Towards the design of complex evolving networks with high robustness and resilience

Zhenghui Sha and Jitesh H. Panchal

School of Mechanical Engineering, Purdue University, West Lafayette, IN 47907 USA

Abstract

Network design and optimization research has traditionally been focused on networks where the designers have direct control over the nodes and their connectivity. However, there is increasing importance of social, economic and technical networks whose structures are not under the direct control of the designers, but evolve as a result of decisions and behaviors of individual self-directed entities. These networks are endogenous in nature, where the local characteristics and behaviors of nodes affect the overall structures. The structure of a network affects its properties, and the properties affect the system’s performance. Hence, the problem of designing such endogenously evolving networks involves determining the node-level characteristics and behaviors through appropriate incentives to achieve the desired system-level performance. In this paper, our goal is to illustrate the problem of designing endogenously evolving networks, and to present a specific illustrative example. We perform a conceptual exploration of the problem, present the current state of the art, and identify research gaps. The illustrative example involves designing an endogenous network with two objectives, robustness to random node failure and resilience to targeted attack, considering specific node-level characteristics, additional attractiveness, as the design variables. The impact of the design variables on the performance of the network, and potential applications are discussed.

© The Authors.

Keywords: Complex networks, evolutionary systems, complex adaptive systems, systems design, resilience

1. Introduction – Design of Endogenous Networks

Many complex systems such as infrastructure systems can be analyzed and designed as networks. Traditionally, network design and optimization research has been focused on two classes of problems: a) optimizing flows on existing networks, and b) designing networks. Examples of the former include problems involving finding the shortest path, maximum flow, and minimum cost flow [1] with applications to various systems including communication systems, mechanical systems, and transportation systems. Examples of problems associated with the latter include design of circuit layouts, power grids, and other distribution networks. In these design problems, the network designer has direct control over the nodes and their connectivity. Since the structure of these networks is directly controlled by an external network designer, we refer to them as exogenously designed networks.

Recently, a new class of networks has gained interest in diverse research communities ranging from social networks to economic and technical networks. These are networks whose structures are not directly controlled by the designers, but evolve as a result of decisions and behaviors of individual self-directed entities (represented as nodes). Such networks are referred to as endogenously evolving networks. The key characteristic of an endogenous network is that the local behaviors of nodes affect the network’s global structure, the structure affects its properties,
and the properties affect the resulting performance. Consider the example of the Internet at an autonomous system (AS) level, where a node represents an AS and a link represents communication between two autonomous systems [2]. The nodes make strategic decisions about linking with other autonomous systems in order to route data. These local decisions affect the global structure of the Internet. The global structure in turn affects the performance of the Internet in terms of its robustness and resilience to node failure.

Existing research efforts on complex networks can be classified based on the mappings across four levels: 1) node-level behavior, 2) network structure, 3) network properties and 4) system-level performance (see Figure 1). In both endogenous and exogenous networks, the properties and system-level performance are directly dependent on the network structure. As discussed above, the defining characteristic of endogenous networks is that the network structure emerges from the node-level behavior. Hence, modeling the inter-relationships between these four levels is important. The process of traversing the levels from bottom (Level 1) to the top (Level 4), where the performance of the network is determined in terms of the node-level behavior, can be referred to as the analysis problem. As an example, the Barabási-Albert (BA) model [3] uses a preferential attachment mechanism (node-level behavior) for network formation. The resulting networks have a characteristic network topology with a power-law degree distribution. The networks have unique properties such as high clustering coefficient and low diameter [4]. The networks are highly robust to random node failure but have low robustness against targeted attack (system-level performance).

On the other hand, determining what the micro-behaviors should be is considered a design problem. Since the performance of such endogenous networks can be influenced by modifying local node-level behaviors, the overarching research question that motivates the work presented in this paper is: how can we achieve targeted performance in large-scale complex networks whose structures are not directly controlled by designers, but emerge dynamically from the local decisions and self-organization of individual entities? Although endogenous networks have gained significant attention from the network science community, the problem of achieving targeted performance (i.e., design) in such networks is still an open research area. Network science literature is primarily focused on analyzing specific networks and their structures (see Section 2 for details). From the design perspective, the design variables are individual incentives, and the objectives are the system performance. Hence in this context, design involves directing the evolution rather than deciding who should be linked to whom.

In the following section, we review the relevant network science literature on endogenous networks and identify the research gaps. In Section 3, a generalized model of the design problem in endogenous networks is discussed, a specific model based on the generalized model is proposed, and the approach for addressing the gaps is presented. The results and key findings of the proposed approach are presented in Section 4. Finally, conclusions are drawn and closing thoughts are presented in Section 5.

2. Review of Relevant Literature

2.1. Models Focused on Network Properties

Existing literature consists of a class of models focusing on developing node-level mechanisms to achieve network structures and properties similar to real-world networks. Such models can be classified into static and dynamic models [5]. Static models are based on a single snapshot of the network, whereas dynamics network models account for network evolution through addition/removal of nodes and links. Static models focus on certain local and global network statistics and the extent to which they capture important properties of real-world networks. The first static model can be traced back to Erdos and Renyi [6]. The model, referred to as ER model, assumes that the probability of an edge between any pair of nodes is \( p \in [0,1] \). The presence of a link is independent of the other links. An extended model of this ER model, called “exchangeable graph models” [7], introduces a weak form of
dependence among the probability of sampling edges in the form of node-specific binary strings. Another class of models, widely used in the social network literature, is the p* model [8]. The p* models are based on the assumption that the network is generated by some statistical process and the observed network is one realization from a set of possible networks with similar characteristics (e.g., number of actors). The probability of realizing a specific network is given by $Pr(Y = y) = \left(\frac{1}{k}\right) \exp \{\sum_A \eta_A g_A(y)\} [9]$ where $Pr(Y=y)$ represents the probability that a network $y$ emerges, $k$ is a normalizing parameter which ensures that the probability falls in a proper distribution. $A$ is the set of substructure configurations, $g_A(y)$ is the network statistic corresponding to the configurations $A$. Based on the observed network, the parameters $\eta_A$ are calculated using statistical estimation methods.

While static networks are focused on estimating statistical parameters from a single snapshot, dynamic network models explicitly model the evolutionary process. Typical examples of such models are the Barabasi-Albert (BA) model designed for generating scale-free (SF) networks [10] and its variations. The BA model and its variants have been used to model various real-world networks including the World Wide Web (WWW), the Internet, collaboration networks, etc. Models for generating SF networks with tunable cluster coefficient have been proposed by Herrera [11], Holme [12], and Klemm and Eguíluz [13, 14]. Dynamic network models have also been generated using the principles of Markov chains. Both continuous time and discrete time Markov chain models have been proposed in the literature [15-17]. These models are based on the assumption that networks evolve by modifying one edge at a time and the state of the network in the future is dependent on the current state only. The transition between states is dependent on node-level statistical parameters that can be estimated using longitudinal network data.

In contrast to the models discussed above, there is another class of models that directly manipulate the topology for achieving desired network properties. Molloy and Reed [18] present a model to describe how to construct graphs in which any degree distribution is permitted. The main approach is to directly control the number of edges to be assigned to a node based on the targeted degree distribution. Through this direct assignment, desired network properties can be achieved. Models in this group often belong to static models because direct topology change is made to induce a network property for a single snapshot of the real-world network. Relationships between the structure and the node-level behaviors are not established in this class of models.

2.2. Models Focused on Network Performance

The models discussed in this section are aimed at achieving desired system-level performance, and analyzing how changes in the network structure affect the system-level performance. However, such performance is achieved by designing or optimizing the network topology (through edge modification and node deletion). Beygelzimer et al. [19] propose an approach to improve the network robustness by testing several different strategies that modify the network topology by rewiring a fraction of the edges or by adding new edges. Schneider et al. [20] propose a simple modification scheme resulting in small changes in the network structure, but significantly increasing the robustness of diverse networks while having minimal impact on the functionality. Zhuo [21] proposes a strategy which removes a fraction of crashed hub nodes to improve network robustness against coordinated attack.

While these models apply subjective modification on the network topology, other models adopt evolutionary ideas to guide the modification of edges/nodes. Bornholdt [22] proposes a model constrained solely by the requirement of robustness from an evolutionary standpoint. The network evolves a new single network from an old network by accepting rewiring mutation schemes. Some authors have also considered multiple objectives for network design. Shin and Namatame [23] present a model in which the network is optimized for two performance characteristics: low congestion and design cost. Network optimization is carried out using genetic algorithms. Shargel et al. [24] propose a node-level mechanism for generating a so called “(1,0) network” that has interconnectedness closer to that of a scale-free network, a robustness to attack closer to that of an exponential network, and a resistance to failure better than both of those networks.

Since the emphasis of the models in the first two categories is on determining the node-level properties and network structures that explain existing networks, these models are primarily analysis models. Although the models in the third category modify the structure to achieve the desired system-level performance objectives, it is unclear how to modify the node-level behaviors to achieve the designed network structures. Hence, such approaches are suitable for exogenous networks but not for endogenous networks. In this paper, we present our initial steps for designing the node-level behaviors and/or incentives to achieve the desired network structure and performance.
3. Formulating the Design Problem

3.1. Design Objectives: Performance of the Network

The system performance considered in this paper is the network’s robustness against two processes: random failure of nodes and targeted attack. The robustness of networks is important for various infrastructure networks such as the Internet, power grids, and transportation networks. The effect of random failure of nodes on the topology of networks such as Internet can be analyzed using fragmentation analysis, as suggested by Albert et al. [25]. In fragmentation analysis, nodes are randomly removed from the network and the corresponding effect on the network structure is observed. On the other hand, targeted attack involves focused elimination of nodes with certain properties. Such a process can be used to represent a computer hacker trying to bring down the routers with the highest connectivity. In targeted attacks on highly connected nodes, the nodes with the highest degree are removed at each step. In both these scenarios, after a certain fraction of nodes (say \( f_c \)) is removed from the network (after \( k \) steps of attacks), the network becomes fragmented. The robustness of the network is proportional to the fraction of nodes that need to be removed before fragmentation occurs.

To quantify robustness in terms of \( f_c \), it is important to choose a measure that indicates when the network is fragmented. There are many such measures [26-29]. Two of the widely used measures are average path length (APL) index, and largest connected component (LCC) index. The average path length is the average distance between a pair of nodes within a network. The largest connected component is the number of nodes in the largest component. As the nodes are removed from the network, the changes in APL and LCC are monitored. Figure 2 shows an example of the changes in these indices as nodes are sequentially removed from the network. The initial network is a scale free network with 2000 nodes and 5703 edges generated by the BA model. As shown in the figure, in both the scenarios of random failure and targeted attack, after a certain fraction of nodes is removed, the APL decreases dramatically, indicating fragmentation of the network. The fraction of nodes \( f_c \) at which the APL reaches a maximum is used as a measure of robustness. Similarly, after a certain fraction of nodes are removed, the size of the LCC drops nearly to 0, indicating the critical fraction point \( f_c \) when the network breaks down. The value of \( f_c \) at which the LCC reaches down to less than 2% of the original network size is chosen as an indicator of the robustness.

3.2. Design Variables: Node-level Behaviors

Having decided the performance measures, the next step is to identify the design variables for the problem. Ideally, the node-level behaviors and the design variables are modeled based on the system under consideration. In this paper, we choose a general class of node-level behaviors in which a node links to other nodes based on the degree of the target node. This choice is inspired by the network science literature which has shown that many real networks exhibit scale-free structures, which result from preferential attachment. A preferential attachment process belongs to “a class of processes in which some quantity, typically some form of wealth or credit, is distributed among a number of individuals or objects according to how much they already have, so that those who are already wealthy receive more than those who are not” [30]. In the context of network generation models, such as the BA model [3], this “wealth” or “credit” is the degree of each node. A number of variations of the BA model have been developed to account for the differences among real world networks. In these models, a general index of “wealth” or “credit” is used to decide which node to connect to. Dorogovtsev et al. [31] proposed a generalized form of the preferential attachment model in which the credit of a node is given by:

\[
U(s,t) = G(s,t)k^\tau(s,t) + A(s,t) \quad (1)
\]

where the \( U \), \( G \) and \( A \) are all functions of the node \( s \) and time \( t \). \( U \) stands for the credit, \( G \) is the fitness value of node \( s \) at time \( t \), and \( A \) is the additional attractiveness of node \( s \) at time \( t \). In a network with \( n \) nodes, the probability for a new link to be attached to an existing node \( i \) at time \( t \) is proportional to:

\[
P(i,t) \propto \frac{U(i,t)}{\sum_{j=1}^{n} U(j,t)} \quad (2)
\]

Using this generalized preferential attachment model of the node-level behavior, different variants of the scale free networks can be created. For example, the model generates a scale free network at \( \tau = 1 \). If \( \tau = 1 \), \( G(s,t)=1 \) and \( A(s,t)=0 \) the generalized model become the BA model. By changing \( G(s,t) \) or \( A(s,t) \) to be time and node
dependent, the generalized models can be transformed into various different forms, as listed in Table 1. When \( \tau = 1 \), each model generates scale-free networks with different exponents of the power-law. By configuring corresponding parameters, different networks topologies can be achieved.

Table 1 - Generalized scale free model with preferential attachment

<table>
<thead>
<tr>
<th>Preferential attachment mechanism</th>
<th>Degree distribution</th>
<th>Different scenarios</th>
<th>Exponent ( \gamma ) of the power-law under different scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power-law</td>
<td>( \tau = \frac{G(s,t)}{U(s,t)} )</td>
<td>( G(s,t)=1, A(s,t)=0 ) (BA model)</td>
<td>( \gamma = 3 )</td>
</tr>
<tr>
<td>Asymptotically linear pref. attachment</td>
<td>( G(s,t)=\text{const}, A=\text{A}(t) )</td>
<td>( G(s,t)=\text{const}, A=\text{A}(s) )</td>
<td>( \gamma = 3 + \frac{\text{A}}{m}, \text{A} ) is the average value of A(s)</td>
</tr>
<tr>
<td>Aging of vertices</td>
<td>( G(s,t)=f(t-s), A=\text{const} )</td>
<td>( G(s,t)=\text{const}, A=\text{A}(t) )</td>
<td>( \gamma = 1 + \left[ \frac{\text{A}(t)}{1+(t-\text{A}(t))^t} \right]^{-1} ). The value of the exponent is between 2 and ( \infty ).</td>
</tr>
<tr>
<td>Multiplicative node fitness</td>
<td>( G,G(s), A=\text{const} )</td>
<td>To keep the network SF, the function has to be of a power-law form.</td>
<td>( \gamma = 2, \text{if } G_{\infty} \rightarrow \infty )</td>
</tr>
<tr>
<td></td>
<td>( \tau &lt; 1 ) sub-linear case</td>
<td>( \gamma \rightarrow \infty, \text{if } G_{\infty} \rightarrow 0 )</td>
<td></td>
</tr>
<tr>
<td>“Winner-takes-all”</td>
<td>( \tau &gt; 1 ) super-linear case</td>
<td>( G=G(s), A=\text{const} )</td>
<td>( P(k) \propto \frac{k^{\gamma} (1+1/k)^{\mu}}{(1+k)^{\mu^{-1}}} ) (When G is homogeneously distributed in the range ( 0, 1 ))</td>
</tr>
<tr>
<td></td>
<td>( \gamma = \frac{\mu^2}{\mu^2} )</td>
<td>( P(k) = \frac{1}{k^a} \prod_{i=1}^{k} (1 + \frac{1}{i^a})^{-1} )</td>
<td></td>
</tr>
</tbody>
</table>

The generalized preferential attachment model is used in this paper due to its flexibility and its capability of representing the topologies of a wide range of real-world networks. In this paper, we choose the additional attractiveness \( A(s,t) \) as a tunable parameter for designing endogenous networks. The primary effect of the additional attractiveness of a node is to increase the preference of that node. If the additional attractiveness of all nodes increases simultaneously, then the effect of a node’s degree on the probability of attachment is reduced. In contrast, reducing the additional attractiveness of all nodes makes the attachment more sensitive to the node’s degree. In the following section, we explore the design space and investigate how the additional attractiveness of each node affects the network’s structure, properties, and performance. The objective in the following section is to discern whether using the additional attractiveness as a design variable can result in desired network properties and performance.

4. Exploring Different Designs of Endogenous Networks based on Additional Attractiveness

4.1. Assumptions about Network Evolution

A network generation model is developed based on the generalized preferential attachment model presented in Section 3.2. The assumptions in the model are as follows:
The network is undirected, initialized as an initial random network, and grows linearly.

The probability that a new node connects to a node $i$ is given by Equation (2).

The fitness value for all the nodes is the same and is time independent, thus $G(s, t) = \text{constant}$.

The additional attractiveness for each node is time independent and a constant, thus $A(s, t) = \text{constant}$.

Random failure and targeted attack are modeled as a fraction of nodes removed from the network.

The initial network is a random network with $m_0 = 10$ nodes, where each link is present with probability of 0.2. At each time step, we assume that one new node is added with $m = 3$ edges that link the new node to $m$ different nodes already present in the network. The network grows until the number of nodes reaches $N=5000$. If $G(s, t)$ is the same for all nodes, its impact can be accounted for by scaling the additional attractiveness parameter as follows:

$$P(s, t) = \frac{\sum_i U_s(t) G(s) + A(s)}{\sum_i G(s) + A(s)} = \frac{\sum_i G(s) + A(s)}{\sum_i G(s) + A(s)} = \frac{k(s) + \frac{A(s)}{G}}{k(s) + \sum \frac{A(s)}{G}}$$

We also assume that $A(s, t)$ is a constant and $A \in (-1, +\infty)$. So the final form of the credit is: $U(s, t) = k(s, t) + A$. Since the model is stochastic in nature, we execute it 50 times at each $A$ value. To simulate random failure and targeted attacks, 1% of the existing nodes in the network are removed at each time step. When studying the network robustness, each network goes through either the random failure process or targeted attack 10 times at each $A$ value, as carried out by Beygelzimer [19]. After obtaining the raw data for each run, we calculate the 95% confidence interval for each dataset using the $t$-distribution. In the following sections, we investigate how the additional attractiveness of each node affects the network’s structure, properties, and performance (robustness).

4.2. Effects of Additional Attractiveness on the Network Structure

Use the continuum-based approach proposed by Albert et al. [10], the effect of additional attractiveness on the structure, specifically the degree distribution of the resulting network, can be analyzed. According to the model proposed in Section 3.2, the rate of change of a node’s degree $d_i$ is given by:

$$\frac{d t}{\partial d_i} = m \frac{d_i + A}{\sum_{j=1}^{N-1} (d_j + A)}$$

where $m$ is the number of edges linking to a new node in each timestep. Following the steps in [10], the asymptotic degree distribution, as the network size grows, is:

$$P(d) \propto f(m, A)(m + A)^{(m, A)} d^{-\gamma}$$

Here, $f(m, A) = (2 + \frac{A}{m})$ and $\gamma = f(m, A) + 1$. Thus, we can achieve a wide range of degree distributions by varying the additional attractiveness parameter, $A$. The degree distributions generated for representative values of $A$ are shown in Figure 3.

4.3. Effects of Additional Attractiveness on Network Properties

The effect of additional attractiveness on two network properties: average clustering coefficient and average path length are considered. The clustering coefficient represents the probability of two neighbors of node $i$ being connected [32]. It is defined as:

$$C_i = \frac{2E_i}{k_i(k_i - 1)}$$

where $E_i$ represents the number of edges between neighbors of node $i$, and $k_i$ is the degree of node $i$. The average clustering coefficient $<C>$ is the average over the cluster coefficients of all the nodes in the network:

$$<C> = \frac{1}{N} \sum_{i=1}^{N} C_i = \frac{1}{N} \sum_{i=1}^{N} \frac{2E_i}{k_i(k_i - 1)}$$

Figure 3 - Comparison of cumulative degree distributions of different networks
Figure 4 shows how the network’s average clustering coefficient decreases as the additional attractiveness of each node increases. With increasing A, the average clustering coefficient is decreasing, and the rate of the change of the average clustering coefficient also decreases.

The average path length (APL) is defined as the average length of the shortest paths between any two nodes in the network. In contrast to the average clustering coefficient, the APL increases with increase in A. But the rate of increase in the APL decreases.

The reason for the decrease in average clustering coefficient and increase of APL resulting from the increase of A is that the additional attractiveness reduces the impact of degree on the linking process. Therefore, more nodes have the opportunity to be connected rather than only the nodes with higher degree. This process makes the connectivity more homogeneous. As \( A \to \infty \), the process tends towards an exponential network [33]. Thus both the clustering coefficient and APL converge to the values corresponding to a network with exponential degree distribution (\( P(k) \sim \exp(-\beta k) \)). This network is different from the ER random network, as shown in Figure 4 and Figure 5. The additional attractiveness has significant effect on the network properties, and it can be tuned to transform the network structure from scale-free to exponential. Hence, additional attractiveness can be used as a node-level parameter for endogenously achieving the desired system-level properties such as the average cluster coefficient and the average path length.

![Figure 4](image1.png)

**Figure 4 - Effect of addition attractiveness on average clustering coefficient. (The dashed line is for random network with same network size, and the solid line is for an exponential graph)**

![Figure 5](image2.png)

**Figure 5 - Effect of addition attractiveness on average path length. (The dashed line is for a random network with the same size, and the solid line is for an exponential network)**

### 4.4. Effects of Additional Attractiveness on Network Performance

The robustness of real-world networks to random failure or to attacks targeted at the highest degree nodes is of significant interest in various domains, such as in Internet [34] and power grid [20]. Many real-world networks are robust to random failure but vulnerable to targeted attacks on important nodes. In contrast, random networks are robust to targeted attacks but more vulnerable to random failure [25]. Thus, it is important to understand how to design networks that are optimally robust against both types of attacks.

As discussed in Section 4.3, when additional attractiveness \( A \) is zero, a scale-free network is obtained. On the other hand, as \( A \) increases, the network properties approach that of an exponential network. We are interested in determining the value of \( A \) for which the network has a high robustness to the random failure and at the same time a high robustness against the targeted attacks. The networks we tested in this section are generated by the model presented in Section 3.3 with a network size of 2000. The additional attractiveness is in the range \([-1 \quad 1000]\).
a) Robustness against random failure: In order to analyze the effects of additional attractiveness on the network’s robustness, fragmentation analysis is performed for four different networks of the same size: scale free network ($A=0$), the network generated by the proposed model with $A=5$, an exponential network ($A=\infty$) and the random network generated by the ER model. The values of APL and LCC for different fractions of nodes randomly removed from a network are presented in Figure 6. It is observed that the APL indices for the ER random network and the exponential network rapidly achieve the maximum and then begin to decrease, which indicates that they are more vulnerable to random failure. In contrast, the robustness of the network generated by the proposed model and the scale-free network is higher than the other two.

b) Robustness against targeted attack: Fragmentation analysis is also performed on the four networks for evaluating the robustness against targeted attacks. Figure 7 shows how the APL and LCC indices change as the fraction of nodes removed from the network increases. The SF network collapses first after ~22% of nodes are attacked, which indicates that it is more vulnerable to the targeted attack than the other three networks. The network with $A=5$ collapses at $f_c=31\%$ showing that the robustness is increased when the additional attractiveness $A$ is increased from 0 to 5. The ER random network and the exponential network get fragmented at almost the same point, which indicates that they have the same robustness, which is higher than the other two networks.

The APL and LCC indices for different values of $A$ in the range [-1 1000] are presented in Figure 8 for both random failure and targeted attack scenarios. No significant changes in the APL and LCC indices are observed for the random failure scenario. Hence, the design of the network is insensitive to additional attractiveness, as far as
robustness against random failure is concerned.

On the other hand, as the additional attractiveness increases, the robustness against targeted attacks also increases. Hence, if the designer can increase the value of additional attractiveness, the maximum possible value should be chosen to get maximum robustness against targeted attack. This would guide the network to a topology with an exponential degree distribution. However, there may be tradeoffs associated with choosing the maximum value of the additional attractiveness, e.g., when additional attractiveness is attained by providing monetary incentives. Based on the results shown in Figure 8, the increase in the robustness of the system diminishes after a critical value of additional attractiveness (about $A=10$). It is found that the critical value of $A$ is highly dependent on the average degree of the nodes. This critical value of $A$ can be used to guide the design of the network.

5. Closing Comments

In this paper, the problem of designing complex evolutionary networks by designing node-level behaviors is presented. Existing approaches for improving robustness of networks such as though edge modification [19], degree distribution configuration, genetic evolution and optimization [22] are not suitable for addressing this problem because the designers cannot directly control the connectivity of nodes. An illustrative example of the design problem and the use of generalized form of preferential attachment as a model for representing the local node-level behavior are discussed. The effects of additional attractiveness on the network structure and system performance in terms of robustness to random failure and targeted attacks are presented. It is shown that additional attractiveness can be used as an effective design variable for achieving high robustness and resilience. The insights gained in this paper can be used for directing the evolution of real world networks if additional attractiveness can be increased through means such as providing incentives. Further, the evolution of real-world networks is not only a result of nodes’ degrees but may also be affected by other factors such as amount of resources, size, and node type. In certain cases, these other factors can be collectively represented in terms of the additional attractiveness parameter.

There is significant potential for further work in the area of complex network design. It is observed that additional attractiveness as a design variable has a limited impact on the performance space. The additional attractiveness can be used to increase the robustness only to a certain limit. Hence, it is important to investigate the effect of other design variables on the performance. The design problem is multi-objective in nature and the design variables affect all the performance characteristics simultaneously. For example, increasing additional attractiveness decreases the clustering coefficient while increasing the robustness. Further efforts in this direction can be focused on relaxing the assumptions listed in Section 4.1. For example, the additional attractiveness, $A(s,t)$, can vary with time. Similarly, the nodes can be heterogeneous, indicating that the fitness function $G(s,t)$ can be different for different nodes. Taking the AS-level Internet as an example, the preferential connectivity between different autonomous systems may be dependent on the type of the AS (e.g., customer, Internet Service Provider (ISP), or peer). Although we assume the generalized preferential attachment model for the node-level behavior, determining the correct model for real networks is one of the challenging aspects in network design problems. If the network already exists and data can be gathered, statistical models discussed in Section 2 can be used to fit appropriate models for the node-level behaviors. Additionally, it is challenging to determine the right design parameters that can be adjusted in the real world networks.

Acknowledgements

The authors gratefully acknowledge the financial support from the National Science Foundation grants 0954447 and 1201114, and China Scholarship Council award No. 2010628122.

References
