The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 5 (2019) 163–166

www.elsevier.com/locate/icte

Robustness enhancement of complex networks via No-Regret learning

Insoo Sohn

Division of Electronics & Electrical Engineering, Dongguk University, Seoul, Republic of Korea

Received 14 September 2018; accepted 5 October 2018
Available online 11 October 2018

Abstract

Optimizing complex networks to be resilient against various attack models has been an important problem that is actively studied in the academia. In the proposed optimization method, individual node degrees are balanced iteratively based on the No-Regret learning algorithm, resulting in a robust network topology with increased resilience against outside attacks. Through simulation results, we show that the proposed robustness enhanced networks perform well under targeted attacks compared to the conventional optimized networks.

Keywords: Complex networks; Network robustness; No-Regret learning

1. Introduction

One of the popular and important complex networks that have been applied to solve problems in areas such as brain networks, social networks, and wireless networks is the scale-free network (SFN) [1–3]. One of the main advantages of SFN is that it can withstand random attacks compared to other complex networks [4,5]. However, SFN's robustness performance deteriorates with continued targeted attacks [6,7]. There have been many increased research efforts lately, to optimize the SFN topology based on various optimization techniques to solve this important problem. However, many of the techniques that have been proposed are heuristic in nature with high complexity. In this paper, we propose a novel method based on No-Regret learning algorithm to design an optimized robust network. No-Regret algorithm is a powerful tool that adjusts a set of actions based on a strategy set using past patterns of payoff [8–10]. The reason for wide usage of No-Regret algorithm is that it guarantees correlated equilibrium solution in problems that been formulated as a strategic game.

E-mail address: isohn@dongguk.edu.
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

2. Problem formulation

2.1. Robustness metric

Among various metrics used to analyze the robustness of a network with random and intentional attack model, we utilize the R metric proposed by Schenider et al. [11]. In random attack models, the nodes in the network are randomly selected and removed with all the attached links. As for the intentional attack model, the most important nodes with highest number of links or node degree are continuously selected and removed. The R metric is expressed as

$$R = \frac{1}{N} \sum_{q=1/N}^{1} s(q), \tag{1}$$

where N is the total number of nodes in the network, $s(q)$ is the size of the largest cluster, and $q = 1/N \ldots N/N$ is the fraction of the nodes that have been removed. To evaluate the robustness of a network, the R metric adds the number of nodes in the largest cluster for every q fraction of nodes removed and normalizes the result by dividing the sum by N, initial number of nodes in the network. The maximum value that the robustness value R can achieve is 0.5. The reason is that the

https://doi.org/10.1016/j.icte.2018.10.001
2405-9595/

best robust network is the lattice network, where all the nodes are connected to every other nodes, and the robustness metric of the lattice network is calculated as shown below:

$$\begin{aligned} R &= ((N-1)/N + (N-2)/N + \cdots + (N-N)/N)/N, \\ &= ((N-1) + (N-2) + \cdots + (N-N))/N^2, \\ &= (N(N+1)/2)/N^2 = 0.5 + \frac{1}{2N} \approx 0.5 \quad \text{for large } N \end{aligned}$$

2.2. Degree based network optimization

To represent a network topology, the commonly used method is to use the adjacency matrix that contains 0s and 1s, where 1 in row i and column j indicates the existence of a link between node pairs (i, j). Thus, one can easily propose to find an optimum robust network by searching through all possible network topologies with corresponding adjacency matrices and select the network with maximum R. However, this is an impossible task that requires a search process with 2^{N^2} complexity. For example, to find an optimum robust network with $N = 5$, $2^{25} = 33,554,432$ adjacency matrices need to be created and the corresponding R values need to be calculated. Therefore, in this paper, we use node degree information, instead of node and link combinations to represent a network topology as proposed in [12]. Compared to searching through 2^{N^2} adjacency matrices to find an adjacency matrix with maximum R, we only need to search through D^N number of degree information vectors (DIVs). For example, if node degree $D = 3$ and number of nodes $N = 5$, $D^N = 3^5 = 243$ *DIV*s are used to find the network with maximum R. However, to calculate R, we need to obtain actual node and link interaction information, usually represented via adjacency matrix. So the question is, will different networks with same *DIV*s have similar robustness performance. The answer to that question is yes. For example, let us assume that we have multiple networks with $N = 5$, and $DIV = [3\ 3\ 2\ 4\ 2]$, where nodes 1, 2, 3, 4, 5 have degrees 3, 3, 2, 4, 2, respectively. There are 2 possible network topologies with $DIV = [3\ 3\ 2\ 4\ 2]$. The adjacency matrices with $DIV = [3\ 3\ 2\ 4\ 2]$ are shown below and all of the networks have $R = 0.320$.

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Therefore, we can conclude that using *DIV* to represent and find an optimum network is indeed an efficient method. We now have a low complexity optimization method based on *DIV* to find robust networks that are more efficient compared to searching through all possible combinations of adjacency matrices. In Fig. 1, robustness performance R for all possible degree information combination is illustrated for $N = 5$. For networks with $N = 5$, there are $D^N = 4^5 = 1664$ possible *DIVs* and there are 1024 valid network topologies within 1664 *DIVs*. As shown in the figure, The R values vary between 0.1 and 0.4. As one might have expected, the networks with large R have large number of links or have nodes with maximum degree $N - 1$ with $DIV = [4\ 4\ 4\ 4\ 4]$. The brute force method that searches amongst all possible DIVs is still quite inefficient for large networks.

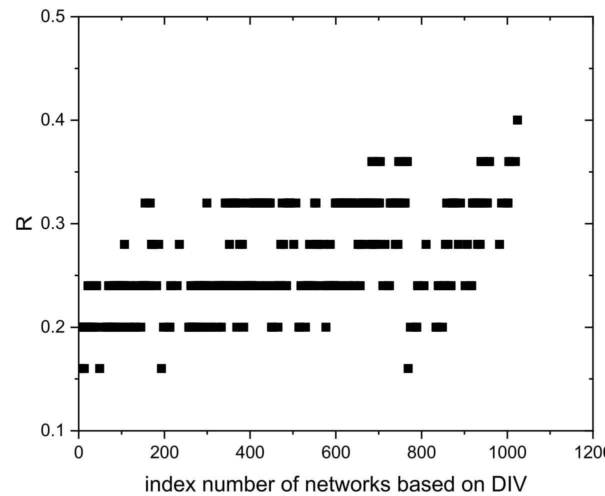

Fig. 1. Robustness performance with $N = 5$.

3. Proposed method

3.1. No-Regret learning

No-Regret learning algorithm is a powerful tool for solving multiagent decision problems or multiplayer repeated games. In a multiplayer repeated game problem, a player is presented with a set of actions or strategies and must choose an action to maximize his or her payoff. The outcome or payoff due to the selection of an action is jointly determined by other players' action. The player plays the game repeatedly and by observing the past pattern of payoffs, the player adjusts the strategy. In a No-Regret learning algorithm, the player evaluates the average regret from not having selected a different set of strategies, and then strategy selection process is adjusted to achieve zero regret. To find an optimum network topology with maximum robustness, we formulate node degree selection problem as a strategic game as follows:

$$\Gamma = \left\langle K,\ \{S_k\}_{k \in K},\ \{u_k\}_{k \in K} \right\rangle, \tag{2}$$

where the components of the strategic game are given as shown below:

1. *set of players:* K corresponds to N nodes in the network,
2. *set of strategies:* S_k is the set of strategies that the player k can select and corresponds to $0 \sim N-1$ possible degree or number of links to other nodes
3. *utility function:* u_k is the utility function defined as

$$u_k(s_k,\ s_{-k}) = R(s_k,\ s_{-k}) - \alpha\, L(s_k,\ s_{-k}), \tag{3}$$

where s_{-k} is the joint strategy of other players, R is the robustness metric defined in (1), L is the total number of links in the network, and α is the weight factor that balances the robustness gain and the link cost.