Hindawi
Complexity
Volume 2017, Article ID 6548362, 12 pages
https://doi.org/10.1155/2017/6548362

Research Article

Resilience of Core-Periphery Networks in the Case of Rich-Club

Matteo Cinelli, Giovanna Ferraro, and Antonio Iovanella

Department of Enterprise Engineering, University of Rome "Tor Vergata", Via del Politecnico 1, 00133 Rome, Italy

Correspondence should be addressed to Matteo Cinelli; matteo.cinelli@uniroma2.it

Received 24 August 2017; Accepted 12 December 2017; Published 28 December 2017

Academic Editor: Ilaria Giannoccaro

Core-periphery networks are structures that present a set of central and densely connected nodes, namely, the core, and a set of noncentral and sparsely connected nodes, namely, the periphery. The rich-club refers to a set in which the highest degree nodes show a high density of connections. Thus, a network that displays a rich-club can be interpreted as a core-periphery network in which the core is made up of a number of hubs. In this paper, we test the resilience of networks showing a progressively denser rich-club and we observe how this structure is able to affect the network measures in terms of both cohesion and efficiency in information flow. Additionally, we consider the case in which, instead of making the core denser, we add links to the periphery. These two procedures of core and periphery thickening delineate a decision process in the placement of new links and allow us to conduct a scenario analysis that can be helpful in the comprehension and supervision of complex networks under the resilience perspective. The advantages of the two procedures, as well as their implications, are discussed in relation to both network efficiency and node heterogeneity.

1. Introduction

Defined as a system's ability to adjust its activity to retain its basic functionality when errors, failures, and environmental changes occur [1, 2], resilience is a crucial property of many networked systems. It has been rapidly tackled by the scientific literature [3, 4] and, as such, is still considered a topic of great interest [2, 5, 6].

Related to concepts such as robustness, redundancy, vulnerability, and sustainability [7], resilience is considered fundamental for a number of practical approaches that involve risk assessment in terms of criticalities related to the eventual failure (or removal) of nodes and links and thus by means of overall systemic tolerance. Indeed, network performances (especially in terms of routing ability and stability) are directly related to their resilience and thus to the capabilities of networks in tolerating loss of important elements such as bridges or hubs. Mainly because of its tangible implications [8–11], resilience has been investigated across many different network structures (both synthetic and real) and there is now knowledge regarding how specific kinds of networks react to specific kinds of losses [12, 13]. In more detail, since resilience is related to the ability to withstand deliberate attacks and incidents, studies about this topic have tended to consider a large variety of structural failures (both induced by attack or naturally occurring) which involve both specific (i.e., chosen by their properties like the centrality indexes) and random nodes.

Moreover, as resilience is strictly related to the network topology [3, 14], results of the stress tests are strongly affected by certain structural measures such as density and the clustering coefficient [15], as well as by the presence of specific substructures like cliques or dense subgraphs, which are, in general, highly fault-tolerant since the loss of any element has no disruptive effect on the interaction between the others.

Among those densely tied substructures that seem to be of interest in terms of resilience [16, 17], the rich-club is particularly well known [18]. The rich-club is a network substructure that is observed when hubs are tightly interconnected. It constitutes the basis for the recognition of the rich-club phenomenon which is, more generally, defined as the tendency of nodes with a high centrality (usually degree) to form highly interconnected communities [19]. Furthermore, it can be even interpreted as the core of a core-periphery network [20], that is, as the core of a network that shows a set of central and densely connected nodes and a set of noncentral and sparsely connected nodes.

The rich-club phenomenon has been observed in many different networks [18, 19] and its importance has been recognized in that it represents an unexpected feature (i.e., nonreplicated by regular models [18, 21]) of many real systems, which is shown to have a relevant effect on certain network measures, especially on assortativity and transitivity [22]. Another important aspect of the rich-club is that while it is possible to evaluate its presence for each value of the node degrees, through a specific coefficient properly normalized over an ensemble of randomized networks [19, 23–27], it is not possible to compute its size a priori [25].

Thus, it is commonly assumed that the rich-club is made up of a certain low percentage of the highest degree nodes [18, 22], whose interconnections are able to strongly affect a number of structural measures. So, despite the fact that a number of studies have investigated the rich-club phenomenon and aspects of resilience within the context of complex networks (like in the case of the Internet [1] and, more recently, of the Darknet [5]), to the authors' knowledge these two problems have never been tackled when taking their conjectured mutual effects into consideration. Indeed, while there have been some statements about the role of the rich-club in terms of its capacity to increase the network stability [5], to act as a super traffic hub [18], and to indicate resilience to specific kind of attacks [28], the literature still lacks a unique general framework able to make the relationship between the rich-club ordering and the resilience of a network explicit.

Under these circumstances, this paper aims to shed some light on the role of the rich-club from a resilience perspective by looking at how the presence and the characteristics of this important substructure are able to affect the network robustness from various points of view.

For these reasons, we consider networks in which we manipulate the set of connections among the highest degree nodes by adding and removing links. By adopting this strategy we obtain a set of different networks that share the same topology other than a small subgraph made up of the rich nodes; that is, we keep the network periphery while altering the network core. The resilience is tested on the resulting networks by means of a number of measures related to both efficiency and cohesion: the diameter, the average path length, the global efficiency, and the global clustering coefficient. The implications of the rich-club presence in terms of resilience lay the basis for the investigation of a different rationale in the positioning of new links. Therefore, we modify the previous manipulation procedure by testing the case in which the same amount of links (which we would add in order to reach certain rich-club densities) is instead added randomly outside the rich-club.

More specifically, we implement two procedures of either core or periphery thickening in order to mimic the decision process of a supra-agent that, with a limited amount of resources constituted by the new links, has to engineer the considered system in an efficient manner. The result of this process will be relevant in understanding where to put new connections in existing networks, such as new routes in airport networks or new cables in power grids or the Internet, being consistent with a set of efficiency criteria that are here represented by the network measures used in the evaluation of resilience.

The investigation of different scenarios leads us to certain conclusions that foster the addition of new links within the network core and thus offer a different insight into the complex task of network reinforcement. Our conclusions could help decision makers in pursuing more appropriate choices when it comes to implementation of precautionary measures and to investment of new resources with the scope of increasing the resilience of a certain network.

In more detail, the outcome of our strategy, in terms of core thickening, also has consequences related to the costs of new links positioning. Indeed, it has been shown that, in a wide range of networks within the technological domain [23], the rich-club emerges because links among hubs have a cost that is, in general, lower than other links since hubs tend to be physically closer. Therefore, rich-club ordering has also a geometric explanation as to its existence. As a consequence, if we have a certain limited amount of resources dedicated to new links positioning, a core thickening strategy is capable of providing both a higher efficiency and a lower cost. This would preserve a delta of resources that could be potentially invested into a periphery thickening strategy able to provide more benefits in the long run through its tendency towards nodes equity.

Lastly, our results allow room for certain additional considerations at different levels, which will be useful in better comprehending and supervising networks that display the rich-club structure.

The paper is organized as follows: Section 2 describes rich-club ordering and network resilience; Section 3 shows the simulation setting; Section 4 displays the simulation results and analysis; Section 5 presents discussions and conclusions.

2. Rich-Club Ordering and Network Resilience

Rich-club ordering is an important topological property firstly observed in the case of technological networks and, in more detail, in the case of the Internet at Autonomous Systems (AS) level [18]. Recognition of this phenomenon is conducted via a comparison between the number of links among the rich nodes and the number of links they might possibly share. In doing so, it is possible to evaluate the density of the subgraph made up of such nodes. The rich nodes are those that have a degree higher than a certain threshold k and a rich-club occurs when such nodes are more densely interconnected than expected; that is, they have more interconnections with respect to the average of the interconnections found among the same nodes in an ensemble of rewired networks [19].

However, as the threshold value of degree k for which we may observe that the rich-club is unknown, the size of the rich-club is therefore assumed, in accordance with the empirical evidence, to be around the 1% of the network nodes [18, 22, 25]. The empirical evidence of small rich-club size is present in many different domains from technological

[27] to social [29] and biological networks where, especially in neuroscience [30–32], the investigation of the rich-club phenomenon has provided important insights from a brain functionality perspective.

Thus, while this property has been recognized as relevant, its effect on the network metrics has been mainly tested for cohesion measures such as the clustering coefficient and the degree assortativity and only marginally for path-based measures that should be, in case of rich-club ordering, more of interest since such measures are associated with information flow. Indeed, the efficiency of a network is mainly based on path metrics and it has been shown that the rich-club is an emergent property of certain networks [23] in which hubs need to be interconnected in order to avoid losses, as in the case of electric current in power grid networks [23, 33]. In this respect, the knowledge and the investigation of the rich-club effect on other measures, closer to the concept of distances among nodes, may be of interest in terms of both static analysis, that is, in terms of the effect of a progressively denser rich-club on certain measures, and dynamic analysis, that is, in terms of resilience. Indeed, the investigation of network resilience can be seen as a what-if analysis that considers a large set of network topologies and metrics that derive, through a procedure of nodes and links deletion, from the original one.

Resilience has been traditionally studied in two different cases (or scenarios): error and attack. By error we mean the random removal of elements; by attack we mean a removal process that targets specific or crucial elements. Thus, the error case considers randomness while the attack case is conducted by removing elements with high values of certain centrality measures in two different ways: sequential and simultaneous [13]. If we consider node removal, in the sequential targeted attack the centrality measures are computed at the beginning of each iteration and the node with the greater centrality score is eliminated; in the simultaneous targeted attack the centrality measures are computed at the beginning and the order of the nodes to be removed is known before the procedure starts. In the previous cases and even in the case of error, the basic properties and effect of the removal procedures are well known in the literature for both real and synthetic networks [12, 13]. For instance, it is known that scale-free networks are particularly resilient in case of error and particularly vulnerable in case of attack due to the variance of their degree distribution, that is, because of a topology that includes hubs [3]. Obviously, many other cases could be mentioned, but none of them would include, to our knowledge, a clear perspective on the role of the rich-club in such networks. Thus, under these circumstances and given the relevance of both network resilience and rich-club ordering from a number of perspectives, it is important to extend the current knowledge as deriving from the literature to the case of networks displaying a rich-club structure.

3. Simulation Setting

We analyze resilience by considering undirected and unweighted scale-free networks G, with $N = 5000$ nodes and mean degree value $\langle k \rangle = 6$. We manipulate the connections among the top 1% nodes of highest degree by adding/removing links in order to create subgraphs (cores) with various density values. In adopting this strategy we are able to obtain different networks sharing the same topology other than the subgraph made up of the rich nodes.

As shown in Figure 1, the obtained densities of the induced subgraphs are $d = \{0, 0.09, 0.25, 0.5, 0.75, 1\}$, where $d = 0.09$ is the density, averaged over ten instances, of the subgraph made up of rich nodes in the original (i.e., nonmanipulated) network. This last case represents the default case among the different generated networks. In the six different scenarios we test the robustness of the network to node removal in case of error and in case of simultaneous degree-targeted attack. The choice of this kind of attack (instead of the sequential degree-targeted attack in which the centrality scores are computed at each iteration) is motivated by the fact that our aim is to observe the effect of the rich-club, as realized by our manipulation, on certain measures that characterize the considered network. Indeed, with the simultaneous degree-targeted attack we know a priori the nodes that are going to be removed, while in case of sequential degree-targeted attack the ensemble of rich nodes may be subjected to variations due to the recomputation of the centrality scores at every iteration.

After the removal of each node, we compute a number of different metrics that refer to aspects of both information flow and network cohesion. The considered measures are global in the sense that they are computed on the whole network and not on the single node, and they are the diameter, the average path length, the global clustering coefficient, and the global network efficiency (see Table 1).

The diameter provides information about the ease in which communication occurs between the farthest elements of the network. It measures the longest geodesic path considering the two most distant nodes and it can be considered as a extremal measure that, despite having a low value in most real world networks, is subject to relatively large changes in response to local modifications. Thus, it has to be coupled with other measures that take into account the mean distance among nodes and that are more stable when local changes occur. For this reason, we also consider the average path length which is computed as the mean of all the shortest (geodesic) paths among nodes. These two measures, which take into account paths, are however related and affected by another feature of many real world networks: the cohesiveness of nodes. Indeed, it is often observed that two neighbors of a certain node are themselves neighbors and the probability of such an event (which determines the network cohesiveness) is known as clustering coefficient. The clustering coefficient is also an overall network measure that takes into account the number of triangles in the network and compares such a number with the amount of connected triples (ordered paths of the length 2). The two global measures called average path length and global clustering coefficient are generalized into a unique measure that embeds their informative content. This measure, which quantifies the overall efficiency in communication among nodes, is called network efficiency. For our purposes, the average efficiency formulation (reported in Table 1) is then normalized by

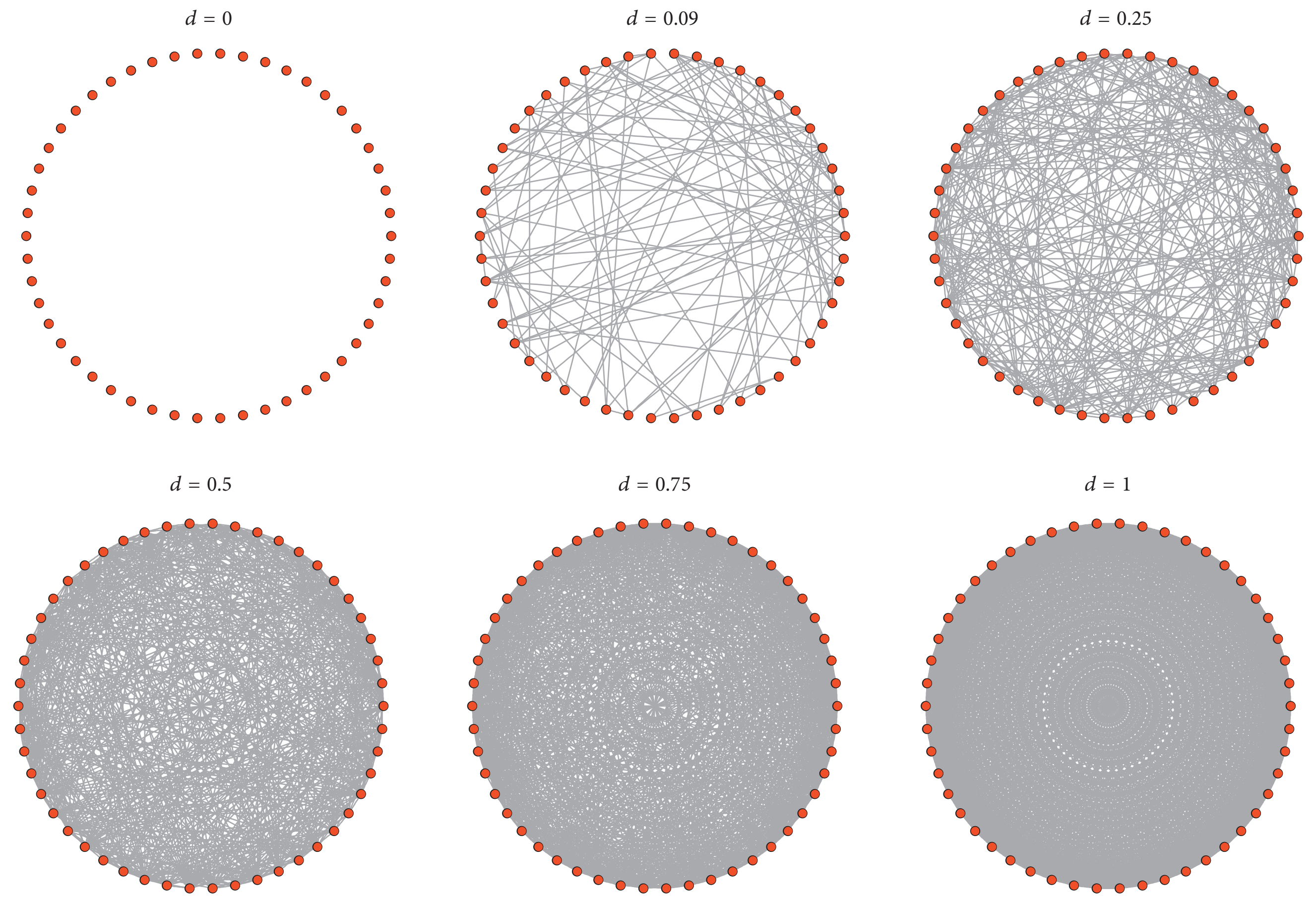

Figure 1: Process of link addition/removal of the subgraph made up of the highest degree nodes in order to reach different density values.

Table 1: Short glossary of metrics computed during simulations (note that d_{ij} is the shortest path between nodes i and j in G).

Measure	Definition	Formula
Diameter (D)	The length of the shortest path between the most distanced nodes.	$D = \max_{i,j\in G} d_{ij}$
Average path length (APL)	The mean of all the shortest paths between all couples of nodes.	$\mathrm{APL} = \frac{1}{N(N-1)} \sum_{i,j\in G} d_{ij}$
Global clustering coefficient (C)	The average of the local clustering coefficients C_i of all individual nodes.	$C = \frac{1}{N} \sum_{i\in G} C_i$
Global network efficiency (E)	A measure of how efficiently the network exchanges information.	$E = \frac{1}{N(N-1)} \sum_{i<j\in G} \frac{1}{d_{ij}}$

considering the average efficiency value of a complete graph of size N. Having the possibility of observing these four measures during the process of node removal allows us to evaluate the local and global aspects related to network performance, both specifically and in a more general sense.

The obtained results are averaged over 10 replicas of the resilience tests and on 10 different networks realized using the same degree sequence (i.e., the same list of node degrees).

For all the considered cases we focus on the initial effect of a denser/sparser rich-club on the measures from the above and on its effect throughout the process of node removal. Additionally, we test the case in which the same amounts of links that we would add in order to reach certain rich-club densities are instead added randomly outside the rich-club. In other words, by recalling the core/periphery nature of networks that display rich-club ordering, we test two procedures of either core or periphery thickening. The comparison between the two procedures allows us to perform a scenario analysis and to simulate a decision process of a supra-agent that, with a limited amount of resources (the links), has to engineer the considered system (the network) in an efficient (from the point of view of the described measures) manner.

It is worth adding at this point that the two indicated procedures (i) to add links within the rich-club and (ii) to add

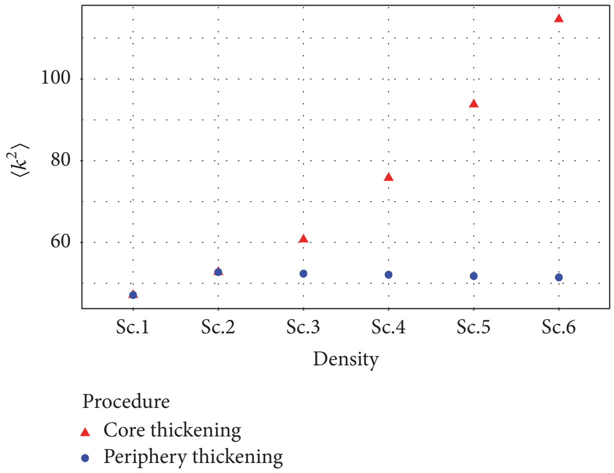

Figure 2: Variance of the degree $\langle k \rangle^2$ after the procedure of core and periphery thickening. All results are averaged on 10 instances.

links outside the rich-club alter the degree distribution (and the degree sequence) of the considered networks. These alterations depend on many factors, including the number of links to be added and their location, as well as the consequent size and density of the rich-club. Placement of the new links has an effect on the different portions of the degree sequence, meaning the two procedures end up turning the network into either more irregular or regular structure. We illustrate this process of degree sequence modification by plotting the variance $\langle k \rangle^2$ of the node degrees (see Figure 2), that is, the degree-related network heterogeneity [34, 35], in the described cases.

We summarize the described simulation procedures as shown in Table 2 where column 2 is the required local density for the rich-club subgraph, column 3 is the average values of links to be added in order to obtain such a density, and column 4 reports the number of links removed or added randomly in the network core, while column 5 highlights the number of links that are randomly removed or added in the network periphery. Note that links are reported as averages over ten instances, while in the network manipulation each of the ten instances was modified with the proper number of links. Note also that in the second setting the default rich-club is preserved together with its density, since we are adding links in the network periphery.

Data processing, the network analysis, and all simulations (all the implemented functions are available at https://github.com/cinHELLi) were conducted using the software *R* [36] with the *igraph* package [37].

4. Simulation Results

4.1. Core Thickening. Analyzing Figures 3 and 4 we notice that the rich-club is not highly relevant with respect to simultaneous degree-targeted attack in networks that display a power-law degree distribution. Rather, it positively alters the initial statistics of the network; this is why, without the zoom of Figure 4, we would only be able to observe the stacked curves of Figure 3.

In more detail, when we take into account scale-free networks, we observe that the overall trend of the considered measures is very close, in the long run, to that of the nonmanipulated scale-free networks; in our case the curve is with density $d = 0.09$ and related to Scenario 2. Indeed, the presence of the rich-club has an effect on the values of the considered measures until the 1% of the nodes have been removed, as shown in Figure 4. In decreasing order of impact, such an effect has an impact on the global clustering coefficient, the global efficiency, the average path length, and the diameter. The effect on all these metrics is further amplified by the density of the rich-club; thus, the higher its density, the higher the overall centrality value. This is true in particular for the global clustering coefficient case in which, called n_{rc}, the number of nodes of the rich-club is progressively generated up to $\binom{n_{rc}}{3}$ triangles, that is, the number of triangles displayed by a complete subgraph of size n_{rc}. The core thickening procedure also has a relatively strong impact on the global efficiency and on the average path length. Indeed, when we consider these two measures, the addition of new links provides a reasonable number of new shortcuts that, despite being suboptimal with respect to other strategies, are still suitable in order to reduce the average path length, for example, when new links are added among nodes with the highest betweenness centrality [38].

As previously mentioned, the effect of the rich-club is relatively strong for all the initial values of the computed measures. This does not, however, include the diameter, whereby a denser rich-club provides relatively useful shortcuts when considering the distance between two specific nodes. This is because the clustering coefficient, the efficiency, and the average path length are measures averaged over all the network nodes (while the diameter is a more extremal measure) and are thus affected by the centrality values retained by the rich-club. This bias is especially evident in scale-free networks whose heterogeneity in the degree distribution contributes to phenomena like the friendship paradox, which holds if the average degree of nodes in the network is smaller than the average degree of their neighbors [39].

Table 2: Simulation scenarios for core and periphery thickening.

	Rich-club density	Links	Core thickening	Periphery thickening
Scenario 1	$d_{\mathrm{rc}} = 0$	$\overline{m}_1 = 111$	Remove m_1 links	Remove m_1 links
Scenario 2	$d_{\mathrm{rc}} = 0.09$	$\overline{m}_2 = 0$	Default case	Default case
Scenario 3	$d_{\mathrm{rc}} = 0.25$	$\overline{m}_3 = 194$	Add m_3 links	Add m_3 links
Scenario 4	$d_{\mathrm{rc}} = 0.50$	$\overline{m}_4 = 500$	Add m_4 links	Add m_4 links
Scenario 5	$d_{\mathrm{rc}} = 0.75$	$\overline{m}_5 = 807$	Add m_5 links	Add m_5 links
Scenario 6	$d_{\mathrm{rc}} = 1$	$\overline{m}_6 = 1113$	Add m_6 links	Add m_6 links

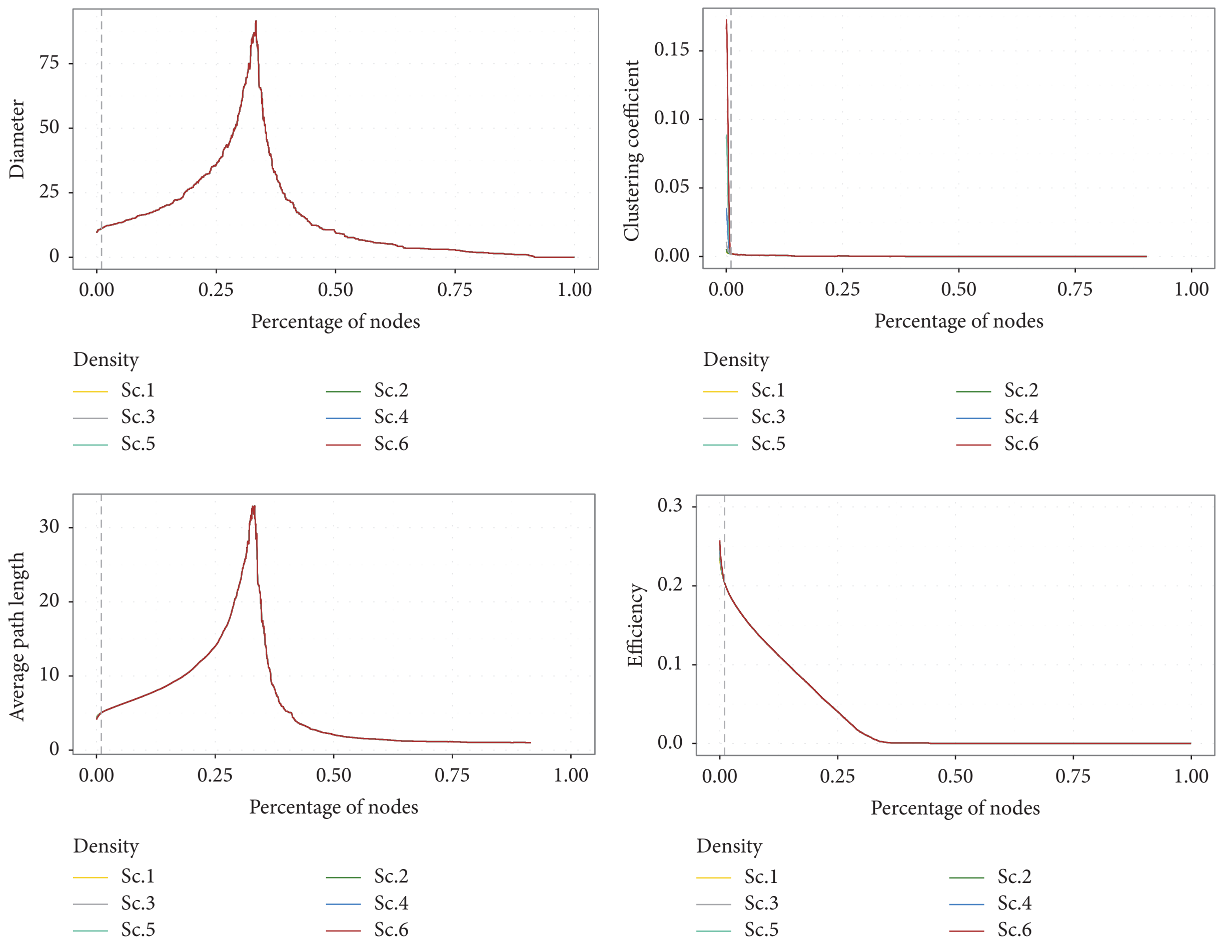

Figure 3: Resilience for simultaneous attack simulations with progressive manipulation of the number of links in the network core. The dashed line is placed in correspondence with the rich-club size. All results are averaged over 10 instances.

The origin of the paradox is attributed to the existence of hub nodes and to the variance of the degree that contributes to altering the mean values of the degree over the neighborhoods of the nodes. Therefore, the observed deviations of the computed measures may be motivated by similar reasoning if we further consider the increase in the degree sequence variance induced by our manipulations. In summary, exacerbating the interconnections among hubs (i.e., to create progressively denser cores) has a relevant effect on the centrality measures averaged over the network nodes but has no relevant effect in terms of resilience to a degree-targeted attack.

In the case of error the rich-club in Figure 5, according to its density, provides a very high fault tolerance to the considered system. Indeed, the nodes that constitute the core make up a low portion (1%) of the whole number of nodes and are thus less likely to be randomly removed. The low probability of hubs removal has an effect on the resilience of the system, which is guaranteed for all the observed measures. For instance, the diameter doubles only when about 75%

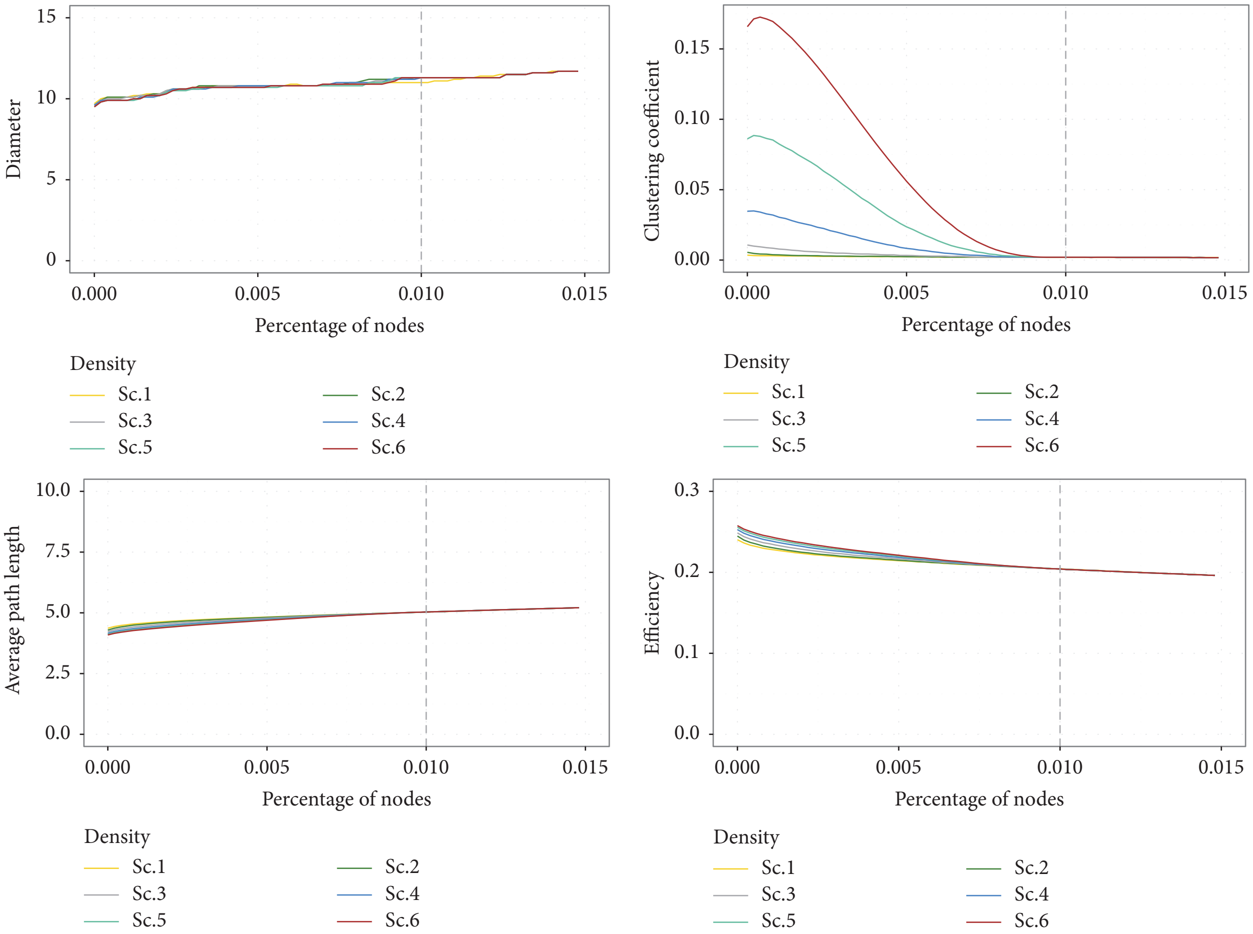

Figure 4: Resilience for simultaneous attack simulations with progressive manipulation of number of links in the network core; magnification of the area of Figure 3 in which the rich-club lays. The dashed line is placed in correspondence with the rich-club size. All results are averaged over 10 instances.

of the elements are removed, and the global clustering coefficient is kept during the simulations since the majority of triangles are located within the rich-club.

Figure 6 focuses on the area of the rich-club where the behavior of the considered measures follows a straight line, indicating a certain network stability for similar reasons as those discussed before.

4.2. Periphery Thickening. As shown in Figure 7, networks with a denser periphery are more resilient to targeted attacks than networks with a denser core. Intuitively, this happens because, in this setting, the core nodes maintain their initial characteristics in terms of interconnectedness, while the periphery nodes become progressively more interconnected. This process of node homogenization is also the reason that the different curves of Figure 7 are not stacked and present clear differences throughout the removal process. When we look at the diameter and at the average path length, the peaks related to the two metrics occur in correspondence with a higher percentage of removed nodes (between 30% and 40% approximately) and, differently from the case of core thickening, the number of added links has a role in determining the robustness to targeted removal. This observation is consistent with the fact that, by adding links to the network periphery, we decrease the degree sequence variance; thus we somehow regularize the considered networks. The obtained results recall the resilience to simultaneous degree-targeted attack in case of degree homogeneous networks [4]. Additionally, the initial global clustering coefficient is much lower as links are not placed in order to thicken a small subgraph (the rich-club); consequently the likelihood to close a connected triple (to create a new triangle) is lower. Even in the case of global efficiency we observe a proportionately more resilient behavior across the number of added links as confirmed by the distance among the six different curves.

In the case of error (see Figure 8), the periphery thickening procedure leads to results that are similar to those of core thickening except for two considerations. The clustering coefficient is much lower, for the reasons discussed before, and the curves relating to different scenarios have similar and almost stacked trends; in other words, they refer to results that are comparable, although the number of added links in the various scenarios is much different. This is because, as we lower the variance of the degree, the contribution of

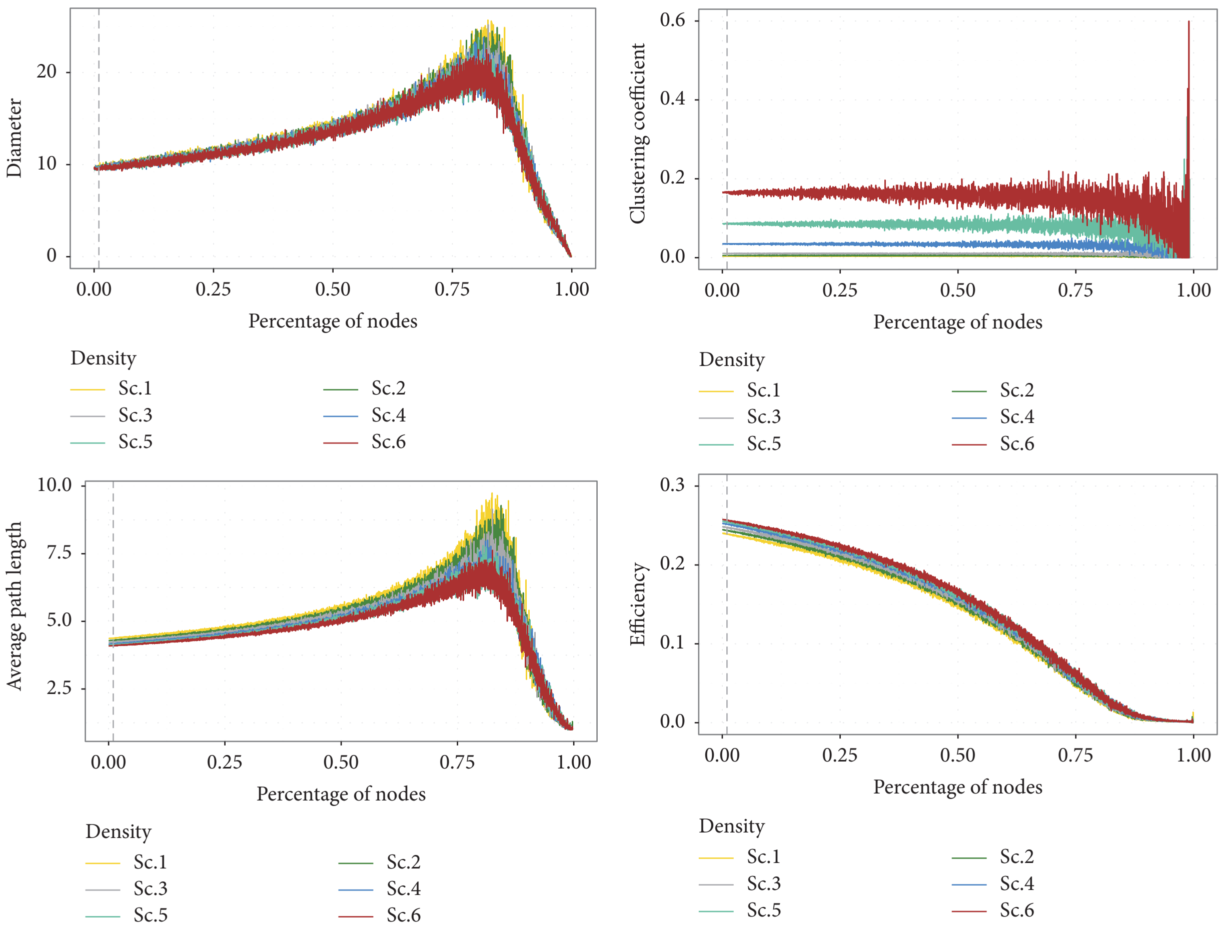

Figure 5: Resilience for simultaneous error simulations with progressive manipulation of the number of links in the network core. The dashed line is placed in correspondence with the rich-club size. All results are averaged over 10 instances.

each node to the considered network metrics tends to be progressively the same. In more detail, the curves related to diameter and to the average path length follow a similar trend to that of the core thickening case, even if the various curves tend to behave more similarly among each other because of the homogenization procedure. This is also the case when it comes to the global efficiency and the global clustering coefficient, as the latter shows a much lower overall value based on the fact that it is, somehow, not biased by a high concentration of triangles in the network core.

5. Discussion and Conclusions

Herein we discuss the results of the simulations by looking at both their theoretical and practical meaning and implications. Consideration of both the theoretical and practical aspects regarding the results is helpful in better understanding the role of the rich-club in terms of network resilience and in providing insights into the demanding task of network supervision and engineering.

If we consider attack tolerance, the rich-club thickening initially guarantees a greater global cohesion predominantly in the core, as well as an overall better performance when removing a number of nodes below the 1% threshold. Thus, the network provides better performance when only a few high-degree nodes are removed. The main drawback is that this high proportion of cohesion measure is retained by the nodes that are actually the most likely to be removed in the case of an attack.

Considering attack tolerance once again, the periphery thickening has the main advantage in that it alters the network into a more resilient structure, which is able to keep its properties in the long run. This means that the network tends to maintain stable values of the performance measures when a high portion of the nodes is removed, since in this case the paths tend to be preserved. These aspects of network resilience are mainly regulated by the manipulation of the network degree-related heterogeneity (i.e., by the manipulation of the variance of node degrees) that we perform through the procedures of core and periphery thickening.

In the case of error, the networks that display a dense core provide overall better performances that improve accordingly with the core density. Indeed, the trend of the different curves in the cases of core and periphery thickening are similar, but the former case provides also a better initial global efficiency and a higher value of clustering that lasts throughout the simulations.

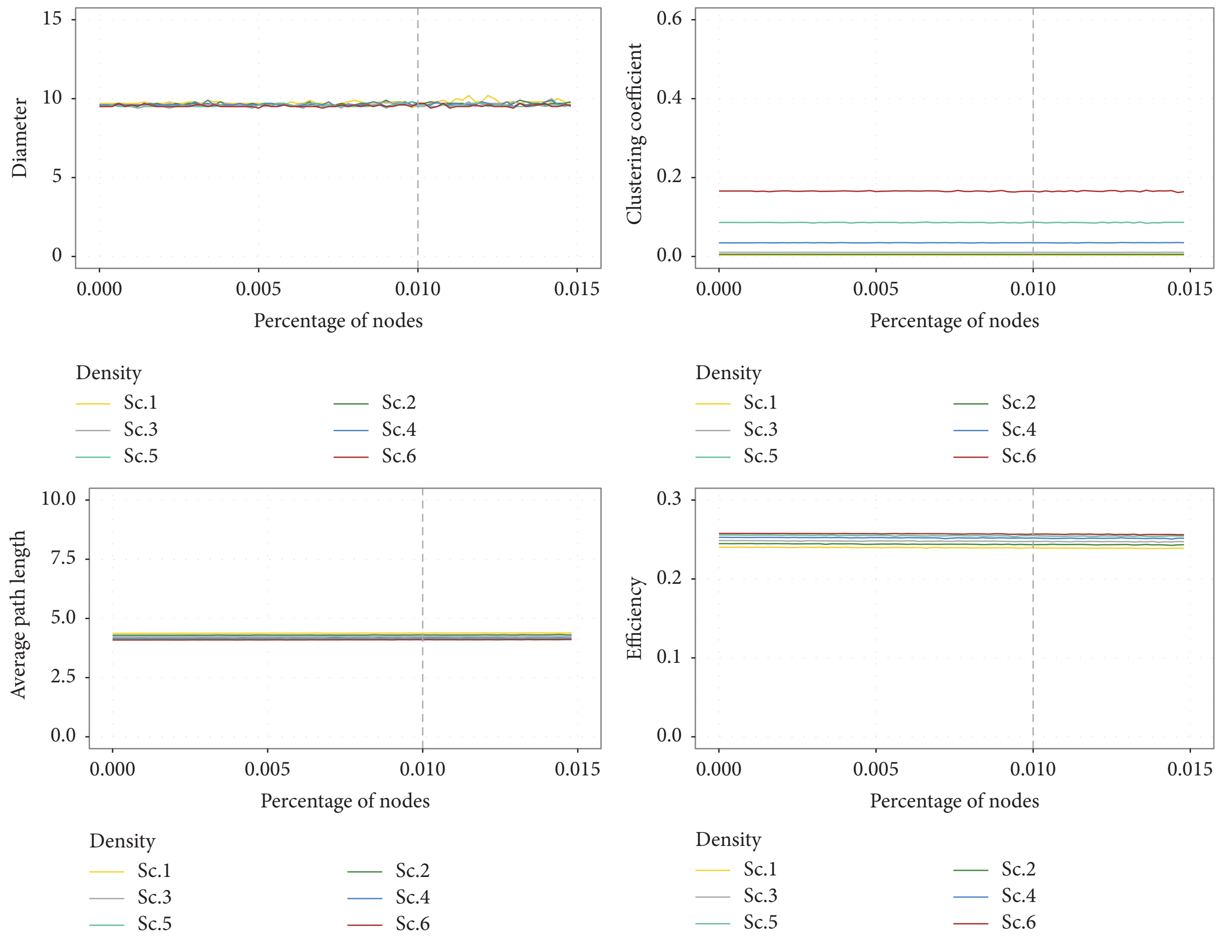

Figure 6: Resilience for simultaneous error simulations with progressive manipulation of the number of links in the network core; magnification of the area of Figure 5 in which the rich-club lays. The dashed line is placed in correspondence with the rich-club size. All results are averaged over 10 instances.

Thus, if by looking at the simulations, a decision maker would evaluate where to put a set amount of links with respect to random node failure, the logical conclusion would be that it is better to increase the density of the network core and to increase that density as much as possible, compatibly with the amount of available links and addressed resources. The observations in the case of attack should be of different nature and should be weighted on an eventual foresight about the magnitude of possible attacks to the network. Indeed, if massive attacks on the network are possible, the periphery thickening (i.e., a network homogenization) should be preferred while if there is a higher likelihood of few hubs being removed, the core thickening (i.e., a network heterogenization) should be preferred.

In other words, considering, for instance, the diameter, that is, an extremal measure of communication, in the case of periphery thickening the curves have both shifted peaks and a lower slope according to the network density. It means that the network performance degenerates after a greater number of removed nodes and the considered performance measures are directly proportional to the network density. Indeed, for a fixed percentage of removed nodes the diameter is smaller as the density grows.

The concepts of attack magnitude and attack likelihood constitute two important aspects, related to the risk profile of the network under observation that should be considered when different strategies of link addition are taken into account.

However, these conclusions could be further discussed especially in case of resilience to massive attacks provided by networks treated with the periphery thickening procedure. Indeed, in case where about 25% of the network nodes (or more) are lost, issues regarding the performance could be discarded in favor of other issues regarding network recovery and catastrophes management. Thus, a decision maker may be not that interested in the performance measures from the above once the system has been dramatically disrupted. Using this consideration as a baseline, we may argue that once the percentage of removed nodes has passed such a right-shifted threshold, an advantage in terms of resilience is not particularly realistic due to the fact that any benefit can be only obtained once a loss of significantly large dimensions

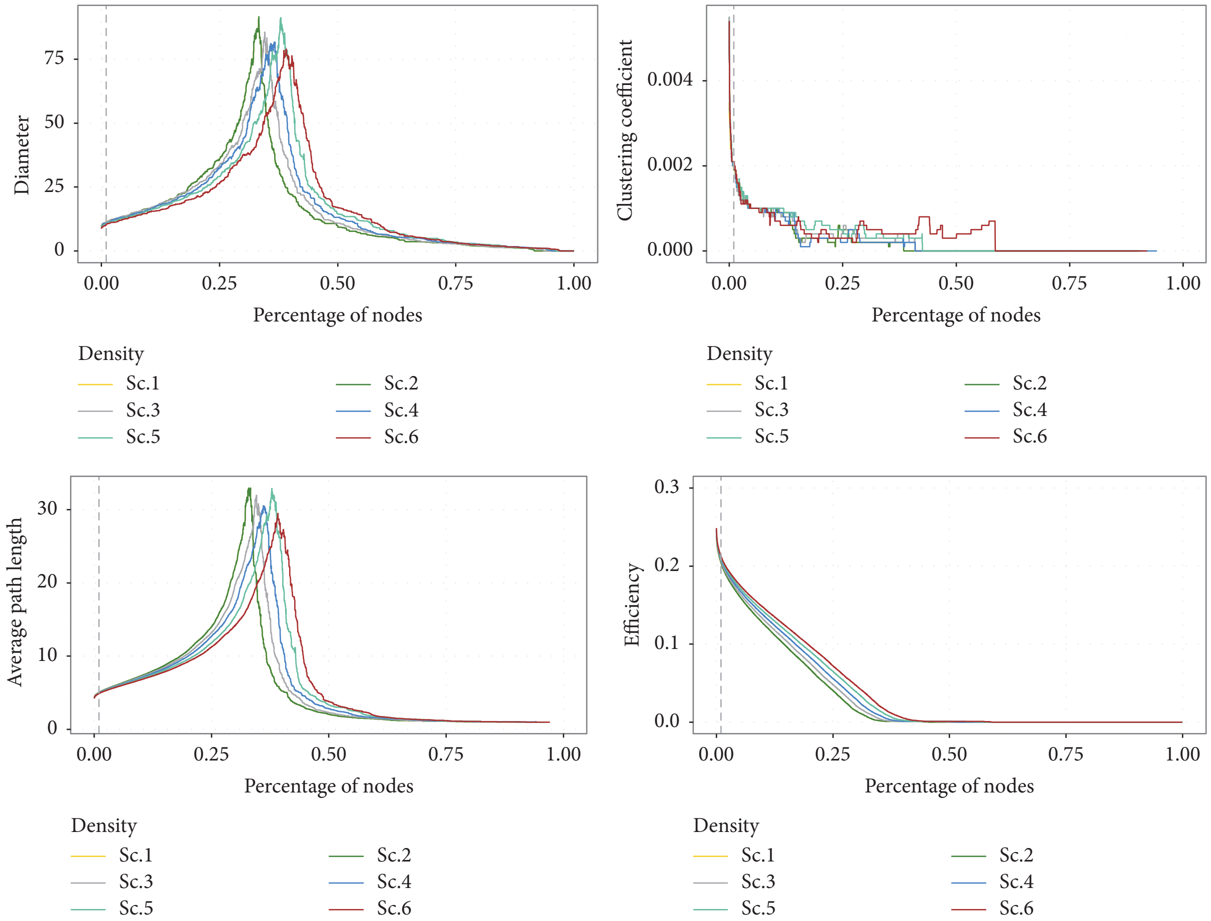

Figure 7: Resilience for simultaneous attack simulations with progressive manipulation of the number of links in the network periphery. The dashed line is placed in correspondence with the rich-club size. All results are averaged over 10 instances.

occurs. This may lead us to conclude that the core thickening procedure, that is, the increase of the rich-club density, has to be considered as a practically better procedure to follow in order to enhance the network resilience.

In summary, the simulations highlight the relationship between the rich-club size and the attack magnitude, indicating that if the former is greater than the latter then a reasonable policy would be to perform a core thickening strategy.

Two aspects have to be considered further: on the one hand, the core thickening strategy provides a better resilience to errors and to small attacks (to hubs) but on the other hand this procedure, in accordance with the size and the density of the rich-club, exacerbates the degree-related asymmetry and thus entails a problem of equity of nodes that is invariably of interest in a number of real networks. When the attack magnitude exceeds the rich-club size then simulations suggest a strategy of periphery thickening.

Therefore, a decision maker has to face controversial decisions regarding the adoption of a strategy that is affected by two parameters, the rich-club size, and the attack magnitude, which are two measures generally difficult to obtain and foresee. This reinforces the notion that a better understanding of the network structure and of the rich-club is relevant, especially when coupled with other concepts related to the risk profile and to the type of system that is taken into account.

These observations reveal a number of discussion points concerning the management of man-made systems such as the Internet and certain airport networks. Indeed, these networks already display rich-club ordering because hubs have been progressively interconnected for reasons relating to both efficiency of traffic and the cost of new links. Moving forward, it will also be important to consider cascade failures, since in this case eventual failures or attacks seemingly propagate faster within a network with a dense core than in a network in which hubs are less interconnected. Therefore, the implementation of the core thickening procedure, as well as the management of a network that already displays rich-club ordering, suggests that stronger monitoring activities of the network nodes are needed in order to avoid attack and isolate those that are the source of failure.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

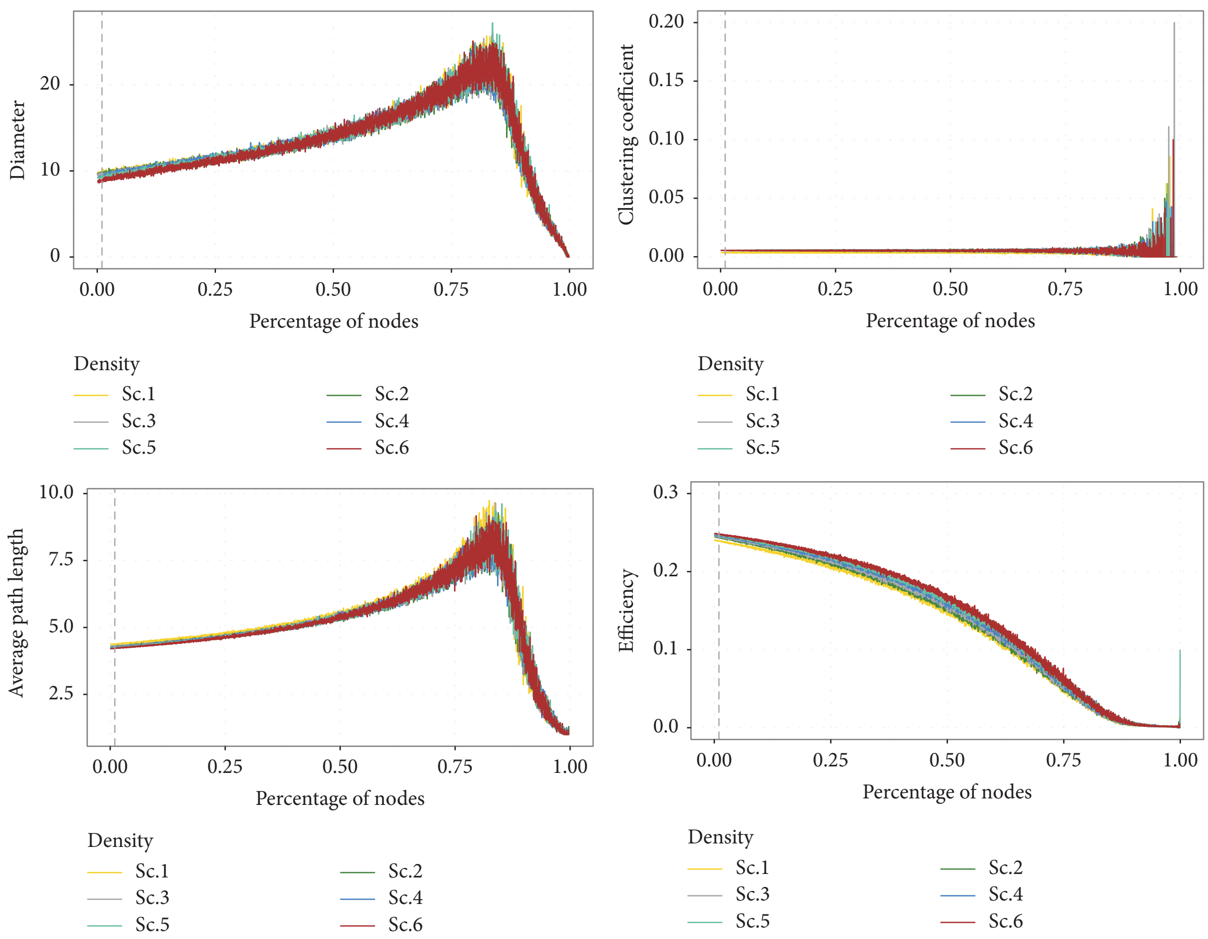

FIGURE 8: Resilience for simultaneous error simulations with progressive manipulation of the number of links in the network periphery. The dashed line is placed in correspondence with the rich-club size. All results are averaged over 10 instances.

References

[1] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Resilience of the Internet to random breakdowns," *Physical Review Letters*, vol. 85, no. 21, pp. 4626–4628, 2000.

[2] J. Gao, B. Barzel, and A.-L. Barabási, "Universal resilience patterns in complex networks," *Nature*, vol. 530, no. 7590, pp. 307–312, 2016.

[3] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[4] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Error and attack tolerance of complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 340, no. 1-3, pp. 388–394, 2004.

[5] M. De Domenico and A. Arenas, "Modeling structure and resilience of the dark network," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 95, no. 2, article 022313, 2017.

[6] L. Fraccascia, I. Giannoccaro, and V. Albino, "Rethinking Resilience in Industrial Symbiosis: Conceptualization and Measurements," *Ecological Economics*, vol. 137, pp. 148–162, 2017.

[7] M. E. O'Kelly, "Network hub structure and resilience," *Networks and Spatial Economics*, vol. 15, no. 2, pp. 235–251, 2015.

[8] M. Modica and A. Reggiani, "Spatial Economic Resilience: Overview and Perspectives," *Networks and Spatial Economics*, vol. 15, no. 2, pp. 211–233, 2015.

[9] M. Rubinov and O. Sporns, "Complex network measures of brain connectivity: Uses and interpretations," *NeuroImage*, vol. 52, no. 3, pp. 1059–1069, 2010.

[10] M. M. Williamson, "Resilient infrastructure for network security," *Complexity*, vol. 9, no. 2, pp. 34–40, 2003.

[11] K. Zhao, A. Kumar, T. P. Harrison, and J. Yen, "Analyzing the resilience of complex supply network topologies against random and targeted Disruptions," *IEEE Systems Journal*, vol. 5, no. 1, pp. 28–39, 2011.

[12] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 65, no. 5, article 056109, 2002.

[13] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, "Attack robustness and centrality of complex networks," *PLoS ONE*, vol. 8, no. 4, pp. 1–17, 2013.

[14] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Efficiency of scale-free networks: Error and attack tolerance," *Physica A: Statistical Mechanics and its Applications*, vol. 320, pp. 622–642, 2003.

[15] G. Ferraro and A. Iovanella, "Clairvoyant targeted attack on complex networks," *International Journal of Computational Economics and Econometrics*, vol. 8, no. 1, pp. 41–62, 2017.

[16] A. Gutfraind, "Optimizing topological cascade resilience based on the structure of terrorist networks," *PLoS ONE*, vol. 5, no. 11, pp. 1–7, 2010.

[17] Y. Yang, Z. Li, Y. Chen, X. Zhang, and S. Wang, "Improving the robustness of complex networks with preserving community structure," *PLoS ONE*, vol. 10, no. 2, pp. 1–14, 2015.

[18] S. Zhou and R. J. Mondragón, "The rich-club phenomenon in the internet topology," *IEEE Communications Letters*, vol. 8, no. 3, pp. 180–182, 2004.

[19] V. Colizza, A. Flammini, M. A. Serrano, and A. Vespignani, "Detecting rich-club ordering in complex networks," *Nature Physics*, vol. 2, no. 2, pp. 110–115, 2006.

[20] A. Ma and R. J. Mondragón, "Rich-cores in networks," *PLoS ONE*, vol. 10, no. 3, pp. 1–13, 2015.

[21] P. Csermely, A. London, L. Wu, and B. Uzzi, "Structure and dynamics of core/periphery networks," *Journal of Complex Networks*, vol. 1, no. 2, pp. 93–123, 2013.

[22] X.-K. Xu, J. Zhang, and M. Small, "Rich-club connectivity dominates assortativity and transitivity of complex networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 82, no. 4, Article ID 046117, 2010.

[23] M. Csigi, A. Kőrösi, J. Bíró, Z. Heszberger, Y. Malkov, and A. Gulyás, "Geometric explanation of the rich-club phenomenon in complex networks," *Scientific Reports*, vol. 7, no. 1, 2017.

[24] Z.-Q. Jiang and W.-X. Zhou, "Statistical significance of the rich-club phenomenon in complex networks," *New Journal of Physics*, vol. 10, no. 4, article 043002, 2008.

[25] M. Cinelli, G. Ferraro, and A. Iovanella, "Rich-club ordering and the dyadic effect: Two interrelated phenomena," *Physica A: Statistical Mechanics and its Applications*, vol. 490, pp. 808–818, 2018.

[26] R. J. Mondragón and S. Zhou, "Random networks with given rich-club coefficient," *The European Physical Journal B*, vol. 85, no. 9, article 328, 2012.

[27] S. Zhou and R. J. Mondragón, "Structural constraints in complex networks," *New Journal of Physics*, vol. 9, no. 6, article 173, 2007.

[28] G. Thedchanamoorthy, M. Piraveenan, D. Kasthuriratna, and U. Senanayake, "Node assortativity in complex networks: An alternative approach," in *Proceedings of the 14th Annual International Conference on Computational Science, ICCS 2014*, pp. 2449–2461, June 2014.

[29] N. Masuda and N. Konno, "VIP-club phenomenon: Emergence of elites and masterminds in social networks," *Social Networks*, vol. 28, no. 4, pp. 297–309, 2006.

[30] O. Sporns, D. R. Chialvo, M. Kaiser, and C. C. Hilgetag, "Organization, development and function of complex brain networks," *Trends in Cognitive Sciences*, vol. 8, no. 9, pp. 418–425, 2004.

[31] M. P. van den Heuvel, R. S. Kahn, J. Goñi, and O. Sporns, "High-cost, high-capacity backbone for global brain communication," *Proceedings of the National Acadamy of Sciences of the United States of America*, vol. 109, no. 28, pp. 11372–11377, 2012.

[32] M. P. van den Heuvel and O. Sporns, "Rich-club organization of the human connectome," *The Journal of Neuroscience*, vol. 31, no. 44, pp. 15775–15786, 2011.

[33] J. W. Simpson-Porco, F. Dörfler, and F. Bullo, "Voltage collapse in complex power grids," *Nature Communications*, vol. 7, Article ID 10790, 2016.

[34] R. Jacob, K. P. Harikrishnan, R. Misra, and G. Ambika, "Measure for degree heterogeneity in complex networks and its application to recurrence network analysis," *Royal Society Open Science*, vol. 4, no. 1, 2017.

[35] T. A. B. Snijders, "The degree variance: An index of graph heterogeneity," *Social Networks*, vol. 3, no. 3, pp. 163–174, 1981.

[36] R Development Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria, 2008. ISBN 3-900051-07-0.

[37] G. Csardi and T. Nepusz, "The igraph software package for complex network research," *International Journal of Complex Systems*, vol. 1695, 2006.

[38] X.-B. Cao, C. Hong, W.-B. Du, and J. Zhang, "Improving the network robustness against cascading failures by adding links," *Chaos, Solitons & Fractals*, vol. 57, pp. 35–40, 2013.

[39] Y.-H. Eom and H.-H. Jo, "Generalized friendship paradox in complex networks: The case of scientific collaboration," *Scientific Reports*, vol. 4, article 4603, 2014.