is decreased
 1083 from 1 (resp. increased from 0). More interesting is: for **I2**, AAMR produces better results than
 1084 all other instantiations except for MaxA while OWA produces the worst; conversely, for **I5**,
 1085 OWA produces the best results while AAMR produces the worst. By relaxing constraints **I3** and
 1086 **I4**, it has similar but less pronounced findings. However, the quality of the results produced by
 1087 MaxA and MinA is significantly worsen if it moves away from the extreme cases reflected by **I2**
 1088 and **I5**. In the general case, represented by **I1**, the Hurwicz ($\alpha = 0.4$) and OWA instantiations
 1089 are the best choices, with the former producing more results in the higher ranks and the latter
 1090 producing fewer results in the lower ranks.

1091 6.3. Unreliable payoffs

1092 Let A_a be a singleton set of targets and u_i^+ (resp. u_i^-) be a positive (resp. negative) point-
 1093 valued payoff for A_a with respect to a player $i \in N$ and an attacker type $t \in T$. Given some

^{‡‡}Note that figure 3 and figure 6 have only 9 unique ranks because the maximum expected payoff for MinA and MaxA are identical to the ground truth game under constraints **I2** and **I5**, respectively.

Figure 2. Maximum expected payoff ranking for transformation rules with interval constraint I1.

Figure 3. Maximum expected payoff ranking for transformation rules with interval constraint I2

Figure 4. Maximum expected payoff ranking for transformation rules with interval constraint I3

Figure 5. Maximum expected payoff ranking for transformation rules with interval constraint I4

Figure 6. Maximum expected payoff ranking for transformation rules with interval constraint I5

Figure 7. Maximum expected payoff ranking for each transformation rule with reliability constraint L1.

Figure 8. Maximum expected payoff ranking for each transformation rule with reliability constraint L2.

Figure 9. Maximum expected payoff ranking for each transformation rule with reliability constraint L3.

random $1-\tau \in (0, 1)$ for A_a and t , a random positive (resp. negative) unreliable payoff for A_a and each $i \in N$ with respect to t can be defined as $\{u_i^+ : 1-\tau\}$ (resp. $\{u_i^- : 1-\tau\}$). To analyse each transformation rule's effect on an ambiguous security game with unreliable payoffs, our experiments consider the three constraints:

- L1: No constraints on $1-\tau$;
- L2: $0 < 1-\tau < 0.5$;
- L3: $0.5 < 1-\tau < 1$.

Intuitively, **L1** requires that each new reliability degree is valid (*i.e.*, a value between 0 and 1) of the ground-truth payoff. Instead, **L2** (resp. **L3**) requires that the ground-truth payoff be assessed as mostly unreliable (resp. mostly reliable).

Figures 7–9 show the results for each constraint for 1,000 randomly generated ground-truth games, where the ranking for each transformation rule are determined as before. These figures show that the choice of transformation rule impacts less on the quality of results when dealing with unreliable payoffs than with interval-valued payoffs. In other words, the numbers of samples found across all the rankings for each instantiation are broadly similar, whether the point-valued payoffs are mostly unreliable in **L2** or mostly reliable in **L3**. However, there are some exceptions. For example, the AAMR transformation rule produces significantly fewer results in the lower ranking in **L3**, where the results are mostly reliable. Instead, the MinA and Hurwicz ($\alpha = 0.8$) rules produce more results in the higher rankings in **L2**, where the results are mostly unreliable. This latter finding may be explained by the pessimistic nature of the two rules. In the general case, represented by **L1**, the Hurwicz ($\alpha = 0.2$ and $\alpha = 0.4$) instantiations are arguably the best choices, with the former producing more results in the higher ranks and the latter producing fewer results in the lower ranks.

7. RELATED WORK

This section will discuss related work to show how our work advances the state of the art in the area of security game and ambiguous game.

7.1. Bayesian Stackelberg games

The problem of modelling uncertainty has become a key challenge in the realm of security. Existing approaches are primarily based on Bayesian Stackelberg games, which model

probabilistic uncertainty over the attacker’s motivation.^{3,4,5} Paruchuri et al.⁴¹ provide a mixed-integer linear programming formulation for solving Bayesian Stackelberg games. Kar et al.¹¹ present a stochastic human behaviour model with attractiveness and probability weighting for repeated Stackelberg Security game. Blocki et al.⁴² propose a generalised Stackelberg audit game model, called fully polynomial time approximation scheme, to address the practical auditing application with multiple audit resources. Brown et al.⁹ introduce a formal threat screening game model based on Bayesian Stackelberg games to optimally utilise limited screening resources. Zhang et al.⁴³ propose a Bayesian Stackelberg game between a defender and an adversary for improving chemical plant protection from threats of suicide bombers and environmental activists, considering multiple types of adversaries. Bai et al.⁴⁴ apply Bayesian Stackelberg games to mobile edge computing to deal with potential security and privacy issues of mobile users. Jiang and Liu⁴⁵ build a Bayesian Stackelberg game model for preventing an interdiction on water supply networks. However, Bayesian Stackelberg games can only address uncertainty in the form of risk and require precise point-valued payoffs and a probability distribution over attacker types. As such, this model cannot handle security games with ambiguity, where exact probabilities cannot always be assigned to possible payoffs.

7.2. Ambiguous security games

Recently, there has been much interest in the subject of ambiguity in security games. Kelsey et al.^{46,47} show that ambiguous preferences can cause players to pursue strategies with high equilibrium payoffs and ambiguity-aversion can make strategies with low equilibrium payoffs less attractive. Similarly, De Marco and Romaniello⁴⁸ study the effect of various preferences in strategic form games under ambiguous belief. And since various preferences provide an explicit parametrisation of the attitude of a decision maker to ambiguity, their work adds more flexibility to the game theory with ambiguity. Bade⁴⁹ proposes a game-theoretic framework with the nature of ambiguity-aversion on equilibrium outcomes based on the relaxation of randomised strategies. Battigalli et al.⁵⁰ analyse a notion of self-confirming equilibrium with non-neutral ambiguity attitudes, which generalises the traditional equilibrium concept. They show that a higher ambiguity aversion implies a weaker incentive to deviate from an equilibrium strategy. Moreover, Battigalli et al.⁵¹ discuss self-confirming equilibrium in sequential games with different attitudes to ambiguity. However, none of these studies handle the types of ambiguity addressed in the framework proposed in this paper.

Researchers also introduce some non-equilibrium solution concepts to handle ambiguity in security games. Kiekintveld et al.¹⁵ propose a method to find a strategy for the defender, which can maximise their worst-case payoff when the defender’s uncertainty over the attacker’s payoffs are intervals. The major disadvantage of the maximin strategy is that it may result in overly pessimistic behaviour. For example, suppose a lottery game sells \$1 per ticket with a 99% chance of winning \$5,000, then the maximin strategy would reject the offer, since the potential loss of \$1 could lead to lower minimum payoff than not playing at all. To overcome this problem, Nguyen et al.¹⁹ propose a method which uses minimax regret as a decision criterion for interval-valued payoffs. The disadvantage of this approach is that it has the potential for unaffordable losses. For example, suppose a lottery sells \$1,000 per ticket with a 1% chance of winning \$5,000, then the minimax regret strategy would always accept this offer. Our framework solves these issues by allowing the selection of different transformation rules (including the maximin or minimax regret rules) in different situations. Thus, our framework is more general than any other model that can handle imprecise payoffs only, because ours handle other types of ambiguity, such as unreliable payoffs, absent payoffs, and ambiguous payoff assignments.

Nguyen et al.¹⁸ propose a unified robust algorithm for handling three aspects of security games which may be affected by uncertainty: the attacker’s payoffs, the defender’s strategy commitment, and the attacker rationality. Yet this work again assumes that the attacker only has interval-valued payoffs and so cannot handle other types of ambiguity commonly found in real-world problems.

Our conference paper²⁵ (only 8-page long) studies a security game with ambiguous payoffs as well. However, our work in the current paper is different in the following aspects. First, the transform method is extended in our conference paper into a set of the underlying tenets of the existing rules from decision theory. Therefore, our method in this paper can characterise different attitudes to ambiguity during the transformation of ambiguous payoffs into point payoffs. The one in the conference can reflect one attitude to ambiguity (*i.e.*, the ambiguity aversion of minimax regret) only. Second, this paper introduces the concept of a projected point-valued payoff function with the properties: Boundary, Preference, Conservative Estimation, and Uniform Convex Combination. The concept reflects the essence of the transform methods. Thus, a set of underlying principles of the existing rules from decision theory can be considered for transforming ambiguous payoffs to point-valued payoffs. Third, our framework has been proved holds some good properties: it subsumes traditional security games when no ambiguous payoffs exist, a uniform margin of error in estimating ambiguous payoffs does not affect the result of the game studied, and the influence of complete ignorance on payoffs can be minimised. Fourth, our framework is evaluated by using nine different transformation rules, under various conditions and constraints, against 73,000 randomly generated games (a first comprehensive empirical evaluation to date). The evaluation reveals the benefits of each transformation rule and confirms that different rules can model individuals' different attitudes to ambiguity.

Another paper⁵² of ours also deal with security games with ambiguous payoffs. However, the current paper uses security games for solving the problem of offline patrol scheduling under ambiguity, while the previous one uses security for solving the problem of online surveillance-driven resource allocation. As a result, these two papers are different in the aspects of conceptualization, methodology, formal analysis, motivations, validation and experiments.

In addition, Zhang et al.⁵³ deal with the issue that in a Bayesian Stackelberg game model, the defender does not precisely have the probability of each type of the attacker, and define a new kind of security games with ambiguous information about the attacker's types. They also propose a method for finding the optimal mixed strategy for the defender in a game of this kind. Besides, they do lots of experiments to evaluate their model. However, their game model is not concerned with ambiguous payoffs in the game.

7.3. Ambiguous games

Some researchers apply D-S theory to matrix games with ambiguous payoff. Ma et al.¹⁶ study how to solve a matrix game with missing, imprecise, ambiguous lottery payoffs, and even compound strategy profile. They also reveal some properties of matrix games of this kind and give an example to illustrate how their approach solve such a game in real-life. However, the previous work is different from the current one in the following aspects. First, the previous work theoretically extends tradition matrix game with ambiguities, while the current one is the application of security game with ambiguities. As a result, the focus of the previous one is on the theoretical innovation of game theory and giving a new solution concept: ambiguous Nash equilibrium. Instead, the current one focuses on the application of ambiguous Nash equilibrium in security game with ambiguities. Second, since the ambiguous Nash equilibrium cannot directly be applied in security game with ambiguities, some important improvement have been made: (i) a set of underlying principles of the existing rules from decision theory are used, as a way to characterise different attitudes to ambiguity, during the transformation of ambiguous payoffs into point payoffs; (ii) the concept of a projected point-valued payoff function is introduced to make a set of decision rules applied in security game with ambiguities. Third, the current one also conducts extensive experiments (73,000 randomly generated games) to evaluate our framework using nine different transformation rules, while the previous one does not make any experiments.

Similarly, Zhou and Xiao⁵⁴ present a new matrix game with payoffs of generalised Dempster-Shafer structures. Their generalized Dempster-Shafer structures mean to present probability nonspecificity and inaccuracy as interval-values and then payoffs in such a game

are determined by linear programming. They use a zero-sum matrix game to illustrate the effectiveness of their method. Deng et al.⁵⁵ develops a zero-sum matrix game model with ambiguous payoffs represented by Dempster-Shafer belief structure. They also propose a Monte Carlo simulation approach to solve the game. Besides, they apply their model to the sensor selection and intrusion detection of sensor networks and shows its applicability and effectiveness. However, in each of these matrix games, all players take their strategies at the same time, while in a security game studied in this paper, one player takes a strategy first and then the other takes a strategy accordingly. Moreover, the meaning of their ambiguous payoffs is also different from ours.

There are also some researchers who use other theories similar to D-S theory to handle matrix games with ambiguous payoffs. For example, Yager and Alajlan⁵⁶ propose Maxitive Belief Structure (MBS) as an alternative class of belief structure. Similar to D-S theory, it can also model both probability nonspecificity and imprecise. Thus, Han and Deng⁵⁷ present a novel matrix game with payoffs of MBS and develop an effective method to find the solution of such a game through reaching an equilibrium point. They also give a numerical example to show the effectiveness of their model. This work is different from ours in two aspects: (i) it is based on MBS, while ours is based on D-S theory; and (ii) their game model is matrix game, while ours is Bayesian Stackelberg game.

There are some studies involving other forms of game. In a Bayesian game, a player can have a precise probability of each type of the other players. However, in reality, it is not always the case. Sometimes it is likely that one player just has a probability distribution over some sets of the types of the other players. To this end, Zhang et al.⁵⁸ extend the model of Bayesian games to the one with ambiguous types of players. They also discuss how to solve this kind of games and some properties of a solution. However, they did not concern any ambiguous payoff in their game model, and their model is irrelevant to security games. Yu et al.⁵⁹ study the uncertain coalition structure game with payoffs of belief structure based on belief structures of DCS theory. They propose a method to solve a game of this kind and enable the players to choose their allocation scheme according to their risk tolerance. However, coalition structure game is completely different from Bayesian Stackelberg game that studied in this paper. Deng et al.⁶⁰ study zero-sum polymatrix games with uncertain links modelled by Dempster-Shafer evidence theory. In a conventional polymatrix game, multiple players interact pairwise. That is, one player interacts with another that directly links to it. In their uncertain link one, the connections between players become ambiguous. Then, they propose a method to calculate the equilibrium payoffs of players and find the equilibria of the zero-sum polymatrix games with belief links. Also, they illustrate the potential applications of their method by a numerical example.

However, this kind of games are different from ours, and its ambiguity just involves links between its players rather than its payoffs like ours.

8. CONCLUSIONS AND FUTURE WORK

Handling ambiguity (or uncertainty in general) is essential for the real applications of intelligent systems, so there is no exception for security games. However, since security games is an emerging field, compared to many well-established areas in Artificial Intelligence, there has not been much work concerning various types of uncertainty, besides probabilistic information over attacker types. Thus, this paper addresses security games with ambiguous payoffs. Our work advances the theoretical research in security games in the following aspects. (i) It handles different types of ambiguous payoff of defenders and attackers. (ii) Different decision-theoretic approaches have been examined to interpreting their ambiguous payoffs. And (iii) our method has been empirically evaluated for solving ambiguous security games in different conditions and reveal some insights into its behaviours in practice. Our work in this paper is also valuable for the theoretical understanding of the connection between ambiguous and traditional security games and how our new framework copes with the transition from ambiguous games to

1276 traditional ones. Moreover, some intrinsic insights into this connection have been revealed as
 1277 follows: (i) our framework subsumes traditional games; (ii) a uniform margin of error cannot
 1278 affect the results; and (iii) our framework can minimise the effect of complete ignorance on the
 1279 final result.

1280 However, in the future, it is worth improve and extend our work in many aspects, such as
 1281 the following ones. (i) Some psychological studies on different attitudes to ambiguity can be
 1282 done to confirm our different the ambiguity-aversion instantiations. (ii) The event reasoning
 1283 framework^{61,62} can be used as a platform to check the power of our work in practice. (iii)
 1284 It is also significant to study games with complicated fuzzinesses modelled by Pythagorean
 1285 fuzzy set^{63,64}, Fermatean fuzzy sets⁶⁵ and maxitive belief structure theory⁵⁶. Perhaps some
 1286 decision methods^{66,67} on these complicated fuzzy sets can be applied to security games of such
 1287 fuzzy payoffs. (iv) The performance of some new uncertainty measures in information science
 1288 (e.g., the Pseudo-Pascal triangle based the maximum Deng entropy⁶⁸, probability transform
 1289 based on the ordered weighted averaging and entropy difference⁶⁹, and the interval-valued
 1290 Pythagorean prioritized operator⁷⁰, etc.) can be examined based on our framework.

ACKNOWLEDGMENTS

1291 The work was supported by EPSRC PACES project (Ref: EP/J012149/1), the
 1292 National Natural Science Foundation of China (Nos. 61772210, 61272066, 61806080, and
 1293 61762016), Humanities and Social Sciences Foundation of Ministry of Education of China
 1294 (No. 18YJC72040002), Guangzhou Key Laboratory of Big Data and Intelligent Education
 1295 (No.201905010009), Guangdong Province Universities and Colleges Pearl River Scholar
 1296 Funded Scheme (2018), the Project of Science and Technology in Guangzhou in China
 1297 (No. 201807010043), Key Project in Universities in Guangdong Province of China (No.
 1298 2016KZDXM024), Key Projects of the National Social Science Foundation of China (No.
 1299 19ZDA041), the Project of Department of Education of Guangdong Province of China (No.
 1300 2017KQNCX048), the Doctoral Start-up Project of Natural Science Foundation of Guangdong
 1301 Province of China (No. 2018A030310529), and a research fund of Guangxi Key Lab of Multi-
 1302 Source Information Mining & Security (No. 19-A-01-01). Also, it was partially undertaken by
 1303 some authors at Queen's University Belfast, Northern Ireland.

REFERENCES

- 1304 [1] C. Casorrán, B. Fortz, M. Labbé, and F. Ordóñez, "A study of general and security
 1305 Stackelberg game formulations," *European Journal of Operational Research*, vol. 278,
 1306 no. 3, pp. 855–868, 2019.
- 1307 [2] W. Ma, W. Liu, X. Luo, K. McAreavey, Y. Jiang, and J. Ma, "A Dempster-Shafer
 1308 theory and uninorm-based framework of reasoning and multiattribute decision-making
 1309 for surveillance system," *International Journal of Intelligent Systems*, vol. 34, no. 11,
 1310 pp. 3077–3104, 2019.
- 1311 [3] D. Kar, T. H. Nguyen, F. Fang, M. Brown, A. Sinha, M. Tambe, and A. X. Jiang, "Trends
 1312 and applications in Stackelberg security games," *Handbook of Dynamic Game Theory*,
 1313 pp. 1–47, 2017.
- 1314 [4] A. Sinha, F. Fang, B. An, C. Kiekintveld, and M. Tambe, "Stackelberg security games:
 1315 Looking beyond a decade of success," in *Proceedings of the 27th International Joint*
 1316 *Conference on Artificial Intelligence*, pp. 5494–5501, 2018.
- 1317 [5] M. Tambe, *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*.
 1318 Cambridge University Press, 2011.

- 1319 [6] B. Wang, Y. Zhang, Z.-H. Zhou, and S. Zhong, “On repeated Stackelberg security game
1320 with the cooperative human behavior model for wildlife protection,” *Applied Intelligence*,
1321 vol. 49, no. 3, pp. 1002–1015, 2019.
- 1322 [7] Q. Guo, J. Gan, F. Fang, L. Tran-Thanh, M. Tambe, and B. An, “On the inducibility of
1323 Stackelberg equilibrium for security games,” in *Proceedings of the 33rd AAAI Conference*
1324 *on Artificial Intelligence*, vol. 33, pp. 2020–2028, 2019.
- 1325 [8] T. H. Nguyen and H. Xu, “Imitative attacker deception in Stackelberg security games,”
1326 in *Proceedings of the 28th International Joint Conference on Artificial Intelligence*,
1327 pp. 528–534, 2019.
- 1328 [9] M. Brown, A. Sinha, A. Schlenker, and M. Tambe, “One size does not fit all: A game-
1329 theoretic approach for dynamically and effectively screening for threats,” in *Proceedings*
1330 *of the 30th AAAI Conference on Artificial Intelligence*, pp. 425–431, 2016.
- 1331 [10] L. Jian, A. M. Smith, and Y. Vorobeychik, “Multidefender security games,” *IEEE*
1332 *Intelligent Systems*, vol. 32, no. 1, pp. 50–60, 2017.
- 1333 [11] D. Kar, F. Fang, F. Delle Fave, N. Sintov, and M. Tambe, “A game of thrones: When
1334 human behavior models compete in repeated Stackelberg security games,” in *Proceedings*
1335 *of the 14th International Conference on Autonomous Agents and Multiagent Systems*,
1336 pp. 1381–1390, 2015.
- 1337 [12] C. Kiekintveld, J. Marecki, and M. Tambe, “Approximation methods for infinite Bayesian
1338 Stackelberg games: Modeling distributional payoff uncertainty,” in *Proceedings of the 10th*
1339 *International Conference on Autonomous Agents and Multiagent Systems*, pp. 1005–
1340 1012, 2011.
- 1341 [13] D. Ellsberg, “Risk, ambiguity, and the Savage axioms,” *Quarterly Journal of Economics*,
1342 vol. 75, pp. 643–669, 1961.
- 1343 [14] F. Fang, T. H. Nguyen, R. Pickles, W. Y. Lam, G. R. Clements, B. An, A. Singh,
1344 M. Tambe, and A. Lemieux, “Deploying PAWS: Field optimization of the protection
1345 assistant for wildlife security,” in *Proceedings of the 28th Annual Conference on*
1346 *Innovative Applications of Artificial Intelligence*, pp. 3966–3973, 2016.
- 1347 [15] C. Kiekintveld, T. Islam, and V. Kreinovich, “Security games with interval uncertainty,”
1348 in *Proceedings of the 12th International Conference on Autonomous Agents and Multi-*
1349 *agent Systems*, pp. 231–238, 2013.
- 1350 [16] W. Ma, X. Luo, and Y. Jiang, “Matrix games with missing, interval, and ambiguous
1351 lottery payoffs of pure strategy profiles and compound strategy profiles,” *International*
1352 *Journal of Intelligent Systems*, vol. 33, no. 3, pp. 529–559, 2018.
- 1353 [17] T. H. Nguyen, F. M. Delle Fave, D. Kar, A. S. Lakshminarayanan, A. Yadav, M. Tambe,
1354 N. Agmon, A. J. Plumptre, M. Driciru, F. Wanyama, *et al.*, “Making the most of
1355 our regrets: Regret-based solutions to handle payoff uncertainty and elicitation in
1356 green security games,” in *International Conference on Decision and Game Theory for*
1357 *Security*, pp. 170–191, Springer, 2015.
- 1358 [18] T. H. Nguyen, A. X. Jiang, and M. Tambe, “Stop the compartmentalization: Unified
1359 robust algorithms for handling uncertainties in security games,” in *Proceedings of the 13th*
1360 *International Conference on Autonomous Agents and Multi-Agent Systems*, pp. 317–
1361 324, 2014.
- 1362 [19] T. H. Nguyen, A. Yadav, B. An, M. Tambe, and C. Boutilier, “Regret-based optimization
1363 and preference elicitation for Stackelberg security games with uncertainty,” in *Proceedings*
1364 *of the 28th AAAI Conference on Artificial Intelligence*, 2014.

- 1365 [20] X. Gao and Y. Deng, "Quantum model of mass function," *International Journal of*
1366 *Intelligent Systems*, vol. 35, no. 2, pp. 267–282, 2020.
- 1367 [21] Z. Luo and Y. Deng, "A vector and geometry interpretation of basic probability
1368 assignment in Dempster-Shafer theory," *International Journal of Intelligent Systems*,
1369 vol. 35, no. 6, pp. 944–962, 2020.
- 1370 [22] G. Shafer, *A Mathematical Theory of Evidence*. Princeton University Press, 1976.
- 1371 [23] R. R. Yager, "Satisfying uncertain targets using measure generalized Dempster-Shafer
1372 belief structures," *Knowledge-Based Systems*, vol. 142, pp. 1–6, 2018.
- 1373 [24] T. Seidenfeld, "A contrast between two decision rules for use with (convex) sets of
1374 probabilities: Γ -maximin versus E-admissibility," *Synthese*, vol. 140, no. 1-2, pp. 69–88,
1375 2004.
- 1376 [25] W. Ma, X. Luo, and W. Liu, "An ambiguity aversion framework of security games under
1377 ambiguities," in *Proceedings of the 23rd International Joint Conference on Artificial*
1378 *Intelligence*, pp. 271–278, 2013.
- 1379 [26] W. Ma, W. Xiong, and X. Luo, "A model for decision making with missing, imprecise, and
1380 uncertain evaluations of multiple criteria," *International Journal of Intelligent Systems*,
1381 vol. 28, no. 2, pp. 152–184, 2013.
- 1382 [27] M. J. Osborne *et al.*, *An introduction to game theory*. New York: Oxford University
1383 Press, 2004.
- 1384 [28] E. T. Jaynes, *Probability theory: The logic of science*. Cambridge University Press, 2003.
- 1385 [29] T. M. Strat, "Decision analysis using belief functions," *International Journal of*
1386 *Approximate Reasoning*, vol. 4, no. 5-6, pp. 391–417, 1990.
- 1387 [30] D. Dubois and H. Prade, "A note on measures of specificity for fuzzy sets," *International*
1388 *Journal of General Systems*, vol. 10, no. 4, pp. 279–283, 1985.
- 1389 [31] A.-L. Jousselme, C. Liu, D. Grenier, and E. Bossé, "Measuring ambiguity in the evidence
1390 theory," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and*
1391 *Humans*, vol. 36, no. 5, pp. 890–903, 2006.
- 1392 [32] J. Pita, M. Jain, F. Ordóñez, C. Portway, M. Tambe, and C. Western, "Using Game
1393 Theory for Los Angeles Airport Security," *AI Magazine*, pp. 43–57, 2009.
- 1394 [33] R. Yang, F. Ordóñez, and M. Tambe, "Computing optimal strategy against quantal
1395 response in security games," in *Proceedings of the 11th International Conference on*
1396 *Autonomous Agents and Multiagent Systems*, pp. 847–854, 2012.
- 1397 [34] J.-Y. Jaffray and M. Jeleva, "Information processing under imprecise risk with the
1398 Hurwicz criterion," in *Proceedings of the 5th International Symposium on Imprecise*
1399 *Probability: Theories and Applications*, pp. 233–242, 2007.
- 1400 [35] P. Smets and R. Kennes, "The transferable belief model," *Artificial Intelligence*, vol. 66,
1401 no. 2, pp. 191–234, 1994.
- 1402 [36] R. R. Yager, "Families of OWA operators," *Fuzzy Sets and Systems*, vol. 59, no. 2,
1403 pp. 125–148, 1993.
- 1404 [37] W. Ma, X. Luo, and W. Xiong, "A novel D-S theory based AHP decision apparatus under
1405 subjective factor disturbances," *Advances in Artificial Intelligence*, vol. 7691, pp. 863–
1406 877, 2012.

- 1407 [38] J. C. Harsanyi and R. Selten, “A generalized Nash solution for two-person bargaining
1408 games with incomplete information,” *Management Science*, vol. 18, no. 5-Part-2, pp. 80–
1409 106, 1972.
- 1410 [39] J. W. Weibull, *Evolutionary Game Theory*. The MIT Press, 1995.
- 1411 [40] D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, and M. Tambe, “Stackelberg vs.
1412 Nash in security games: An extended investigation of interchangeability, equivalence, and
1413 uniqueness,” *Journal of Artificial Intelligence Research*, vol. 41, no. 2, pp. 297–327, 2011.
- 1414 [41] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordóñez, and S. Kraus, “Playing
1415 games for security: An efficient exact algorithm for solving Bayesian Stackelberg games,”
1416 in *Proceedings of the 7th International Joint Conference on Autonomous Agents and*
1417 *Multiagent Systems*, pp. 895–902, 2008.
- 1418 [42] J. Blocki, N. Christin, A. Datta, A. D. Procaccia, and A. Sinha, “Audit games with
1419 multiple defender resources,” in *Proceedings of the 29th AAAI Conference on Artificial*
1420 *Intelligence*, pp. 791–797, 2015.
- 1421 [43] L. Zhang and G. Reniers, “Applying a bayesian Stackelberg game for securing a chemical
1422 plant,” *Journal of Loss Prevention in the Process Industries*, vol. 51, pp. 72–83, 2018.
- 1423 [44] Y. Bai, L. Chen, L. Song, and J. Xu, “Bayesian Stackelberg game for risk-aware edge
1424 computation offloading,” in *Proceedings of the 6th ACM Workshop on Moving Target*
1425 *Defense*, pp. 25–35, 2019.
- 1426 [45] J. Jiang and X. Liu, “Bayesian Stackelberg game model for water supply networks against
1427 interdictions with mixed strategies,” *International Journal of Production Research*,
1428 pp. 1–21, 2020.
- 1429 [46] J. Eichberger and D. Kelsey, “Are the treasures of game theory ambiguous?,” *Economic*
1430 *Theory*, vol. 48, no. 2, pp. 313–339, 2011.
- 1431 [47] D. Kelsey and S. Le Roux, “Dragon slaying with ambiguity: Theory and experiments,”
1432 *Journal of Public Economic Theory*, vol. 19, no. 1, pp. 178–197, 2017.
- 1433 [48] G. De Marco and M. Romaniello, “Variational preferences and equilibria in games under
1434 ambiguous belief correspondences,” *International Journal of Approximate Reasoning*,
1435 vol. 60, pp. 8–22, 2015.
- 1436 [49] S. Bade, “Ambiguous act equilibria,” *Games and Economic Behavior*, vol. 71, no. 2,
1437 pp. 246–260, 2011.
- 1438 [50] P. Battigalli, S. Cerreia-Vioglio, F. Maccheroni, and M. Marinacci, “Self-confirming
1439 equilibrium and model uncertainty,” *American Economic Review*, vol. 105, no. 2, pp. 646–
1440 77, 2015.
- 1441 [51] P. Battigalli, E. Catonini, G. Lanzani, and M. Marinacci, “Ambiguity attitudes and self-
1442 confirming equilibrium in sequential games,” *Games and Economic Behavior*, vol. 115,
1443 pp. 1–29, 2019.
- 1444 [52] W. Ma, K. McAreevey, W. Liu, and X. Luo, “Acceptable costs of minimax
1445 regret equilibrium: A solution to security games with surveillance-driven probabilistic
1446 information,” *Expert Systems with Applications*, vol. 108, pp. 206–222, 2018.
- 1447 [53] Y. Zhang, X. Luo, and W. Ma, “Security games with ambiguous information about
1448 attacker types,” in *AI 2013: Advances in Artificial Intelligence*, vol. 8272 of *Lecture*
1449 *Notes in Computer Science*, pp. 14–25, 2013.

- 1450 [54] L. Zhou and F. Xiao, "A new matrix game with payoffs of generalized Dempster-Shafer
1451 structures," *International Journal of Intelligent Systems*, vol. 34, no. 9, pp. 2253–2268,
1452 2019.
- 1453 [55] X. Deng, W. Jiang, and J. Zhang, "Zero-sum matrix game with payoffs of Dempster-
1454 Shafer belief structures and its applications on sensors," *Sensors*, vol. 17, no. 4, p. 922,
1455 2017.
- 1456 [56] R. R. Yager and N. Alajlan, "Maxitive belief structures and imprecise possibility
1457 distributions," *IEEE Transactions on Fuzzy Systems*, vol. 25, no. 4, pp. 768–774, 2016.
- 1458 [57] Y. Han and Y. Deng, "A novel matrix game with payoffs of Maxitive Belief Structure,"
1459 *International Journal of Intelligent Systems*, vol. 34, no. 4, pp. 690–706, 2019.
- 1460 [58] Y. Zhang, X. Luo, W. Ma, and H.-f. Leung, "Ambiguous Bayesian games," *International*
1461 *Journal of Intelligent Systems*, vol. 29, no. 12, pp. 1138–1172, 2014.
- 1462 [59] X. Yu, M. He, H. Sun, and Z. Zhou, "Uncertain coalition structure game with payoff of
1463 belief structure," *Applied Mathematics and Computation*, vol. 372, p. 125000, 2020.
- 1464 [60] X. Deng, W. Jiang, and Z. Wang, "Zero-sum polymatrix games with link uncertainty:
1465 A Dempster-Shafer theory solution," *Applied Mathematics and Computation*, vol. 340,
1466 pp. 101–112, 2019.
- 1467 [61] X. Hong, Y. Huang, W. Ma, S. Varadarajan, P. Miller, W. Liu, M. J. S. Romero, J. M.
1468 del Rincon, and H. Zhou, "Evidential event inference in transport video surveillance,"
1469 *Computer Vision and Image Understanding*, vol. 144, pp. 276–297, 2016.
- 1470 [62] M. J. Santofimia, J. Martinez-del Rincon, X. Hong, H. Zhou, P. Miller, D. Villa, and J. C.
1471 Lopez, "Hierarchical task network planning with common-sense reasoning for multiple-
1472 people behaviour analysis," *Expert Systems with Applications*, vol. 69, pp. 118–134, 2017.
- 1473 [63] R. R. Yager, "Pythagorean fuzzy subsets," in *Proceedings of 2013 Joint IFSA World*
1474 *Congress and NAFIPS Annual Meeting*, pp. 57–61, 2013.
- 1475 [64] R. R. Yager, "Properties and applications of pythagorean fuzzy sets," in *Imprecision*
1476 *and Uncertainty in Information Representation and Processing*, vol. 332 of *Studies in*
1477 *Fuzziness and Soft Computing*, pp. 119–136, 2016.
- 1478 [65] T. Senapati and R. R. Yager, "Fermatean fuzzy sets," *Journal of Ambient Intelligence*
1479 *and Humanized Computing*, vol. 11, no. 2, pp. 663–674, 2020.
- 1480 [66] C. Jana, T. Senapati, and M. Pal, "Pythagorean fuzzy dombi aggregation operators and its
1481 applications in multiple attribute decision-making," *International Journal of Intelligent*
1482 *Systems*, vol. 34, no. 9, pp. 2019–2038, 2019.
- 1483 [67] D. Liu, Y. Liu, and X. Chen, "Fermatean fuzzy linguistic set and its application in
1484 multicriteria decision making," *International Journal of Intelligent Systems*, vol. 34,
1485 no. 5, pp. 878–894, 2019.
- 1486 [68] X. Gao and Y. Deng, "The pseudo-pascal triangle of maximum deng entropy,"
1487 *International Journal of Computers Communications & Control*, vol. 15, p. 1006, 02
1488 2020.
- 1489 [69] L. Pan and Y. Deng, "Probability transform based on the ordered weighted averaging and
1490 entropy difference," *International Journal of Computers Communications & Control*,
1491 vol. 15, p. 3743, 06 2020.

- 1492 [70] Y. Han, Y. Deng, Z. Cao, and C. Lin, “An interval-valued pythagorean prioritized
1493 operator-based game theoretical framework with its applications in multicriteria group
1494 decision making,” *Neural Computing and Applications*, vol. 32, no. 12, pp. 7641–7659,
1495 2020.