ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

A Security Game Model under Cognitive Uncertainty

Xiaoyi Yan

P.G. Student, Department of Mathematics, Wuhan University of Science and Technology, Wuhan, Hubei, China

ABSTRACT: In today's information age, security problems are becoming increasingly complex, and the adversarial behavior between attackers and defenders constitutes a typical scenario of security games. Although the traditional Bayesian game model can address security game problems under incomplete information, it still has limitations when facing parameter uncertainty (e.g., interval data). In this paper, we propose a security game model under cognitive uncertainty, which extends the Bayesian game model to cope with interval uncertainty. This is achieved by introducing the Minimax Regret Principle and the idea of robust optimization. Our contributions are threefold: firstly, we introduce interval uncertainty into the security game model, describing the uncertainty of the attacker's and defender's capabilities, resources, and utility functions through interval data. This makes the model closer to realistic scenarios and enables it to handle more complex uncertainty problems. Secondly, we innovatively combine the Minimax Regret Principle with the idea of robust optimization. This provides a robust strategy choice for the defender's decision-making under uncertain environments and ensures the minimization of potential loss in the most unfavorable situation. Finally, we propose a security game model applicable to multiple types of defenders and attackers, thereby expanding the scope of application of Bayesian game models. And the effectiveness of the model is verified through numerical experiments. The results show that the model can provide defenders and attackers with reasonable decision-making basis under uncertain environments. This offers new theoretical support for the allocation of resources in the field of information security.

KEY WORDS: Cognitive Uncertainty, Security Game, Robust Optimization, Minimax Regret Principle.

I. INTRODUCTION

In the contemporary era of rapidly evolving information technology, security issues have permeated every facet of social production and daily life. Consequently, the application of game theory to the realm of network information security has gradually emerged as a novel research hotspot [1,2]. Security threats, ranging from network attacks and information leakage to the protection of physical infrastructure, are both complex and diverse, posing significant challenges to individuals, enterprises, and nations. How to effectively counter potential attack threats under limited resource constraints has become a focal point of interest in both academia and industry [3]. The essence of security problems lies in their inherently adversarial nature. Attackers typically seek to gain benefits or cause system damage, while defenders strive to safeguard the functionality and integrity of the system [4]. This adversarial dynamic renders many security-related issues amenable to analysis as typical game-theoretic problems. Modeling and analyzing offensive and defensive confrontations using game-theoretic methods can provide a theoretical foundation for developing defensive strategies [5]. Security game theory is a vital theoretical instrument for examining the strategic interactions between attackers and defenders in security contexts. It aims to explore, through mathematical modeling and analysis, how both parties can formulate optimal strategies to maximize their respective benefits or utilities under conditions of resource constraints and uncertainty. The core of security game theory lies in providing guidance for addressing practical security problems through the quantitative description and equilibrium analysis of strategy selection [6].

In traditional security game research, Bayesian games have been extensively employed to address type uncertainty, with applications spanning various security domains, including cybersecurity, critical infrastructure protection, and privacy preservation [7]. In security games characterized by incomplete information, participants—such as attackers and defenders—possess only partial knowledge of each other's types, intentions, or payoff functions. This lack of complete information significantly increases the complexity of the game. Bayesian games provide a framework for handling incomplete information by allowing participants to form probabilistic assessments of the types of other participants. Each participant is aware of their own type but holds only probabilistic estimates of the types of others. The types of participants

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

are characteristics that influence their payoffs, and their beliefs regarding the types of other participants are based on probability distributions. Defenders and attackers select strategies based on these probabilistic beliefs. Due to the incomplete information, these strategies are often determined based on expected payoffs.

In real life, there are various situations in which domain experts can learn about the embodiment of incomplete information, including ambiguities or uncertainties in the types, capabilities, resources, and intentions of attackers and defenders, as well as dynamic changes in the information and interference from the external environment. These situations have also been widely noticed and explored in existing studies, such as dealing with the ambiguity of information by introducing the fuzzy set theory [8,9], or analysing the impact of dynamic changes in information on strategy selection by means of dynamic game models [10]. In addition to these conducted researches, this paper further extends the Bayesian game and discusses the security game model under interval uncertainty by introducing the Minimax Regret Principle of acceptable gains [11], meanwhile, the security game model constructed in this paper is applicable to the case of multiple defenders and multiple types of attackers, and the defenders and attackers take actions almost at the same time. At the end of this paper, the constructed model is applied in a scenario of resource allocation in the field of information security, and the relationship between interval data information and optimal game solution is revealed through analysis and experimental comparison. The innovations of this paper are: (1) Introducing interval uncertainty into attack and defence security game models to make them more relevant to the complexity in real scenarios (2) Combining the Minimax Regret Principle with the idea of robust optimization, it extends the Bayesian security game model in the general case, and provides a new approach for decision-making in cognitively uncertain environments, especially for the defender strategies (3) The model is applicable to a security game that contains multiple types of defenders and attackers, and the model is applied in a resource allocation scenario in the field of information security.

II. BAYESIAN SECURITY GAMES WITH INCOMPLETE INFORMATION

In the field of security, attackers and defenders often face a situation of incomplete information: one side usually does not have a complete picture of the other side's capabilities, intentions or resources, which are crucial for strategic decisions. Bayesian security games under incomplete information provide an effective modelling approach for such problems by introducing type spaces and belief mechanisms. This model analyses how both parties can formulate optimal strategies to maximise gains or utility under information asymmetry by portraying uncertainty and strategy dependence in the types of participants [12]. Bayesian games, also known as incomplete information games, are an extended form of Stackelberg games. The classical Stackelberg game is a leader-follower game model that usually consists of a defender (leader) and an attacker (follower), where the defender acts first and chooses a mixed strategy, and then the attacker chooses his own attack strategy based on the observed strategy of the defender, in order to maximise his own gain [8]. In Bayesian game modelling, each participant in a Stackelberg game can be expanded into multiple possible types, each corresponding to a different payoff function [3]. The unique feature of the Bayesian game is the introduction of incomplete information: participants cannot be completely sure of the type of the opponent or the specific payoff function, but need to rely on some kind of a priori distribution or beliefs to speculate on the type of the opponent, and this feature of incomplete information significantly increases the complexity of the game, so that the participants need to balance the benefit and risk in the uncertainty in the choice of strategy.

Definition 1. Bayesian Security Game Model

The Bayesian security game introduces the following key elements to the classical security game:

1) Participant space:

$N=\left(N_A, N_D\right)$ is the participant space, N_A is the attacker space, N_D is the defender's space.

2) Player type space:

$S=\left(S_A, S_D\right)$ is the space of game participant types, where $S_A=\left(s_1^A, s_2^A, \ldots, s_{m_1}^A\right)$ is the set of attacker N_A's types, e.g. attacker's ability is classified as {high attack, medium attack, low attack}; and $S_D=\left(s_1^D, s_2^D, \ldots, s_{m_2}^D\right)$ is the set of defender N_D's types, similarly defender's ability can be classified as {high defence, medium defence, low defence}.

3) Player's Strategy Space:

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

Also called the set of targets of the attacker-defender: $\theta = \{t_1, t_2, ..., t_n\}$, i.e., the set of pure strategies of the attacker-defender, where n is the total number of targets.

4) Space of a priori probability distributions:

$P = (P_A, P_D)$ is the set of prior beliefs of the game participants, where $P_A(S_D \mid S_A)$ denotes the probability that the attacker knowing only his own type distribution, judges the defender to be of type S_D when the attacker is of type S_A. Similarly, $P_D(S_A \mid S_D)$ denotes the probability of judging the opponent to be a type S_A when the defender is a type S_D.

5) Space of revenue functions:

$U = (U_A, U_D)$ is the set of payoff functions for the participants of the game, where for $\forall t_i \in \theta, t_j \in \theta, s_A \in S_A, s_D \in S_D$, $U_A(t_i, t_j, s_A)$ denote the payoffs obtained by an attacker of type S_A adopting strategy i when the attacker attacks target i and the defender defends target j. $U_D(t_i, t_j, s_D)$ denotes the payoffs obtained by a defender of type S_D adopting strategy j when the attacker attacks target i and the defender defending target j.

The core feature of Bayesian attack-defense game models is their ability to handle incomplete information. By introducing types and prior distributions, these models can quantify and analyze the optimal strategy choices of attackers and defenders under uncertain conditions. Compared to traditional complete-information game models, Bayesian security game models better reflect the complexities of real-world scenarios, especially in uncertain environments with limited resources and high security risks.

Definition 2. Equilibrium Analysis in Game Theory

In a Bayesian security game with given participant space, type space, strategy space, prior probability distribution space and payoff function space, Bayesian Nash equilibrium refers to a combination of strategies where each participant's chosen strategy is his/her optimal response under the condition of knowing his/her own type and prior probability distributions about the types of other participants. In the actual network attack and defence game, when the types of the game participants are $S_A(S_D)$, and master the a priori beliefs about each other's types, each participant hopes to maximize its own gains through a reasonable choice of strategies. Under this condition of incomplete information, both parties will eventually reach a stable state through the game confrontation. In this state, neither party will actively change its action strategy, because any deviation from the current strategy will lead to a decline in its expected return, such a stable state is the Bayesian Nash Equilibrium [13].

Formal definitions:

In the Bayesian attack-defence game model (N, S, θ, P, U), i.e. $((N_A, N_D), (S_A, S_D), (t_i, t_j), (P_A, P_D), (U_A, U_D))$, where: the mixed strategy of the attacker is $F_A(s_A) = \{f_{A_1}(s_A), f_{A_2}(s_A), ..., f_{A_i}(s_A)\}$, denoting the mixed strategy distribution when the type of the attacker is s_A; and the mixed strategy of the defender is $F_D(s_D) = \{f_{D_1}(s_D), f_{D_2}(s_D), ..., f_{D_j}(s_D)\}$, denoting the mixed strategy distribution when the type of the defender is s_D. $\sum_i f_{A_i}(s_A) = 1$, $\sum_j f_{D_j}(s_D) = 1$, When the following

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

two conditions are satisfied at the same time, the combination of strategies $\left(F_A^*(s_A), F_D^*(s_D)\right)$ is called the mixed strategy Bayesian Nash Equilibrium of this game model:

1) Optimality conditions for the attacker:

$$\sum_{s_D \in S_D} P_A(s_D \mid s_A) \cdot U_A\left(F_A^*(s_A), F_D^*(s_D), s_A\right) \geq \sum_{s_D \in S_D} P_A(s_D \mid s_A) \cdot U_A\left(F_A(s_A), F_D^*(s_D), s_A\right).$$

2) Optimality conditions for the defender:

$$\sum_{s_A \in S_A} P_D(s_A \mid s_D) \cdot U_D\left(F_A^*(s_A), F_D^*(s_D), s_D\right) \geq \sum_{s_A \in S_A} P_D(s_A \mid s_D) \cdot U_D\left(F_A^*(s_A), F_D(s_D), s_D\right).$$

III. SECURITY GAME MODELING UNDER COGNITIVE UNCERTAINTY

In the previous section, we defined a Bayesian security game model under incomplete information and analyzed how participants update their strategies based on prior beliefs when the opponent's type is unknown. However, in practice, incomplete information may arise from multiple sources of uncertainty. For example, participants may not be able to obtain complete information about their opponent's behaviors or strategies. In security games, some model parameters—such as the attacker's capabilities, resources, and intentions—may not be accurately estimated. Additionally, the environments in which attackers and defenders operate may change, leading to fluctuations in game parameters. These uncertainties can hinder participants' ability to update their strategies effectively. In the face of ambiguous or imprecise information, participants may struggle to make clear decisions. Furthermore, there may be differences between attackers and defenders in their understanding of the game model, interpretation of information, or ability to predict future events.

In this paper, we focus on cognitive uncertainty caused by interval data, which is often characterized by ranges rather than precise values. For example, an attacker's capabilities may fluctuate within a certain range, and a defender's resources may be uncertain due to external factors. This type of uncertainty arises from various factors, such as measurement errors, environmental fluctuations, and external influences. Specifically, the attacker's capabilities and the defender's resources are often not fixed but may vary within specific intervals. Accurately predicting the outcomes of chosen strategies can be challenging, especially in complex and dynamic security environments. In security games, attackers and defenders typically face multiple objectives whose values or importance are difficult to quantify precisely. Given these challenges, we need to introduce interval analysis methods into security game models. These methods describe the uncertainties in participants' capabilities (types), resources (strategies), and payoffs by handling interval data. Under interval uncertainty, participants must choose strategies by considering worst-case scenarios to maximize their gains or utility in an uncertain environment.

In this section, we introduce the Minimax Regret Principle [11] as a foundation for constructing Bayesian security game models under cognitive uncertainty. Specifically, we focus on modeling scenarios where parameter uncertainty is represented by interval data. To address this, we model the payoff function using interval parameters and incorporate the concept of robust optimization. Robust optimization is an approach that deals with uncertainty by finding an optimal solution that performs well in the worst-case scenario, without relying on specific distributions or exact estimates of uncertain parameters [14]. When dealing with interval data, participants face a range of possible values rather than specific values. This means that at the time of decision-making, participants cannot know the exact parameter values and must consider all possible values within the given intervals. The goal of robust optimization is to maximize participants' gains while accounting for all possible values within these intervals, thereby avoiding excessive losses in the worst-case scenario. For example, an attacker's capabilities may fluctuate within a certain interval. In response, a defender must choose a strategy that ensures system stability even when the attacker's capabilities are at their maximum.

A. Minimax Regret Principle [11]

The core idea of the Minimax Regret Principle is that when faced with uncertainty, the decision-maker does not directly seek to maximize gains but instead aims to minimize the maximum possible regret values. This principle is particularly applicable to defenders in security games. Rather than seeking to maximize gains in each situation, defenders focus on reducing potential losses in the most unfavorable scenario. This type of strategy selection is crucial in environments with

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

high uncertainty or incomplete information. For defenders, who know their own type but not the opponent's, the gains depend on both the types of the participants and the strategies chosen. Therefore, defenders prefer to minimize the worst-case maximum regret value rather than maximize the expected gain in their strategy selection.

The regret value is the value of the loss due to not using the relatively optimal solution in a given state. The maximum regret value of a strategy is the difference between the minimum gain value of selecting the strategy and the maximum gain value that can be obtained in a given state. The smaller the difference, the closer the strategy is to the maximum return. According to the Minimax Regret Principle, the defender selects the strategy that minimises the maximal regret value based on the consideration that the minimum expected gain value of the strategy is an acceptable gain. On the other hand, attackers are usually more concerned about the optimal gain and less concerned about the regret value or potential risk in strategy selection. Their goal is to obtain the most favourable outcome by selecting the strategy that maximises their gain, often regardless of the consequences. Such different strategy selection principles reflect the different decision-making patterns of attackers and defenders under uncertainty.

This principle is particularly important when dealing with the uncertainty introduced by interval data. In practice, attackers and defenders often do not know the precise values of their opponent's capabilities, resources, or modus operandi, but only the interval ranges of these parameters. By combining the Minimax Regret Principle with robust optimization, defenders can select an optimal strategy within these uncertain intervals to minimize the maximum regret value. Even if the attacker's behavior or capabilities fluctuate, the defender can remain robust through this strategy. This approach helps avoid wrong decisions due to incomplete information in the uncertain gaming environment and ensures that the best possible gain can still be achieved in the worst-case scenario. In a context where attackers tend to seek maximum gains while ignoring risks, this strategy allows the defender to achieve greater stability and responsiveness in the game.

B. Optimal Strategy Problem Construction

Next we construct a Bayesian security game model under incomplete information, and we will introduce some new notation definitions for the convenience of the discussion. The defender knows all possible attacker types S_A, but not their exact probability distributions. The defender needs to learn the probability distribution function $P_D\left(S_A \mid S_D\right)$ of the attacker types, and understand the attacker's type information. In order to obtain the optimal game strategy, in addition to the defender's payoff matrix, the defender needs to know the acceptable loss τ_{s_D} of the strategy it chooses, and the value is determined by the game strategy adopted by both the attacker and the defender and by its own payoff matrix. Similarly, the attacker needs to learn the information about the adversary and consider the acceptable loss τ_{s_A} before choosing a strategy. The attacker's gain represents the reward that the attacker obtains from an attack, i.e., the degree of threat posed to the data and information, and the damage caused to the entire system under attack. The larger value of the attacker's gain indicates that the information asset acquired is more sensitive and important, the greater the threat, and the greater the damage caused to the attacked system. The defender's gain indicates how much the defender is rewarded for adopting a defensive strategy against an attack strategy, i.e., the degree of containment of the attacker's attack and the ability to protect the entire system assets. The larger the value of defender's gain, the more effective the containment of the attacker's behaviour and the more powerful the protection of the entire system assets.

The defender minimises the maximum regret value: the defender seeks to minimise the maximum regret value $r_j^{s_D}$ in the face of the attacker's different strategies by choosing strategy $x_j^{s_D}$, thus reducing the worst-case losses.

The attacker maximises gains while considering acceptable losses: the attacker chooses strategy $q_i^{s_A}$ to maximise its own gains $U_A\left(t_i, t_j, s_A\right)$ by considering the likelihood of the defender's strategy while focusing on acceptable losses to ensure that the worst-case losses are not excessive.

We construct a Bayesian security game model as follows:

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

$$
\begin{aligned}
&\min_{X} \sum_{j\in\theta} x_j^{s_D} r_j^{s_D} \\
&s.t. \\
&r_j^{s_D} = \sum_{S_A} P_D \cdot \max_{i\in\theta}\left(\max_{k\in\theta, k\neq j} u_{s_D}(i,k) - u_{s_D}(i,j) \right) \\
&\sum_{j\in\theta} x_j^{s_D} = 1 \\
&0 \le x_j^{s_D} \le 1 \\
&\min_{i\in\theta} \sum_{S_A} P_D \cdot u_{s_D}(i,j) \ge \max_{k\in\theta} \min_{i\in\theta} \sum_{S_A} P_D \cdot u_{s_D}(i,k) - \tau_{s_D} \\
&\tau_{s_D} = \max_{k\in\theta} \min_{i\in\theta} \sum_{S_A} P_D \cdot u_{s_D}(i,k) - \min_{k\in\theta} \min_{i\in\theta} \sum_{S_A} P_D \cdot u_{s_D}(i,k)
\end{aligned}
\quad \text{……(1)}
$$

$$
\begin{aligned}
&\max_{Q} \sum_{i\in\theta} q_i^{s_A} U_A(i,j) \\
&s.t. \\
&\sum_{i\in\theta} q_i^{s_A} = 1 \\
&0 \le q_i^{s_A} \le 1 \\
&U_A(i,j) = \sum_{S_D} P_A \sum_{j\in\theta} x_j^{s_D} \cdot u_{s_A}(i,j) \\
&\min_{j\in\theta} \sum_{S_D} P_A \cdot u_{s_A}(i,j) \ge \max_{k\in\theta} \min_{j\in\theta} \sum_{S_D} P_A \cdot u_{s_A}(k,j) - \tau_{s_A} \\
&\tau_{s_A} = \max_{k\in\theta} \min_{j\in\theta} \sum_{S_D} P_A \cdot u_{s_A}(k,j) - \min_{k\in\theta} \min_{j\in\theta} \sum_{S_D} P_A \cdot u_{s_A}(k,j)
\end{aligned}
\quad \text{……(2)}
$$

With the introduction of the Minimax Regret Principle, we can more comprehensively understand the participants' strategy selection process under uncertainty. This lays the foundation for constructing a security game model under cognitive uncertainty induced by interval data. In the face of such uncertainty, robust optimization provides an effective strategy to ensure an optimal solution in the worst-case scenario by optimizing decision-making across all possible intervals. Meanwhile, the Minimax Regret Principle offers defenders a way to minimize potential losses and make robust decisions in uncertain environments. Together, these approaches can help us better address uncertainty in security games, thereby improving the quality of decision-making for both defenders and attackers in complex environments.

C. Discussion under Interval Data

Cognitive uncertainty typically arises from participants' incomplete or inaccurate estimation of critical information, especially when confronted with multiple possible attack methods, defense strategies, and changes in the external environment. This uncertainty affects not only the strategic choices of adversaries but also the estimation of their own resources, capabilities, and threats. In this context, traditional game-theoretic approaches face significant challenges, particularly in handling uncertainty parameters. To address these challenges, we introduce robust optimization and the Minimax Regret Principle into incomplete information game models. This integration provides participants with a decision-making framework that can still achieve desirable outcomes even in the worst-case scenario.

In the Bayesian security game framework under incomplete information proposed in the previous section, cognitive uncertainty refers to participants having imprecise knowledge about certain game parameters, such as the capabilities and resources of attackers or defenders. This imprecision affects their strategic choices. When introducing cognitive uncertainty, the key challenge is handling parameters that cannot be precisely known, typically represented as interval

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

data. This uncertainty means participants cannot explicitly know their exact gains or losses at the time of decision-making; instead, they only know the range of possible values. In other words, under interval uncertainty, the attacker's capabilities, the defender's resources, and their respective gain functions are all represented by intervals. In the model, each relevant parameter is adjusted to an interval form to account for the impact of these uncertainties on strategic choices and decision-making.

In summary, the problem of finding the defender's optimal strategy is described as:

$$
\begin{aligned}
&\min_{x}\left(\max_{P_D,u_{s_D}}\left(\sum_{j\in\theta} x_j^{s_D} r_j^{s_D}\right)\right)\\
&s.t.\\
&\sum_{j\in\theta} x_j^{s_D}=1\\
&0\le x_j^{s_D}\le 1\\
&P_D\in\left[P_{D,\min},P_{D,\max}\right]\\
&u_{s_D}(i,j)=\left[u_{s_D,\min},u_{s_D,\max}\right]\\
&r_{j,\min}^{s_D}=\sum_{S_A}\sum_{P_D\in\left[P_{D,\min},P_{D,\max}\right]} P_D\left(\left(u_{s_D,\min}(i,k)-u_{s_D,\max}(i,j)\right)\right)\\
&r_{j,\max}^{s_D}=\sum_{S_A}\sum_{P_D\in\left[P_{D,\min},P_{D,\max}\right]} P_D\left(\left(u_{s_D,\max}(i,k)-u_{s_D,\min}(i,j)\right)\right)\\
&\min_{i}\sum_{S_A} P_{D,\min}\cdot u_{s_D,\min}(i,j)\ge \max_{k\in\theta}\min_{i\in\theta}\sum_{S_A} P_{D,\min}\cdot u_{s_D,\min}(i,k)-\tau_{s_D}\\
&\tau_{s_D}=\max_{k\in\theta}\min_{i\in\theta}\sum_{S_A} P_{D,\max}\cdot u_{s_D,\max}(i,k)-\min_{k\in\theta}\min_{i\in\theta}\sum_{S_A} P_{D,\min}\cdot u_{s_D,\min}(i,k)
\end{aligned}
\qquad \text{……(3)}
$$

The objective function is to minimise the worst-case possible loss, in line with the idea of robust optimization, to effectively deal with the uncertainty introduced by interval data. The interval data is embodied in the attacker's capability and the defender's gain function transformed within a certain range. The regret value is calculated by extracting the minimum and maximum values of the regret value from the interval data in order for the defender to make a decision in the worst case, and the constraints also include that the minimum gain of the defender in the worst case will not be lower than a certain range of acceptable losses, i.e., the defence strategy is optimised based on the Minimax Regret Principle, and since P_D and $u_{s_D}(i,j)$ are uncertain, we take the minimum value of each of them to ensure that even in the most unfavourable scenario, the inequality still holds. The acceptable loss is calculated as the difference between the maximum and minimum of the minimum possible gains under all objectives. The first term calculates the maximum and minimum gain under all strategies k, where P_D and $u_{s_D}(i,k)$ are taken to be the maximum, ensuring that the term is calculated in the best case scenario. The latter term calculates the minimum minimum return under all strategies k, where P_D and $u_{s_D}(i,k)$ take the minimum value, ensuring that the term is calculated in the worst case.

Similarly, the problem of finding the attacker's optimal strategy is described as:

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

$$\max_{q} \min_{P_A, u_{s_A}} \sum_{j\in\theta} q_i^{s_A} U_A(i,j)$$
$$0 \le q_i^{s_A} \le 1$$
$$\sum_{i\in\theta} q_i^{s_A} = 1$$
$$P_A = \left[P_{A,\min}, P_{A,\max}\right]$$
$$u_{s_A}(i,j) = \left[u_{s_A,\min}(i,j), u_{s_A,\max}(i,j)\right]$$
$$U_{s_A,\min}(i,j) = \sum_{S_D} \underset{P_A\in\left[P_{A,\min},P_{A,\max}\right]}{P_A} \sum_{j\in\theta} x_j^{s_D} \cdot u_{s_A,\min}(i,j)$$
$$U_{s_A,\max}(i,j) = \sum_{S_D} \underset{P_A\in\left[P_{A,\min},P_{A,\max}\right]}{P_A} \sum_{j\in\theta} x_j^{s_D} \cdot u_{s_A,\max}(i,j)$$
$$\min_{j}\left(\sum_{S_D} P_A \cdot u_{s_A,\min}(i,j)\right) \ge \max_{k\in\theta} \min_{j\in\theta}\left(\sum_{S_D} P_A \cdot u_{s_A,\min}(k,j)\right) - \tau_{s_A}$$
$$\tau_{s_A} = \max_{k\in\theta} \min_{j\in\theta}\left(\sum_{S_D} P_{A,\max} \cdot u_{s_A,\max}(k,j)\right) - \min_{k\in\theta} \min_{j\in\theta}\left(\sum_{S_D} P_{A,\min} \cdot u_{s_A,\min}(k,j)\right)$$

……(4)

The model effectively handles the security game problem under incomplete information by combining Bayesian games, the Minimax Regret Principle and robust optimization, which needs to be solved by transforming the interval uncertainty into a worst-case deterministic optimisation problem and solving it by linear programming or pairwise methods.

In the current era of information technology, security problems are becoming more and more prominent, especially under the game model of incomplete information, the study of security games is particularly important. Especially for fields such as network security, not only the limited resources of attackers and defenders should be taken into account, but also the game relations under different types and objectives should be dealt with. Our proposed security game model under cognitive uncertainty can well address the situation of uncertainty in the types of attackers and defenders, and can help to formulate optimal attack and defence strategies. Finally, we will show how to find the equilibrium point in this extended model through a numerical case to further illustrate the effect of interval data on strategy selection and game outcome.

IV. NUMERICAL EXAMPLES

In order to verify the validity of the model, we design a simple numerical experiment to simulate a scenario of resource allocation in the security domain. Before the simulation we need to determine the set of the attacker and defender's types S_A, S_D, the interval of the payoff function for different scenarios, and the a priori probability. Suppose a network enterprise contains three key objectives: $\theta = \{t_1, t_2, t_3\}$, for ease of understanding and solving with the model, we can also represent the objectives as follows: against attacker policy: $\theta = \{i_1, i_2, i_3\}$; against defender policy: $\theta = \{j_1, j_2, j_3\}$. The enterprise needs to allocate limited defence resources to protect these assets, and an attacker tries to attack these assets to gain benefits. We assume that attackers and defenders are classified into two types according to their ability to attack and defend. Attacker Type: S_{A_1} (High Threat Attacker), S_{A_2} (Low Threat Attacker); Defender Type: S_{D_1} (High Protection Capability), S_{D_2} (Low Protection Capability). A priori probability distribution space:

attacker's a priori belief in the type of defender:

$$P_A\left(S_{D_1}\right) \in [0.3, 0.7], P_A\left(S_{D_2}\right) = 1 - P_A\left(S_{D_1}\right)$$

defender's a priori belief in the attacker:

$$P_D\left(S_{A_1}\right) \in [0.4, 0.6], P_D\left(S_{A_2}\right) = 1 - P_D\left(S_{A_1}\right)$$

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

Benefits for both attackers and defenders in Table1. Table2. (reflecting intervals of uncertainty, assuming intervals of data):

Table1. Attacker Benefits

S_{D_1} \ S_{A_1}	i_1	i_2	i_3
j_1	$[12,15]$	$[8,10]$	$[5,7]$
j_2	$[6,8]$	$[10,12]$	$[7,9]$
j_3	$[9,11]$	$[4,6]$	$[14,16]$

S_{D_2} \ S_{A_1}	i_1	i_2	i_3
j_1	$[10,12]$	$[6,8]$	$[3,5]$
j_2	$[5,7]$	$[8,10]$	$[9,11]$
j_3	$[7,9]$	$[2,4]$	$[12,14]$

S_{D_1} \ S_{A_2}	i_1	i_2	i_3
j_1	$[5,7]$	$[9,11]$	$[4,6]$
j_2	$[8,10]$	$[6,8]$	$[7,9]$
j_3	$[10,12]$	$[3,5]$	$[8,10]$

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

S_{D_2} \ S_{A_2}	i_1	i_2	i_3
j_1	$[7,9]$	$[4,6]$	$[5,7]$
j_2	$[3,5]$	$[7,9]$	$[6,8]$
j_3	$[6,8]$	$[9,11]$	$[5,7]$

Table2. Defender Benefits

S_{A_1} \ S_{D_1}	j_1	j_2	j_3
i_1	$[8,10]$	$[5,7]$	$[3,5]$
i_2	$[6,8]$	$[9,11]$	$[4,6]$
i_3	$[7,9]$	$[4,6]$	$[10,12]$

S_{A_2} \ S_{D_1}	j_1	j_2	j_3
i_1	$[4,6]$	$[7,9]$	$[2,4]$
i_2	$[5,7]$	$[3,5]$	$[8,10]$
i_3	$[9,11]$	$[6,8]$	$[5,7]$

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 12, Issue 3, March 2025

S_{A_1} \ S_{D_2}	j_1	j_2	j_3
i_1	$[3,5]$	$[6,8]$	$[2,4]$
i_2	$[5,7]$	$[4,6]$	$[7,9]$
i_3	$[8,10]$	$[3,5]$	$[5,7]$

S_{A_2} \ S_{D_2}	j_1	j_2	j_3
i_1	$[7,9]$	$[4,6]$	$[6,8]$
i_2	$[2,4]$	$[5,7]$	$[3,5]$
i_3	$[5,7]$	$[8,10]$	$[4,6]$

The solution is solved through a two-stage optimisation process: the defender adopts linear programming to determine the optimal hybrid strategy with the objective of minimising the maximum regret value, while the attacker selects the counter-strategy through robust optimisation under probability intervals with the objective of maximising the worst-case gain. The simulation results show that when the defender is of high protection type $\left(S_{D_1}\right)$, its optimal strategy is j_3, which corresponds to minimising the maximum regret value of 3.6; and when the attacker is of high threat type $\left(S_{A_1}\right)$, it chooses i_3, which yields a gain of 12.6 under the worst-case probability distribution. This also confirms the reasonableness and effectiveness of the model's decision-making in uncertain environments.

V. CONCLUSION AND RECOMMENDATION

In this paper, we propose a new game model for the security game problem under cognitive uncertainty, aiming to provide theoretical support for decision-making by attackers and defenders under conditions of incomplete information and interval uncertainty. First, we review the Bayesian security game model under incomplete information and analyze its advantages and limitations in handling type uncertainty. On this basis, we introduce the Minimax Regret Principle and the concept of robust optimization. We extend the traditional Bayesian game model to effectively address uncertainty caused by interval data and construct a security game model applicable to multiple defenders and multiple types of attackers. The model not only handles the uncertainty of participant types and payoff functions but also provides robust strategy choices for defenders in worst-case scenarios. Additionally, we verify the model's validity through numerical experiments. The results demonstrate that the model can provide a reasonable decision basis for both attackers and defenders in uncertain environments and reveal the impact of interval data on strategy selection and game outcomes. Although this paper achieves significant theoretical and practical results, several areas warrant further research. These include applying the model in more complex dynamic environments, optimizing computational efficiency for large-scale game scenarios, and exploring additional uncertainty modeling methods for broader security applications. In conclusion, the proposed security game model under cognitive uncertainty offers a novel approach and tool for addressing real-world security problems, especially in the context of incomplete information induced by interval data. This model can help participants make more robust decisions.

REFERENCES

[1]. Ni L M, Liu Y, Lau Y C, et al. "LANDMARC: Indoor location sensing using active RFID", Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003, pg no: 407-415.
[2]. YuanzhuoWang, JianyeYu, Wen Qiu, et al. "Evolutionary game model and analysis methods for network group behavior", Chinese Journal of Computers, 2015, 38(02), pg no: 282-300.
[3]. Zhang Y, Luo X, Ma W, et al. "Ambiguous bayesian games", International Journal of Intelligent Systems, 2014, 29(12), pg no: 1138-1172.
[4]. ZengguangWang, Yu Lu, Xi Li. "Active defense strategy selection for military information networks based on incomplete information game", Acta Armamentarii, 2020, 41(3), pg no: 607-617.
[5]. WeihuiYu. "Security analysis of media convergence platform network based on OSI reference model", Television Technology, 2022, 46(6), pg no: 191-193.
[6]. ChaohuiDing, Wei Zhang, GuoyuYang. "Research on network security defense system based on dynamic camouflage technology", Application of Electronic Technology, 2022, 48(1), pg no: 129-132.
[7]. TiequanRuan. "Research on network attack-defense strategies and proactive defense based on game theory", Computer Applications and Software, 2013, 30(9), pg no: 312-315.
[8]. QiankunMi, Bing Wu, Ning Du, et al. "Information system security risk assessment based on incomplete information game model", Computer and Modernization, 2019, pg no: 118-126.
[9]. Yun Zhang, ChengjianWei, Hang Shen. "Fuzzy security game model for information uncertain systems", Journal of Mini-Micro Electronic Systems, 2017, 38(9), pg no: 2045-2050.
[10]. Yan Li, GuangqiuHuang, Bing Zhang. "Markov evolutionary game model for security analysis of dynamic attack networks", Journal of Computer Science and Exploration, 2016, 10(9), pg no: 1272-1281.
[11]. Ma W, Liu W, Mcareavey K. "Game-theoretic resource allocation with real-time probabilistic surveillance information", Symbolic and Quantitative Approaches to Reasoning with Uncertainty, Springer International Publishing, 2015, pg no: 151-161.
[12]. DongxuWu, Jian Liu. "Game analysis of mine safety inspection", Journal of Liaoning Technical University (Natural Science), 2006, pg no: 7-9.
[13]. JunnanYang, HongqiZhang, ChuanfuZhang. "Defense decision-making method based on incomplete information stochastic game", Journal of Network and Information Security, 2018, 4(8), pg no: 12-20.
[14]. Dey A, Zaman K. "A robust optimization approach for solving two-person games under interval uncertainty" Computers and Operations Research, 2020, 119: 104937