Leader-follower security games in UAV communication with deception

Boyang He[a], Jian Gao[b], Xiangmin Guan[*cd] and Zhaoyang Cheng[#e]
[a]Zhengzhou Aerotropolis Institute of Artificial Intelligence, Zhengzhou, Henan, China; [b]Shenzhen High Great Innovation Technology Development Co., Ltd., Shenzhen, Guangzhou, China; [c]CAAC Key laboratory of General Aviation Operation Civil Aviation Management Institute of China, Beijing 100102, China; [d]Key Laboratory of General Aviation Operation Technology of Zhejiang Province, Hangzhou, Zhejiang, China; [e]Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China

ABSTRACT

In this paper, we study the leader-follower unmanned aerial vehicle (UAV) security game with deception. The robustness under the UAV game with deception describes the model's ability to maintain players' profits. We propose a UAV security model with one-leader and multi-followers and define the deception strong Stackelberg equilibrium (DSSE) in the game with deception. Besides, we analyze the robustness of the DSSE to find the boundary that the leader can not improve its utility from deception.

Keywords: UAV, leader-follower security game, deception, robustness

1. INTRODUCTION

In recent years, due to the rapid development of Unmanned aerial vehicles (UAVs), UAVs have been widely used in military, rescue, and topographic reconnaissance[1,2]. Civilian UAVs are widely used in commercial performance, video photography and other fields. The competition among UAVs is also widely adopted in military reconnaissance and academic competitions. The confrontation among UAVs models the interaction between a UAV defender and UAV attackers. In fact, the UAV defender often has a defensive advantage that ensures that UAV attackers observe its strategy[3]. Thus, the UAV defender is always a leader and chooses a strategy first, while UAV attackers make decisions with the knowledge of the defender's strategy.

There are many uncertain phenomena in the confrontation among UAVs[4,5]. For example, the random communication among drones may be not synchronous. Also, different UAVs may have different cognition of unstructured environment information. Actually, deception is one of the most important reasons for this uncertainty[6,7]. The equilibrium in the leader-followers UAVs security game with deception can be defined as the deception strong Stackelberg equilibrium (DSSE)[8]. These phenomena have been studied extensively in recent years. For example, Bakker[9] and Cheng[10] considered a case that the attacker and defender have a misperception of a parameter, while the attacker can manipulate the attacker's perception of parameters. Xu[11] studied how to deceive the attacker by exploiting the defender's knowledge.

Moreover, whether players have motivations to explore the different cognitions among them is a crucial question in security games. It was also widely discussed in References[12,13]. Concretely, if the different cognitions have little influence on players' profits, revealing or utilizing the cognitive differences will not bring players benefits, and then players may not have motivations to explore the fact even if they realize the existence of different cognitions.

Fortunately, hypergame theory provide a framework to analyze the equilibrium's robustness. Hypergame theory extends game theory by allowing for an unbalanced game model that each player has a different view of the game[14]. It allows players to play different games and can account for the strategies of each player in deception. In addition, the hypergame framework has advantages in analyzing whether players have motivations to explore the different cognitions among them since the robustness under hypergame frameworks can describe the different cognitions' influences on players' profits. The robustness under hypergame frameworks describes the model's ability to maintain players' profits[15]. Thus, these inspire us to analyze the different cognitions with hypergame frameworks.

* guanxiangmin@camic.cn
# chengzhaoyang@amss.ac.cn

Third International Conference on Computer Science and Communication Technology (ICCSCT 2022)
edited by Yingfa Lu, Changbo Cheng, Proc. of SPIE Vol. 12506, 125061I
 · 0277-786X · doi: 10.1117/12.2662028

Therefore, the motivation of this paper is to model and analyze the leader-followers UAV security games with deception based on hypergame theory. Main contributions are summarized as follows. We propose a UAV hypergame model with one-leader and multi-followers and define the DSSE in the game with deception. Besides, we analyze the robustness of the DSSE in hypergame framework to find the boundary that the leader can not improve its utility from deception. Moreover, we provide several experiments to show the validity of our resluts.

The remainder is organized as follows. Section 2 formulates UAV security game with deception by hypergame theory. Then Section 3 analyzes the robustness of DSSE in hypergame framework. Moreover, Section 4 presents numerical examples for illustration of the validity of the robustness in real UAV applications. Finally, Section 5 concludes the paper.

2. PROBLEM FORMULATION

In this section, we model a leader-follower hypergame with resource allocation constraints to study the UAVs' interactions between a defender and multiple attackers.

We consider a single-leader-multiple-follower UAV security game. Followers are UAV attackers and allocate resources to attack some targets. The leader is a UAV defender and allocates resource to protect targets, as shown in figure 1.

We consider that $\theta_0$is is a fixed parameter generated by nature and each player may have a different observation of θ_0. All possible observation of θ_0 is Θ. We take $G(\theta') = \{P, \Omega, U, \theta'\}$ as the security game under the observation θ', where $\theta' \in \Theta$. $P = \{l, 1, \dots, n\}$ is the player set, l is the leader UAV and $1, \dots, n$ represents for follower UAVs. $\Omega = \Omega_l \times \Omega_1 \times \cdots \times \Omega_n$ is the strategy of all players, where $\Omega_l \subseteq \mathbb{R}^K$ is the leader UAV's strategy set and $\Omega_i \subseteq \mathbb{R}^K$ is the follower UAVs' strategy set. $U = \{U_l, U_1, \dots, U_n\}$ is the utility function set of all players, where $U_l: \Omega_l \times \Omega_1 \times \cdots \times \Omega_n \to \mathbb{R}$ is the leader's utility function and $U_i: \Omega_l \times \Omega_i \to \mathbb{R}$ is the ith follower UAV's utility function.

Now, we give the concrete formalization of the leader-followers UAV security game by formalize the strategy sets and utility functions. We take $T = \{t_1, .. t_K\}$ as the target set, where each UAV attacker choose to attack the target and the UAV defender tries to prevent attacks by covering targets. The UAV defender has R_0 resources and assign them to each target, i.e., x^k is the resources that the defender assign to target k. Then the defender's strategy is $x = [x^1, x^2, \dots, x^K]^T$. Similarly, the ith UAV attacker has R_i resources and attack target k with y_i^k resources. Then the ith UAV attacker's strategy is $y_i = [y_i^1, y_i^2, \dots, y_i^K]^T$. The player's strategy sets can be wrote as $\Omega_l = \{x | \sum_{k=1}^K x^k = R_0, x^k \geq 0\}$, and $\Omega_i = \left\{y \middle| \sum_{k=1}^K y_i^k = R_0, y_i^k \geq 0\right\}$, for all $i = 1, \dots, N$.

Then we consider the utility functions of all the players. In this leader-followers UAV security game, $C_l(t_k)$ is the UAV defender's utility when the UAV defender allocates each unit of resource to target t_k and the UAV attackers allocate each unit of resource to target t_k. $Q_l(t_k)$ is the UAV defender's utility when the UAV defender does not allocate each unit of resource to target t_k and the UAV attackers allocate each unit of resource to target t_k.

On the other hand, $C_i(\theta', t_k)$ is the i-th UAV attacker's utility when the defender allocates each unit of resource to the target t_k and the UAV attacker allocates each unit of resource to target t_k. $Q_i(\theta', t_k)$ is i-th UAV attacker's when the defender does not allocate each unit of resource to target t_k and the UAV defender allocates each unit of resource to target t_k. Then if strategy profile $[x, y_1, \dots, y_n]$ is played under observation θ', each player's utilities is computed as follows:

$$U_l(x, y_1, \dots, y_n) = \sum_{k=1}^{K} \left(\sum_{i=1}^{n} y_i^k \right) \left(x^k \, C_l(t_k) + (R_0 - x^k) Q_l(t_k) \right),$$

$$U_i\,(x, y_i, \theta') = \sum_{k=1}^{K} y_i^k (x^k C_i(\theta', t_k) + (R_0 - x^k) Q_i(\theta', t_k)).$$

Each UAV always hopes to maximize its own utility. There are also some other practical communication networks[16-20], while we consider a star communication network. Actually, as a key property of UAV security problems, we always suppose that $C_l(t_k) > Q_l(t_k)$, for all $k = 1, \dots, K$. It means that the unit utility from defending a target is greater than it from not defending the same target for the defender. Besides, we also suppose that $C_i(\theta, t_k) < Q_i(\theta, t_k)$, for all $i = 1, \dots, n$, $k = 1, \dots, K$, $\theta \in \Theta$. It denotes that the unit utility from attacking a target is greater than it from not attacking the same target for each UAV attacker. Both of them has been widely consider in the UAV security problem, since the UAV attackers tend to invade vulnerable targets, and the UAV defender prefer to prevent the invasion. Besides, we always suppose that

Θ is compact, convex, and nonempty, and there exists k such that $C_i(\theta_0, t_k) \geq Q_i(\theta_0, t_l)$ for $i \in P$, $l \neq k$. We mainly consider that there exists a most attractive target to the UAV attacker.

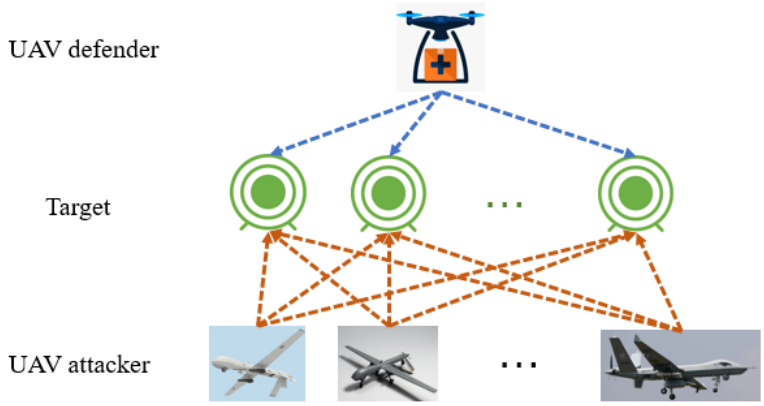


Figure 1. Leader-followers UAV security game.

Moreover, in order to describe the deception in leader-followers UAV security games, we use the hypergame framework to help us analyze. We consider that the UAV defender deceives all UAV attackers such that the UAV attackers think the value of θ_0 is θ' where $\theta' \in \Theta$. Take G_{ij} as the game of i-th UAV attacker as it is perceived by j-th UAV attacker, where $i, j \in P$. In the UAV defender's perceptive, $G_{ll} = G(\theta_0)$ since it knows the real value of the parameter, and $G_{jl} = G(\theta')$ since it deceives all UAV attackers such that the UAV attackers think the value of θ_0 is θ'. Similarly, In the i-th UAV attacker's perceptive, $G_{ji} = G(\theta')$ since it is not conscious of the deception. Thus, $H_i = \{G_{ji}, j \in P\}$ is the first level hypergame observed by i-th UAV. The second level hypergame under deception can be denoted as $H(\Theta) = \{H_l, H_1, \ldots, H_n\}$, which is a set of first level hypergame perceived by each UAV.

Now, we denote $BR(x, \theta') = argmax_{y_i \in \Omega_i} U_i(x, y, \theta')$ as the set of all UAV attackers' best response to the UAV defender's strategy x under the deception θ'. In the hypergame framework with deception, the leader chooses the strategy first, and the followers choose the strategy by observing the leader's choice. Actually, the leader also knows that followers make decisions based on their strategy. Then the standard solution concept is Deception Strong Stackelberg Equilibrium (DSSE). A strategy profile (x^*, y^*) is said to be a DSSE in $H(\Theta)$ if

$$(x^*, y^*) = argmax_{x \in \Omega_l, y \in BR(x, \theta^*)} U_l(x, y),$$

where $\theta^* = argmax_{\theta' \in \Theta}\ argmax_{x \in \Omega_l, y \in BR(x, \theta^*)} U_l(x, y)$.

3. MAIN RESULTS

In this section, we mainly discuss the robustness of DSSE under hypergame frameworks. The robustness of DSSE focus on players' motivations to explore the different cognitions among them

We take (x_{DSSE}, y_{DSSE}) as the DSSE of $H(\theta)$ and θ^* as the corresponding deceptive parameter. Also, we take $(x(\theta_0), y(\theta_0))$ as the strategy when all players' observations are θ_0, which is actually no deception in the UAV security games. We aim to find whether there exists a deceptive set δ, where $\delta \subset \Theta$, such that

$$U_l(x_{DSSE}, y_{DSSE}) = U_l\big(x(\theta_0), y(\theta_0)\big).$$

Then the following theorem shows the robustness of the DSSE.

Theorem 1: There exists a convex nonempty set δ such that $U_l(x_{DSSE}, y_{DSSE}) = U_l\big(x(\theta_0), y(\theta_0)\big)$.

Proof: We take $\Gamma_i(x, \theta) = argmax_{k=1,\ldots K} x^k C_i(\theta, t_k) + (R_i - x^k) Q_i(\theta, t_k)$. According to Reference[10], for any $k \in \Gamma_i$, $l \neq \Gamma_i$, we have $x^k C_i(\theta, t_k) + (R_l - x^k) Q_i(\theta, t_k) \geq x^l C_i(\theta, t_l) + (R_i - x^i) Q_i(\theta, t_i)$. Since $C_i(\theta, t_k)$ and $Q_i(\theta, t_k)$ are continuous with respect to $\theta \in \Theta$ for any k. There exists a convex set δ such that for all $\theta \in \delta_i$, we have

$$x^k C_i(\theta, t_k) + (R_l - x^k)Q_i(\theta, t_k) \geq x^l C_i(\theta, t_l) + (R_i - x^i)Q_i(\theta, t_i).$$

We take $\delta = \cap_{i=1}^{n} \delta_i$ and then δ is nonempty. Then for any $\theta \in \delta$, when the i-th UAV attacker still invades targets in $\Gamma_i\ (x(\theta_0), \theta_0)$, which leads to the same profits as $y_i(\theta_0)$. According to Reference[21], the UAV defender does not change its strategy under δ.

Thus for any $U_l(x_{DSSE}, y_{DSSE}) = U_l\big(x(\theta_0), y(\theta_0)\big)$.

Theorem 1 shows that there is always a nonempty subset of the observation parameter such that the leader does not implement deception in this region, since tiny deception does not bring the leader more benefits.

Moreover, we also hope to find the bound of the subset δ and the following theorem give a Quantized boundary of the deceptive set.

Theorem 2: For all $k = 1, \dots, K$, $i \in P$, if $C_i(\theta, t_k)$ and $Q_i(\theta, t_k)$ are λ-Lipschitz continuous in $\theta \in \Theta$, then there exists $\delta = \{\theta \in \Theta: ||\theta - \theta_0|| < \Delta\}$, where $\Delta = \min_{i \in P} \frac{L_i^1 - L_i^2}{2\lambda R_i}$,

$$L_i^1 = x^k C_i(\theta, t_k) + (R_i - x^k)U_i^u(\theta, t_k), k \in \Gamma_i(x(\theta_0), \theta_0),$$

$$L_i^1 = \max_{l \notin \Gamma_i(x(\theta_0), \theta_0)} x(\theta_0)^l C_i(\theta_0, t_l) + (R_i - x(\theta_0)^k)U_i^u(\theta_0, t_l),$$

such that for all δ, $U_l(x_{DSSE}, y_{DSSE}) = U_l\big(x(\theta_0), y(\theta_0)\big)$.

Proof: According to Reference[10], $\Gamma_i(x(\theta_0), \theta_0)$ is the set with a unique element. We take $k_1 \in \Gamma_i(x(\theta_0), \theta_0)$ and $k_2 \in argmax_{l \notin \Gamma_i(x(\theta_0), \theta_0)} x(\theta_0)^l C_i(\theta_0, t_l) + (R_i - x(\theta_0)^k)Q_i(\theta_0, t_l)$. Thus, k_1 and k_2 represent the corresponding target set of the two most attractive utility to the i-th UAV attacker under the leader's strategy $x(\theta_0)$ and the observation θ_0. Since $C_i(\theta, t_k)$ and $Q_i(\theta, t_k)$ are λ-Lipschitz continuous in $\theta \in \Theta$, take $f_i(x, \theta, k) = x^k C_i(\theta, t_k) + (R_i - x^k)Q_i(\theta, t_k)$. According to Reference[10], $f_i(x, \theta, k)$ is $R_i\lambda$- Lipschitz continuous in $\theta \in \Theta$. Thus, for any $k \notin \Gamma_i(x(\theta_0), \theta_0)$

$$\big||f_i(x(\theta_0), \theta, k) - f_i(x(\theta_0), \theta_0, k)|\big| \leq R_i\lambda\big||\theta - \theta_0|\big|.$$

Then $f_i(x(\theta_0), \theta, k) - f_i(x(\theta_0), \theta_0, k) \leq R_i\lambda\big||\theta - \theta_0|\big|$.

Also, $f_i(x(\theta_0), \theta_0, k) \leq f_i(x(\theta_0), \theta_0, k_2)$ since $k_2 \in argmax_{l \notin \Gamma_i(x(\theta_0), \theta_0)} x(\theta_0)^l C_i(\theta_0, t_l) + (R_i - x(\theta_0)^k)U_i^u(\theta_0, t_l)$. Thus,

$$f(x(\theta_0), \theta, k) - f_i(x(\theta_0), \theta_0, k_2) \leq R_i\lambda\big||\theta - \theta_0|\big|.$$

Besides, $f_i(x(\theta_0), \theta, k_1) - f_i(x(\theta_0), \theta_0, k_1) \geq R_i\lambda\big||\theta - \theta_0|\big|$. Thus,

$$f_i(x(\theta_0), \theta, k_1) - f_i(x(\theta_0), \theta, k) \geq f_i(x(\theta_0), \theta_0, k_1) - f_i(x(\theta_0), \theta_0, k_2) - 2R_i\lambda\big||\theta - \theta_0|\big|.$$

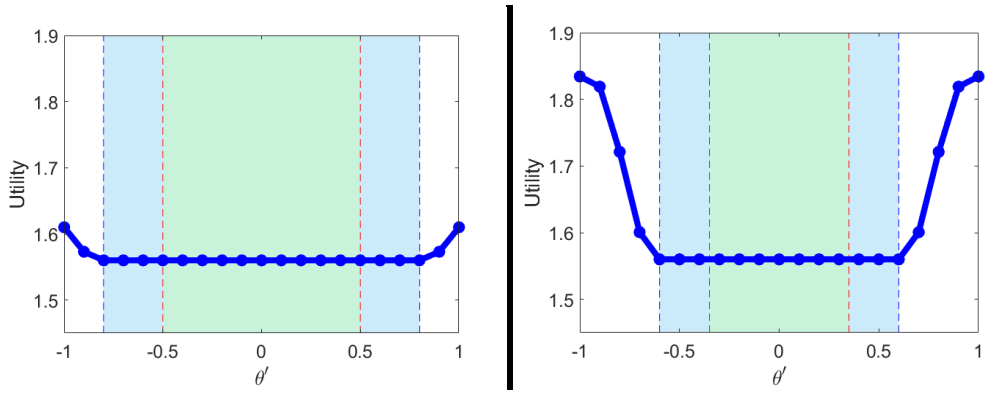
Therefore, for any $\theta \in \delta$, $f_i(x(\theta_0), \theta, k) < f_i(x(\theta_0), \theta, k_1)$. According to Reference[10], for x_{DSSE}, the equation also holds. Thus, the UAV defender has no will to change its own strategy. Then $U_l(x_{DSSE}, y_{DSSE}) = U_l\big(x(\theta_0), y(\theta_0)\big)$.

Theorem 2 gives a lower bound if the utility function is Lipschitz continuous. In addition, if the leader wants to benefit more from deception, it needs to pay no less energy than the lower bound δ. Therefore, it can be regarded as a trade-off for the leader.

4. NUMERICAL EXPERIMENTS

In this section, we provide several experiments to show the validity of theorems.

We consider a UAV security problems with 1 UAV defender and 5 UAV attackers. We take $R_l = R_1 = \cdots = R_5 = 1$. And we sample $C_l(t_k), Q_l(t_k), C_i(t_k), Q_i(t_k)$ from [0,4]. Then we take $\theta_0 = 0$, $\Theta = [-1,1]$, $C_i(\theta, t_k) = C_i(t_k)$, and $Q_i(\theta, t_k) = Q_i(t_k) + d_k\theta^2$, where d_k is generaed in the range $A \subset \mathbb{R}$.



(a) $A = [0,1]$ (b) $A = [0,2]$

Figure 2. Utilities of the UAV defender in different ranges D.

As shown in figure 2, to show the validity of our theorem, we take two different range D, where $A = [0,1]$ in Figure 2a and $A = [0,2]$ in Figure 2b. The blue lines are the UAV defender's utility if the UAV defender take deception θ'. The light blue region represent the value of θ' such that the utilities of the UAV defender and UAV attackers are invariant. The light green region shows that the bounds according to Theorem 2. Actually, the bule line of $\theta' = 0$ is the utility of the the UAV defender if it does not deceieve. Notice that the light green region is always contained in the light blue region. Thus, our robust boundary according to Theorem 2 is contained in the invariant region of players' utilites.

5. CONCLUSION

In this paper, we have studied the leader-followers unmanned aerial vehicle (UAV) security game based on hypergame theory. The robustness under hypergame frameworks describes the model's ability to maintain players' profits. We have propoed a UAV hypergame model with one-leader and multi-followers and defind the DSSE in the game with deception. Besides, we have analyzed the robustness of the DSSE in hypergame framework to find the boundary that the leader can not improve its utility from deception.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (No. U1933130, No. 71731001), and is also supported by research and demonstration of key technologies for the air-ground collaborative and smart operation of general aviation (No.2022C01055).

REFERENCES

[1] Gupte, S., Mohandas, P. and Conrad, J. M., "A survey of quadrotor unmanned aerial vehicles,"2012 Proc. of IEEE Southeastcon, 1-6 (2012).
[2] Tahir, A., Böling, J., Haghbayan, M. H., Toivonen, H. T. and Plosila, J., "Swarms of unmanned aerial vehicles—A survey," Journal of Industrial Information Integration, 16, 100106 (2019).
[3] Liang, Y., Qi, D. and Yanjie, Z., "Adaptive leader-follower formation control for swarms of unmanned aerial vehicles with motion constraints and unknown disturbances," Chinese Journal of Aeronautics, 33(11), 2972-2988 (2020).
[4] Jun, M. and D'Andrea, R., "Path planning for unmanned aerial vehicles in uncertain and adversarial environments," [Cooperative Control: Models, Applications and Algorithms. Cooperative Systems] (vol 1) ed S. Butenko, R. Murphey, P. M. Pardalos, Springer, Boston, 95-110 (2003).
[5] Chen, G., Ming, Y., Hong, Y. and Yi, P., "Distributed algorithm for ε-generalized Nash equilibria with uncertain coupled constraints," Automatica 123, 109313 (2021).
[6] Zhang, T. and Zhu, Q., "Strategic defense against deceptive civilian GPS spoofing of unmanned aerial vehicles," Inter. Conf. on Decision and Game Theory for Security, 213-233 (2017).

[7] Xu, G., Chen, G., Qi, H. and Hong, Y., "Efficient algorithm for approximating Nash equilibrium of distributed aggregative games," IEEE Transactions on Cybernetics, 1-13 (2022).
[8] Nguyen, T. and Xu, H., "Imitative attacker deception in stackelberg security games," Inter. Joint Conf. on Artificial Intelligence, 528-534 (2019).
[9] Bakker, C., Bhattacharya, A., Chatterjee, S. and Vrabie, D. L., "Learning and information manipulation: Repeated hypergames for cyber-physical security," IEEE Control Systems Letters 4(2), 295-300 (2019).
[10] Cheng, Z., Chen, G. and Hong, Y., "Single-leader-multiple-followers Stackelberg security game with hypergame framework," IEEE Transactions on Information Forensics and Security 17, 954-969 (2022).
[11] Chen, G., Cao, K. and Hong, Y., "Learning implicit information in Bayesian games with knowledge transfer," Control Theory and Technology, 18(3), 315-323 (2020).
[12] Cheng, Z., Chen, G. and Hong, Y., "Misperception influence on zero-determinant strategies in iterated Prisoner's Dilemma," Scientific Reports 12(1), 1-9 (2022).
[13] Chen, G., Zeng, X. and Hong, Y., "Distributed optimisation design for solving the Stein equation with constraints," IET Control Theory and Applications 13(15), 2492-2499 (2019).
[14] Kovach, N. S., Gibson, A. S. and Lamont, G. B., "Hypergame theory: A model for conflict, misperception, and deception," Game Theory, 1-20 (2015).
[15] Sasaki, Y., "Preservation of misperceptions-stability analysis of hypergames," Proc. of the 52nd Annual Meeting of the ISSS-2008, (2008).
[16] Xu, G., Chen, G. and Qi, H., "Algorithm design and approximation analysis on distributed robust game," arXiv preprint arXiv:2204.01548, (2022).
[17] Liang, S., Zeng, X., Chen, G. and Hong, Y., "Distributed sub-optimal resource allocation via a projected form of singular perturbation," Automatica 121, 109180 (2020).
[18] Chen, G., Li, W., Xu, G. and Hong, Y., "Distributed mirror descent algorithm with Bregman damping for nonsmooth constrained optimization," arXiv preprint arXiv:2108.12136, (2021).
[19] Chen, G., Yi, P. and Hong, Y., "Distributed optimization with projection-free dynamics," arXiv preprint arXiv:2105.02450, (2021).
[20] Wang, Y., Geng, X., Chen, G. and Zhao, W., "Achieving social optimum in non-convex cooperative aggregative games: A distributed stochastic annealing approach," arXiv preprint arXiv:2204.00753, (2022).
[21] Carmona, G., "Existence and stability of Nash equilibrium," World Scientific, (2012).