Exploring Robustness to Targeted Attacks in Core-Periphery Networks

Charif El Gataa[a]

This manuscript was compiled on November 20, 2024

Robustness properties of a network heavily depend on its topology. Despite considerable attention has been given to this topic, there is no unified framework to study the problem. Moreover, algorithms developed to increase robustness of a network without altering its structure are currently limited to cases in which the network is structured in communities. In this paper, we model the resilience of networks with a core periphery structure against targeted attacks. We develop a strategy to enhance a network's robustness while preserving its core-periphery structure.

Robustness | Targeted Attacks | Core-Periphery Structure | Centrality measures

Significance Statement

Networks with a core-periphery structure are vulnerable against intentional attacks. Enhancing their robustness against this type of attacks is still an open problem. We aim to discuss previous work regarding the theoretical understanding of the core-periphery structure and its robustness against different types of attacks. Then, we study the relation between the core-periphery structure of a network and its robustness. Finally, we propose some possible strategies to improve the network's robustness while preserving its structure and its degree distribution.

A network is a mathematical model that represents the interaction between a set of objects or components. These components are called nodes, and their interactions are called edges. The dynamics and structure of many real life systems can be described by complex networks. These systems include on-line social networks, where nodes are users and edges are social contacts, or city transportation networks, where nodes are stations and edges are the lines which connect them, or also biochemistry networks, where nodes are proteins or enzymes and edges are interactions in a biological process. The word "complex" refers to the fact that these networks are non-trivial in their structure and in their function. Many researchers have proven that a large part of these networks tends to be "robust yet fragile" (1), meaning that they are robust against random component failures, but are vulnerable to target attacks to important components, which are usually called "hubs". Hubs are nodes that either have many more connections than others, or have connections that are crucial for the network connectivity and the flow of information. Therefore, attacking one or more of these nodes may make the network fragile and may heavily compromise its functionality. There are many different ways to mitigate the effect of attacks on a network and they usually imply a reconfiguration of the connections between nodes. Such modifications may affect different properties of the network, in particular its degree distribution and its topology. The degree distribution provides important information about the structure and the properties of a network, while its topology, which describes how the different nodes are placed and interconnected, mainly depends on the network's nature and function. For example, a network can exhibit a community structure or a core-periphery structure. In the first case, networks can be divided into multiple modules of densely interconnected nodes with sparse connections to the nodes of other modules. In the second case, nodes can be divided into two groups: a core of nodes which are highly connected to each other, and a periphery of nodes that are moderately connected to the core and sparsely connected to each other. These properties generally depend on the network's nature and the way it has developed over time. Altering them might compromise the network's functionality and make it significantly different from its original purpose and its original design. Therefore, when we want to improve a network's robustness, we need to take into account the importance of maintaining its properties as close to those of the original network as possible. As an example, let's consider the network of internal flights in the United States (2), where each node is an airport and each edge represents a flight route. The majority of U.S. airline companies operate with a hub-and-spoke system, meaning that they centralize their routes around one or few airports. Passengers traveling to or from smaller regional airports have to transfer through these hub airports. Hub airports are highly interconnected with each other, and other airports have one or few connections to the hubs.

Therefore, the network is characterized by a core-periphery structure. If one of the main airports becomes non-operational (for example, because of a storm), the functionality of many peripheral airports is affected, making the transportation service vulnerable to disruptions of the hub airports.

Author affiliations: [a]University of Zurich

E-mail: charif.elgataa@uzh.ch.

In order to increase the robustness of the network, one could introduce routes between airports that are not part of the main hubs; however, this strategy can be economically unfeasible due to low passenger demand for these routes.

Core-Periphery Structure

Intuitively speaking, a network exhibits a core-periphery (CP) structure when nodes can be partitioned into two classes with the following characteristics: a cohesive subgraph where nodes are densely connected with each other (namely the core), and a second set of nodes that are loosely connected to the core, with little to no connection among themselves (the periphery).

This model is useful for explaining various network phenomena, such as technological infrastructures (3), transportation networks (4), and critical pathways for disease diffusion (5).

Moreover, the distinction between central and peripheral nodes allows for a more precise classification of the functional and dynamic roles of nodes based on their structural position (6).

Although a universal definition of CP structure does not exist, there are different metrics for quantifying such type of structure in a network.

Borgatti and Everett (7) introduced a quantitative measure which relies on the assumption of a block core-periphery structure, i.e. the adjacency matrix of the network has a block structure, in particular, it is divided into 3 blocks that are different to each other: one related to core-to-core connections, one related to core-to-periphery edges (plus its symmetric counterpart with respect to the main diagonal, for periphery-to-core connections) and one for periphery-to-periphery edges. Their aim is to estimate the similarity between the structure of an observed network and an ”ideal” core-periphery configuration. In this ideal configuration, core-to-core entries in the adjacency matrix are expected to be mostly equal to 1, core-to-periphery entries are expected to be in large part equal to 0 and periphery-to-periphery entries are expected to be almost all equal to 0. Similarly to the concept of modularity, given a partition of the network into core and periphery, this measure compares the number of links inside the periphery with the expected value for a random graph with same number of edges and peripheral nodes. The score, that they call ρ, is defined as

$$\rho = \frac{1}{2} \sum_{i,j=1}^{N} A_{ij} g_i g_j - p \binom{n_p}{2}$$

where N is the number of nodes in the network, $A \in \mathbb{R}^{NxN}$ is the adjacency matrix, g_i is equal to 1 if node i is in the periphery and 0 if not, $n_p = \sum_{i=1}^{N} g_i$ and $p = M / \binom{N}{2}$ is the average edge probability if the same number M of edges were placed at random.

Since we have $\sum_i g_i = n_p$ and, if $n_p >> 1$, it holds that $\binom{n_p}{2} \approx \frac{1}{2} n_p^2$, then we can write the score as

$$\rho = \frac{1}{2} \sum_{i,j=1}^{N} (A_{ij} - p) g_i g_j$$

By minimizing this score, we can identify the best approximation of the partition into core and periphery that this method provides.

Previous works

Random failures and percolation theory. Peixoto et al. (8) employed percolation theory to explore how networks evolve to develop a robust structure with respect to random failures and targeted attacks. Specifically, they modeled a large-scale network using a block model and derived the structures which optimize percolation properties against different types of attacks. They found that the core-periphery structure is the most robust topology against random failures, because all the network's functions are concentrated in the core, which is densely connected. Therefore, failures of one node in the core will not compromise the network's resilience. Meanwhile, failures of peripheral nodes have limited impact on the network's overall functionality.

Furthermore, deriving percolation thresholds analytically for a network with a core-periphery structure is a difficult task, since core and periphery may percolate at different critical values (9). This happens because the percolation model exhibits a double transition: first, there's a regular transition where the core percolates, followed by the formation of a (macroscopic) sub-graph in the periphery, and a final phase transition where the periphery percolates, regardless of the core.

Cascading failures. A common risk in networked systems is that the failure of a single element might trigger failures of other connected elements. This phenomenon is known under the name of ”cascading failures” and is the case of many real world networks, for example power grids or financial crises.

There are different ways to model cascading failures, the two which are mostly used are overload based models and branching processes (10).

In overload based models, each node contains an agent that can be in one of two states: 0 (active or healthy) or 1 (inactive or failed). Since information or traffic is usually transmitted along the shortest path, it has been found that a good measure to capture the information load at node i, denoted as L_i, is its betweenness centrality, which is the number of times that a node is in the shortest path between two other nodes (11). The maximum load that a node i can bear is called capacity and denoted as C_i. It is usually assumed to be proportional to nodes' initial load, i.e.

$$C_i = \alpha L_i(0) \quad \forall\, i = 1, 2, ..., n$$

for some tolerance parameter $\alpha \geq 1$.

At time t=0, all agents are in healthy state. However, it may happen that at some time $t > 0$, one or more nodes fail. At each subsequent time t, an active node fails if its load at time t is greater than its capacity.

Tran et al. (12) showed that core-periphery structure has a negative effect on robustness of a network against overload based cascading failures, while networks with a homogeneous load distribution are optimal. In fact, in networks with a homogeneous load distribution, if one or more nodes fail, the load is spread across the network, reducing the probability of other failures. On the other hand, in networks with a CP structure, nodes in the core are more responsible to network's load than nodes in the periphery, therefore, if one core node fails, the load is disproportionately redistributed to the remaining core nodes.

Targeted attacks. Core-periphery networks are extremely fragile against targeted attacks. In fact, these attacks primarily impact the core, causing the network to collapse more rapidly, since the functioning of peripheral nodes heavily depends on the operation of nodes in the core.

A particular case of core-periphery structure is represented by the onion-like structure. In networks that exhibit such configuration, nodes with similar importance (for example, a centrality measure) are connected to each other. The result is that nodes with higher importance form a "hub" and as we gradually move away from this hub, nodes become less and less important. Onion-like structures are shown to be the most robust against both targeted attacks and random failures (13).

Yang et al. (3) addressed the issue of robustness of core-periphery structure against both targeted attacks and random failures. They proposed a new measure of robustness of the CP structure and developed algorithms that seek to optimize it. However, optimizing robustness of the CP structure of a network is a different task than optimizing robustness of the network itself. It may occur that, after attacks on some core nodes, the largest connected component might experience huge losses of peripheral nodes that were connected to the core only through the attacked nodes, but the remaining nodes in the largest connected component still retain a CP structure that is similar to the original one.

In this work, we will analyze robustness of networks with a CP structure and we will focus both on the network's resilience and on retaining its initial structure. Moreover, we will only consider targeted attacks.

Robustness

There are three common types of approaches that can be employed to improve robustness of a network.

The first method consists in adding new edges to the network (14). The resulting network is more robust than the original one, due to the introduction of alternative paths and redundancies. However, this method is subject to some limits, in particular when considering our analysis. First, it modifies the degree distribution of the network. Second, it may not always be feasible, such as due to high costs of adding an airline route. Lastly, it may change the core-periphery structure of the network. For example, in a core-periphery network, if we randomly add a number of edges between nodes in the periphery, we will increase the robustness of the network, but we may unintentionally create a second core, or even two different communities within the network.

A second method involves reconnecting edges in order to create a network where the distribution of node importance is more balanced. For example, if we are interested in lowering a network's vulnerability to degree-based attacks, we can randomly select an edge that connects a node to a high degree node, and rewire it to another random node. This strategy is powerful when it reduces the number of hubs in the network, but it is not always feasible. For example, in the case of power grids, the presence of hubs is necessary to guarantee an efficient and cost-effective energy distribution. Moreover, it will modify the degree distribution and the topology of the network. In particular, networks with a core-periphery structure will have their structure dismantled.

The third method consists in swapping two different edges: for each step, we select edge e_{jk} that connects nodes j and k and edge e_{mn} that connects m and n, and substitute them with edge pair e_{nj} and e_{mk} or edge pair e_{mj} and e_{nk}. This method will not change the degree distribution of the nodes, but it may change the structure of the network. For example, in core-periphery networks, we may weaken the core-periphery structure if we perform multiple steps of edge rewiring where we replace two edges that connect peripheral nodes to core nodes with one edge between peripheral nodes and one edge between nodes in the core. Even if this could increase the robustness of the network, for example against betweenness-based attacks, it may overmodify the network's original structure. In our strategy, we will use the third method, but we will be careful in preserving as much of the defining characteristics of the network as possible.

Materials and Methods

Robustness measure. Traditional robustness measures, like the average path length, do not take into account cases in which the network suffers a big damage without completely collapsing. Schneider et al. (13) introduced a robustness measure R that is based on the sizes of the largest connected component after the removal of all possible numbers of nodes. Let N be the number of nodes in the network. Define $s'(Q) = s(Q)/N - 1$ where $s(Q)$ denotes the size of the largest connected component after removing $Q = qN$ nodes, with $q \in \{1/N, .., 1\}$ being the fraction of damaged nodes. The robustness measure is defined as

$$R = \frac{1}{N} \sum_{Q=1}^{N} s'(Q)$$

Attack procedure. In targeted attacks, nodes are removed based on their importance, which can be assessed by utilizing a centrality measure, for example, betweenness, degree, eigenvector or closeness centrality.

There are two different types of targeted attack strategies (we will consider both):

1. Simultaneous targeted attacks: the importance of nodes is calculated at the beginning, prior to the network attack, and, then, a predetermined fraction of the nodes are removed in decreasing order of their importance measure.

2. Sequential targeted attacks: first, the importance measure is calculated for all nodes in the original network, then, the node with highest importance is attacked and, finally, the importance of the remaining nodes is computed again, since it may differ than the one computed at the beginning. The process is repeated until all nodes are removed.

According to Iyer et al. (15) findings, in general, sequential attack strategies cause bigger damages than simultaneous ones, and, in sequential attacks, the differences in the attack effects for different centrality measures are small.

Relation between Core-Periphery Structure and Robustness

In this section, we aim to interpret the relation between core-periphery structure and robustness against targeted attacks.

We will consider attacks based on different centrality measures, namely degree, betweenness, closeness and eigenvector centrality.

We simulate a core-periphery network by modifying an Erdős-Rényi model. We first divide a prespecified number N of nodes into two groups (core and periphery), respectively of n_1 and n_2 nodes, and we define three different values for the probability of an edge forming between any two nodes. Specifically, we will have p_{11}=probability that two nodes in the core are connected, $p_{12} = p_{21}$=probability of connecting one node in the core and one node in the periphery, and p_{22}=probability of forming an edge between two nodes in the periphery. In order to get a CP structure, we set $p_{11} > p_{12} > p_{22}$. Then, we iteratively select an edge in the network, remove it and replace it between any two nodes uniformly at random. As measure of the quality of the core-periphery structure, we use the Borgatti-Everett coefficient that we previously described. To assess robustness, we use the coefficient introduced by Schneider et al. In our simulation, we set $n_1 = 30$, $n_2 = 70$, $p_{11} = 0.5$, $p_{12} = 0.2$, $p_{22} = 0.01$.

The results in Fig. 1 show that both the robustness coefficient and the Borgatti-Everett coefficient increase, meaning that the CP structure of the network is gradually being dismantled and its robustness improves. In all four simulations, the increase in robustness is faster at the beginning and tends to stabilize over time. In fact, after only 200 iterations, the robustness scores increased by more than 60% of their initial value. In particular, the initial increase is much higher when considering closeness and eigenvector centrality. This may happen because reshuffling edges respectively shortens the length of shortest paths to or from peripheral nodes, and, secondly, increases the connection of core nodes (initially with high eigenvector centrality) and peripheral nodes (initially with low eigenvector centrality), therefore balancing both centrality measures.

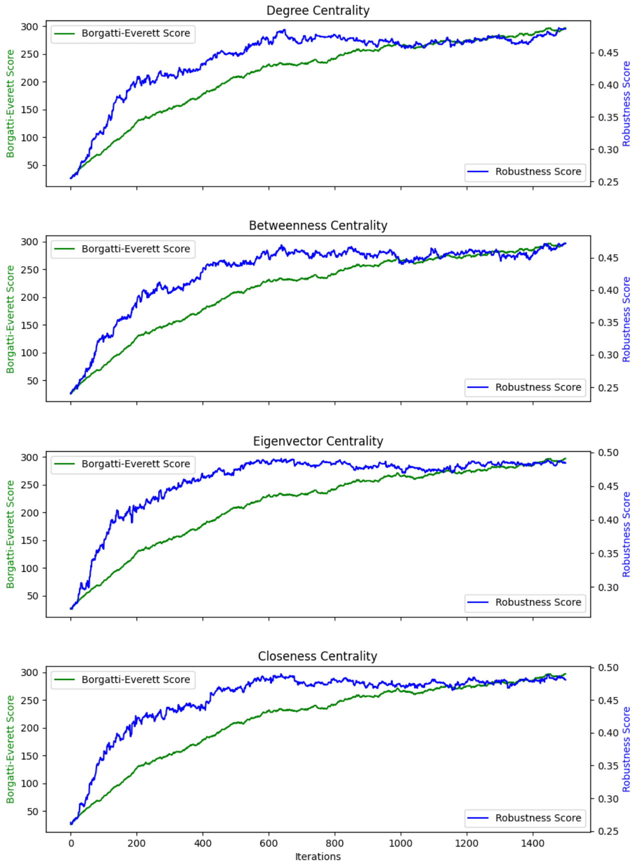

Fig. 1. Comparison of Borgatti-Everett score and Robustness score for different centrality measures. Each subplot shows the evolution of the Borgatti-Everett score (green) and the Robustness score (blue) over 1500 iterations for networks attacked based on four different importance measures: (a) Degree centrality, (b) Betweenness centrality, (c) Eigenvector centrality, and (d) Closeness centrality. The results indicate how the core-periphery structure and network robustness change when edges are reshuffled.

Strategies to Optimise Robustness

In networks with a CP structure, in general core nodes have higher centrality measures than peripheral nodes, due to their dense connectivity. This means that targeted attacks will likely remove most core nodes before reaching peripheral nodes. Therefore, to enhance the robustness of these networks through edge rewiring without significantly altering their structure, we can intervene in two ways:

1. Rewire edges within the core in order to improve its robustness

2. Rewire edges between core and periphery in order to minimize losses of peripheral nodes in the largest connected component when core nodes are targeted. This is particularly important because the presence of peripheral nodes in the connected component relies on few connections with core nodes and even fewer connections with other peripheral nodes.

These are the only two effective paths that we can follow. In fact, rewiring peripheral edges will not consistently improve robustness against targeted attacks. Additionally, replacing one edge within the core and one edge within the periphery with two edges from core to periphery may lead to dissolution of the core for a sufficiently large number of iterations (provided that there are enough peripheral nodes and edges within them).

According to the first approach, we can rewire core edges so that the core forms an onion-like structure. Under the second approach, we can rewire edges so that connections between core and periphery occur as much as possible from core nodes that have lower importance, and nodes with higher importance have few or no edges to the periphery.

We apply the first strategy by randomly sampling two edges in the core, check if they do not overlap, and swap them if the robustness coefficient of the new network is strictly greater than the coefficient of the previous network.

We implement the second strategy by randomly sampling one edge between core and periphery and one edge within the core. In the first sampling we assign higher weight to edges where the core node has more importance, in the second sampling we give higher weights to core nodes which have lower importance. If the edges are non overlapping, we rank the three core edges based on their importance. Finally, we connect the two core nodes with higher importance with each other, and connect the third node with the peripheral node.

Simulated example. We implement both the strategies on a simulated core-periphery network built as a modification of the ER network, as above. In our simulation, we set $n_1 = 100$, $n_2 = 100$, $p_{11} = 0.6$, $p_{12} = 0.1$, $p_{22} = 0.01$.

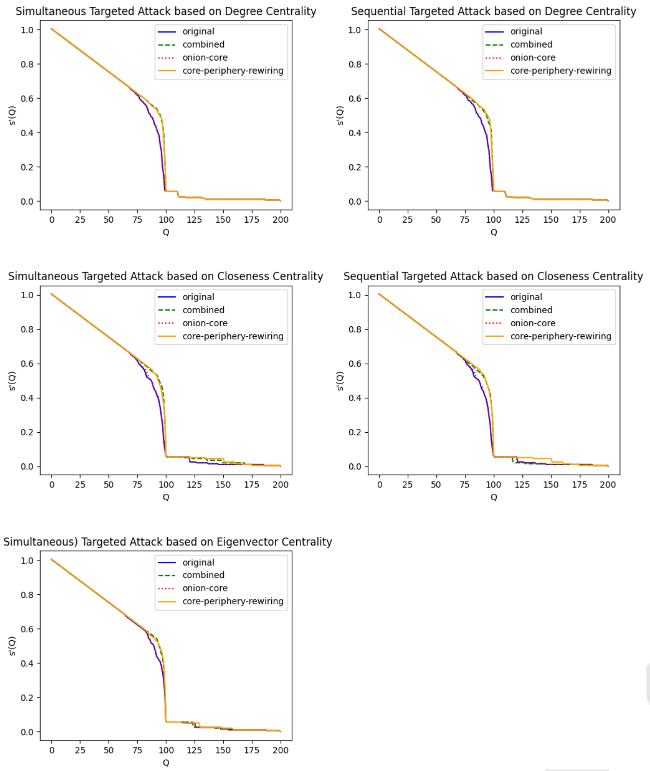

Fig. 2. Network robustness under different centrality-based attack strategies. The first column represents robustness under simultaneous attacks, while the second column shows sequential attacks. Each row corresponds to a different centrality measure: Degree centrality (first row), Closeness centrality (second row), and Eigenvector centrality (third row). The y-axis denotes the normalized size of the largest connected component and the x-axis denotes the number of removed nodes. Graphs corresponding to different strategies are used, including the original network, a network with onion-like core structure (first strategy), a network where we apply the second strategy (that we called core-periphery rewiring), and a network with both the interventions. Eigenvector centrality is not well defined for disconnected networks, therefore we only provide simulation of a simultaneous targeted attack.

Plots in Fig. 2 show us that the strategy of connecting peripheral nodes to less important core nodes successfully improves robustness of the network against targeted attacks. In fact, nodes with less importance are targeted later in the attack, letting shuffled peripheral nodes remain connected to the core for a longer time. On the other hand, the first strategy performs poorly in enhancing robustness. This is due to the method used to construct the simulated networks. In fact, core nodes do not have big differences in importance, since the probabilities with which they are connected to other nodes are the same across the entire core. Therefore, it is difficult to find an efficient onion-like structure in this case.

Empirical example. We applied the same strategies to a social network representing a subset of interaction between users on Telegram (16). Data are collected from September 2015 to June 2019 and represent different types of interactions between users (forward, mention or url).

Here, our first step is to partition the network into core and periphery. By only looking at the degree distribution, and partitioning based on degree, we may find a good approximation of the core and the periphery (10). Researchers developed different methods for core-periphery detection. We use the algorithm developed by Kojaku and Masuda (17), since it allows to control for the effect of nodes' degree and works well in networks with a high number of nodes. The Telegram network is composed of 698 nodes, of which 183 are identified as core and 515 as periphery. Thus, the core constitutes a small fraction of the network. Starting from this network, we make four different simulations of a degree-based targeted attack on it. The first simulation is with the original network, the second uses the network modified with our first strategy, the third after applying our second strategy, and the last uses the network after combining the two strategies.

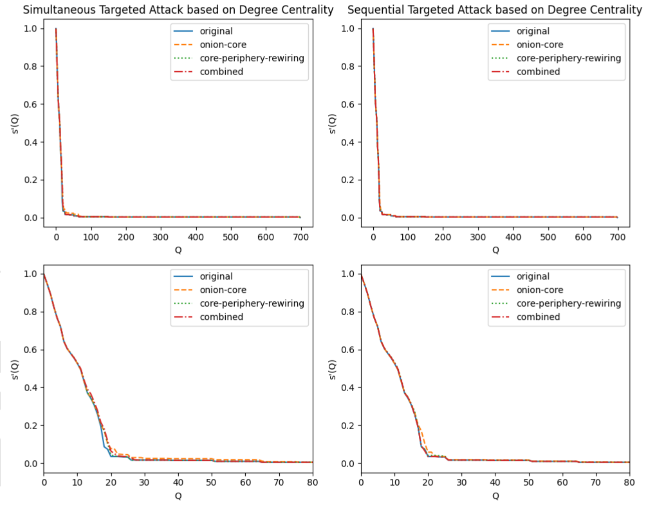

Fig. 3. Robustness score of the Telegram network after simultaneous (left) and sequential (right) targeted attacks based on degree centrality. The y-axis denotes the normalized size of the largest connected component and the x-axis denotes the number of removed nodes. The bottom row includes an inset focusing on the first 80 node deletions.

Since the network has a small core, its robustness declines relatively fast after the first attacks, which target core nodes. This happens because nodes in the periphery are sparsely connected to each other and are more connected to the core. In this network, our second strategy does not perform well, as there is not a sufficient number of core nodes to rewire the core-periphery edges towards them and let high importance core nodes be connected mostly to other core nodes. However, our first strategy works better than before, suggesting that there is a less homogeneous degree distribution in the core compared to the case of the synthetic networks.

Betweenness centrality-based attacks. Our strategies perform poorly in the scenarios of targeted attacks based on betweenness centrality.

In networks with a CP structure, nodes in the core exhibit an homogeneous distribution of betweenness centrality values, while peripheral nodes have a much lower and close to zero centrality. In fact, the betweenness centrality measures are mainly driven by shortest paths from and/or to peripheral nodes, since the core is densely connected. Therefore, our first strategy will not change the structure of the core in a relevant way.

The second strategy is also not the well suited for this problem. In fact, assume we swap two edges and connect a core node with low importance with a periphery node. In the subsequent iteration, when centrality values are recomputed, that core node will have a higher value, therefore will be less likely to be selected for another swap, meaning that it will be less likely to be connected to another peripheral node. Therefore, the connections to the periphery will become more homogeneously distributed over all core nodes. This strategy might enhance the robustness of the network, but not in the way it is intended for, which is by connecting multiple peripheral nodes to few core nodes and connecting highly important nodes only to other core nodes.

Thus, we developed a new strategy: at each iteration, we select the core node with highest betweenness centrality, we will call it ”node 1”, and we randomly select a second core node, with weights that are inversely proportional to their centrality value, we will call it ”node 2”. Then, we randomly select one edge from node 1 to the periphery and one edge from node 2 to the core. If they exist and do not overlap, we swap them.

We simulated both the second strategy and the new strategy in a synthetic ER network with parameters $n_1 = 100$, $n_2 = 100$, $p_{11} = 0.6$, $p_{12} = 0.1$, $p_{22} = 0.01$. As shown in Fig. 4, both strategies result in a similar increase in robustness of the network.

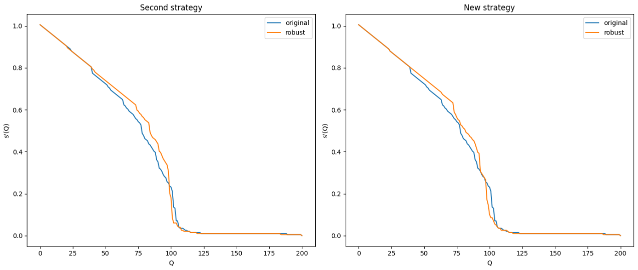

Fig. 4. Robustness score of the simulated network after a sequential targeted attack based on betweenness centrality. The y-axis denotes the normalized size of the largest connected component and the x-axis denotes the number of removed nodes. The simulation performed on the network after we applied the second strategy (left) and the new strategy (right).

Discussion

We reviewed previous studies on the robustness of core-periphery structures. We analysed the relationship between core-periphery structure of a network and its resilience. We found that as the core-periphery structure is dismantled, the network becomes more resilient to targeted attacks based on specific centrality measures. Then, we developed three strategies to strengthen the network against these types of attacks. However, these strategies present some limitations. For instance, one of the limits of the second strategy is that, after a sufficiently large number of iterations, low importance nodes in the core may have almost all edges connected to peripheral nodes and few edges connected to other core nodes. Another limitation is in the first strategy: as previously mentioned, its impact is quite limited when core nodes have a homogeneous importance distribution.

Future research can focus on overcoming these limitations, or it could analyze how the connections of core and periphery determine the robustness of the network. Moreover, our paper focuses on intentional attacks on nodes, while attacks on edges are another significant area of research that can be explored.

Bibliography

1. D John C., et al., The “robust yet fragile” nature of the internet. *Proc. Natl. Acad. Sci. United States Am.* **102**, 14497–14502 (2005).
2. E Yanchenko, S Sengupta, Core-periphery structure in networks: a statistical exposition (2023).
3. B Yang, et al., Optimizing robustness of core-periphery structure in complex networks. *IEEE Transactions on Circuits Syst. II: Express Briefs* **68**, 3572–3576 (2021).
4. MP Rombach, MA Porter, JH Fowler, PJ Mucha, Core-periphery structure in networks (2013).
5. M Kitsak, et al., Identification of influential spreaders in complex networks. *Nat. Phys.* **6**, 888–893 (2010).
6. RJ Gallagher, JG Young, BF Welles, A clarified typology of core-periphery structure in networks. *Sci. Adv.* **7** (2021).
7. SP Borgatti, MG Everett, Models of core/periphery structures. *Soc. Networks* **21**, 375–395 (2000).
8. TP Peixoto, S Bornholdt, Evolution of robust network topologies: Emergence of central backbones. *Phys. Rev. Lett.* **109** (2012).
9. PC de Simon, M Boguna, Double percolation phase transition in clustered complex networks (2014).
10. M Newman, Chapter 14 in *Networks.* (Oxford), pp. 498–514 (2018).
11. A Bovet, Complex networks: 03 - centrality measures (2023) Lecture slides for MAT933 - Autumn 2023. Email: alexandre.bovet@math.uzh.ch.
12. HAQ Tran, A Namatame, A Widyotriatmo, E Joelianto, An optimization procedure for enhancing network robustness against cascading failures in *the 2014 Seventh IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA).* pp. 1–7 (2014).
13. CM Schneider, AA Moreira, JS Andrade, S Havlin, HJ Herrmann, Mitigation of malicious attacks on networks. *Proc. Natl. Acad. Sci.* **108**, 3838–3841 (2011).
14. A Beygelzimer, G Grinstein, R Linsker, I Rish, Improving network robustness by edge modification in *Elsevier.* Vol. 357(3), pp. 593–612 (2005).
15. S Iyer, T Killingback, B Sundaram, Z Wang, Attack robustness and centrality of complex networks. *PLOS ONE* **8**, 1–17 (2013).
16. A Bovet, Replication Data for: Organization and evolution of the UK far-right network on Telegram (2022).
17. S Kojaku, N Masuda, Core-periphery structure requires something else in the network. *New J. Phys.* **20**, 043012 (2018).