# 4. Analysis

## 4.1 Robustness

The goal of our analysis was to test the robustness of the Swiss Railway network, or in other words, to measure the connectedness of the network in case of failures or attacks on the network. For this purpose, we removed nodes or edges from the network in a random or targeted fashion. This simulates failures or disasters on certain routes or in certain train stations. Then we observed the effects of this simulation on the development of the biggest connected component in the network.

## 4.1 Random vs targeted attacks

Testing the robustness of the network by removing random nodes shows the stability of the network. If you start removing nodes randomly you need to remove over 200 nodes to half the size of the giant component. If you remove over 500 nodes the network is almost completely broken down and less than 10 % of the network is connected in one giant component.

Compared to random failures, targeted attacks on the network, as seen in Figure 2, breaks down the giant connected component a lot faster. After removing the 100 most central nodes, based on degree centrality, the biggest connected component is only about 1/6th of the giant connected component from the original network.

Figure 1: Random attacks on the Swiss rail network

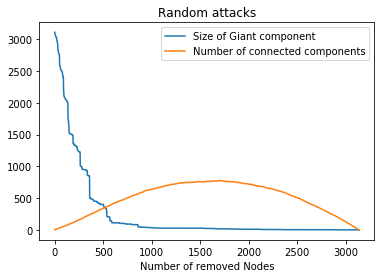
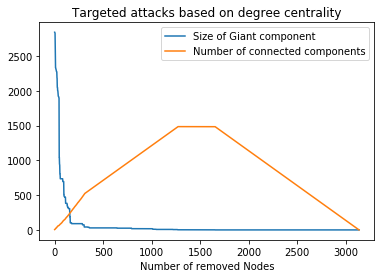


Figure 2: Targeted attacks on the Swiss rail network

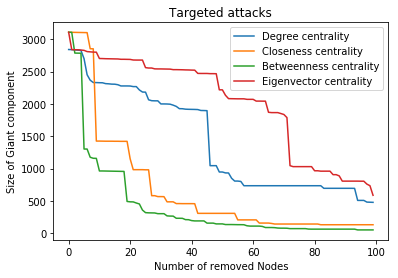


## 4.3 Different targeted node attacks

If we compare different centrality measures on the network, we find very different results. Degree centrality and eigenvector centrality show “Zürich, Altstetten” and “Zürich, Langstrasse” as the most central nodes. Both of those are very close together and in close proximity of the “Zurich, Main station”, which is the biggest train station in Switzerland and one of the most frequented train stations of the world. Compared to those measures, the most central node according to the closeness centrality measure is the station “Olten, Bhf”, which lies in the center of the railway network and right in the center of the cities of Zurich, Bern and Basel. The most central node according to the betweenness centrality is the station “Wanzwil” near Herzogenbuchsee, this is a station that might be geographically in the center of the network but does not hold any significance to the Swiss railway system. -> seems to be significant in the Figure3!!!

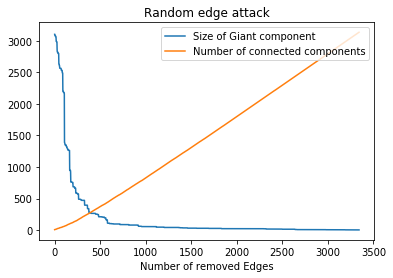
Comparing the importance of these different measures, we simulated a targeted attack on the network by removing 100 nodes according to these different centrality measures. As seen in Figure 3, removing nodes based on the betweenness centrality was the most effective way of breaking down the giant connected component. Followed by the strategy of removing the nodes based on closeness, degree and eigenvector centrality.

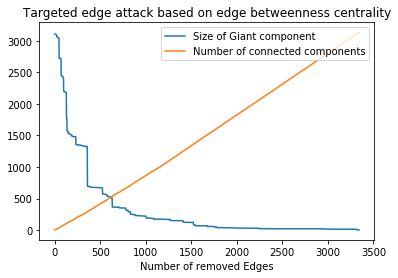
Figure 3: Targeted attacks on 100 nodes of the Swiss railway network



## 4.2 Attacks on nodes vs. Edges

While failures that take down an entire train station and stops any train from passing trough it, do happen, they are rarer than failures on a certain track that stops all traffic from using that connection. This leads us to also simulate the failure of multiple edges of the railway network. As before, with the attacks on nodes, we also simulated random and targeted attacks on the edges of the network. As a measure of centrality, we used the edge betweenness centrality. As in the simulation before, the targeted attacks were more effective in breaking down the giant connected component than random failures.





## 4.3 Comparison to random networks

References ?

Random graph models are frequently used to predict the behavior of networks with pretended characteristics. These characteristics are for example the degree distribution or the global clustering in the network. To compare the behavior of the Swiss Railway network to failures, we used an Erdös-Renyi (ER) random model as well as a Barabási-Albert (BA) random model.

When creating an ER random model a graph with a given number of nodes is generated. Between every pair of node, with probability p, an edge is added to the graph. This random generated model are characterized by a degree distribution, which follow a poisson distribution with <k> = n\*p as well as a clustering coefficient close to the edge creation probability p.

The degree distribution of many networks observed in reality do no not follow a poisson distribution. Therefore the need for random models with different characteristics arises. Often observed networks follow a power-law distribution of node degrees. The power-law distribution is characterized by the existence of a very high number of low-degree nodes and the existence of few nodes with very high degree. Since the Swiss Railway network has a high number of nodes with degree equal to two and only a few nodes that have a degree up to 7, it might be worth to compare the network to a random graph following a power-law distribution. An example of such a random graph is the BA model. This model incorporates the two mechanisms «growth » and «preferential attachment» which are often observed in reality and lead to power-law distributions. The nodes in the BA random graph are created one after another and every new node is connected to a given amount of existing nodes, where nodes with higher degree are preferred.

The theoretical characteristics of the two random graph models suggests that ER graphs are equally vulnerable to random as well as targeted attacks. BA graphs on the other hand are more vulnerable to targeted attacks than to random attacks. That is because when the nodes fail randomly, the probability is high, that a low degree node fails. In contrast targeted attacks might aim at high degree nodes.

# 5. Conclusion

Even though small parts of the network can be disconnected from the giant component quite easily, the giant connected component is quite robust on random failures of the network. Sure the capacity of trains might be impacted if an important node or edge of the network is defective, but the overall connectedness of the network only starts to break down if hundreds of nodes or edges fail at the same time.

Further analysis has shown that the Swiss railway network is at risk of targeted attacks. If it would be possible to break down the traffic in 10 selected stations the whole network would be cut down significantly. Even the biggest connected part of the remaining network would be less than half as big as it was before.