Colonel Blotto Games in Network Systems: Models, Strategies, and Applications

Sanghai Guan, Jingjing Wang, *Student Member, IEEE*, Haipeng Yao, *Member, IEEE*, Chunxiao Jiang, *Senior Member, IEEE*, Zhu Han, *Fellow, IEEE*, and Yong Ren, *Senior Member, IEEE*

***Abstract*—Network systems, such as Internet, smart grids, transportation networks, social networks, etc., play a critical role in human society. However, due to their inherent vulnerability as well as the limited management and operational capability, these network systems are constantly under the threat of malicious attackers. Therefore, in such attack-defense scenarios, it is particularly significant to make the best use of defenders' limited resources and capability. In this paper, we propose a networked Colonel Blotto game for the attack–defense strategy, where the attackers and defenders allocate the limited resources on each node, and their utility depends on certain network performance metrics, which are defined for evaluating the performance of the whole network system. Furthermore, considering the complexity of the equilibrium analysis in large-scale network systems, a coevolution-based algorithm is proposed for obtaining the practical action sets as well as achieving the mixed-strategy Nash equilibrium. Finally, relying on four real-world network systems, i.e., computer networks, Internet of vehicles, air transportation systems, and social networks, simulation results show the effectiveness and feasibility of our proposed model, which is conducive to the design, management, and maintenance of network systems.**

***Index Terms*—Colonel Blotto game, network attack-defense security, resource allocation, system reliability.**

I. Introduction

With the rapid development of engineering technology, network systems such as Internet, smart grids, social networks and transportation networks become an indispensable part of our daily life. However, various security vulnerabilities threaten their normal operation. Specifically, taking power grid networks as an example, the failure of some power supply and transmission equipment may result in serious cascading failure, which causes a large-scale blackout [1]. Moreover, the outbreak of an infectious disease commonly originates from the infection of a few patients [2]. The spread of rumors also follows similar laws in social networks [3], [4]. Unfortunately, these characteristics provide opportunities for malicious attackers, who can trigger huge damage just by attacking few key nodes of the network system. By contrast, it is also beneficial of improving the reliability of the network system by emphatically protecting these weak key nodes. Considering the limitation of attack-defense resources and capability of both the attacker and defender, rationally allocating depletable attack-defense resource on the whole network system becomes an important issue [5].

In order to model network attack-defense problems, game theory becomes a powerful tool [6]–[8]. As a family member of games, Colonel Blotto game [9] is a useful model for attack-defense resource allocation, where two players are in charge of the force assignment for a number of battlefields. In Colonel Blotto game, a player wins a battlefield if the troops he/she assigns to this battlefield is more than those of his/her counterpart. The goal of both players is to win as many battlefields as possible [10]. It has been widely studied [11] and applied in a range of fields such as military [12], information forecasting [13], social science [14], communication and computer networks [15], [16], etc. In addition, some extended models of Colonel Blotto game have also been proposed, including the games with weighted battlefields, the games with continuous resources, the games with asymmetric resources, and the heterogeneous games [17], [18]. There are also some researchers try to find the quality strategies of Colonel Blotto game from the perspective of experimental economics [19]–[21].

As for network systems, Fuchs and Khargonekar [22] constituted a Colonel Blotto game model for resource allocation with asymmetric information in a wireless sensor network. Hajimirsadeghi et al. [23] proposed a Colonel Blotto game based dynamic spectrum allocation scheme in the multi-user environment. Furthermore, Ferdowsi et al. [24] modeled the interference and anti-interference of multiple communication channels with the aid of Colonel Blotto game. Wu et al. [25]

Manuscript received August 30, 2018; revised February 20, 2019; accepted March 8, 2019. Date of publication March 12, 2019; date of current version June 4, 2020. This work was supported in part by the Young Elite Scientist Sponsorship Program by CAST under Grant 2016QNRC001, in part by the National Natural Science Foundation of China under Grant 91338203, in part by the Preresearch Fund of Equipments of Ministry of Education of China in part by the New Strategic Industries Development Projects of Shenzhen City under Grant JCYJ20170816151922176, Grant 18RT0073, and in part by the US National Science Foundation under Grants CNS-1717454, CNS-1731424, CNS-1702850, and CNS-1646607. Recommended for acceptance by B. Shou. (*Corresponding author: Chunxiao Jiang*.)

S. Guan, J. Wang, and Y. Ren are with the Department of Electronic Engineering, Tsinghua University, Beijing 100084, China (e-mail: gsh17@mails.tsinghua.edu.cn; chinaeephd@gmail.com; reny@tsinghua.edu.cn).

H. Yao is with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: yaohaipeng@bupt.edu.cn).

C. Jiang is with the Tsinghua Space Center, Tsinghua University, Beijing 100084, China and also with the Key Laboratory of EDA, Research Institute of Tsinghua University, Shenzhen 518057, China (e-mail: jchx@tsinghua.edu.cn).

Z. Han is with the University of Houston, Houston, TX 77004, USA and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (e-mail: zhan2@uh.edu).

Digital Object Identifier 10.1109/TNSE.2019.2904530

investigated the optimal power selection problem against jamming attacks. However, these game models just establish a simple and linear relationship between the global utility and the results on each battlefield, i.e., calculating the sum or weighted sum of the result of each battlefield as the global utility. In practical systems, the global utility and the result of each battlefield often have a complex and implicit relationship. Furthermore, in Colonel Blotto games, with the increase of the number of troops and battlefields, the number of feasible actions grows exponentially. Hence, most related works just concentrate on simple toy systems. Efficient solutions for large scale network systems are urgently needed.

To address the aforementioned issues, relying on network theory [26], we propose a networked Colonel Blotto game to study the attack-defence problem in network systems. In this game model, two players, i.e., the attacker and the defender, allocate attack-defence resources on the nodes which represent the battlefields. The goal of both players is to maximize or minimize the network performance, which constitutes a two-player zero-sum game. In this case, utility is based not only on the number of nodes that a player wins, but also on these nodes' impact on the network performance. The original contributions of this paper can be summarized as follows:

- We provide a networked Colonel Blotto game model for the ubiquitous attack-defense resource allocation in network systems. Moreover, four metrics, i.e., network connectivity, path length, degree and transmission capacity, are defined for evaluating the network performance as well as for formulating the utility of this two-player zero-sum game.
- As for large-scale network systems with enormous action sets of both players, considering the complexity of finding the equilibrium, we propose a genetic algorithm based co-evolution algorithm for generating practical action sets and for searching quality strategies for both players.
- Our networked Colonel Blotto game model is applied to four large-scale network systems, i.e., Internet, vehicular networks, air transportation systems and social networks. The real-world data based simulations verify the validity and feasibility of our proposed game model, which is beneficial in terms of supporting the maintenance and management of large-scale network systems.

The remaining content is arranged as follows. We introduce our networked Colonel Blotto game model and network performance metrics in Section II. Section III provides a general solving method of the Nash equilibrium of this zero-sum game for small-scale network systems. In Section IV, we discuss the equilibrium strategies for large-scale network systems and present the co-evolution based algorithms for seeking quality strategies. Simulation results based on the four real-world networks are given in Section V, followed by the conclusions in Section VI.

II. Game Model and Network Performance Metrics

A. Networked Colonel Blotto Game

The networked Colonel Blotto game is a one-shot two-player zero-sum game, where two players are the defender and the attacker, respectively. Firstly, the network system is defined as an undirected graph denoted by $\boldsymbol{G} = \{\mathbb{V}, \mathbb{E}\}$, where $\mathbb{V} = \{v_1, v_2, \ldots, v_N\}$ represents the set of nodes and $\mathbb{E} = \{e_1, e_2, \ldots, e_M\}$ is the set of edges. N represents the total number of nodes, while M denotes the total number of edges. Each edge can be expressed by the set of two nodes it connects. For example, $e_k = \{v_i, v_j\}$ represents that e_k is the edge that connects nodes v_i and v_j. As for the defender, the quantity of defense resources is denoted as A_1, which can be allocated on nodes for preventing potential attacks. Hence, the action of the defender can be represented as:

$$\boldsymbol{a}_1 = [a_1^1, a_1^2, \ldots, a_1^N], \tag{1}$$

where $a_1^i \geq 0$ stands for the quantity of defense resources that allocated on node v_i by the defender, and we have $\sum_{i=1}^{N} a_1^i = A_1$. By contrast, the quantity of attack resources allocated by the attacker is A_2, and the action of the attacker can be denoted as:

$$\boldsymbol{a}_2 = [a_2^1, a_2^2, \ldots, a_2^N], \tag{2}$$

where a_2^i satisfies $a_2^i \geq 0$ as well as $\sum_{i=1}^{N} a_2^i = A_2$. The action sets of the defender and attacker are $\mathbb{A}_1$ and $\mathbb{A}_2$, respectively. In addition, we assume that the maximum self-defense capability of node v_i is $a_0^i \geq 0$, and we obtain:

$$\boldsymbol{a}_0 = [a_0^1, a_0^2, \ldots, a_0^N]. \tag{3}$$

Then, the result of the "battle" on each node depends on the quantity of the attack-defense resources that two players allocate. Hence, we can divide nodes into two sets, i.e., the set of nodes $\mathbb{V}_1$ controlled by the defender, and the set of nodes $\mathbb{V}_2$ controlled by the attacker. The result of the "battle" on node v_i follows:

$$v_i \in \begin{cases} \mathbb{V}_1, & \text{if } a_0^i + a_1^i \geq a_2^i, \\ \mathbb{V}_2, & \text{if } a_0^i + a_1^i < a_2^i. \end{cases} \tag{4}$$

To elaborate, the attacker wins a node if the attack resources deployed on it exceed the sum of defense resources and node's self-defense capability. Furthermore, edges can be divided into three categories according to the nodes they connect. These three sets can be denoted as $\mathbb{E}_{11}$, $\mathbb{E}_{12}$ and $\mathbb{E}_{22}$. Specifically, edge $e_k \in \mathbb{E}_{ij}$ $(i, j \in \{1, 2\},\ i \leq j)$ indicates that the two nodes it connects are from $\mathbb{V}_i$ and $\mathbb{V}_j$, respectively. Fig. 1 provides a diagram which shows the relationship between nodes' attack-defense resource allocated and their affiliation.

In our model, in order to compare the performance of the whole network system, we denote the original network as $\boldsymbol{G}'$, while the network after the game is represented by $\boldsymbol{G}''$. Finally, the utility function of the game can be given by:

$$u_1(\boldsymbol{a}_1, \boldsymbol{a}_2) = -u_2(\boldsymbol{a}_1, \boldsymbol{a}_2) = f(\boldsymbol{G}'') - f(\boldsymbol{G}'), \tag{5}$$

where u_1 represents the utility of the defender, while u_2 is the utility of the attacker, and $f(\cdot)$ denotes the evaluation function of the network performance. In addition, in original network system $\boldsymbol{G}'$, we assume that $a_1^i = a_2^i = 0$, so all the nodes in $\boldsymbol{G}'$ belong to $\mathbb{V}_1$. Therefore, the defender's goal is to minimize

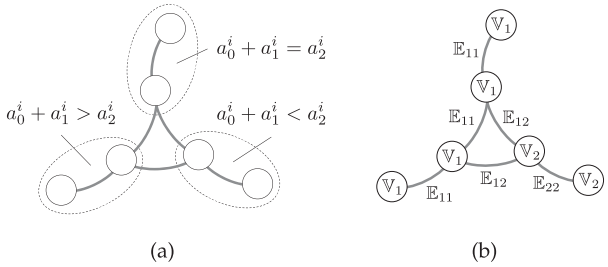


Fig. 1. The relationship between the nodes' attack-defense resources allocated and their affiliation. (a) The quantity relationships of attack-defense resources (a_0^i, a_1^i and a_2^i) allocated on each node. (b) The categories ($\mathbb{V}_i$ and $\mathbb{E}_{ij}$) that nodes and edges belong to.

the performance loss, while the attacker aims for maximizing it, which constitutes a zero-sum game.

B. Network Performance Evaluation

In this subsection, we will introduce some commonly used network characteristics to construct evaluation function $f(\cdot)$. For the convenience of deduction, we adopt the adjacency matrix as $\boldsymbol{W} = (w_{ij})_{N\times N}$ to represent the network topology, i.e.,

$$\boldsymbol{W} = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1N} \\ w_{21} & w_{22} & \cdots & w_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ w_{N1} & w_{N2} & \cdots & w_{NN} \end{bmatrix}. \tag{6}$$

Specifically, in an unweighted graph, $w_{ij} \in \{0, 1\}$ represents the existence of edge $\{v_i, v_j\}$, while $w_{ij} \geq 0$ denotes the weight of edge $\{v_i, v_j\}$ in a weighted graph.

1) Network Connectivity: In many network attack-defense scenarios, if some nodes are controlled and damaged by the attacker, the network connectivity will seriously change. Hence, the survivability of the network system, i.e., the ability of maintaining its connectivity under attack, becomes an critical metric. Here, the weight of edge w_{ij} can be defined as:

$$w_{ij} = \begin{cases} 1, & \text{if } \{v_i, v_j\} \in \mathbb{E}_{11}, \\ 0, & \text{if } \{v_i, v_j\} \in \mathbb{E}_{12} \cup \mathbb{E}_{22}, \end{cases} \tag{7}$$

for an unweighted graph. Because there may exist unconnected parts in the network, the network can be divided into one or more sub-networks. The sub-network with most nodes is named as the giant component. If the giant component contains n nodes, the network connectivity based evaluation function can be denoted as:

$$f(\boldsymbol{G}) = n. \tag{8}$$

2) Average Path Length: Sometimes, attacks may not damage the network's connectivity, but may still influence the performance of edges. Here the path $\boldsymbol{p}_{i_1,i_K}$ between nodes v_{i_1} and v_{i_K} can be represented by an ordered but not repeated node sequence, i.e., $\boldsymbol{p}_{i_1,i_K} = [v_{i_1}, v_{i_2}, \ldots, v_{i_K}]$. As for a pair of adjacent nodes v_{i_k} and $v_{i_{k+1}}$ on the path, there exists $w_{i_k,i_{k+1}} > 0$. The length of a path is defined as the total weight of the edges it includes, i.e.,

$$r(\boldsymbol{p}_{i_1,i_K}) = \sum_{[v_{i_k}, v_{i_{k+1}}] \in \boldsymbol{p}_{i_1,i_K}} w_{i_k,i_{k+1}}, \tag{9}$$

where $[v_{i_k}, v_{i_{k+1}}]$ denotes two adjacent nodes on the path. Note that there often exist multiple paths between two nodes. Hence, the shortest length of the path between two nodes can be given by:

$$r_{ij}^{\star} = \min_{\boldsymbol{p}_{ij}} r(\boldsymbol{p}_{ij}). \tag{10}$$

The average path length of the network is calculated as:

$$\bar{r} = \frac{\sum_{i\neq j} r_{ij}^{\star}}{N(N-1)}. \tag{11}$$

Thus, the average path length based evaluation function can be formulated as:

$$f(\boldsymbol{G}) = -\bar{r}. \tag{12}$$

3) Average Degree: Degree is a critical and universal metric of a network system which reveals its connectivity, structure, or other characteristics. The degree of node v_i is the sum of the weight of all the edges it connected with, which can be written as:

$$d_i = \sum_{j=1}^{N} w_{ij}. \tag{13}$$

The average degree of a network can be calculated as:

$$\bar{d} = \frac{\sum_{i=1}^{N} d_i}{N} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} w_{ij}}{N}, \tag{14}$$

which is proportional to the sum of the weight of all edges in the network. Hence, the average degree based evaluation function of the network system can be defined as:

$$f(\boldsymbol{G}) = \bar{d}. \tag{15}$$

4) Transmission Capability: In some transmission processes such as rumors in social networks and computer virus in computer networks, the susceptible-infection (SI) propagation model is commonly adopted [27]. In this model, nodes have two states, i.e., the susceptible state (S) and the infected state (I). The susceptible node can be infected by its neighboring infected nodes. In this process, $\mathbb{V}_1(t)$ and $\mathbb{V}_2(t)$ represent the susceptible node set and the infected node set at time step t, respectively. Moreover, similar to previous definition, $\mathbb{E}_{ij}(t)$ denotes the edge sets at time step t. We assume that the nodes controlled by the defender in the game constitute $\mathbb{V}_1(0)$, while the nodes controlled by the attacker constitute $\mathbb{V}_2(0)$. Then, relying on the SI propagation model, at each time step t, node v_i may be infected and added into $\mathbb{V}_2(t)$ with the probability of:

$$p_i(t) = \begin{cases} \dfrac{\sum_{\{j:\{v_i,v_j\}\in\mathbb{E}_{12}(t-1)\}} c_j}{\sum_{\{j:\{v_i,v_j\}\in\mathbb{E}\}} c_j}, & \text{if } v_i \in \mathbb{V}_1(t-1), \\ 1, & \text{if } v_i \in \mathbb{V}_2(t-1), \end{cases} \tag{16}$$

where c_j is defined as the influence of node v_j. Correspondingly, node v_i may stay susceptible and fall into $\mathbb{V}_1(t)$ with probability $1 - p_i(t)$. Hence, the infection probability of a susceptible node is the ratio of the total influence of its infected neighbors to that of all its neighbors. Then, we define the average diffusion time $\bar{t}$ as the expected time when the proportion of infected nodes reaches a threshold β, i.e.,

$$\bar{t} = \mathbf{E}\left(\min\left\{t : \frac{|\mathbb{V}_2(t)|}{N} \geq \beta\right\}\right). \tag{17}$$

where $|\mathbb{V}_2(t)|$ represents the number of infected nodes at time step t. Therefore, the transmission capability based performance evaluation function can be given by:

$$f(\boldsymbol{G}) = \bar{t}. \tag{18}$$

III. Strategies in Small-Scale Networks

A. General Equilibrium Solution Algorithm

In this section, we will discuss about the solution method of our game model in small-scale network systems. As mentioned before, our proposed game has infinite actions and discontinuous payoff, which imposes great challenges on the analysis. Therefore, we can adopt the commonly used gridding method to transform it into the game with finite actions for approximating the Nash equilibrium and the expected utility [28], [29]. Here we firstly assume that the amount of resources are integers, i.e., $A_1, A_2, a_l^i \in \mathbb{N}$ $(l = 0, 1, 2,\ i = 1, 2, \ldots, N)$. Hence, the action sets of both players $\mathbb{A}_1$ and $\mathbb{A}_2$ are finite, and the game becomes a zero-sum matrix game. In this matrix game, we can easily find the existence of pure strategy Nash equilibrium. The mixed strategies of both players are represented as $\boldsymbol{s}_1 = [s_1^1, s_1^2, \ldots, s_1^{K_1}]$ and $\boldsymbol{s}_2 = [s_2^1, s_2^2, \ldots, s_2^{K_2}]$, where s_l^k $(l = 1, 2)$ is the probability that player l takes action $\boldsymbol{a}_l^k$, and K_1, K_2 are the size of their action sets. When solving the mixed strategy Nash equilibrium, the main problem is that the number of feasible actions is acutely increased with the augment of the number of nodes and the amount of resources. Hence we usually formulate it into linear programming problems. First, under the mixed strategy Nash equilibrium, neither the defender nor the attacker can increase his/her expected utility by taking a pure strategy instead of the equilibrium strategy unilaterally. In other words, $(\boldsymbol{s}_1^\star, \boldsymbol{s}_2^\star)$ is the mixed strategy Nash equilibrium if and only if:

$$u_1(\boldsymbol{a}_1^{k_1}, \boldsymbol{s}_2^\star) \leq u_1(\boldsymbol{s}_1^\star, \boldsymbol{s}_2^\star) \leq u_1(\boldsymbol{s}_1^\star, \boldsymbol{a}_2^{k_2}), \tag{19}$$

for all $k_1 = 1, 2, \ldots, K_1$ and $k_2 = 1, 2, \ldots, K_2$. When there exist multiple mixed equilibria, due to the indifferent and exchangeable properties of the equilibrium strategies in zero-sum game [30], as long as a player takes one of equilibrium strategies, the maximum expected utility can be guaranteed. Then we rewrite (19) into the form of inequalities as:

$$\begin{cases} \sum_{k_1=1}^{K_1} s_1^{k_1}\ u_1(\boldsymbol{a}_1^{k_1}, \boldsymbol{a}_2^{k_2}) \geq v, & k_2 = 1, \ldots, K_2, \\ \sum_{k_1=1}^{K_1} s_1^{k_1} = 1, & \\ s_1^{k_1} \geq 0, & k_1 = 1, \ldots, K_1, \end{cases} \tag{20}$$

and

$$\begin{cases} \sum_{k_2=1}^{K_2} s_2^{k_2}\ u_1(\boldsymbol{a}_1^{k_1}, \boldsymbol{a}_2^{k_2}) \leq v, & k_1 = 1, \ldots, K_1, \\ \sum_{k_2=1}^{K_2} s_2^{k_2} = 1, & \\ s_2^{k_2} \geq 0, & k_2 = 1, \ldots, K_2. \end{cases} \tag{21}$$

Thus, (20) and (21) can be formulated into a pair of mutually dual linear programming problems as:

$$\begin{aligned} \max \quad & v \\ \text{s.t.} \quad & \sum_{k_1=1}^{K_1} s_1^{k_1}\ u_1(\boldsymbol{a}_1^{k_1}, \boldsymbol{a}_2^{k_2}) \geq v, \quad k_2 = 1, \ldots, K_2, \\ & \sum_{k_1=1}^{K_1} s_1^{k_1} = 1, \\ & s_1^{k_1} \geq 0, \qquad k_1 = 1, \ldots, K_1, \end{aligned} \tag{22}$$

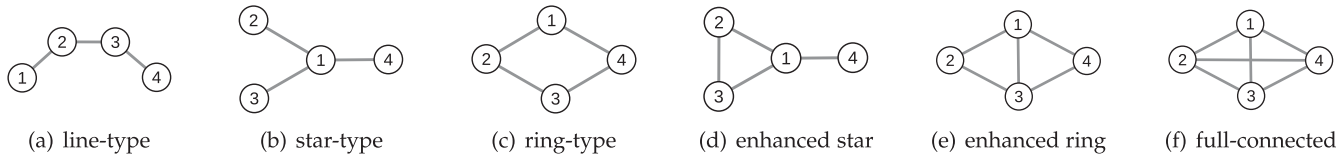
as well as

$$\begin{aligned} \min \quad & w \\ \text{s.t.} \quad & \sum_{k_2=1}^{K_2} s_2^{k_2}\ u_1(\boldsymbol{a}_1^{k_1}, \boldsymbol{a}_2^{k_2}) \leq w, \quad k_1 = 1, \ldots, K_1, \\ & \sum_{k_2=1}^{K_2} s_2^{k_2} = 1, \\ & s_2^{k_2} \geq 0, \qquad k_2 = 1, \ldots, K_2. \end{aligned} \tag{23}$$

By solving the prime problem (22) and its dual problem (23), we get the optimal solution $(\boldsymbol{s}_1^\star, v^\star)$ and $(\boldsymbol{s}_2^\star, w^\star)$, respectively. Due to strong duality property, we have $v^\star = w^\star$, which also equal the defender's expected utility, i.e.,

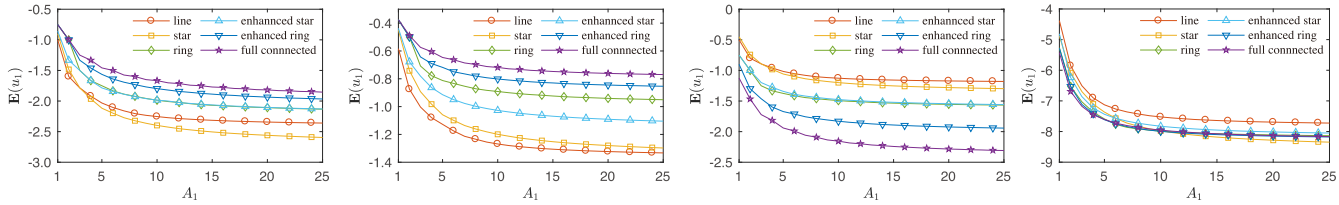
$$\mathbf{E}(u_1) = u_1(\boldsymbol{s}_1^\star, \boldsymbol{s}_2^\star) = \sum_{k_1=1}^{K_1} \sum_{k_2=1}^{K_2} s_1^{k_1}\ s_2^{k_2}\ u_1(\boldsymbol{a}_1^{k_1}, \boldsymbol{a}_2^{k_2}). \tag{24}$$

Therefore, we provide a general solution method as Algorithm 1, where we can increase A_1, A_2 and a_l^i in proportion representing a finer grid density, to approximate the original equilibrium. However, its computational complexity



(a) line-type (b) star-type (c) ring-type (d) enhanced star (e) enhanced ring (f) full-connected

Fig. 2. Topologies of four-node networks.



(a) network connectivity (b) average path length (c) average degree (d) transmission capability

Fig. 3. Expected utility of the defender under mixed Nash equilibrium strategy under different network performance metrics when $A_1 : A_2 = 1 : 1$. (a) Network connectivity metric. (b) Average path length metric, assuming $w_{ij} = 1$ if $\{v_i, v_j\} \in \mathbb{E}_{11}$ and $w_{ij} = 2$ if $\{v_i, v_j\} \in \mathbb{E}_{12} \cup \mathbb{E}_{22}$. (c) Average degree metric, assuming $w_{ij} = 1$ if $\{v_i, v_j\} \in \mathbb{E}_{11}$ and $w_{ij} = 0$ if $\{v_i, v_j\} \in \mathbb{E}_{12} \cup \mathbb{E}_{22}$. (d) Transmission capability metric, node's influence $c_j = 1$, $(j = 1, 2, 3, 4)$, threshold $\beta = 1$, the average diffusion time $\bar{t}$ is set as 10 in the case that all nodes are controlled by the defender in the game.

raises at the same time. Therefore, we should choose a proper gridding to strike a trade-off between accuracy and efficiency.

Algorithm 1: General Equilibrium Solution Algorithm

1: **Input** Network system $\boldsymbol{G}'$, evaluation function $f(\cdot)$;
2: **Initialize** Set A_1, A_2 and $\boldsymbol{a}_0$ considering the real scenario, solving accuracy and computing complexity;
3: Generate the action sets $\mathbb{A}_1 = \{\boldsymbol{a}_1^1, \boldsymbol{a}_1^2, \ldots, \boldsymbol{a}_1^{K_1}\}$ and $\mathbb{A}_2 = \{\boldsymbol{a}_2^1, \boldsymbol{a}_2^2, \ldots, \boldsymbol{a}_2^{K_2}\}$ of both players;
4: Calculate the utility $u_1(\boldsymbol{a}_1^{k_1}, \boldsymbol{a}_2^{k_2})$ for every pair of $\boldsymbol{a}_1^{k_1}$, $\boldsymbol{a}_2^{k_2}$ in $\mathbb{A}_1$, $\mathbb{A}_2$, and construct the payoff matrix;
5: Solve the linear programming problems (22) and (23);
6: **Output** Nash equilibrium strategy $(\boldsymbol{s}_1^\star, \boldsymbol{s}_2^\star)$ and the expected utility $\mathbf{E}(u_1)$;

B. Performance Analysis

In the following, we will discuss the performance of the algorithm by simple examples. Here we take the networks with four nodes seen in Fig. 2 into account. Moreover, we set $a_0^i = 0$ for all nodes and $A_1 : A_2 = 1 : 1$. Because we restrict all resources as integer, hence the values of A_1 and A_2 indicate the number of units that we divide the resources into, namely the grid density. Then we test the convergence performance of utility and equilibrium strategy under different grid densities. Fig. 3 shows the expected utility with finer grid density in the case of various network performance metrics. We can find that the approximate utility in all cases converges gradually when we increase A_1 and A_2 in proportion. Furthermore, Fig. 4 shows the convergence of normalized average resource allocation on nodes (i.e., the proportion of resources allocated on a node to total resources under the equilibrium strategy) of the defender and attacker under the enhanced star topology as Fig. 2(d) and the network connectivity metric. We can conclude that the allocation strategy under the mixed Nash equilibrium also converges with finer grid densities, which shows the effectiveness of our proposed method.

C. Computational Complexity Analysis

In Algorithm 1, after setting A_1, A_2 and $\boldsymbol{a}_0$, the defender has to allocate A_1 units of resources on N different nodes. This can be regarded as a distribution problem and $K_1 = \binom{A_1+N-1}{N} = \frac{(A_1+N-1)!}{(A_1-1)!N!}$. Similarly, we get $K_2 = \binom{A_2+N-1}{N} = \frac{(A_2+N-1)!}{(A_2-1)!N!}$ for the attacker. Therefore, the complexity of generating both action sets can be regarded as $\mathcal{O}\big((K_1 + K_2)N\big)$.

Then, constructing the payoff matrix with the size of $K_1 \times K_2$ includes following steps. Given the action pair of both players, we can get the nodes' status with $\mathcal{O}(N)$ and derive the new adjacency matrix $\boldsymbol{W}$ relying on specific game rule with $\mathcal{O}(N^2)$. Then, the complexity of calculating network performance $f(\boldsymbol{G})$ under different performance metrics are:

- **Network Connectivity**: In order to find out the giant component, we have to traverse through the network with the aid of depth first search (DFS) or breadth first search (BFS). When representing the network by its adjacency matrix $\boldsymbol{W}$, its complexity is $\mathcal{O}(N^2)$.
- **Average Path Length**: For a undirected network with non-negative edge weights, we can firstly derive the shortest paths of all pairs of nodes by Floyd-Warshall algorithm, then calculate the average path length. Its complexity is $\mathcal{O}(N^3)$.
- **Average Degree**: It can be derived directly by adding up the elements of $\boldsymbol{W}$. Its complexity is $\mathcal{O}(N^2)$.
- **Transmission Capability**: We determine the expected diffusion time by Monte-Carol simulation, and take the average diffusion time of several experiments. In each time step of simulation, we calculate each node's infected probability and update its status as (16). The simulation takes $\bar{t}$ time steps in average. Hence its complexity is $\mathcal{O}(\bar{t}\bar{d}N)$, where $\bar{d}$ is the average degree of the network.

In fact, because different action pairs may lead to the same result, the times of calculating $\boldsymbol{W}$ and network performance can be reduced to $\mathcal{O}(2^N)$. Therefore, the total complexity of

this step is $\mathcal{O}(K_1K_2N)$, which is determined by calculating the nodes status under given action pairs.

Thirdly, because the linear programming problem (22) and (23) are mutually dual, we can obtain the equilibrium by solving only one of them by simplex method. Here we assume $A_1 \geq A_2$ ($K_1 \geq K_2$), and hence we solve (22) to reduce complexity. The complexity of each iteration of simplex method is $\mathcal{O}(K_1K_2)$. In the worst case, the number of iterations is exponential to the number of variables, i.e., $\mathcal{O}(2^{K_1})$. But in practice, it is generally accepted that the average number of iterations is linear to the number of constraints, i.e., $\mathcal{O}(K_2)$ [31]. Therefore the total complexity of this step n be given by $\mathcal{O}(K_1K_2^2)$. Similarly, for the case that $A_1 \leq A_2$ ($K_1 \leq K_2$), the complexity of this step is $\mathcal{O}(K_1^2K_2)$.

Therefore, the total computational complexity is determined by solving the linear programming problem and equals $\mathcal{O}(K_1K_2 \min\{K_1, K_2\})$, which is factorial to the network size of N. Moreover, with the increasing of N, in order to maintain the accuracy of solutions, A_1 and A_2 also increase linearly. Hence its computational complexity raises rapidly with the increase of the network scale. In general, this method only supports accurate analysis of small-scale network systems with a dozen of nodes.

IV. Strategies in Large-Scale Networks

A. Practical Action Set and Co-Evolutionary Algorithm

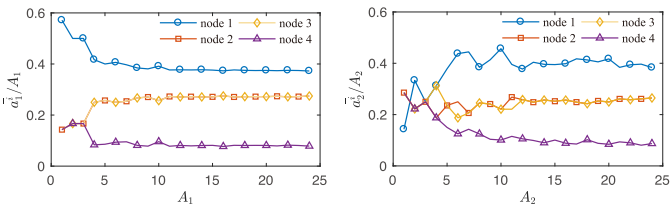
As mentioned above, the action set of the game can be extremely large with the augment of nodes, which makes it difficult to analyze the strategies in large-scale network systems. However, in experiments, researchers found that most respondents' plans just focus on a few actions or allocation schemes [21]. In real network systems, attackers and defenders also have several commonly used patterns for attacking and defending. These specific patterns can be regarded as the common chosen actions in the experiments. Moreover, the rational defender and attacker will only choose the actions yielding high expected utility as its strategy. Therefore, in order to simplify the computation, we assume that the action set of the player is composed of only a small part of the quality practical actions from all the feasible actions, namely the *practical action set*.

In order to find these quality practical actions and to accurately generate the practical action sets of both players, we propose a co-evolution based algorithm as Algorithm 2 inspired by the genetic algorithm [32], [33]. In our algorithm, we first generate some random actions constituting the initial action set $\mathbb{A}_l$ ($l = 1, 2$) for the defender and the attacker. Then the defender and the attacker test these actions by matching against the opponents' action sets and record the average utility of each action. The actions with high average utility will be added directly into the next generation, and the other actions in the next generation will be generated by genetic manipulation, i.e., crossover and random mutation. In such an iterative process, dominated actions will be continuously excluded from the action set, and quality actions can still be retained. Moreover, actions with higher quality can be generated by genetic manipulation, which yields the co-evolution of both players' action sets. Finally, we can take the result as the practical action sets for both players.

Algorithm 2: Co-Evolution Based Equilibrium Solution Algorithm

Input Network system $\boldsymbol{G}'$, evaluation function $f(\cdot)$, number of iterations T, resources A_1, A_2, sizes of action sets K_1, K_2, proportion of actions inherited directly μ_1, μ_2, mutation probability γ_1, γ_2;
Initialize Generate chromosomes $\boldsymbol{g}_l^k$ randomly to build initial gene pools $\mathbb{G}_1$, $\mathbb{G}_2$, and generate initial action sets $\mathbb{A}_1 = \{\boldsymbol{a}_1^1, \boldsymbol{a}_1^2, \ldots, \boldsymbol{a}_1^{K_1}\}$ and $\mathbb{A}_2 = \{\boldsymbol{a}_2^1, \boldsymbol{a}_2^2, \ldots, \boldsymbol{a}_2^{K_2}\}$ from $\mathbb{G}_1$, $\mathbb{G}_2$ as (25) and (26);
for $t = 1, \ldots, T$ **do**
  Calculate the utility for every pair of actions in $\mathbb{A}_1$ and $\mathbb{A}_2$ according to $f(\cdot)$ as (5), and calculate the average utility of every action $\overline{\boldsymbol{u}_1} = [\overline{u_1^1}, \overline{u_1^2}, \ldots, \overline{u_1^{K_1}}]$, $\overline{\boldsymbol{u}_2} = [\overline{u_2^1}, \overline{u_2^2}, \ldots, \overline{u_2^{K_2}}]$ as (27) and (28);
  Calculate the probability that being selected in crossover $\boldsymbol{p}_1 = [\, p_1^1, p_1^2, \ldots, p_1^{K_1}]$, $\boldsymbol{p}_2 = [\, p_2^1, p_2^2, \ldots, p_2^{K_2}]$ for every action in $\mathbb{A}_1$ and $\mathbb{A}_2$ as (29);
  for $l = 1, 2$ **do**
    Generate empty gene pool $\mathbb{G}_l' = \emptyset$ and empty action set $\mathbb{A}_l' = \emptyset$;
    for $k = 1, 2, \ldots, K_l$ **do**
      if $k \leq \mu_l K_l$ **then**
        Choose the action with kth highest utility in $\mathbb{A}_l$ according to $\overline{\boldsymbol{u}_l}$, and add it to $\mathbb{A}_l'$ as $\boldsymbol{a}_l^k$;
      else
        Choose parent chromosomes $\boldsymbol{g}_l^x$, $\boldsymbol{g}_l^y$ according to $\boldsymbol{p}_l$;
        Divide the node index set $\mathbb{V}$ into $\mathbb{V}_x$ and $\mathbb{V}_y$;
        Generate crossover chromosome $\boldsymbol{g}_l^{k'}$ by $\mathbb{V}_x$, $\mathbb{V}_y$ and $\boldsymbol{g}_l^x$, $\boldsymbol{g}_l^y$ as (30);
        Generate child chromosome $\boldsymbol{g}_l^k$ from $\boldsymbol{g}_l^{k'}$ as (31) with mutation probability γ_l, and add it to $\mathbb{G}_l'$;
        Generate child action $\boldsymbol{a}_l^k$ as (25) and (26) and add it to $\mathbb{A}_l'$;
      end
    end
    Update $\mathbb{G}_l = \mathbb{G}_l'$ and $\mathbb{A}_l = \mathbb{A}_l'$;
  end
end
Calculate the utility $u_1(\boldsymbol{a}_1^{k_1}, \boldsymbol{a}_2^{k_2})$ for every pair of $\boldsymbol{a}_1^{k_1}$, $\boldsymbol{a}_2^{k_2}$ in practical action sets $\mathbb{A}_1$, $\mathbb{A}_2$;
Solve the linear programming problems in (22) and (23);
Output Nash equilibrium strategy $(\boldsymbol{s}_1^\star, \boldsymbol{s}_2^\star)$ and the expected utility $\mathbf{E}(u_1)$;

Specifically, first of all, we set K_l ($l = 1, 2$) as the number of actions in the action set for both players, and generate random vectors $\boldsymbol{g}_l^k = [g_l^{k(1)}, g_l^{k(2)}, \ldots, g_l^{k(N)}]$, where $l = 1, 2$, $k = 1, 2, \ldots, K_l$, and $g_l^{k(i)} \geq 0$ ($i = 1, 2, \ldots, N$) are independent and identically distributed random numbers. Depending on specific scenarios, we can select the probability density function of $g_l^{k(i)}$ as exponential distribution $f(x) = e^{-x}$ ($x > 0$), revised normal distribution $f(x) = \sqrt{\frac{2}{\pi}} e^{-\frac{x^2}{2}}$ ($x > 0$), uniform distribution $f(x) = 1$ ($0 < x < 1$), or others for achieving good performance. Then, the initial random actions can be given by:



(a) defender's (b) attacker's

Fig. 4. Both players' normalized average resource allocation on each node under mixed Nash equilibrium strategy (network connectivity metric, enhanced star topology, $A_1 : A_2 = 1 : 1$).

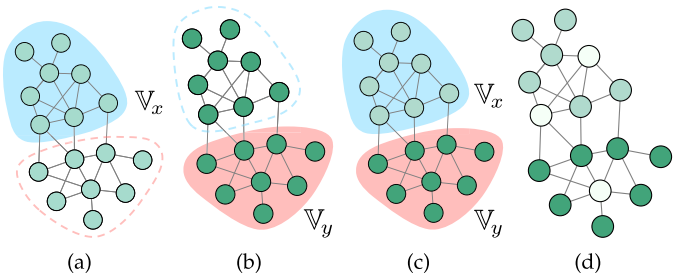


Fig. 5. The process of generating child chromosome $\boldsymbol{g}_l^k$ from parent chromosomes $\boldsymbol{g}_l^x$ and $\boldsymbol{g}_l^y$. (a) parent chromosome $\boldsymbol{g}_l^x$. (b) parent chromosome $\boldsymbol{g}_l^y$. (c) crossover chromosome $\boldsymbol{g}_l^{k'}$. (d) child chromosome $\boldsymbol{g}_l^k$.

$$\boldsymbol{a}_l^k = A_l \cdot \frac{\boldsymbol{g}_l^k}{\sum_{i=1}^{N} g_l^{k(i)}}, \tag{25}$$

Here, $\boldsymbol{g}_l^k$ is also called the *chromosome* of action $\boldsymbol{a}_l^k$, and $g_l^{k(i)}$ $(i = 1, 2, \ldots, N)$ are named *genes* that concatenate it. Moreover, action set $\mathbb{A}_l$ composed by $\boldsymbol{a}_l^k$, is a *population*, and the set of chromosomes $\mathbb{G}_l = \{\boldsymbol{g}_l^1, \boldsymbol{g}_l^2, \ldots, \boldsymbol{g}_l^{K_l}\}$ is a *gene pool*. In addition, according to the rational assumption of players, in order to avoid the case that $a_2^i \le a_0^i$, we adjust the attacker's action $\boldsymbol{a}_2^k = [a_2^{k(1)}, a_2^{k(2)}, \ldots, a_2^{k(N)}]$ as:

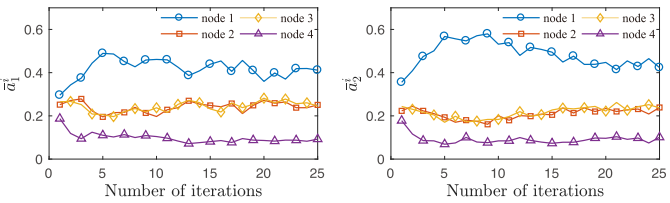
$$a_2^{k(i)} = \begin{cases} 0, & \text{if } i \notin \mathbb{I}^k, \\ a_2^{k'(i)} \cdot \dfrac{A_2}{\sum_{i \in \mathbb{I}^k} a_2^{k'(i)}}, & \text{if } i \in \mathbb{I}^k, \end{cases} \tag{26}$$

where $a_2^{k'(i)}$ is the attacker's original allocated resources generated by (25), while $\mathbb{I}^k$ is the set of node's index i that satisfies $a_2^{k'(i)} > a_0^i$. Given both players' initial action sets $\mathbb{A}_l = \{\boldsymbol{a}_l^1, \boldsymbol{a}_l^2, \ldots, \boldsymbol{a}_l^{K_l}\}$, according to (5), the average utility of each action is:

$$\overline{u_1^{k_1}} = \frac{1}{K_2} \sum_{k_2=1}^{K_2} u_1(\boldsymbol{a}_1^{k_1}, \boldsymbol{a}_2^{k_2}), \tag{27}$$

$$\overline{u_2^{k_2}} = \frac{1}{K_1} \sum_{k_1=1}^{K_1} u_2(\boldsymbol{a}_1^{k_1}, \boldsymbol{a}_2^{k_2}). \tag{28}$$

Thus, we can obtain $\overline{\boldsymbol{u}_l} = [\overline{u_l^1}, \overline{u_l^2}, \ldots, \overline{u_l^{K_l}}]$. Then, we can generate the child actions of the next generation. In our algorithm, $\mu_l K_l$ actions with the highest utility will be directly added into the action set of the next generation, where μ_l is the proportion. The remaining actions are generated by crossover and mutation. In the process of crossover, we first select two parent chromosomes $\boldsymbol{g}_l^x$ and $\boldsymbol{g}_l^y$ with certain probability as:



(a) defender's (b) attacker's

Fig. 6. Both players' average expected resource allocation on each node (network connectivity metric, enhanced star topology, $A_1 = A_2 = 1$, $K_1 = K_2 = 50$, $\mu_1 = \mu_2 = 20$, $\gamma_1 = \gamma_2 = 0.15$, uniform distributed genes).

$$p_l^k = \frac{2(K_l + 1 - h_l^k)}{K_l(K_l + 1)}, \tag{29}$$

where h_l^k is the rank of the average utility of action $\boldsymbol{a}_l^k$ in $\mathbb{A}_l$ in descending order. Then we randomly choose half of the genes that inherited from $\boldsymbol{g}_l^x$, and compose node set $\mathbb{V}_x$. The remaining nodes compose $\mathbb{V}_y = \mathbb{V} \setminus \mathbb{V}_x$, which indicates the the genes inherited from $\boldsymbol{g}_l^y$. Hence, we can denote the crossover gene as:

$$g_l^{k'(i)} = \begin{cases} g_l^{x(i)}, & \text{if } v_i \in \mathbb{V}_x, \\ g_l^{y(i)}, & \text{if } v_i \in \mathbb{V}_y. \end{cases} \tag{30}$$

Finally, in order to increase the diversity of the child population, each gene $g_l^{k'(i)}$ mutates with probability γ_l, i.e.,

$$g_l^{k(i)} = \begin{cases} g^{\text{rand}}, & \text{with probability } \gamma_l, \\ g_l^{k'(i)}, & \text{with probability } 1 - \gamma_l, \end{cases} \tag{31}$$

where g^{rand} is a random value with the same distribution with the initial genes. Hence, we can obtain child chromosome $\boldsymbol{g}_l^k$ composed by genes $g_l^{k(i)}$. Then we generate child action according to (25), and add it to the action set of the next generation. Fig. 5 illustrates the process of crossover and mutation. Lastly, we can solve the mixed strategy Nash equilibrium based on the practical action sets.

Here we firstly verify its performance small-scale networks discussed as exemplified in Section III-B. Here we still take the topology seen in Fig. 2(d) and use network connectivity $f(\boldsymbol{G}) = n$ as the network performance metric. In simulations, we set $A_1 = A_2 = 1$ and $a_0^i = 0$ for all nodes. Both players' average expected resource allocation on each node is shown in Fig. 6. In comparison to the simulation results obtained by Algorithm 1 as shown in Fig. 4, we can conclude that both player's strategies obtained by co-evolution algorithm converge to the original equilibrium, which proves the effectiveness of our proposed method.

B. Quality Response Action with Prior Knowledge

In the management of realistic network systems, the defender or the attacker may have prior knowledge about the opponent's strategy according to their historical experience. For example, through the statistical data, Internet administrators can know the attacking approach, frequency and intensity on each network

device, which can be deemed as the prior knowledge of the attacker's strategy. However, due to the complexity of network systems and the abstractness of performance evaluation, finding the best or a quality response action is still a challenge. Therefore, based on Algorithm 2, we provide a revised algorithm shown in Algorithm 3. In this algorithm, with the prior knowledge of the attacker's strategy, only the defender's action set evolves iteratively, and the output is the action with the highest expected utility, i.e., the best response action of the defender based on $\mathbb{A}_1$ and $\mathbb{A}_2$. On the contrary, we can also analysis the attacker's quality response action with prior knowledge of the defender's strategy.

Algorithm 3. Quality Response Action Solution Algorithm with Prior Knowledge

1: **Input** Network system $\boldsymbol{G}'$, evaluation function $f(\cdot)$, number of iterations T, opponent's action set $\mathbb{A}_2 = \{\boldsymbol{a}_2^1, \boldsymbol{a}_2^2, \ldots, \boldsymbol{a}_2^{K_2}\}$, opponent's strategy $\boldsymbol{s}_2 = [s_2^1, s_2^2, \ldots, s_2^{K_2}]$, resource A_1, size of action set K_1, proportion of actions inherited directly μ_1, mutation probability γ_1;
2: **Initialize** Generate chromosomes $\boldsymbol{g}_1^k$ randomly to build initial gene pool $\mathbb{G}_1$, and generate initial action set $\mathbb{A}_1 = \{\boldsymbol{a}_1^1, \boldsymbol{a}_1^2, \ldots, \boldsymbol{a}_1^{K_1}\}$ from $\mathbb{G}_1$ as (25);
3: **for** $t = 1, 2, \ldots, T$ **do**
4: Calculate the expected utility $\overline{\boldsymbol{u}_1} = [\overline{u_1^1}, \overline{u_1^2}, \ldots, \overline{u_1^{K_1}}]$ for every action in $\mathbb{A}_1$ as (27);
5: Calculate the probability that being selected in crossover $\boldsymbol{p}_1 = [\, p_1^1, p_1^2, \ldots, p_1^{K_1}]$ for every action in $\mathbb{A}_1$ as (29);
6: Execute Step 7 to Step 19 in Algorithm 2 where $l = 1$;
7: **end**
8: **Output** The quality response action $\boldsymbol{a}_1 = \arg\max_{\boldsymbol{a}_1^k \in \mathbb{A}_1} \; u_1(\boldsymbol{a}_1^k, \boldsymbol{s}_2)$;

C. Computational Complexity Analysis

The complexity of Algorithm 2 correlates to the number of nodes N, the sizes of population K_1 and K_2, and the number of iterations T. Firstly, the complexity of initializing the gene pools and generating action sets for both players (line 2) is $\mathcal{O}\big((K_1 + K_2)N\big)$ when the complexity of generating N random numbers is regarded as $\mathcal{O}(N)$.

In the main iteration process, we will firstly calculate the utility for K_1K_2 times for all action pairs (line 4). As discussed in Section III-C, the complexity of calculating nodes' status is $\mathcal{O}(N)$, and the complexity of deriving the new adjacency matrix is $\mathcal{O}(N^2)$. The complexity of calculating the network performance is $\mathcal{O}(g_{f(\boldsymbol{G})})$, where $g_{f(\boldsymbol{G})}$ equals N^2, N^3, N^2 and $\bar{t}\bar{d}N$ for the four metrics, respectively. The complexity of calculating the average utility is $\mathcal{O}(K_1K_2)$. Hence the total complexity of this step can be represented as $\mathcal{O}(K_1K_2\max\{N^2, g_{f(\boldsymbol{G})}\})$.

In order to calculate the probability that being selected in crossover (line 5), the complexity of sorting the utility is $\mathcal{O}(K_1\log K_1 + K_2\log K_2)$ by the quick sort algorithm. Then the complexity of calculating the probability is $\mathcal{O}(K_1 + K_2)$. In the following, we conduct the choosing, crossover and mutation operation, and generate the action sets of next generation (line 6 to line 20). The number of iteration is $(K_1 + K_2)$, and each operation can be completed in the linear time of N. Hence the total complexity of these steps is $\mathcal{O}\big((K_1 + K_2)N\big)$. Finally, the complexity of solving the equilibrium (line 23) based on the practical action sets is no more than $\mathcal{O}(K_1K_2\ \min\{K_1, K_2\})$.

Therefore, the total computational complexity of Algorithm 2 is mainly determined by the step of calculating the utility (line 4), and equals $\mathcal{O}(TK_1K_2\ \max\{N^2, g_{f(\boldsymbol{G})}\})$, which is polynomial to N for the for performance metrics in our paper. Moreover, the size of population K_1 and K_2 and iteration time T do not need to be significantly increased with the increase of N in practice. Comparing with Algorithm 1, it significantly reduces the computational complexity from a factorial complexity of N to a polynomial complexity of N. Hence, it shows great potential in analyzing the strategies in large scale networks.

The complexity analysis of Algorithm 3 is similar to Algorithm 2, and its computational complexity is also determined by the step of calculating of utility (line 4), which equals $\mathcal{O}(TK_1K_2\max\{N^2, g_{f(\boldsymbol{G})}\})$.

V. Applications and Simulations

In this section, we will introduce several applications of our game model in realistic scenarios based on real-world dataset. Concretely, we select four scenarios, i.e., Internet security, communication timeliness of wireless vehicular networks, efficiency and reliability of air transportation systems and rumor spread control in social networks, which correspond four evaluation metrics mentioned above. Firstly, we give an overview of the game models, network characteristics and simulation parameters of these applications in Table I. The network topologies can be found in Fig. 7. Because these real network systems are large scale, our analysis is mainly based on the co-evolution algorithm introduced in Section IV. After iterations in the co-evolution process, we select ten actions with the highest average utility as the practical action set for each player and solve the mixed Nash equilibrium strategies. In order to show the strategies of both players visualized, we calculate the expected resources allocated on each node by taking the weighted average of each action according to the mixed Nash equilibrium, and the detailed results in the case of $A_1 = A_2 = 100$ are illustrated in Fig. 7.

In addition, Fig. 8 provides the relationships between the resources A_1, A_2 and expected utility $\mathbf{E}(u_1)$. Moreover, the blue mesh on it illustrates the expected utility $\mathbf{E}(u_1)$ where the attacker's action set are randomly generated and the defender's action set is still generated by the co-evolution algorithm. Similarly, the red mesh shows $\mathbf{E}(u_1)$ where the defender's action set are randomly generated. We can find that the practical action set generated by the co-evolution algorithm overwhelms the randomly generated action set, which reveals the effectiveness and validity of our proposed algorithm. Further explanation and discussion of specific applications will be given in the following.

A. Internet Security

Resource allocation in Internet attack-defense confrontation is a typical application scenario of our model. The malicious attackers can attack key network devices in Internet by distributed denial of service (DDoS), identity spoofing, intrusion,

TABLE I
SELECTED APPLICATIONS OF THE GAME MODEL

Network Systems and Game Models				
Section	5.1	5.2	5.3	5.4
Scenarios	Internet security	communication timeliness of vehicle networks	efficiency and reliability of transportation systems	rumor spread control in social networks
Network system	computer networks	Internet of vehicles (IoV)	air transportation systems	online social networks
Nodes	autonomous systems	taxis	airports	Weibo users
Edges	network routes	wireless connections	flights	friend relationships
Defenders	Internet administrators	network schedulers	aviation managers	opinion supervisors
Attackers	hackers	interferers	terrorists, saboteurs	rumormongers
Defenders' action	protect network devices by installing firewalls, upgrading hardwares and softwares	enhance anti-jamming capacity of devices by increasing transmitting power	improve airports' prevention and response capacity to various risks	increase social network users' resistance and discernment to rumors
Attackers' action	attack key network devices by DDoS, identity spoofing, malicious intrusion	interferes the communication of vehicles on specific location by jamming	obstruct airline schedules by causing terrorist attacks, accidents and havoc	spread rumors to users and turn them into initial rumor disseminators
Resources	maintenance budget, computing resources	power consumption, devices budget	system maintenance budget, human resources	supervisory capacity, dissemination capacity
Primary goals	protect / break up the Internet connectivity	anti-interfere / interfere with communication timeliness	maintain / disrupt system's transportation capacity	suppress / promote the spread of rumors
Game rule	Eq. (7)	Eq. (32)	Eq. (33)	Eq. (16)
Performance metric	$f(\boldsymbol{G}) = n$	$f(\boldsymbol{G}) = -\bar{r}$	$f(\boldsymbol{G}) = \bar{d}$	$f(\boldsymbol{G}) = \bar{t}$
Network Data and Characteristics				
Original dataset	University of Oregon Route Views Project [34]	Beijing Taxi GPS Dataset in T-Drive Project [35]	US Air Transportation Network Dataset [36], [37]	Microblog PCU Dataset in UCI ML Repository [38]
Type of graph	undirected, unweighted	undirected, unweighted	undirected, weighted	undirected, unweighted
Number of nodes	300	125	50	279
Number of edges	400	425	878	313
Averge degree	2.67	6.80	35.12 (2.2×10^7)*	2.24
Average path length	3.17	8.00	1.28	4.61
Degree distribution	power-law	homogeneous	homogeneous	power-law
Network features	free-scale, small-world	ring network	dense network	free-scale, small-world four degree separate
Simulation Parameters**				
a_0^i	$0.01 \cdot d_i$	0.1	$10^{-8} \cdot {d_i}^*$	$0.01 \cdot d_i$
K_1, K_2	50, 50	50, 50	50, 50	50, 50
μ_1, μ_2	0.4, 0.4	0.4, 0.4	0.4, 0.4	0.4, 0.4
γ_1, γ_2	0.15, 0.15	0.15, 0.15	0.1, 0.1	0.15, 0.15

*Weighted degree.
**The distribution of genes $g_1^{k(i)}$ and $g_2^{k(i)}$ is exponential distribution.

etc. On the other hand, defenders can protect network devices by installing firewalls, upgrading hardwares and softwares, and so on. These behaviors can be abstracted as resources allocation. The more budget consumed on a network device, the higher the level of the attack or defense is. Here we assume that the network devices occupied by the attacker will break down, and hence the weight of these nodes' neighboring edges will become zero, which can be represented as (7). In addition, we set nodes' self-defense capacity $a_0^i = 0.01 \cdot d_i$, which is proportional to the nodes' degree. According to the simulation results shown in Figs. 7(a) and 7(b), the expected utility of the defender is $\mathbf{E}(u_1) = -198.5$ when $A_1 = A_2 = 100$. Hence, there are about 200 network nodes separated from the Internet backbone under given parameters. Furthermore, Fig. 9 shows both players' practical action sets that constitute the allocation scheme as Figs. 7(a) and 7(b) in detail. The attacker tends to allocate much resources on nodes with high degree, which makes their neighboring nodes separated from the giant

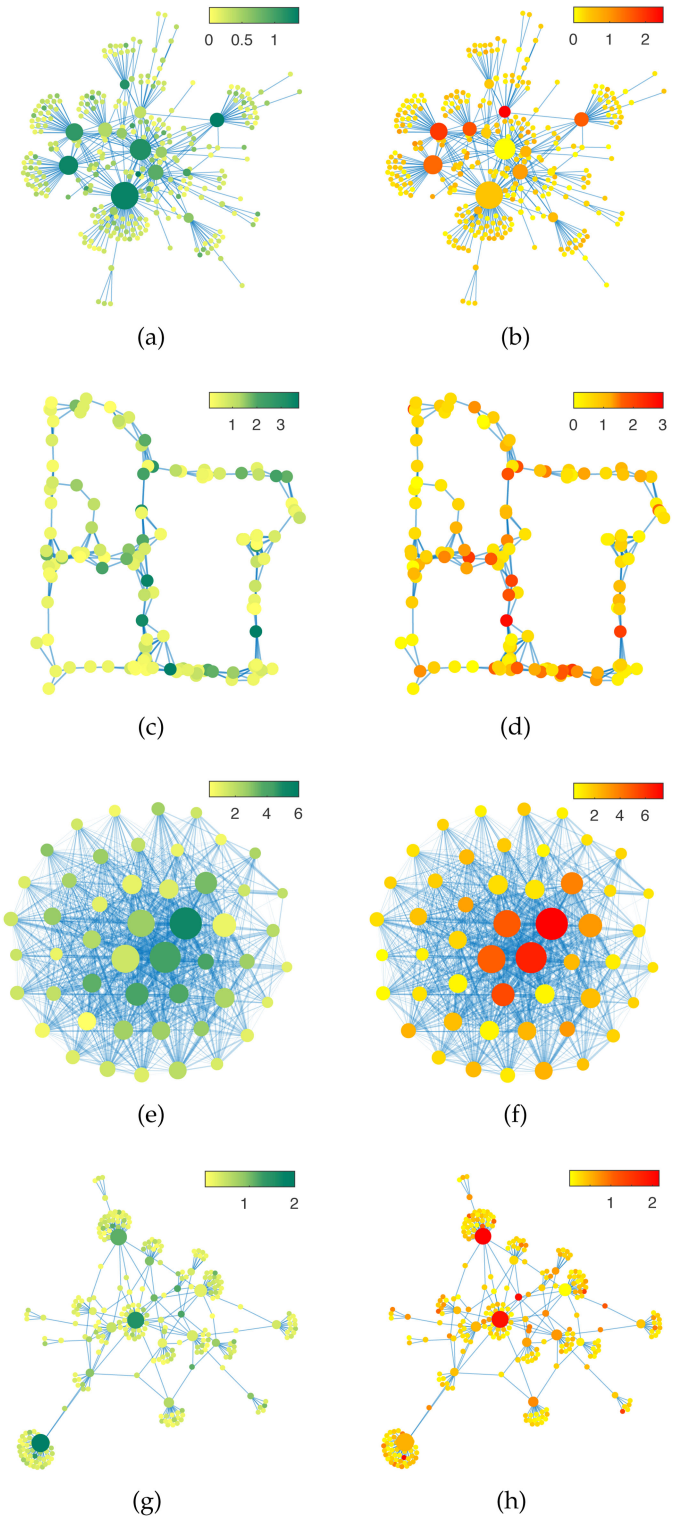


Fig. 7. Expected resource allocation of the defenders and attackers when $A_1 = A_2 = 100$. (The four subfigures on the left are for the defenders, and the right four are for the attackers. The shade of color represents the amount of resources allocated).

component, as well as on nodes with high centrality to make the whole network collapse. In fact, because there are a few nodes with large degree and there exist hierarchical structures, this network is vulnerable to targeted attacks.

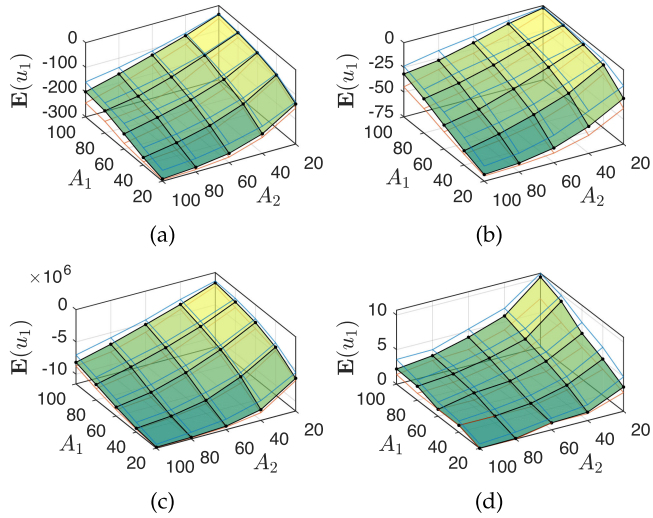


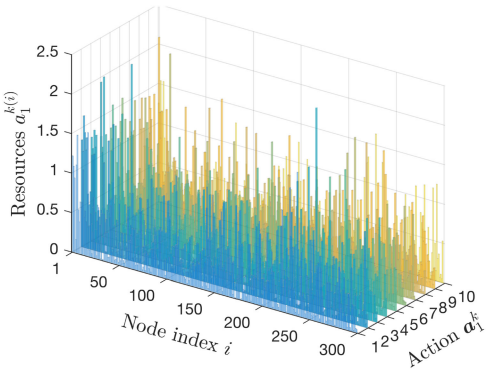
Fig. 8. Expected utility of the defender under different A_1 and A_2.

B. Communication Timeliness of Vehicular Networks

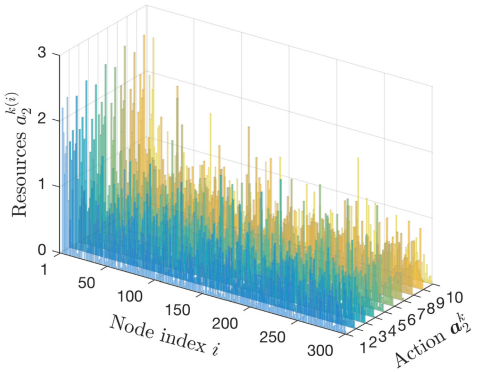
As an emerging paradigm of Internet of things, vehicular networks, or Internet of Vehicles (IoV) develop rapidly nowadays [39], [40]. Through vehicle-vehicle communications, vehicles can quickly share and gather geographic location and road information, so as to realize intelligent management of transportation system [41]. In vehicular ad hoc networks (VANETs), vehicles usually transmit information through multi-hop communications, and hence the timeliness is a key problem [42]. However, in open wireless communication environment, malicious attackers can interfere the communication of some vehicle devices through jamming. Hence, the schedulers of VANETs, which can be staff or softwares, can increase the transmission power and improve anti-interference capacity of these devices. In simulation, we assume that the maximum communication distance of vehicles is 250 meters and all nodes' self-defense capacity $a_0^i = 0.1$. The delay of communication links is represented by the weight of edges. Because malicious interference will cause serious decline of data rate, we assume that:

$$w_{ij} = \begin{cases} 1, & \text{if } \{v_i, v_j\} \in \mathbb{E}_{11}, \\ 10, & \text{if } \{v_i, v_j\} \in \mathbb{E}_{12} \cup \mathbb{E}_{22}, \end{cases} \tag{32}$$

which indicates that the delay of the succeed interfered devices will increase tenfold. As shown in Figs. 7(c) and 7(d), both players tend to allocate more resources on the nodes with high centrality. In particular, the gateway nodes, which are the nodes must be passed in numerous shortest paths, play an important role. This is mainly because when a regular node is controlled by the attacker, there still exist other short paths. However, if a gateway node is controlled, data transmission has only to suffer huge transmission delay by passing this interfered node or detouring to another street. Furthermore, increasing the density of vehicles or increasing vehicles' maximum communication distance will create more intensive links between vehicles, which is beneficial for improving the anti-interfere capacity and timeliness of communication.



(a) The defender's practical action set



(b) The attacker's practical action set

Fig. 9. The practical action sets of the defender and the attacker in the Internet security scenario when $A_1 = A_2 = 100$. (The nodes' indices are sorted by degree in descending order.)

C. Efficiency and Reliability of Transportation Systems

As another kind of network system, transportation systems play an important role in our daily life. Hence, it is critical to maintain its efficiency and reliability [43]. However, such systems are often obstructed by various social or natural effects, such as terrorist attacks, accidents, severe weather, etc. [44]. Therefore, managers have to maximize the system's risk prevention and response capacity under a limited budget, and maintain the operation of the system. Here we study the case of American air transportation network containing the top 50 busy airports, where weighted edges represent the number of available seats between two airports every year[1]. In this model, we assume that the attacker causes havoc with airline schedules of an airport by occupying the node. Hence the traffic of this airport drop to half of the original value, i.e.,

$$w''_{ij} = \begin{cases} w'_{ij}, & \text{if } \{v_i, v_j\} \in \mathbb{E}_{11}, \\ \dfrac{1}{2}\, w'_{ij}, & \text{if } \{v_i, v_j\} \in \mathbb{E}_{12} \cup \mathbb{E}_{22}, \end{cases} \tag{33}$$

where w'_{ij} represents the original edge's weight in $\boldsymbol{G}'$ and w'_{ij} is its weight in $\boldsymbol{G}''$. From the simulation results in Fig. 7(e) and Fig. 7(f), it can be found that both players tend to allocate more resources on the node with a high degree. Because this air network is dense, the results on is similar to the case of traditional Colonel Blotto games with weighted battlefields to a certain extent.

[1]Because the flights between airports are usually symmetric, air traffic is abstracted as an undirected edge in this paper.

D. Rumor Spread Control in Social Networks

Social networks, such as Facebook, Twitter and Weibo, are popular online network systems nowadays. These networks provide a public platform of daily communication and information sharing. However, the powerful transmission capability of these social networks also leads to the rapid and wide spread of rumors [45]. In this subsection, we analyze the rumor spreading in a small community of Sina Weibo, which is a popular online social network in China. Here the undirected edge in the network represents the relationship of "friends", i.e., "following each other", of two users. According to the characteristics of social networks, we use the betweenness centrality to denote the influence c_k of node v_k in transmission. Moreover, we set the threshold proportion $\beta = 0.8$ and node's self-defense capacity $a_0^i = 0.01 \cdot d_i$. According to Figs. 7(g) and 7(h), two players mainly focus on two kinds of nodes. One is the nodes with high influence. The other is the hub nodes connecting the small sub-communities, which also play critical roles in rumor spread. For the convenience of elaborating, we simply set $f(\boldsymbol{G}') = 0$ in Fig. 8 (d). Hence the social network of friends has strong transmission capacity, and it is difficult for the defender to suppress the emergence and spread of rumors unless he/she has much more resources than the attacker.

VI. Conclusions

In this paper, we modeled the attack-defence resource allocation as a networked zero-sum Colonel Blotto game. In contrast to the traditional Colonel Blotto game model, our proposed game broadens the application fields of the resource allocation game model. We proposed four kinds of network performance metrics based on network connectivity, average path length, average degree and transmission capacity, respectively. Furthermore, the co-evolution based algorithm is proposed for obtaining the Nash equilibrium strategies based on practical action sets improved the feasibility of strategies analysis. Sufficient simulations based on four real-world network systems proved the effectiveness of our proposed game.

References

[1] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.

[2] F. D. Sahneh, A. Vajdi, J. Melander, and C. Scoglio, "Contact adaption during epidemics: A multilayer network formulation approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 6, no. 1, pp. 16–30, Jan.–Mar. 2019.

[3] S. Dhamal, K. J. Prabuchandran, and Y. Narahari, "Information diffusion in social networks in two phases," *IEEE Trans. Netw. Sci. Eng.*, vol. 3, no. 4, pp. 197–210, Sep. 2016.

[4] J. Wang, C. Jiang, T. Q. S. Quek, and R. Yong, "The value strength aided information diffusion in online social networks," in *Proc. IEEE Global Conf. Signal Inf. Process.*, Washington, DC, USA, Dec. 2016, pp. 470–474.

[5] L. Wang, S. Ren, B. Korel, K. A. Kwiat, and E. Salerno, "Improving system reliability against rational attacks under given resources," *IEEE Trans. Syst., Man Cybern., Syst.*, vol. 44, no. 4, pp. 446–456, Apr. 2014.

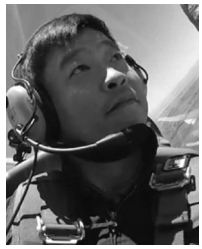
[6] C. Tekin, M. Liu, R. Southwell, J. Huang, and S. H. A. Ahmad, "Atomic congestion games on graphs and their applications in networking," *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1541–1552, Oct. 2012.
[7] L. Duan, J. Huang, and B. Shou, *Cognitive Virtual Network Operator Games*. New York, NY, USA: Springer, 2013.
[8] H. Zhu, D. Niyato, W. Saad, T. Başar, and A. Hjrungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge, U.K: Cambridge Univ. Press, 2012.
[9] E. Borel, "The theory of play and integral equations with skew symmetric kernels," *Econometrica: J. Econometric Soc.*, vol. 21, no. 1, pp. 97–100, Jan. 1953.
[10] O. Gross and R. Wagner, "A continuous Colonel Blotto game," Tech. Rep. no. RM-408, Rand Project Air Force, Santa Monica, CA, USA, Jun. 1950.
[11] B. Roberson, "The Colonel Blotto game," *Econ. Theory*, vol. 29, no. 1, pp. 1–24, Jan. 2006.
[12] M. Shubik and R. J. Weber, "Systems defense games: Colonel Blotto, command and control," *Naval Res. Logistics*, vol. 28, no. 2, pp. 281–287, Jun. 1981.
[13] J. Merolla, M. C. Munger, and M. Tofias, "Lotto, Blotto or frontrunner: An analysis of spending patterns by the national party committees in the 2000 presidential election," in *Proc. Annu. Meet. Midwest Political Sci. Assoc.*, Chicago, IL, USA, Apr. 2003, pp. 1–29.
[14] P. Kohli, M. Kearns, Y. Bachrach, R. Herbrich, D. Stillwell, and T. Graepel, "Colonel Blotto on facebook: The effect of social relations on strategic interaction," in *Proc. 4th Annu. ACM Web Sci. Conf.*, Evanston, IL, USA, Jun. 2012, pp. 141–150.
[15] M. Labib, S. Ha, W. Saad, and J. H. Reed, "A Colonel Blotto game for anti-jamming in the Internet of things," in *Proc. IEEE Global Commun. Conf.*, San Diego, CA, USA, Dec. 2015, pp. 1–6.
[16] A. Ferdowsi, W. Saad, B. Maham, and N. B. Mandayam, "A Colonel Blotto game for interdependence-aware cyber-physical systems security in smart cities," in *Proc. 2nd ACM Int. Workshop Sci. Smart City Operations Platforms Eng.*, Pittsburgh, PA, USA, Apr. 2017, pp. 7–12.
[17] R. Golman and S. E. Page, "General Blotto: Games of allocative strategic mismatch," *Public Choice*, vol. 138, nos. 3/4, pp. 279–299, Mar. 2009.
[18] G. Schwartz, P. Loiseau, and S. S. Sastry, "The heterogeneous Colonel Blotto game," in *Proc. 7th IEEE Int. Conf. Netw. Games, Control Optim.*, Trento, Italy, Oct. 2014, pp. 232–238.
[19] K. Modzelewski, J. Stein, and J. Yu, "An experimental study of classic Colonel Blotto games," Tech. Rep., Massachusetts Institute of Technology, Cambridge, MA, USA, Dec. 2009.
[20] S. M. Chowdhury, D. Kovenock, and R. M. Sheremeta, "An experimental investigation of Colonel Blotto games," *Econ. Theory*, vol. 52, no. 3, pp. 1–29, Apr. 2013.
[21] A. Arad and A. Rubinstein, "Multi-dimensional iterative reasoning in action: The case of the Colonel Blotto game," *J. Econ. Behav. Org.*, vol. 84, no. 2, pp. 571–585, Sep. 2012.
[22] Z. E. Fuchs and P. P. Khargonekar, "A sequential Colonel Blotto game with a sensor network," in *Proc. IEEE Amer. Control Conf.*, Montréal, Canada, Jun. 2012, pp. 1851–1857.
[23] M. Hajimirsadeghi, G. Sridharan, W. Saad, and N. B. Mandayam, "Inter-network dynamic spectrum allocation via a Colonel Blotto game," in *Proc. Annu. IEEE Conf. Inf. Sci. Syst.*, Princeton, NJ, USA, Mar. 2016, pp. 252–257.
[24] A. Ferdowsi, A. Sanjab, W. Saad, and T. Başar, "Generalized Colonel Blotto game," *Annu. Amer. Control Conf.*, pp. 5744–5749. Jun. 2018.
[25] Y. Wu, B. Wang, and K. R. Liu, "Optimal power allocation strategy against jamming attacks using the Colonel Blotto game," in *Proc. IEEE Global Telecommun. Conf.*, Honolulu, HI, Dec. 2009, pp. 1–5.
[26] M. Newman, *Networks: An Introduction*. Oxford, U.K.: Oxford Univ. Press, 2010.
[27] S. Han, V. M. Preciado, C. Nowzari, and G. J. Pappas, "Data-driven network resource allocation for controlling spreading processes," *IEEE Trans. Netw. Sci. Eng.*, vol. 2, no. 4, pp. 127–138, Nov. 2015.
[28] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA, USA: MIT Press, 1991.
[29] P. Dasgupta and E. Maskin, "The existence of equilibrium in discontinuous economic games, II: Applications," *Rev. Econ. Stud.*, vol. 53, no. 1, pp. 1–26, Jan. 1986.
[30] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA, USA: MIT Press, 1994.
[31] M. J. Todd, "The many facets of linear programming," *Math. Program.*, vol. 91, no. 3, pp. 417–436, Feb. 2002.
[32] D. E. Goldberg, *Genetic Algorithms in Search, Optimization and Machine Learning*. Reading, MA, USA: Addison-Wesley, 1989.
[33] D. Whitley, "A genetic algorithm tutorial," *Statist. Comput.*, vol. 4, no. 2, pp. 65–85, Jun. 1994.
[34] M. Newman, "Mark Newman's network data collection," 2006, [Online]. Available: http://www-personal.umich.edu/ mejn/netdata/.
[35] J. Yuan, Y. Zheng, X. Xie, and G. Sun, "T–Drive: Enhancing driving directions with taxi drivers' intelligence," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 1, pp. 220–232, Jan. 2013.
[36] "Cx-Nets: the Complex Networks Collaboratorys website," 2009, [Online]. Available: https://sites.google.com/site/cxnets/usairtransportationnetwork.
[37] V. Colizza, R. Pastor-Satorras, and A. Vespignani, "Reaction–diffusion processes and metapopulation models in heterogeneous networks," *Nature Phys.*, vol. 3, no. 4, pp. 276–282, Mar. 2007.
[38] M. Lichman, "UCI machine learning repository," 2013, [Online]. Available: http://archive.ics.uci.edu/ml.
[39] J. Wang, C. Jiang, Z. Han, Y. Ren, and L. Hanzo, "Internet of vehicles: Sensing aided transportation information collection and diffusion," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 3813–3825, May 2018.
[40] S. A. A. G. Ghahramani, A. M. A. Hemmatyar, and K. Kavousi, "A network model for vehicular ad hoc networks: An introduction to obligatory attachment rule," *IEEE Trans. Netw. Sci. Eng.*, vol. 3, no. 2, pp. 82–94, May 2016.
[41] H. C. Man, F. Hou, V. W. S. Wong, and J. Huang, "Dynamic optimal random access for vehicle-to-roadside communications," in *Proc. IEEE Int. Conf. Commun.*, Kyoto, Japan, Jun. 2011, pp. 1–6.
[42] J. Wang, C. Jiang, G. Longxiang, Y. Shui, H. Zhu, and R. Yong, "Complex network theoretical analysis on information dissemination over vehicular networks," in *Proc. IEEE Int. Conf. Commun.*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
[43] R. Guimera, S. Mossa, A. Turtschi, and L. N. Amaral, "The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles," *Proc. Nat. Acad. Sci.*, vol. 102, no. 22, pp. 7794–7799, May 2005.
[44] Y. Zhou, et al."Multivariate probabilistic collocation method for effective uncertainty evaluation with application to air traffic flow management," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 10, pp. 1347–1363, Oct. 2014.
[45] K. Zhang, J. Wang, C. Jiang, Z. Wei, and R. Yong, "Big data driven information diffusion analysis and control in online social networks," in *Proc. IEEE Int. Conf. Commun.*, Paris, France, May 2017, pp. 1–6.

Sanghai Guan received the B.Eng. degree in electronic engineering from Dalian University of Technology, Dalian, Liaoning, China, in 2017, with the honor of excellent graduate of Liaoning Province. He is currently working toward the M.S. degree in information and electronic engineering with Tsinghua University, Beijing, China. His research interests include complex networks and systems, multiagent networked systems, and network association.

Jingjing Wang (S'14) received the B.S. degree in electronic information engineering from Dalian University of Technology, Dalian, Liaoning, China, in 2014 with the highest honor. He is currently working toward the Ph.D. degree with the Department of Electronic Engineering, Tsinghua University, Beijing, China. From 2017 to 2018, he has been a joint Ph.D. student with the Next Generation Wireless Group chaired by Prof. L. Hanzo, University of Southampton, U.K. His research interests include the resource allocation and network association, learning theory aided modeling, analysis and signal processing, as well as information diffusion theory for mobile wireless networks. He received China Postgraduate National Scholarship Award in 2017, and Best Journal Paper Award of IEEE Technical Committee on Green Communications and Computing in 2018.

Haipeng Yao (M'16) received the Ph.D. degree from the Department of Telecommunication Engineering, University of Beijing University of Posts and Telecommunications, Beijing, China, in 2011. He is an Associate Professor with Beijing University of Posts and Telecommunications. He has been engaged in research on future internet architecture, network AI, big data, cognitive radio networks, and optimization of protocols and architectures for broadband wireless networks. He has published more than 80 papers in prestigious peer-reviewed journals and conferences.

Chunxiao Jiang (S'09–M'13–SM'15) received the B.S. degree in information engineering from Beijing University of Aeronautics and Astronautics (Beihang University), Beijing, China, in 2008 and the Ph.D. degree from Tsinghua University, Beijing, China, in 2013, both with the highest honors. During 2011–2012, he visited the Signals and Information Group, Department of Electrical and Computer Engineering, University of Maryland. During 2013–2016, he was a Postdoc Researcher with the Department of Electronic Engineering, Tsinghua University. He is currently an Assistant Research Fellow with Tsinghua Space Center. His research interests include the applications of game theory and queuing theory in wireless communication and networking. He received Best Paper Award from IEEE GLOBECOM in 2013, Best Student Paper Award from IEEE GlobalSIP in 2015, Tsinghua Outstanding Postdoc Award in 2015, Beijing Distinguished Graduated Student Award, Chinese National Fellowship, and Tsinghua Outstanding Distinguished Doctoral Dissertation in 2013.



Zhu Han (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, MD, USA, in 1999 and 2003, respectively. From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, Boise, ID, USA. Currently, he is a Professor with the Department of Electrical and Computer Engineering as well as in the Department of Computer Science, University of Houston, Houston, TX, USA. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. He received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, IEEE Leonard G. Abraham Prize in the field of Communications Systems (best paper award in IEEE JSAC) in 2016, and several best paper awards in IEEE conferences. He is currently an IEEE Communications Society Distinguished Lecturer.

Yong Ren (SM'16) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Harbin Institute of Technology, Harbin, China, in 1984, 1987, and 1994, respectively. He was a Postdoctoral Researcher wit the Department of Electronics Engineering, Tsinghua University, Beijing, China, from 1995 to 1997. He is currently a Professor with the Department of Electronics Engineering and the Director of the Complex Engineered Systems Lab, Tsinghua University. He holds 12 patents, and has authored or coauthored more than 100 technical papers in the behavior of computer network, P2P network, and cognitive networks. His current research interests include complex systems theory and its applications to the optimization and information sharing of the Internet, Internet of Things and ubiquitous network, cognitive networks, and cyber-physical systems. He has serves as a Reviewer of *IEICE Transactions on Communications*, *Digital Signal Processing*, *Chinese Physics Letters*, *Chinese Journal of Electronics*, *Chinese Journal of Computer Science and Technology*, *Chinese Journal of Aeronautics*, and so on.