

Communication Countermeasure Strategy Decision-Making Based on Incomplete Information Game

Jinyue Liu*, Xiang Gao*, Haowei Yang**, Jihao Zhang*, Yuhao Liu*, Peng Gong*

* National Key Laboratory of Mechatronic Engineering and Control, School of Mechatronic Engineering, Beijing Institute of Technology, Beijing, China

** Institute of Computer Application Technology, Norinco Group, Beijing, China

965491454@qq.com, 937058680@qq.com, bitxianggao@bit.edu.cn, zhangjihao@bit.edu.cn, rainyhelen@163.com, penggong@bit.edu.cn

Abstract—In modern battlefields, the stability of wireless communications is crucial for intelligence transmission, command coordination, and maintaining strategic advantage. However, with the rapid advancement of communication technologies, the electromagnetic environment has become increasingly complex, making intelligent decision-making in communication countermeasures a prominent research focus. However, most existing studies adopt deep learning and reinforcement learning methods, which require extensive data samples and computational resources. To address these limitations, this paper proposes a game-theoretic model for intelligent radio communication countermeasures under incomplete information. It quantitatively evaluates common attack and defense tactics used in communication countermeasures and explores the mixed-strategy equilibrium of the game when both the attackers and defenders consist of multiple types. Furthermore, simulation-based comparative analyses are conducted to assess the factors influencing the utility of both the attacker and defender. The findings offer theoretical insights and decision-making support for the deployment of communication countermeasure strategies in practical military operations, contributing to significant strategic value.

Keywords — communication countermeasures, Harsanyi transformation, incomplete information game, mixed-strategy equilibrium.

I. INTRODUCTION

The battlefield environment is constantly changing and information-rich. Stable, real-time, and efficient transmission of intelligence, commands, and other critical information through wireless communication is essential to securing information dominance and achieving victory. However, as communication technologies advance, the battlefield's electromagnetic environment has become more complex, making communication countermeasures a key focus of research. Communication countermeasures refer to actions taken by opposing sides to degrade the enemy's communication capabilities through jamming and anti-jamming techniques, while safeguarding their own communication security. As a key means of contesting information resources, the strategic importance of

communication countermeasures has grown increasingly critical as the form of warfare evolves towards information warfare.

With the rapid advancement and widespread application of artificial intelligence technologies, communication countermeasures are no longer limited to traditional forms, but are becoming more intelligent, by integrating techniques like reinforcement learning and deep learning. In [1], a radar anti-jamming method based on deep reinforcement learning in the complex domain was proposed for complex multi-jamming scenario. This method effectively addresses main-lobe jamming problem under time-sequence conditions, reducing decision-making time and greatly enhancing radar anti-jamming performance. Reference [2] proposed an intelligent radar combination anti-jamming decision algorithm based on Dyna-Q. This algorithm intelligently navigates through the anti-jamming matrix combining the radar systems and anti-jamming patterns, to quickly find the optimal anti-jamming strategy for coping with the complex jamming environments. Reference [3] introduced dynamic convolution into the task of radio interference recognition, which can quickly capture the change in the interference-to-noise ratio (INR) in electromagnetic countermeasure environments, thereby improving the accuracy of interference identification. Reference [4] proposed a two-stage optimization method for the joint optimization of jamming channel selection and power allocation. The jammer first uses a deep learning classifier to predict the channel state and select the interference frequency band. Then, a multi-armed bandit algorithm is applied to optimize the interference power, achieving effective interference at a low cost. While significant research achievements have been made using reinforcement learning and deep learning, these approaches often require large amounts of high-quality training data. However, in actual communication countermeasure scenarios, the information asymmetry between opposing sides makes it difficult to obtain large datasets from the opponent. Therefore, these methods have limitations.

Game theory describes the process in which participants, constrained by specific game rules, choose their strategies based on available information to maximize their utilities. It originated in the field of economics and has now been widely applied in various fields such as politics, management, automatic control, and communication. Jointly considering both the action strategies and timing strategies of the attackers and defenders, reference [5] combined time game with differential game. This time-differential game model enhanced network defense efficiency and provide support for selecting proactive network defense strategies. Reference [6] employed a two-player zero-sum game to derive the optimal attack and defense strategies within a limited decision space and constrained resource allocation. Based on this, considering the completeness of information available to both sides, the paper analyzed how attack and defense strategies involve under different levels of information symmetry and power grid topology scales and ultimately achieved optimal defense resource deployment. Reference [7] proposes a Network Attack-Defense Game Model (NADGM), leveraging epidemiological dynamics theory to define the attack-defense posture of the network based on the density of nodes in different security states. It analyzes the transition paths of network node security states and demonstrates the effectiveness and feasibility of the method through comparative experiments using a ransomware attack-defense scenario. Game theory has been widely applied in the field of attack and defense. However, most existing game-theoretical studies focus on network security confrontations, with relatively little research conducted in the area of radio communication countermeasures.

In summary, to address the decision-making needs for attack and defense strategies in communication countermeasures under incomplete information, this paper constructs a game model for communication countermeasures based on incomplete information. The model analyzes and quantifies common attack and defense tactics in communication countermeasures, while considering multiple types of attackers and defenders. By solving for the mixed-strategy equilibrium of both sides, the model provides a valuable reference for commanders in deploying attack and defense strategies.

II. COMMUNICATION COUNTERMEASURE GAME MODEL

A. The Relationship Between Communication Countermeasures and Game Theory

In communication countermeasures, attackers employ tactics like eavesdropping or jamming to gather enemy information or disrupt the opponent's communication capabilities. The attacker and defender counterbalance each other, aiming to maximize their own interests and weaken the opponent's. Similarly, in non-cooperative games, players are guided by individual rationality and act to maximize their own utilities without considering the utilities of others. Player utilities conflict and mutually influence each another.

Essentially, communication countermeasures can be viewed as a non-cooperative game. Usually, in the early stages of communication countermeasures, both attackers and defenders have limited knowledge of each other's resource allocation and operational strength. In other words, one side in the game does not have complete information about the strategy space, payoff functions, and other relevant details of the opponent. As a result, communication countermeasures can be further categorized as a non-cooperative game with incomplete information.

B. Communication Countermeasure Game Model

Based on the above analysis, the problem of communication countermeasures can be modeled as a strategic game, denoted as $G = \{N, \Theta, P, S, U\}$, with the elements defined as follows:

1) Players

Players are the decision-makers in the game. In communication countermeasures, players are divided into two sides: one side aims to attack and disrupt the target communication system, while the other side works to protect it. Denote the set of players as $N = \{N_a, N_d\}$, where $N_a = \{n_{a1}, n_{a2}, \dots, n_{an}\}$ represents the attackers and $N_d = \{n_{d1}, n_{d2}, \dots, n_{dm}\}$ represents the defenders. n and m represent the number of attackers and defenders, respectively.

2) Types of players

The set of player types in the game is denoted as $\Theta = \{\Theta_a, \Theta_d\}$, where $\Theta_a = \{\Theta_{a1}, \Theta_{a2}, \dots, \Theta_{ag}\}$ represents the set of attacker types and $\Theta_d = \{\Theta_{d1}, \Theta_{d2}, \dots, \Theta_{dk}\}$ represents the set of defender types. g and k represent the total number of attacker types and defender types, respectively.

3) Strategy space

The strategy space is denoted as $S = \{S_a, S_d\}$, where $S_a = \{s_{a1}, s_{a2}, \dots, s_{au}, \dots, s_{ai}\}$ represents the set of attacker strategies, and i is the total number of attacker strategies. $s_{au} = \{a_1, a_2, \dots, a_h\}$ represents the set of attack actions within a given attack strategy s_{au} , and h is the total number of attack actions. $S_d = \{s_{d1}, s_{d2}, \dots, s_{dv}, \dots, s_{dj}\}$ represents the set of defender strategies, and j is the total number of defender strategies. $s_{dv} = \{d_1, d_2, \dots, d_l\}$ represents the set of defense actions within a given defense strategy s_{dv} , and l is the total number of defense actions.

4) Prior belief of player types

The prior belief of player types refers to the estimation of the probabilities of other players' type when a player has known its own type, which can be represented as $P = \{P_a, P_d\}$. Specially, $P_a = \{P_a(\Theta_{dq} | \Theta_{ap}), 1 \leq q \leq k, 1 \leq p \leq g\}$ and

$$\sum_{p=1}^g P_a(\Theta_{dq} | \Theta_{ap}) = 1 \quad . \quad P_d = \{P_d(\Theta_{ap} | \Theta_{dq}), 1 \leq p \leq g, 1 \leq q \leq k\} \quad \text{and} \\ \sum_{q=1}^k P_d(\Theta_{ap} | \Theta_{dq}) = 1.$$

5) Utility

Utility is the payoff of the players during the game and is also the optimization objective of the players, denoted as $U = \{U_a, U_d\}$. $U_a = \{U_{a1}, \dots, U_{an}\}$ represents the utility function of the attackers, while $U_d = \{U_{d1}, \dots, U_{dm}\}$ represents the utility function of the defenders. Furthermore, $\forall s_{au} \in S_a, s_{dv} \in S_d, \Theta_{ag} \in \Theta_a, \Theta_{dk} \in \Theta_d, U_{ag}(\Theta_{dk}, s_{au}, s_{dv})$ denotes the payoff obtained by an attacker of type Θ_{ag} when employing strategy s_{au} , while the defender is of type Θ_{dk} and adopts defense strategy s_{dv} . Similarly, $\forall s_{dv} \in S_d, s_{au} \in S_a, \Theta_{dk} \in \Theta_d, \Theta_{ag} \in \Theta_a, U_{dk}(\Theta_{ag}, s_{dv}, s_{au})$ represents the payoff obtained by a defender of type Θ_{dk} when employing strategy s_{dv} , while the attacker is of type Θ_{ag} and adopts attack strategy s_{au} .

III. COMMUNICATION COUNTERMEASURE TACTICS

A. Attack Methods Based on Jamming

Based on the spectral width of the jamming signals, jamming attack methods in communication countermeasures can be categorized into three types: blocking jamming, spot jamming, and sweeping jamming.

Blocking jamming: Blocking jamming refers to transmitting jamming signals that cover the entire communication frequency band of the enemy. The method is relatively simple, as it does not require precise knowledge of the enemy's communication frequency. It can simultaneously disrupt multiple radio systems working on different frequency bands. However, due to power limitations, although block jamming has a wide jamming bandwidth, the power density within the bandwidth is low, resulting in weaker jamming intensity[8].

Spot jamming: Compared to block jamming, spot jamming is classified as narrowband jamming. Firstly, it requires scouting the working frequency of the enemy's communication system. Then it adjusts the jamming signal frequency to target the enemy's frequency, and transmit jamming signals within a narrow bandwidth. The jamming power of spot jamming is concentrated, resulting in high power utilization and good jamming results. However, the disadvantage is that it requires a high overlap between the carrier frequency of the jamming signal and the enemy's communication signal frequency, necessitating high precision in frequency reconnaissance and targeting[9].

Sweep jamming: In sweeping jamming, the center frequency of narrowband jamming signal periodically scans within a certain frequency band. When the jamming frequency scans into the bandwidth of the communication system's receiver, it generates interference. Due to the time-varying nature of the sweep jamming signal frequency, it is more difficult to filter out compared to other jamming methods.

B. Defense Methods Based on Anti-jamming

Variable speed frequency hopping: When the frequency-hopping pattern of the communication system is detected by the enemy, the enemy can implement jamming

using the same pattern, which will cause the communication system to malfunction. At this point, the communication system can employ the variable speed frequency hopping method [10], adjusting the dwell time at each frequency point so that it varies pseudo-randomly over time. It increases the difficulty for the enemy to lock onto communication signals and reduces the success rate in jamming.

Adaptive frequency hopping: In the process of communication countermeasures, the defending side continuously scans the jamming frequencies and real-time removes communication frequency points that fall within the jamming bands, so that the communication can be implemented on non-jamming frequency points. When the frequency hopping communication system faces block jamming, it may result in few available frequency points in the hopping frequency table. In this case, the communication system can switch frequency tables to avoid being paralyzed[11].

Increase power: When other anti-jamming methods are ineffective and communication needs are urgent, a hard countermeasure can be implemented by increasing transmission power. When the equipment and countermeasure tactics of both sides are certain, increasing the power is usually the last available measure.

C. Quantification of Communication Countermeasure Tactics

When the attacker conducts jamming attacks, it is possible for the attack to fail even if the defender does not implement any defensive measures. This can occur because limitations such as jamming power or targeting accuracy prevent the jamming signal from fully covering the defender's communication frequency band. Denote the probability of a successful attack by the attacker as μ , when no defensive measures are implemented. Since the defender usually first conducts reconnaissance of the electromagnetic environment when implementing defensive strategies, and then selects appropriate anti-jamming method based on the identified jamming patterns, the probability of a successful attack is related to both the probability of the jamming measures being detected and the defender's probability of successful defense. Denote the probability of the defender successfully detecting the jamming as α_r , and r represents the index of an attack action in a given attack strategy. The probability of a successful defense is β_s , while s denotes the index of a defense action in a given defense strategy. Furthermore, we consider the attacker gains a payoff R_a when the attack is successful, and gains nothing if the attack fails. And regardless of whether the attack succeeds or fails, an attack cost $C(a_r)$ must be paid. Therefore, the utility for the attacker when choosing attack action a_r can be expressed as

$$U_{a_r} = \mu(1 - \alpha_r \beta_s) R_a - C(a_r)$$

For the defender, a payoff is obtained regardless of whether the defense's success. Even if the defense fails, the defender can gain valuable information about the attacker's tactics, which can be used to improve future defense strategy

selection. Let R_d denote the payoff obtained by the defender when the defender successfully defends. Then the utility obtained by the defender from the defense action d_s upon a successful defense can be expressed as

$$U_{d_s} = \alpha_r \beta_s (R_d - C(d_s)),$$

where $C(d_s)$ is the cost of defensive action d_s . The utility obtained by the defender upon defense failure is

$$U_{d_s} = (1 - \alpha_r \beta_s)(\eta R - C(d_s)),$$

where η is the discount factor for defense failure. Thus, the expected utility for the defender can be expressed as

$$U_{d_s} = \eta(1 - \alpha_r \beta_s)R_d + \alpha_r \beta_s R_d - C(d_s).$$

If the attacker chooses strategy s_{au} to take action, then its utility can be expressed as

$$\begin{aligned} U_{s_{au}}(\Theta_{ap}, s_{au}, s_{dv}) &= \sum_{r=1}^h \sum_{s=1}^l U_{ar} \\ &= \sum_{r=1}^h \sum_{s=1}^l (\mu(1 - \alpha_r \beta_s)R_a - C(a_r)) \end{aligned}$$

Similarly, when the defender chooses strategy s_{dv} to take action, its utility can be expressed as

$$\begin{aligned} U_{s_{dv}}(\Theta_{dq}, s_{au}, s_{dv}) &= \sum_{s=1}^l \sum_{r=1}^h U_{ds} \\ &= \sum_{s=1}^l \sum_{r=1}^h (\eta(1 - \alpha_r \beta_s)R_d + \alpha_r \beta_s R_d - C(d_s)) \end{aligned}$$

IV. MIXED-STRATEGY BAYESIAN NASH EQUILIBRIUM OF THE GAME

Definition 1 (Mixed-Strategy): If the attacker of type Θ_{ap} chooses pure-strategy s_{au} with probability $b_{s_{au}}(\Theta_{ap})$, where $0 \leq b_{s_{au}}(\Theta_{ap}) \leq 1$ and $\sum_{u=1}^i b_{s_{au}}(\Theta_{ap}) = 1$, then $B(\Theta_{ap}) = \{b_{s_{a1}}(\Theta_{ap}), \dots, b_{s_{au}}(\Theta_{ap}), \dots, b_{s_{ai}}(\Theta_{ap})\}$ is referred to as a mixed-strategy of the attacker under type Θ_{dq} .

Definition 2 (Mixed-Strategy Bayesian Nash Equilibrium): For a given game $G = \{N, \Theta, B(\Theta), P, U\}$, if the mixed-strategy $(B^*(\Theta_{ap}), B^*(\Theta_{dq}))$ satisfies the following conditions:

for $\forall \Theta_{dq} \in \Theta_d$,

$$\begin{aligned} &\sum_{q=1}^k P_a(\Theta_{dq} | \Theta_{ap}) U_{s_{ai}}(\Theta_{ap}, B^*(\Theta_{ap}), B^*(\Theta_{dq})) \\ &\geq \sum_{q=1}^k P_a(\Theta_{dq} | \Theta_{ap}) U_{s_{ai}}(\Theta_{ap}, B(\Theta_{ap}), B^*(\Theta_{dq})) \end{aligned}$$

And for $\forall \Theta_{ap} \in \Theta_a$,

$$\begin{aligned} &\sum_{p=1}^g P_d(\Theta_{ap} | \Theta_{dq}) U_{s_{dj}}(\Theta_{dq}, B^*(\Theta_{ap}), B^*(\Theta_{dq})) \\ &\geq \sum_{p=1}^g P_d(\Theta_{ap} | \Theta_{dq}) U_{s_{dj}}(\Theta_{dq}, B(\Theta_{ap}), B(\Theta_{dq})) \end{aligned}$$

then the mixed-strategy $(B^*(\Theta_{ap}), B^*(\Theta_{dq}))$ is called a Bayesian Nash equilibrium.

Theorem 1: For a given game $G = \{N, \Theta, B(\Theta), P, U\}$, there must exist a mixed-strategy Bayesian Nash equilibrium.

Proof: According to Brouwer's fixed-point theorem, there must exist a mixed-strategy Nash equilibrium in finite normal-form games. In the game G constructed in this paper, both the types and strategies of the attacker and defender are finite. Thus, the game is a finite normal-form game, and Theorem 1 is proved.

V. SIMULATION EXPERIMENTS AND ANALYSIS

A. Simulation Parameter Settings

In this paper, we assume that the defender includes two types: advanced and elementary defenders, while the attacker includes three types: aggressive, balanced, and conservative. Considering the common defensive and attack tactics in communication countermeasure, the strategies for different types of defenders and attackers are shown in Tables 1 and 2, respectively.

Table 1 Strategies for Different Types of Defenders

Defensive Actions	Defender Strategies			
	Advanced Defender Θ_{d1}		Elementary Defender Θ_{d2}	
	s_{d1}	s_{d3}	s_{d2}	s_{d3}
Idle Channel Search	√	√	√	√
Frequency Hopping Networking	√	√	√	
Variable Speed Frequency Hopping	√			
Adaptive Frequency Hopping	√			
Increase Power	√		√	

Table 2 Strategies for Different Types of Attackers

Attack Actions	Attacker Strategies					
	Aggressive Attacker Θ_{a1}		Balanced Attacker Θ_{a2}		Conservative Attacker Θ_{a3}	
	s_{a1}	s_{a4}	s_{a2}	s_{a4}	s_{a3}	s_{a4}
Blocking Jamming					√	
Spot jamming			√			
Sweep jamming	√					

The costs $C(d)$ of the defensive strategies and probabilities β of successful defensive are shown in Table 3. And the costs $C(a)$ of the attack strategies and probabilities α of being detected are shown in Table 4.

Table 3 Costs of Defensive Strategies and Probabilities of Successful Defensive

Strategies	s_{d1}	s_{d2}	s_{d3}	s_{d4}
Costs $C(d)$	9	5	3	1
Probabilities of Successful	0.8	0.6	0.05	0.01

Defense β

Table 4 Costs of Attack Strategies and Probabilities of being Detected

Strategies	s_{a1}	s_{a2}	s_{a3}	s_{a4}
Costs $C(a)$	8	6.5	5	0.5
Probabilities of being Detected α	0.7	0.8	0.9	0

Set the attacker's prior belief as (aggressive attacker, balanced attacker, conservative attacker) = (0.6, 0.3, 0.1) and the defender's prior belief as (advanced defender, elementary defender) = (0.2, 0.8). Other parameter settings are shown in Table 5.

Table 5 Simulation Parameters for the Game

Parameters	Value
------------	-------

Payoff from Successful Attack R_a 15Payoff from Successful Defense R_d 10Probability of Successful Attack without Defense μ 0.7Discount Factor for Defense Failure η 0.4

By using the Harsanyi transformation to introduce a virtual player, 'Nature,' which selects the defender types, the above incomplete information game can be converted into an imperfect information game. We can then analyze and solve this game using standard methods. Based on the parameter settings mentioned provided, the communication countermeasure game tree is constructed as shown in Figure 1.

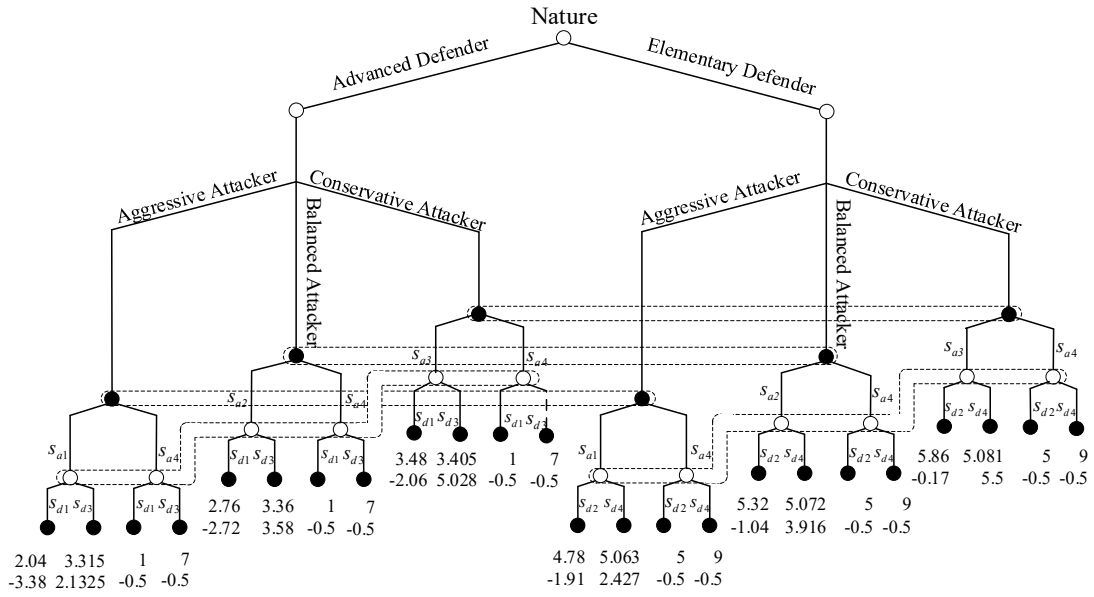


Figure 1 Communication Countermeasure Game Tree

B. Selection of Attack and Defense Strategies

Based on the communication countermeasure game tree shown in Figure 1, we analyze and solve the mixed-strategy equilibrium of the constructed communication countermeasure game. As the iterations progress, the changes in strategy selection probabilities for different types of attackers and defenders are depicted in Figure 2. It is evident that the probabilities gradually converge over the iterations, ultimately stabilizing at the mixed-strategy Bayesian Nash equilibrium, which is shown in Table 6.

The probability of the attacker selecting the jamming strategy increases in the order of adventurous, balanced, and conservative types. This is because the corresponding costs of these jamming strategies decrease progressively, making it more profitable for the conservative attackers to adopt their attack strategies under the given parameter settings. Regarding the defenders, the advanced defenders are more likely to choose the defensive strategy compared to the elementary defenders. Although they incur higher strategic costs, their

greater probability of successful defense ensures that the benefits gained from successful defenses are sufficient to offset those costs.

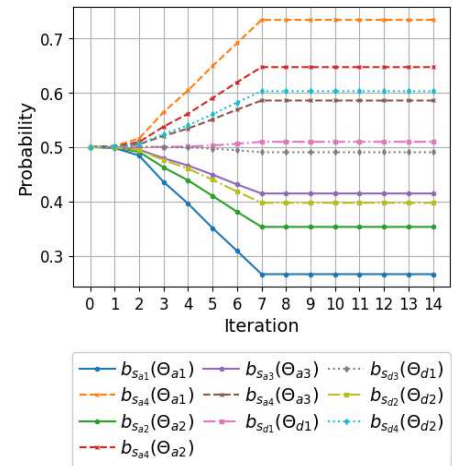


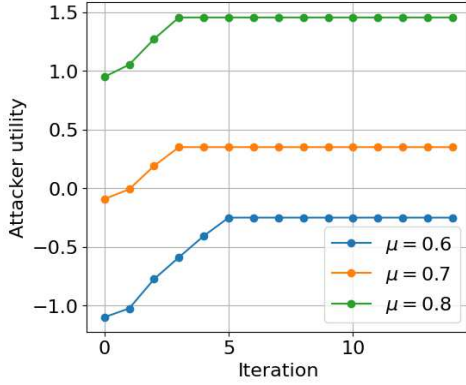
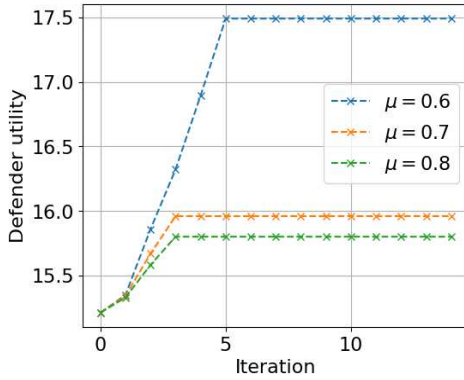
Figure 2 Changes in Strategy Selection Probabilities

Table 6. Mixed-strategy Bayesian Nash Equilibrium

Types of Players	Probability Distribution of Mixed-strategy Bayesian Nash Equilibrium
Aggressive Attacker	$B(\Theta_{a1}) = \{b_{s_{a1}}(\Theta_{a1}), b_{s_{a4}}(\Theta_{a1})\} = \{0.266, 0.734\}$
Balanced Attacker	$B(\Theta_{a2}) = \{b_{s_{a2}}(\Theta_{a2}), b_{s_{a4}}(\Theta_{a2})\} = \{0.353, 0.647\}$
Conservative Attacker	$B(\Theta_{a3}) = \{b_{s_{a3}}(\Theta_{a3}), b_{s_{a4}}(\Theta_{a3})\} = \{0.415, 0.585\}$
Advanced Defender	$B(\Theta_{d1}) = \{b_{s_{d1}}(\Theta_{d1}), b_{s_{d3}}(\Theta_{d1})\} = \{0.510, 0.490\}$
Elementary Defender	$B(\Theta_{d2}) = \{b_{s_{d2}}(\Theta_{d2}), b_{s_{d4}}(\Theta_{d2})\} = \{0.397, 0.603\}$

C. The Impact of μ on the Utilities of the Players

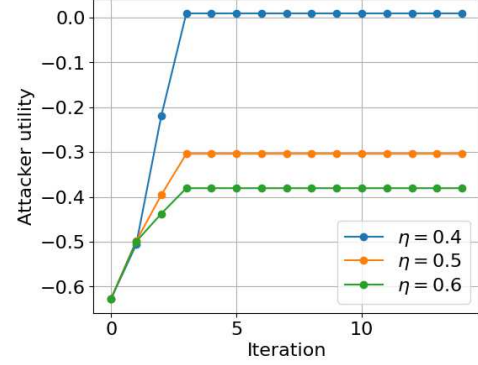
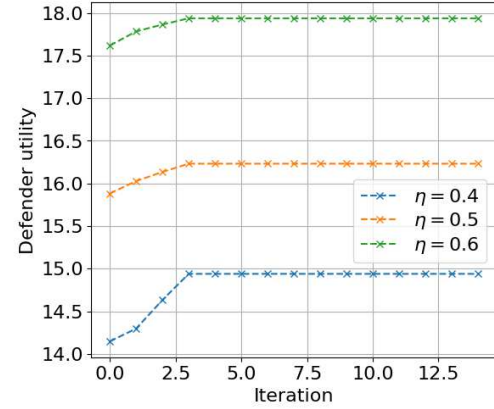
To investigate the impact of the probability of successful attack without defense μ on the utilities of the players in the communication countermeasure game, the probabilities are set as follows: $\mu = 0.6$, $\mu = 0.7$, $\mu = 0.8$. The other parameters remain consistent with those in Tables 3 to 5, resulting in attackers' and defenders' utilities shown in Figures 3 and 4, respectively.

Figure 3 The impact of μ on the utility of the attackerFigure 4 The impact of μ on the utility of the defender

From Figures 3 and 4, it can be seen that the higher the probability of successful attack without defense, the greater the utility of the attacker at equilibrium, while the utility of the defender decreases. This is because a higher probability of successful attack without defense makes defense more difficult, leading to poorer defensive outcomes, resulting in a gradual decrease in the utility of the defender at equilibrium.

D. The Impact of η on the Utilities of the Players

To investigate the impact of the discount factor for defense failure on the utilities of the players in the communication countermeasure game, the discount factor for defense failure are set as follows: $\eta = 0.4$, $\eta = 0.5$, $\eta = 0.6$. The other parameters remain consistent with those in Tables 3 to 5, resulting in attackers' and defenders' utilities shown in Figures 5 and 6, respectively.

Figure 5 The impact of η on the utility of the attackerFigure 6 The impact of η on the utility of the defender

From Figures 5 and 6, it can be seen that as the discount factor for defense failure increases, the utility of the attacker at equilibrium decreases, while the utility of the defender increases. When the discount factor for defense failure is relatively high, even if the defender fails, they can still obtain significant benefits by obtaining the information related to the attack. At this point, the defender is more willing to engage in defense, hindering the attack and thereby reducing the utility of the attacker.

VI. CONCLUSION

This paper designs an incomplete information countermeasure game based on the actual situation of information opacity in communication countermeasures, fully considering the impact of attacker and defender types on the game process. Additionally, it comprehensively analyzes and quantifies common attack and defense tactics by taking into account factors such as the probability of successful attack without defense for the attacker, the probability of being detected and the probability of successful defense, ensuring that the utility functions in the game are constructed based on

objectivity. Finally, the mixed-strategy Bayesian Nash equilibrium is solved to predict the decisions of both the attacker and defender, providing a reference for operational personnel in deploying attack and defense strategies.

ACKNOWLEDGMENT

This research was supported in part by National Natural Science foundation of China (No.62073039). Corresponding author: Peng Gong.

REFERENCES

- [1] F. Xie, H. Y. Liu, X. K. Hun, P. Zhong and J. B. Li, "A Radar Anti-jamming Method under Multi-jamming Scenarios Based on Deep Reinforcement Learning in Complex Domains," *Journal of Radars*, vol. 4, pp. 1290-1304, Dec. 2023.
- [2] S. S. Shi, Q. S. Zhou, J. L. Qian, Q. X. Chen and Z. H. Li, "Intelligent Radar Combination Anti-jamming Decision based on Dyna-Q," *Modern Radar*, to be published.
- [3] H. Yan, G. Wang, F. Gao and W. Yuan, "Dynamic Convolutional Neural Network for Wireless Interference Identification," *IEEE Communications Letters*, vol. 28, no. 1, pp. 83-87, Jan. 2024.
- [4] Z. Feng, Y. Xu, Y. Jiao, G. Li, W. Li and G. Fang, "Fight Against Smart Communication Rival: An Intelligent Jamming Approach With Trend-Oriented Efficacy Evaluation," *IEEE Wireless Communications Letters*, vol. 11, no. 11, pp. 2290-2294, Nov. 2022.
- [5] P. Y. Sun, J. L. Tan, C. W. Li and H. W. Zhang, "Network Security Defense Decision-Making Method Based on Time Differential Game," *Netinfo Security*, vol. 22, no. 05, pp. 64-74, May, 2022.
- [6] N. Shu, "Research on Power-communication Coupled Network Model and Vulnerability," M. S. dissertation, Defont. Elect. Eng., North China Electr. Power Univ., Beijing, China, 2023.
- [7] B. Yuan, "Research on the Decision-making Method of Network Defense Strategy Based on Dynamic Game Theory," M.S. dissertation, Defont. Software. Eng., Zhengzhou Univ. Light Ind., Zhengzhou, China, 2022.
- [8] X. D. Ji, H. Zhang, "A Discussion on Jamming and Anti-jamming Technologies in Military Wireless Communication," *Digital Communication World*, no. 10, pp. 70-71, Oct. 2019.
- [9] Z. Y. Liu, X. B. Liu, F. Zhao, Z. M. Xiu, A. L. Xie, "Anti aiming jamming method of LFM signal based on ACM," *Systems Engineering and Electronics*, vol. 46, no. 08, pp. 2546-2553, Apr. 2024.
- [10] S. C. Yu, W. Z. Yan, D. P. Gao, D. J. Ji, S. X. Zhang, "A New Method for Anti-jamming in Wireless Communication: Real-Time Adaptive Frequency Hopping Technique," *Gansu Science and Technology*, no. 16, pp. 41-43, Aug. 2008.
- [11] Z. L. Du, Y. M. Wang, "Analysis of interference and anti-interference technologies for military wireless communications," *Rada and ECM*, vol. 40, no. 04, pp. 29-32, Dec. 2020.



Jinyue Liu received the BS degree in Automation from Beijing Institute of Technology in 2019, and the MS degree in Mechatronical Engineering from Beijing Institute of Technology in 2022. She is currently pursuing her Ph.D degree. Her research interests include network simulation, wireless communication countermeasure and game theory.



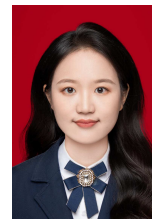
Xiang Gao received the BS degree, the MS degree and the Ph.D. degree in school of Mechatronical Engineering from Beijing Institut in 2014, 2016, and 2021, respectively. Now he is a associate professor in Beijing Institute of Technology. His research interests include network simulation and emulation, NOMA, VLC, D2D communications, IoT, cryptography and so on.



Haowei Yang received the BS degree, the MS degree and the Ph.D. degree in school of Mechatronical Engineering from Beijing Institut in 2015, 2018, and 2024, respectively. Now he is working in Institute of Computer Application Technology. His research interests include network simulation, D2D communications and so on.



Jihao Zhang received the BS degree in Mechatronical Engineering from Beijing Institute of Technology in 2018, and then he received the MS degree in Beijing Institute of Technology in 2021. Now he is a DS candidate in School of Mechantronical Engineering, Beijing Institute of Technology. His research interests include wireless network simulation and emulation, wireless communication.



Yuhua Liu received the BS degree in North China Institute of Science and Technology in 2020, and followed by the MS degree in Beijing Institute of Technology in 2024, respectively. Now she is a Ph.D. candidate in School of Mechantronical Engineering, Beijing Institute of Technology. Her research interests include communication network simulation, radio fuse effectiveness evaluation and so on.



Peng Gong received the BS degree in Mechatronical Engineering from Beijing Institute of Technology, Beijing, China, in 2004, and the MS and Ph.D. degrees from the Inha University, Korea, in 2006 and 2010, respectively. In July 2010, he joined the School of Mechatronical Engineering, Beijing Institute of Technology, China. His research interests include link/system level performance evaluation and radio resource management in wireless systems, information security, and the next generation wireless systems such as 3GPP LTE, UWB, MIMO, Cognitive radio and so on.