Advances in Computer Science Research, volume 80
International Conference on Computer Science, Electronics and Communication Engineering (CSECE 2018)

Modeling Confrontations in Complex Networks Based on Game Theory

Yapeng Li[1] and Jun Wu[1,*]
[1]College of Systems Engineering, National University of Defense Technology, Changsha, Hunan 410073, China
*Corresponding author

***Abstract*—To fully understand the structure robustness of complex networks where confrontations of attackers and defenders happen, we build a game model which is a zero-sum game in simultaneous form. We assume that the attack and defense are only against the top-n vital nodes and evaluate the payoffs using the full information of the network. A mapping process is introduced which maps the probabilities of pure strategies onto nodes. The experimental results in random scale-free networks reveals that the attacker pay more emphasis on attacking the nodes with relatively small degrees while the defender allocates more resource to nodes which play a more important role in maintaining the connectivity of the network.**

Keywords—complex networks; game theory; nash equilibriums; scale-free networks

I. INTRODUCTION

Complex networks describe a myriad of systems in real-world, such as the Internet, electric power grids, urban road networks, the world trade web, among many others. In the last decades, a great deal of interest in studying complex networks has been stimulated since the discovery of small-world [1] and scale-free [2]. As we know, the structures of networked systems have a significant influence on their functions and behaviors, making the structural robustness, as one of the critical structural features, become a central topic in complex networks and receive growing attention. [3-5]

To enhance the structural robustness of a networked system, many studies have proposed a wide range of methods, i.e., designing robust networks [6, 7] and optimizing the existing networks [8-10]. Besides, many studies investigate the attack or defense strategies in existing networks. These researches measure the structural robustness of a network by some explicit measure functions and investigate how these measure functions will change when a set of nodes are removed. The original work is done by Albert et al, where they introduced two typical strategies, i.e., random failure and intentional attack, and suggested that scale-free networks are robust against random failure but very fragile against intentional attack. [11] This "robust yet fragile" feature of scale-free networks leads to a lot of interests in finding the optimal attack or defense strategies.[12,13] However, most of these studies have an implicit assumption that there exists only one decision maker, either the attacker or the defender, and this process is static. So, these problems are actually identifying vital nodes. [14] But in many real-world scenarios, the activities of attack and defense probably occur simultaneously in many confrontations of networked systems such as transportation networks. The attacker or the defender can predict the other's probable actions and make his/her best decisions. In this dynamic case where the attacker considers the probable defense strategy when plotting an attack, and vice versa, attacking or defending the vital nodes may no longer be the best choice for them.

To investigate the behaviors of attackers and defenders in confrontations of complex networks, we will build a game model in this paper, using the framework and methods of game theory which provides useful mathematical tools to model conflicts between intelligent decision-makers.

II. THE GAME MODEL

Firstly, we make some basic assumptions of the game. We only consider one attacker and one defender in our game model, which are the players. Besides, it's assumed that both players can obtain the complete information of the network and they fully understand the other's preference and possible strategies. So, they are perfectly informed of the opponent's payoff for all possible strategy profiles. We also assume that this game is a simultaneous-move game, which means they don't know each other's decisions before they move.

III. BUDGET CONSTRAINTS AND STRATEGIES

We consider a complex network described by a simple undirected graph $G(V,E)$, where V is the set of nodes and $E \subseteq V \times V$ is the set of edges. Let $N = |V|$ be the number of nodes. Denote $A(G) = (a_{ij})_{N \times N}$ as the adjacency matrix of G, where $a_{ij} = a_{ji} = 1$ if nodes v_i and v_j are adjacent, and $a_{ij} = a_{ji} = 0$ otherwise. Let k_i be the degree of node v_i, which is the number of edges connected to it. In real-world networks, the costs of attacking different targets for the attacker as well as the defender are different. In this game, the attack and defense approaches are both against nodes and it's assumed that the attached edges are removed if one node is removed. Thus, we assume that the cost c_i^A or c_i^D of node v_i is a function of its degree k_i with the following forms:

$$c_i^A = k_i^{\alpha_A},\ c_i^D = k_i^{\alpha_D} \tag{1}$$

In eq. 1, $\alpha_A \geq 0$ is called the attack-cost-sensitivity and $\alpha_D \geq 0$ is the defense-cost-sensitivity. A larger α_A means the attacker is more sensitive to the costs among different nodes. In the extreme case where $\alpha_A = 0$, the attack costs of all targets are equal. The parameter α_D has similar meaning for the defender. As we know, many real-world networks are heterogeneous, which means there are a few hub nodes which play a significant role in maintaining the connectivity of the network. These nodes are called vital nodes where both the attacker and the defender pay a lot of attention because the removal of these nodes can collapse the network. There are many methods to identify vital nodes in complex networks [14]. But in this paper, what we focus is not the methods about vital nodes identification but exploring what the attacker and the defender will do when they consider the opponent's probable action. So, we assume that both the attacker and the defender only consider the attack or defense toward top-n hub nodes with the largest degrees. In the extreme case that $n = N$, all the nodes are considered. Although only n hub targets are considered, the costs of different targets and the connectivity should be measured in the whole network. So, we sort the nodes in descending order of their degree and the budgets of the two players which are often limited are defined as

$$\hat{C}^A = \beta_A \sum_{i=1}^{n} c_i^A = \beta_A \sum_{i=1}^{n} k_i^{\alpha_A} \tag{2}$$

And

$$\hat{C}^D = \beta_D \sum_{i=1}^{n} c_i^D = \beta_D \sum_{i=1}^{n} k_i^{\alpha_D}, \tag{3}$$

Where $\beta_A \in [0,1]$ and $\beta_D \in [0,1]$ are the cost-constraint parameter of the attacker and the defender, respectively. Denote by $V^A \subseteq V$ the attack set. We define an attack strategy as $X = [x_1, x_2, ..., x_n]$, where $x_i = 1$ if $v_i \in V^A$, otherwise $x_i = 0$. Let $C_X = \sum_{v_i \in V^A} c_i^A$ be the total cost of an attack strategy X. So,

$$C_X = \sum_{v_i \in V^A} c_i^A = \sum_{i=1}^{n} x_i c_i^A = \sum_{i=1}^{n} x_i k_i^{\alpha_A} \tag{4}$$

To satisfy the budget constraint of the attacker, we have

$$C_X = \sum_{i=1}^{n} x_i k_i^{\alpha_A} \leq \hat{C}^A = \beta_A \sum_{i=1}^{N} k_i^{\alpha_A}. \tag{5}$$

Any solution X that satisfies Eq. 5 is a feasible attack strategy. But it is easy to know that the attacker will get higher payoff when he/she attacks more nodes. So, we only consider the attack strategies where the addition of any nodes into the attack set violates the budget constraint. Similarly, defense set V^D, defense budget $\hat{C}^D$ and defense strategy $Y = [y_1, y_2, ..., y_n]$ are defined in the same way. We now use a simple example to illustrate the attack and defense strategies of the game model. If $n = 4$, $\alpha_A = \alpha_D = 0$ and $\beta_A = \beta_D = 0.5$, which means the costs of each target are equal for both players, there are 6 attack strategies totally which are $x_1 = \{v_1, v_2\}$, $x_2 = \{v_1, v_3\}$, $x_3 = \{v_1, v_4\}$, $x_4 = \{v_2, v_3\}$, $x_5 = \{v_2, v_4\}$, $x_6 = \{v_3, v_4\}$ and the defense strategies are the same.

IV. Definition of Payoffs

In the confrontations of the attacker and the defender, we assume that the attacker successfully attacks a node v_i if it is attacked but not defended, namely, $x_i = 1$ and $y_i = 0$. Denote by Γ the measure function of network performance which decreases monotonically when a set of nodes are removed. The common measure functions include the size of largest connected component, the efficiency and so on. Denote by $\hat{G}$ the network when a set of nodes are removed from the initial network G, the payoff functions of the attacker are defined as

$$U^A(X,Y) = \frac{\Gamma(G) - \Gamma(\hat{G})}{\Gamma(G)} \in [0,1], \tag{6}$$

And the payoff of the defender is

$$U^D(X,Y) = \frac{\Gamma(\hat{G}) - \Gamma(G)}{\Gamma(G)} \in [-1,0]. \tag{7}$$

attacker \ defender	Y_1	Y_2	···	Y_t
X_1	$u_{11}, -u_{11}$	$u_{12}, -u_{12}$	···	$u_{1t}, -u_{1t}$
X_2	$u_{21}, -u_{21}$	$u_{22}, -u_{22}$	···	$u_{2t}, -u_{2t}$
⋮	⋮	⋮	···	⋮
X_s	$u_{s1}, -u_{s1}$	$u_{s2}, -u_{s2}$	···	$u_{st}, -u_{st}$

FIGURE I. PAYOFF MATRIX OF THE ATTACKER-DEFENDER GAME IN ALL STRATEGY PROFILES WHERE THE ATTACKER HAS s POSSIBLE ATTACK STRATEGIES TOTALLY AND THE DEFENDER HAS t DEFENSE STRATEGIES IN ALL

Noting that $U^A(X,Y)+U^D(X,Y)=0$, our game is a zero-sum game. The payoff matrix under all strategy profiles is showed in Fig. 1 where the row player is the attacker and the column is the defender. Nash equilibrium is calculated using the following linear programming.

$$\begin{aligned} &min \quad z \\ &s.t. \quad \sum_{j\in S_D} u_{ij}\cdot y_j \le z \qquad \forall i \in S_A \\ &\quad \sum_{j\in S_D} y_j = 1 \\ &\quad y_j \ge 0 \qquad \forall j \in S_D \\ &\quad S_D = \{Y_1, Y_2, ..., Y_t\} \end{aligned} \tag{8}$$

$$\begin{aligned} &max \quad z \\ &s.t. \quad \sum_{i\in S_A} u_{ij}\cdot x_i \ge z \qquad \forall j \in S_D \\ &\quad \sum_{i\in S_A} x_i = 1 \\ &\quad x_i \ge 0 \qquad \forall i \in S_A \\ &\quad S_A = \{X_1, X_2, ..., X_s\} \end{aligned} \tag{9}$$

Nash equilibrium (x^*, y^*) is obtained and the equilibrium payoff of the attacker is $z = x^{*T}\cdot U\cdot y^*$.

Denote the probabilities of each pure attack strategy in Nash equilibrium by $P_S^A = \left[p_1^A, p_2^A, ...p_s^A\right]$ and that of each pure defense strategy by $P_S^D = \left[p_1^D, p_2^D, ...p_t^D\right]$. Then, we use a mapping mechanism to distribute the probabilities toward each node, which shows the probabilities of attacking or defending each node. The probabilities toward each node is obtained by

$$P_N^A = \sum_{i=1}^{s} p_i^A \cdot X_i, P_N^D = \sum_{i=1}^{t} p_i^D \cdot Y_i \ . \tag{10}$$

According to this probability distributions, the attacker and defender can determine the proportion of their resource toward the top-n nodes. For example, if $X_1 = [1\ 1\ 0]$, $X_2 = [1\ 0\ 1]$, $X_3 = [0\ 1\ 1]$, $P_S^A = \left[0.5,\ 0.3,\ 0.2\right]$, $P_S^D = \left[0.2,\ 0.3,\ 0.5\right]$, so, $P_N^A = [0.8,\ 0.7,\ 0.5]$ and $P_N^A = [0.5,\ 0.7,\ 0.8]$.

V. EXPERIMENTAL RESULTS

Because of the ubiquity of scale-free networks in most natural and man-made systems, we execute the experiments in random scale-free networks whose degree distributions follow $P(k):\ k^{-\lambda}$. In this paper, we use the efficiency as measure function Γ and set that $\alpha_A = \alpha_D \equiv 0$ and $\beta_A = \beta_D \equiv \beta$. In this case, the size of the attack set V^A and V^D are both equal to $n\cdot\beta$. For the convenience of calculation and analysis, we set $n = 10$. We use the configuration model[15] to get the random scale-free network and the computations of Nash equilibriums are done in MATLAB R2015b using CPLEX 12.5.

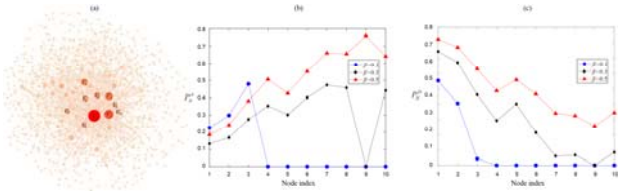

FIGURE II. TOPOLOGY STRUCTURE OF A RANDOM SCALE-FREE NETWORK (A) AND THE PROBABILITIES TOWARD EACH NODE IN EQUILIBRIUMS FOR THE ATTACKER (B) AND THE DEFENDER (C). THE DEGREE DISTRIBUTION FOLLOWS $p(k) = (\lambda-1)m^{\lambda-1}k^{-\lambda}$, WHERE $N = 1000$, $\lambda = 3$ AND $m = 2$. THE NODE INDEX OF (B) AND (C) ARE IN THE DESCENDING ORDER OF THEIR DEGREES AND THESE 10 NODES ARE SHOWED IN (A)

We play the game in a random scale-free network and map the mixed strategy of pure strategies onto the nodes. The results are showed in Fig. 2 which shows the topology structure of the network and probabilities toward each node of the attacker and defender. It's easy to see that both the attacker and the defender allocate all probabilities onto only 3 nodes with the largest degree when $\beta = 0.1$. When β is larger, the probabilities are mixed in all the top-10 nodes. Moreover, the attacker pays more attention to the nodes with relatively small degrees while the defender allocates larger probabilities onto the nodes with largest degrees regardless of β. This result means that the attacker is less concentrated on attacking the most important nodes with largest degrees while the defender allocates more resource to these nodes. It can be understood by the interactive

process of the two players, where the defender can't afford the loss of abandoning the vital nodes and thus the attacker attacks the nodes with relatively lower importance to dodge the defense. We also do the experiments in other scale-free networks with different degree exponent and average degree and get similar results.

VI. SUMMARY

The study of structural robustness of complex networks is a hot topic in the past decades. However, most researches neglect the confrontations in complex networks where the attacker and defender exist simultaneously. To model this situation and explore the behaviors of them in equilibriums, we first proposed a two-player game model and define the strategies and payoffs. Because the attacker and defender in real-world always focus vital nodes, we assumed that the attack and defense are only against the top-n vital nodes while the payoffs are evaluated through the whole network. We then introduced the mapping mechanism which mapped the mixed strategy of pure strategies onto the nodes. The experimental results in random scale-free networks revealed that the attacker was less concentrated on attacking the most important nodes with the largest degrees while the defender allocated more resource to these nodes.

ACKNOWLEDGEMENT

This research was financially supported by the National Science Foundation of China under Grant No. 71371185 and the Program for New Century Excellent Talents in University under Grant No. NCET-12-0141.

REFERENCES

[1] Watts D J, Strogatz S H. Collective dynamics of 'small-world' networks, Nature, 393(1998): 440.

[2] Barabási A, Albert R. Emergence of Scaling in Random Networks, Science, 286(1999): 509.

[3] Jun Wu, S-Y T, Zhong Liu, Yue-Jin Tan, Xin Lu. Enhancing structural robustness of scale-free networks by information disturbance, Sci. Rep., 7(2017).

[4] Carlson J, Doyle J, Complexity and robustness, Proc. Natl. Acad. Sci. USA, 99(2002): 2538-45.

[5] Gao J, Barzel B, Barabási A L. Universal resilience patterns in complex networks, Nature, 530(2016): 307-12.

[6] Valente A X C N, Sarkar A, Stone H A. Two-peak and three-peak optimal complex networks, Phys. Rev. Lett. 92(2004): 118702.

[7] Peng G-S, Tan S-Y, Wu J, et al. Trade-offs between robustness and small-world effect in complex networks, Sci. Rep., 6(2016)

[8] Hayashi Y, Matsukubo J. Improvement of the robustness on geographical networks by adding shortcuts, Physica A, 380(2007): 552-62.

[9] Li Y, Wu J, Zou A Q. Effect of Eliminating Edges on Robustness of Scale-Free Networks under Intentional Attack, Chin. Phys. Lett., 27(2010): 068901.

[10] Ash J, Newth D. Optimizing complex networks for resilience against cascading failure, Physica A, 380(2007)673-83.

[11] Albert R, Jeong H, Barabási A L. Error and attack tolerance of complex networks, Nature, 406(2000): 378-82.

[12] Deng Y, Wu J, Tan Y J. Optimal attack strategy of complex networks based on tabu search, Physica A, 442(2016): 74-81.

[13] Tan S Y, Wu J, Lü L, et al. Efficient network disintegration under incomplete information: the comic effect of link prediction, Sci. Rep., 6(2016)22916

[14] Lü L Y, Chen D, Ren X-L, et al. Vital nodes identification in complex networks, Phys. Rep., 650(2016)1-63.

[15] Newman M E J. The structure and function of complex networks, SIAM Rev., 45(2003): 167-256.