Vulnerabilities of complex networks

Melvyn Tyloo (m.s.tyloo@exeter.ac.uk)
(Dated: June 17, 2026)

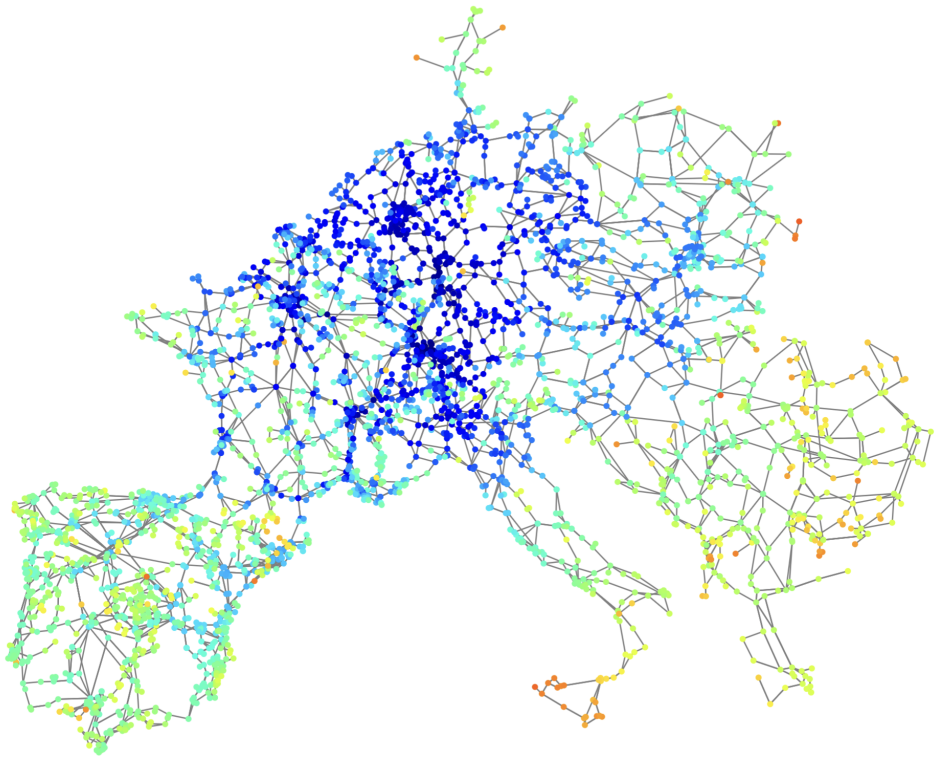

FIG. 1. Complex network modelling the high-voltage transmission power grid of continental Europe. The colours correspond to the resistive centrality of the nodes [1].

Complex networks [2] are mathematical tools that are useful to describe the interaction or relationship between multiple individuals. They are made of two ingredients: nodes and edges. The nodes correspond to the individual units, and the edges describe the connection or interaction between the nodes. To make it more clear, let us list a few concrete examples where complex networks are useful. The internet network is composed of computers and routers that exchange information. In this case, each computer or router can be modelled as a node. The cable or wireless connection between a pair of computers or routers can be modelled as an edge. In electric power grids, the generators and substations connecting different voltage levels can be represented as nodes, while the transmission lines are represented by edges. Complex networks are also useful in biology. For example, in the brain, neuronal cells can be modelled as nodes in a network where the edges corresponds to the synaptic coupling that enables communication amongst the neurons. These are just a few examples where complex networks are a powerful mathematical tool to model and understand the system.

Let us discuss how to mathematically describe a complex network. Formally, we say that a complex network is a graph with (i) a set of nodes identified by their index $\mathcal{N} = \{1, 2, ...N\}$ where the number of nodes is $|\mathcal{N}| = N$; (ii) a set of edges $\mathcal{E} = \{e_1, ...e_M\}$ with $|\mathcal{E}| = M$ the number of edges and where each edge is a pair of node indices, i.e. $e_1 = (1, 2)$ would correspond to an edge between node 1 and 2. Here, we will focus on undirected networks, meaning that the order of the node indices for each edge is not important, i.e. $e_1 = (1, 2)$ and $e_2 = (2, 1)$ represent the same edge. The set of nodes and edges of a complex network can be intuitively encoded in the *adjacency matrix* of the network. The latter is a table of N rows and N columns defined as,

$$A_{ij} = \begin{cases} 1 \text{ if there is an edge between node } i \text{ and } j \\ 0 \text{ if there is no edge between node } i \text{ and } j\,. \end{cases} \tag{1}$$

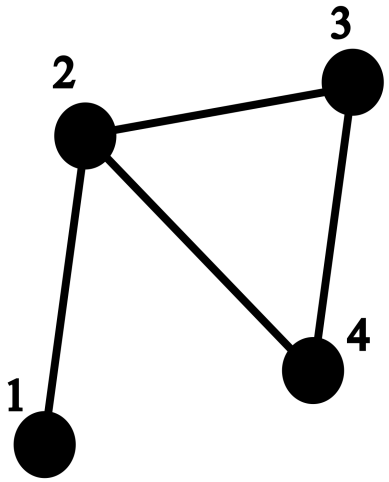

FIG. 2. Network with 4 nodes and 4 edges.

for $i, j = 1, ...N$. Each row/column corresponds to a node in the network. Let us look at a concrete example. Consider the network shown in Fig. 2 . The adjacency matrix for this network reads,

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} . \tag{2}$$

The first row/column of the matrix corresponds to node 1 which has a single edge connecting it to node 2 . Therefore, one has $A_{12} = A_{21} = 1$ and the other entries of the first row/column are set to zero. Node 2 has three edges connecting it to nodes 1, 3, 4, which are represented by the three entries set to 1 in the second row/column. One can proceed similarly for the two remaining nodes.

Now that we have a way to describe a complex network, let us consider metrics that characterize network properties and allow to differentiate one from another.

1. **Node degree**: The degree of node i , denoted k_i , is the number of edges that are linked to it. It can be obtained from the adjacency matrix by summing all the entries in the row or column corresponding to the node, i.e. $k_i = \sum_{j=1}^{N} A_{ij}$.

2. **Shortest path distance**: The shortest path distance between node i and j is the smallest number of edges one needs to follow to go from node i to j . Using the shortest path distance, one can compute the shortest path centrality of node i defined as $c_i = \frac{1}{\sum_{j=1}^{N} d_{ij}}$. To obtain a gloabl network metric, one can also compute the average shortest path distance as $\overline{d} = \frac{1}{N^2} \sum_{i,j=1}^{N} d_{ij}$.

3. **Betweenness centrality**: The betweenness centrality of node i , corresponds to the number of shortest paths that go through node i .

4. **Largest component**: A network does not need to be made of a single component where there exists a path between every pair of nodes. It can be that the network is composed of disconnected components. The largest component is the largest group of nodes such that there exists a path between each pair of nodes within the group. To characterize the largest component, we define the fraction of nodes that belongs to it as $F = \frac{N_L}{N}$ where N_L is the number of nodes in the largest component.

Exercise: *Compute all the three metrics for the network shown in Fig. 2 .*

The metrics defined above are useful to identify the vulnerabilities of complex networks. There are many ways one can define the vulnerability of a network. Here, we are going to focus on the size of the largest component, and how it is reduced by different attack strategies. We want to compare the vulnerability defined this way, for different types of complex networks.

Project: *We first consider the synthetic networks shown in Figs. 3, 4 .*

1. *Define indices for the nodes, and build the network adjacency matrix for each network.*

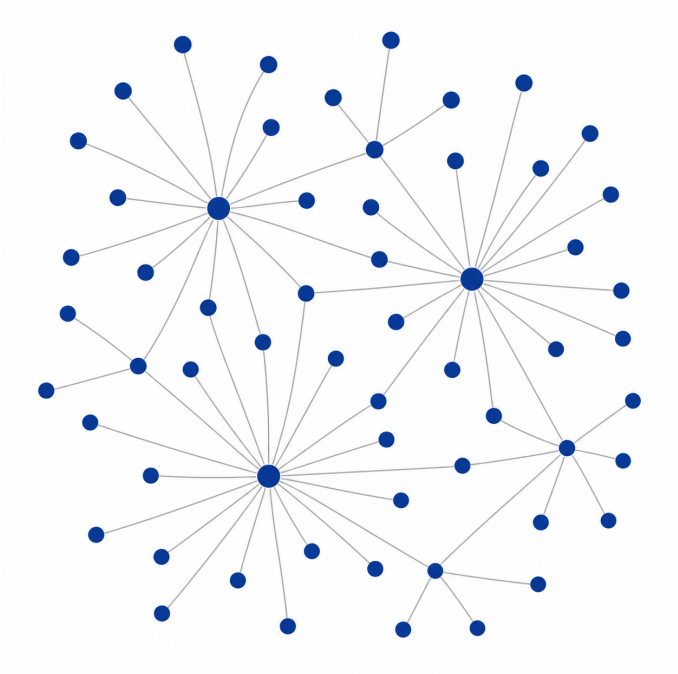

FIG. 3. Network 1

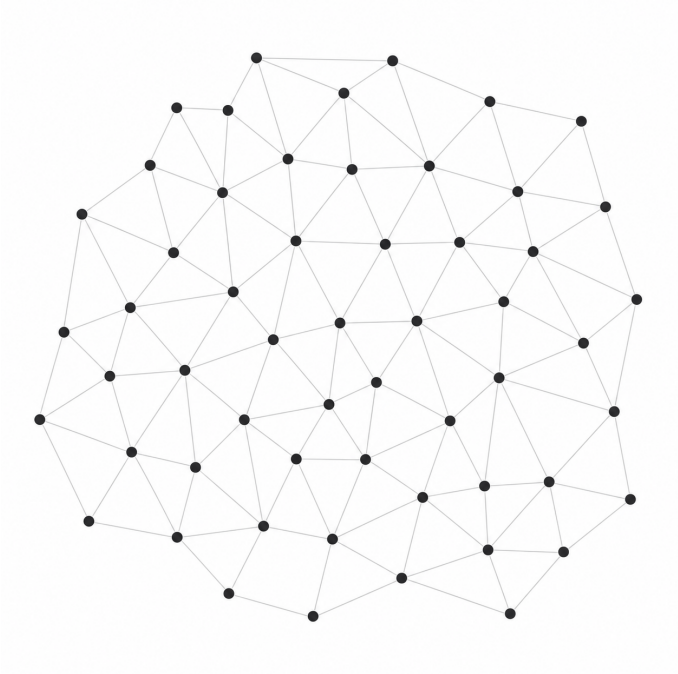

FIG. 4. Network 2

2. *Find the degree of each node for both networks and compare the two degree distributions.*

3. *Compute the shortest path centrality and the average shortest path distance for each network, and compare them.*

4. *For each network, identify the nodes with the largest betweenness centrality.*

We are now interested in investigating how the fraction of nodes in the largest component evolve when nodes are sequentially removed from the networks. To do that, count the number of nodes in the largest component when the following attack strategies are applied:

1. *Iteratively select a node at random in the largest component and remove it.*

2. *Iteratively select the node in the largest component that has the highest degree and remove it.*

3. *Iteratively select the node in the largest component that has the highest shortest path centrality and remove it.*

Eventually, use the results to identify which network structure is the most robust for each attack strategy.

Going further: *Instead of using the synthetic networks shown in Figs. 3, 4 , find real-world networks from different fields such as transportation networks, social networks or biological network, and redo the above analysis using these networks. These networks can be found in databases or extracted from available images, e.g. a highway road network from a map. Identify the difference between the types of networks using the metrics defined above and compare their vulnerabilities when applying the above attack strategies. You can consider the additional strategies:*

1. *Iteratively select the node with the largest betweenness centrality and remove it.*

2. *Devise yourself an attack strategy based on the edges instead of the nodes.*

---

[1] The key player problem in complex oscillator networks and electric power grids: Resistance centralities identify local vulnerabilities, Science advances **5**, eaaw8359 (2019).
[2] M. Newman, *Networks* (Oxford university press, 2018).