der Bundeswehr
Universität München

# Aggregation-based Decision Support Framework for Resilience Analysis of a Transportation Network

Zhonglin Wang

Vollständiger Abdruck der von der Fakultät für Informatik der Universität der Bundeswehr München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation.

Gutachter:

1. Univ.-Prof. Dr. Stefan W. Pickl
2. Univ.-Prof. Dr. Oliver Rose

Die Dissertation wurde am 19.11.2020 bei der Universität der Bundeswehr München eingereicht und durch die Fakultät für Informatik am 13.04.2021 angenommen. Die mündliche Prüfung fand am 20.05.2021 statt.

# Abstract

As one example of critical infrastructures, the German high-speed train network (ICE) is a prime target for terrorism. To decrease the impact of attacks, key stations need to be identified as the most likely targets. One approach for doing so is modeling the network as a graph and then applying suitable graph measures to it.

The central concern of this thesis is the fact that there is a large number of old and new measures, which all provide their unique perspective, but which eventually lead to an information overload for the decision-makers.

The solution presented takes the "Technique for Order Preference by Similarity to Ideal Solution" (TOPSIS) from Multi-criteria Decision Making field (MCDM) and adapts it to produce a new aggregation framework of different graph measures. For the vital step during this process, a novel, mathematical methodology is being presented, replacing the traditional expert knowledge needed.

Furthermore, to verify the effectiveness of the aggregation measure compared to other graph measures, a new network performance metric is being introduced and validated. As an outlook, a special vector-based approach based on the obtained results is addressed.

# Zusammenfassung

Als Beispiel für kritische Infrastrukturen ist das deutsche Hochgeschwindigkeitszugnetz (ICE) ein vorrangiges Ziel des Terrorismus. Um die Auswirkungen von Angriffen zu verringern, müssen wichtige Stationen als die wahrscheinlichsten Ziele identifiziert werden. Ein Ansatz hierfür besteht darin, das Netzwerk als Graph zu modellieren und dann geeignete Graph-Maße darauf anzuwenden.

Das zentrale Anliegen dieser These ist die Tatsache, dass es eine große Menge von alten sowie neuen Maßen existiert, die alle ihre einzigartige Perspektive anbieten, allerdings letztendlich zu einer Informationsüberflutung für die Entscheidungsträger führen.

Die vorgestellte Lösung übernimmt die Methode "Technique for Order Preference by Similarity to Ideal Solution" (TOPSIS) aus dem "Multi-Criteria Decision Making" (MCDM) Feld und passt diese TOPSIS, damit ein neuer Aggregationsrahmen verschiedener Graph-Maßen erstellt wird. Für den entscheidenden Schritt während dieses Prozesses wird eine neuartige mathematische Methodik vorgestellt, die das erforderliche traditionelle nötige Expertenwissen ersetzt.

Darüber hinaus, wird zur Überprüfung der Wirksamkeit der Aggregationsmaß im Vergleich zu anderen Graph-Maßen eine neue Netzwerkleistungsmetrik eingeführt und validiert. Als Ausblick wird ein spezieller vektorbasierter Ansatz nach den gewonnenen Resultaten angesprochen.

# Acknowledgments

This work was developed during my time as a research associate at the Institute for Theoretical Computer Science, Mathematics and Operations Research at the University of the Bundeswehr (German Armed Forces) in Munich.

First of all, I want to express my deep gratitude to my supervisor, Univ.-Prof. Dr. Stefan Pickl, for giving me the opportunity to write the thesis at the institute and for granting me all the scientific freedom during the work. His open-minded and unreserved support led to many valuable and fruitful discussions. Without his support, constructive feedback and time for fruitful conservations, this dissertation would not have been possible.

Furthermore, I warmly thank all my colleagues for the open and intensive discussions on plenty of research topics and for providing a good working atmosphere. Among them, I want to mention especially Dr. Marian Sorin Nistor, Dr. Maximilian Moll, Gonzalo Barbeito and Dr. Truong Son Pham, who inspired my work with numerous discussions, and also Christine Strobel, Andrea Ferstl and Verena Krüger, who did the proofreading of my thesis.

Finally, I would like to thank my family for always staying by my side and support me. Their steady encouragement has given me the necessary strength, confidence and optimism.

# Table of Contents

# 1 Introduction

## 1.1 Motivation: Critical Infrastructure, Terror Attacks and Vulnerability

As the USA PATRIOT Act pointed out, the critical infrastructures are those "systems and assets, whether physical or virtual, so vital to a country that the incapacity or destruction of such systems and assets will have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Amoaning-Yankson 2013, Rinaldi 2004, Seager et al. 2017, Todorovic et al. 2017). The critical infrastructures consist of a lot of sectors, including chemical and commercial facilities as well as communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors including materials and waste, transportation systems as well as water (White House 2013). These critical infrastructures provide us with the essential functions and "services that underpin our society and serve as the backbone" of a country (Dinh 2010). These critical infrastructures are so essential and vital that once they are disturbed by adverse events, such as natural disasters or unintended accidents (Dinh 2010), our lives will be affected to a large extent. Especially terrorist attacks could mostly result in lots of casualties and economic losses. According to the Global Terrorism Database (START 2021), in total, there are 201,183 terrorist acts happened worldwide from 1970 to 2020. As one of the critical targets, more than 7,000 terrorist attacks were aiming at transportation systems, whose percentage is shown in Figure 1.1. Moreover, due to characteristics such as the accessibility, affordability, and availability of transportation systems, once the elaborately planned terrorist attacks (Keeney and Winterfeldt 2010) happen on the transportation systems, they would always lead to a large number of casualties, economic losses and maybe even other unpredictable incidents.

For example, the September 11 attacks, which happened in the United States on September 11, 2001, resulted in 2,996 people killed, over 6,000 others injured, at least USD 10 billion in property and infrastructure damage, and USD 3 trillion in total costs. Sadly, in the following few years, the terrorist attacks aiming at transportation systems were continuing, for instance the train bombings that happened in Madrid on March 11, 2004, which resulted in 192 people killed and around 2,000 people injured. And since the Madrid train bombings occurred three days before Spain's general elections, this therefore also had some political effects. Nevertheless, on July 7, 2005, another train bombing happening in London resulted in 52 people killed and 784 people injured. On July 11, 2006, during the Mumbai train bombings, 209 people were killed and more than 700 were injured. Even recently, on March 22, 2016, the train bombing happening in Brussels caused the death of 14 people and more than 200 people were injured.

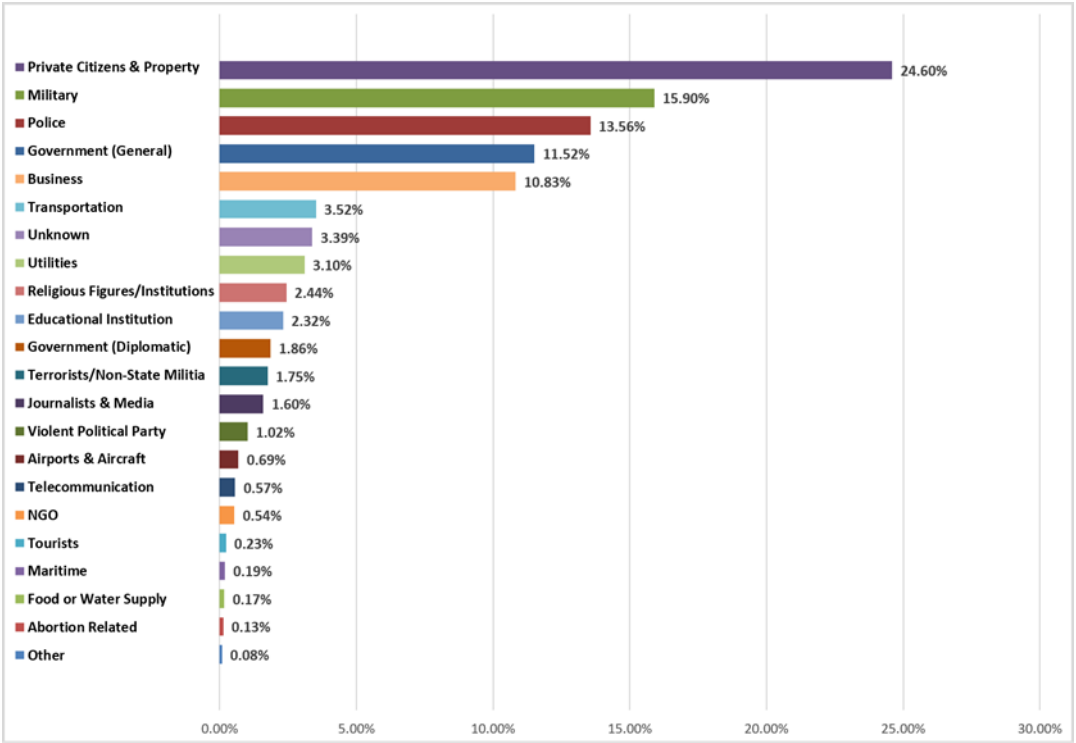



Figure 1.1: Percentages of terrorist incidents aiming at different kinds of targets

As we know, after the September 11 attacks, the security checks of air transport systems around the world have become much stricter. Therefore, air transport systems have become much harder to be attacked by terrorists.

However, comparing to air transport systems, other public transport systems, such as bus transport systems, metro systems in a city or train transport systems in a country, will still be easy to access because of less security checks, especially in European countries like Germany, where all of the bus, metro, and intercity train transport systems are open for everyone to access without any security checks. Therefore, they are easier targets for terrorists (Keeney and Winterfeldt 2010). Therefore, it is vital for decision-makers of governments to know which station (or city) has more potential to be attacked by terrorists in a metro transport system (or intercity train transport system). Afterward, they can decide to deploy more security resources in advance around these key stations (or cities). When the terrorist attacks happen in these key spots, governments can respond quickly, and social panic, economic loss as well as casualties would be reduced to a lower level. Meanwhile, the system can be recovered to a normal operation level quickly. Furthermore, if one potential terrorist attack is reported by some people in advance, the governments can take quick and effective measures to prevent it from happening.

Shocked but also motivated by these terrorist attacks, researchers and governments have been trying to find some solutions on how to prevent these kinds of horrible incidents from happening and how to reduce their impacts. It is very necessary, important and significant to detect especially the key parts or spots of critical infrastructures which have more potential to be hit by deliberately and meticulously planned terrorist attacks, because when the terrorist attacks happen at these vital parts, they are likely to cause a massive panic of society, economic loss and even enormous casualties. Normally, researchers try to resolve this kind of problem from two perspectives:

On the one hand, there is *qualitative analysis*; for example, risk analysis can solve problems by answering questions such as: what kinds of weapons terrorists may use; how many weapons they will use; how large the destructions of each kind of weapon can be, and so on. However, this is actually not the focus of our research. On the other hand, there is *quantitative analysis*, which is a solution-oriented approach, and it is also the central aspect we consider in this thesis. To identify the essential spots of critical infrastructures, we focus on first implementing some existing mathematical algorithms and their diverse improved variants.

Furthermore, we also develop *new methods* to identify the significant spots. Up to this stage, we have applied multiple approaches to detect the critical spots in a system. But because different approaches will lead to distinctive results, applying multiple methods together will result in information overflow for decision-makers. Therefore, for the sake of resolving the issue of information overflow, we adapt and improve an aggregation technique from the Multi-criteria Decision Making (MCDM) field (Muruganantham and Gandhi 2016) to aggregate many approaches into a new comprehensive method in order to identify the key spots. After that, in order to verify and validate the effectiveness of the aggregation approach (that is, whether it is a promising, much more suitable and practical approach that can detect the critical spots of critical infrastructures), we conduct the quantitative resilience analysis by developing a new network performance metric.

## 1.2 Background

As one of the critical infrastructures, transportation systems are strictly related to us and play a significant role in our life. Every day, hundreds of millions of people around the world commute or travel by public transport systems. Especially because of the lower price and much easier access than air transport systems, most common public transports are the bus transport or metro system in a city, or the train transport system connecting almost every city in nearly every country.

Moreover, all of these public transport systems have one specific network character, which means that they can be abstracted into mathematical models. Therefore, researchers can analyze these public transport systems from a mathematical point of view.

In the field of mathematics, especially when studying the characteristics of a complex network, some approaches based on graph theory can be used. Over the last several decades, the importance of assessment of nodes in complex networks has so far drawn wide attention from researchers and practitioners from diverse fields. In a network, to identify the critical nodes is one crucial research.

However, due to the fact that it is a complex network with an essentially non-homogenous topology, thus, the importance of nodes (which are distinctive from each other) in the given network are determined. To unearth and detect the critical nodes in various complex networks and then specifically analyze the properties of these critical nodes has essential significance on how to take advantage of them effectively. For instance, in a criminal relationship network, the importance ranking of every member can help distinguish who is a primary criminal member, who are backbone criminal members and who are just followers.

This can help to quickly locate the leader of criminal gangs. It has high practical value to conduct the importance analysis of nodes for detecting the critical nodes on the specific networks (Gaertler 2005), such as social networks, research cooperation networks, power networks and especially transportation networks, under terrorist attacks. Because once decision-makers have realized which parts are the most critical points, they can deploy security resources in advance around these points to protect them from being destroyed or at least reduce the impacts of such terrorist attacks to a certain relatively low extent.

During my studies for Ph.D., I was involved in the German-French joint project RE(H)STRAIN (REsilience of the Franco-German High-Speed TRAIn Network) (Amokrane et al. 2017, RE(H)STRAIN 2021), led by my supervisor Prof. Pickl, and collaborated with other significant research partners between Germany and France. This project was funded for two years by BMBF and ANR (RE(H)STRAIN 2021).

In this project, the objective was to analyze the vulnerability of rail-bound DE-FR high-speed train systems (ICE, TGV) as a part of critical infrastructure transport under threats from terrorism as well as the derivation of measures for the improvement of their resilience.

But, in this dissertation, our research object is mainly focusing on the German high-speed train network (ICE network) (Deutsche Bahn 2018), shown in Figure 1.2 as critical infrastructure. The German ICE network is obtained from Deutsch Bahn. The analysis at hand is based on the data from Deutsche Bahn (2018):

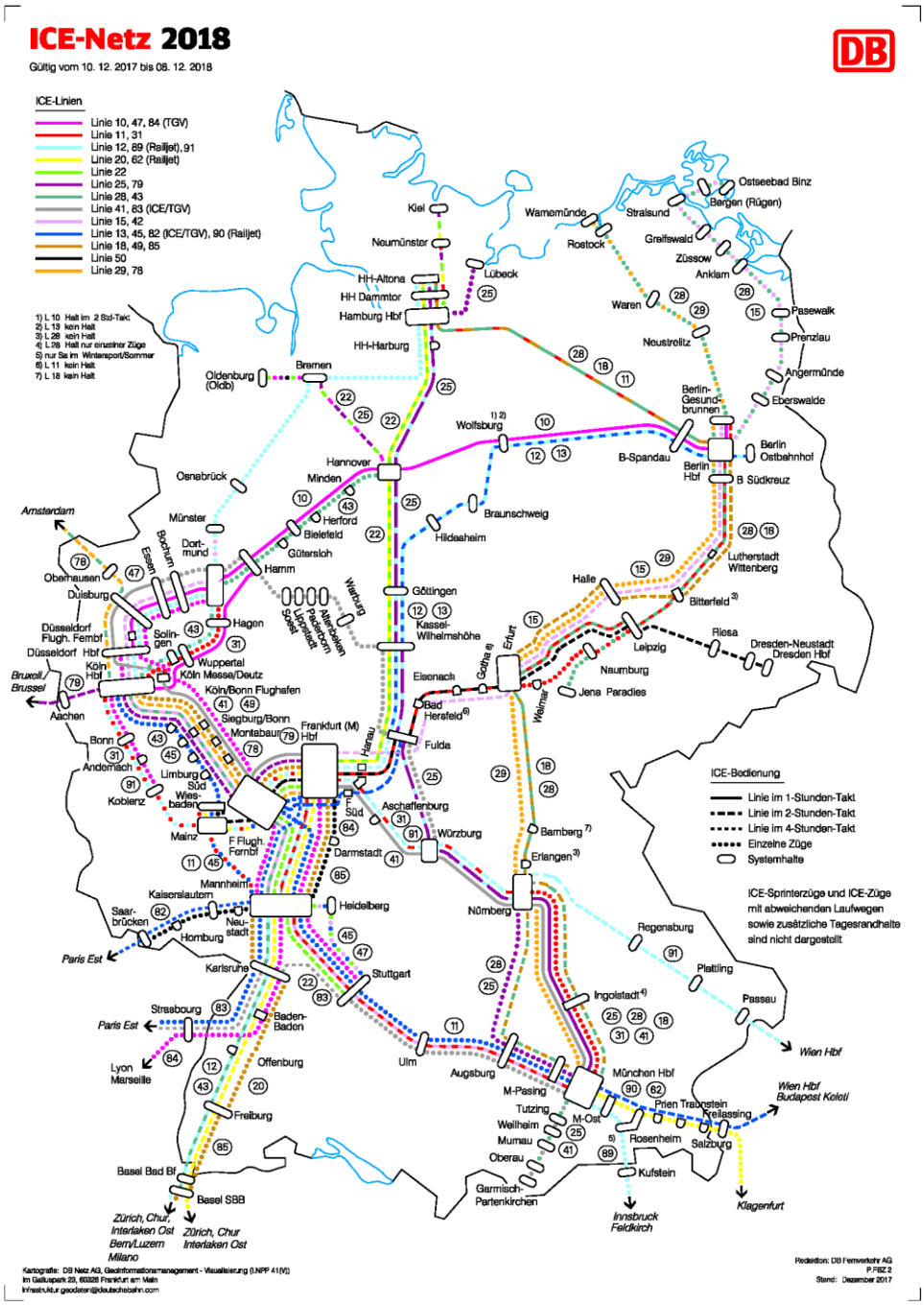



Figure 1.2: German ICE train network

The aim of this thesis is to establish a new kind of network modeling with a suitable analysis measurement.

### 1.2.1 Network Modeling and Network Technologies

As aforementioned in this chapter, in this thesis, the research object is the German high-speed railway transportation system (ICE train network). As shown in Figure 1.2, the ICE train network consists of 121 stations and 168 links between stations.

Due to the mesh characteristic of the ICE train network, based on graph theory, we thus abstract it as an undirected weighted graph $G(V,E)$ shown in Figure 1.3, where $V=\{v_i \mid i=1,2,3,...,n\}$ represents the set of nodes (stations) and $E=\{e_{ij} \mid v_i, v_j \in V\}$ denotes the set of edges (the links between each pair of stations) of the network. The matrix $A=[a_{ij}]_{n\times n}$ is the weighted adjacency matrix, where $a_{ij}=\omega_{ij}$ if $(v_i, v_j) \in E$, otherwise, $a_{ij}=0$.

Here, $n$ denotes the number of nodes in a graph and $\omega_{ij}$ the distance length between every pair of adjacent nodes with the unit of 100 km.

In order to compute the flow-weighted efficiency measure (we will introduce it in Chapter 3) applied on the ICE network, another weighted adjacency matrix is considered:

We define $B=[b_{ij}]_{n\times n}$, where $b_{ij}=\varpi_{ij}$, if there is at least one train passing on the edge between the adjacent nodes $v_i$ and $v_j$, otherwise, $b_{ij}=0$. Here, $\varpi_{ij}$ represents the train flow defined as the number of trains passing through the edge between the adjacent nodes $v_i$ and $v_j$ in a day.

By applying the existing or the new proposed mathematical algorithms from the field of graph theory to graph model $G(V,E)$, we can deduce some structural characteristics of the original network and then detect and pinpoint which part or parts are critical ones that have a higher potential to be targets of terrorists based on Figure 1.3:

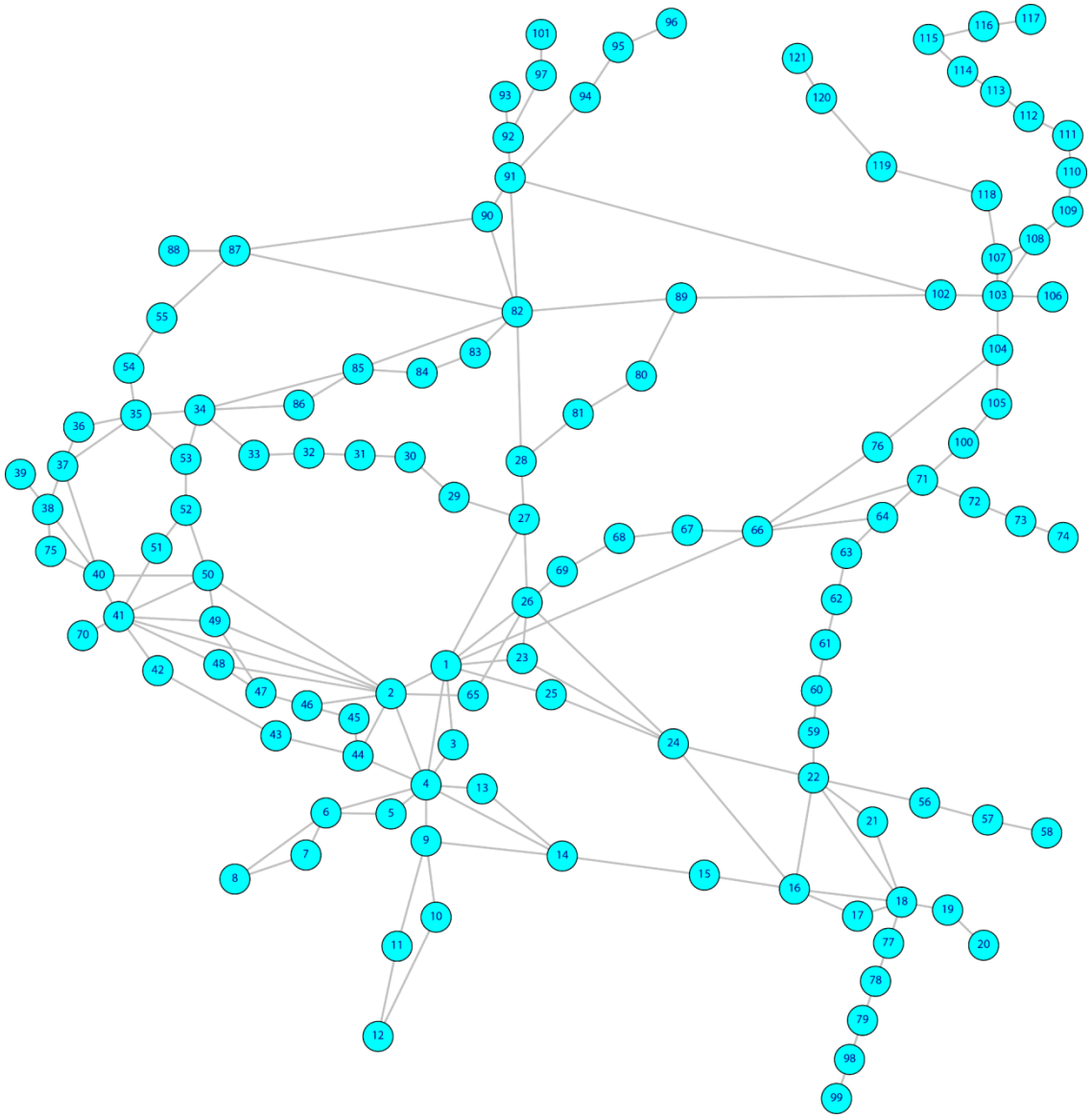



Figure 1.3: Graph model $G(V, E)$ of ICE train network

According to Figure 1.3, the following questions may now occur:

- Which single node (such as node 1) or which group of nodes (for instance group nodes 1,2,4) can be regarded as the critical nodes?
- Which measures can be applied in Figure 1.3 to identify these critical nodes?
- How to validate if the implemented measures applied in Figure 1.3 are suitable and effective to detect these critical nodes?

### 1.2.2 Vulnerability Measures and Multi-criteria Decision Making

In complex networks, to identify the crucial nodes using quantitative approaches has drawn considerable attention from researchers. Currently, there are two kinds of analysis methods. One approach is based on the idea "importance is equivalent to saliency" which means that the critical nodes in a network can be detected without destroying the integrity of the given network; commonly, these vital nodes can be identified by centrality measures like degree, betweenness, eigenvector, closeness centralities, and so on (Freeman 1978, Landherr et al. 2010). The other method is according to the idea "importance equals the damage extent of network structure after deleting certain nodes or set of nodes", which means that after removing the given nodes from a network, the given nodes can be seen as the key ones, if the change extent of network connectivity indicators is highest. In general, the key nodes can be detected using vulnerability measures.

Regardless of the method (or even its variant, which can also be used to identify the key nodes), so far, lots of researchers have mainly focused on one or finite kinds of characteristics related to the network structure and have analyzed the importance of nodes from one single perspective or few limited perspectives only. For instance, degree centrality emphasizes the number of its straightforwardly connected adjacent nodes, and it can show the importance to a certain extent, but the nodes with the same degree centralities are not of equal importance. Since one method analyzes the network from different points of view and is applied to a specific problem in different fields, complex networks in the real-world are various, and it is hardly only based on a single approach to demonstrate if one node is essential or not, because it will lead to a rather large one-sidedness when dealing with different network structures using only one method. It is known that "in graph theory the importance of a node in a network is related to the overall structure of the network" (Lü et al. 2016, Qi et al. 2012, Rueda et al. 2017, Wang et al. 2018). Thus, if we can make use of multiple structure-based node importance *indicators*, it could be useful and practical to comprehensively evaluate the significance of nodes from different perspectives.

In this thesis, we introduce a "Multiple-criteria Decision Making method based on the Technique for Order Preference by Similarity to an Ideal Solution (TOPSIS)" (Hwang and Yoon 1981), which can aggregate different measures (like network centrality measures, network nodal efficiency measures and network nodal vulnerability measures) into a new one, comprehensively analyzing the network for identifying the critical nodes from diverse perspectives. Furthermore, we present the details of TOPSIS and how to adapt them to this thesis in Chapter 3.

### 1.2.3 The Resilience of Complex Networks: Resilience Phases and Suitable Metrics

In the RE(H)STRAIN project, resilience is understood to be the ability of high-speed systems to maintain central functions and system states during and after the impact of threats and to restore impaired functions quickly. Generally, "the definition of resilience is the ability of a system to prepare and plan for, absorb, quickly recover from, and more successfully adapt to adverse events" (Cutter and Ahearn 2013).

When analyzing the resilience of a network, researchers primarily carry out the resilience analysis from two perspectives, namely qualitative and quantitative approaches. In this thesis, we mainly focus on the *quantitative resilience analysis*. So far, one general and easily understandable way is to represent resilience graphically by using performance curves, considering the time consumption.

For instance, Nan and Sansavini (2017) split system resilience into "four different phases, which are (i) original steady phase, (ii) disruptive phase, (iii) recovery phase, and (iv) new stable phase".

The detail of each stage is depicted in Figure 1.4; here, most of the researchers mainly focus on the disruptive and recovery phases to quantify the network resilience, because during these two phases the amount of time consumed can lead to different resilience levels of a network.

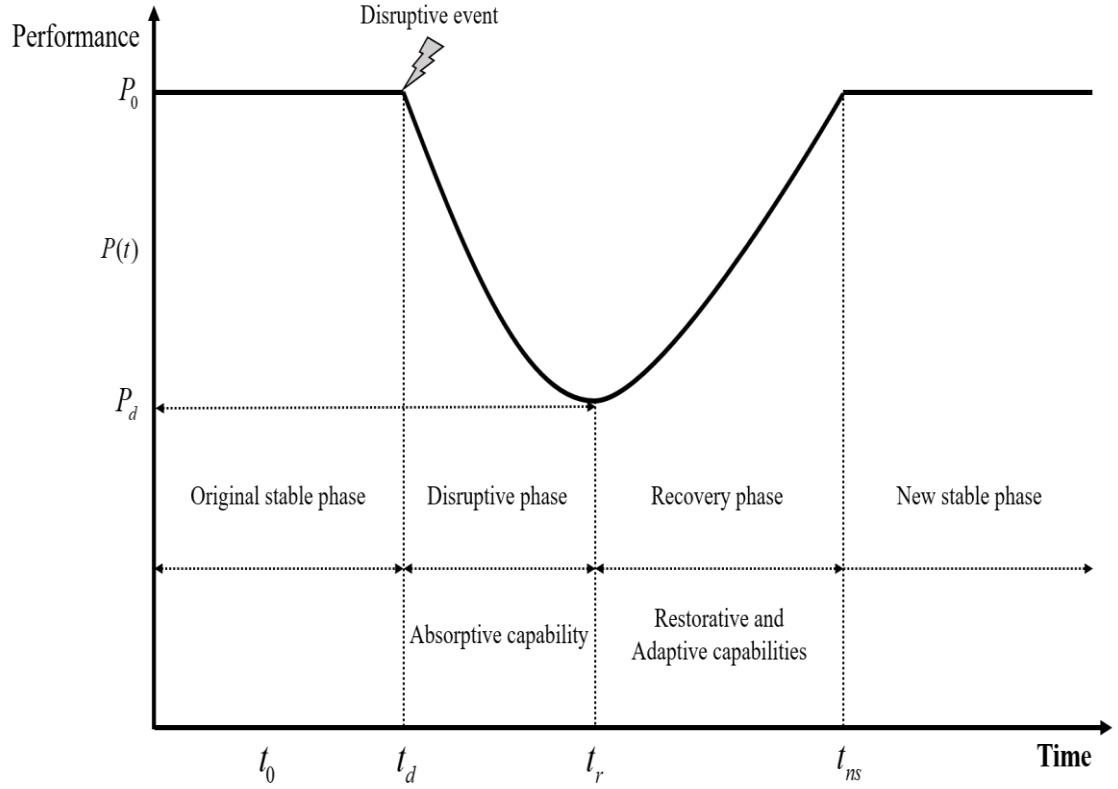



Figure 1.4: Resilience phases [adapted from Nan and Sansavini (2017)]

In this thesis, we suppose that the network performances in both the original steady phase and the new stable phase are the same. Furthermore, due to the fact that we mainly consider terrorist attacks as the disruptive events, the time consumed in the disruptive and recovery phases is thus not a necessary factor. Because in reality, once terrorist attacks happen, the whole network would probably almost immediately be shut down.

For instance, after the gun shooting that occurred in Munich in July 2016, all the local transportation networks, including subways, buses and trams were immediately shut down until midnight. Regarding the time consumed in the recovery phase, it depends on the decision-makers to carefully consider the corresponding status of the terrorist attacks in advance and then properly decide whether and when to let the network start to recover gradually until the network recovery is back to a completely normal state. In such a case, the distinctive phases in Figure 1.5 of network resilience are different from the ones in Figure 1.4.

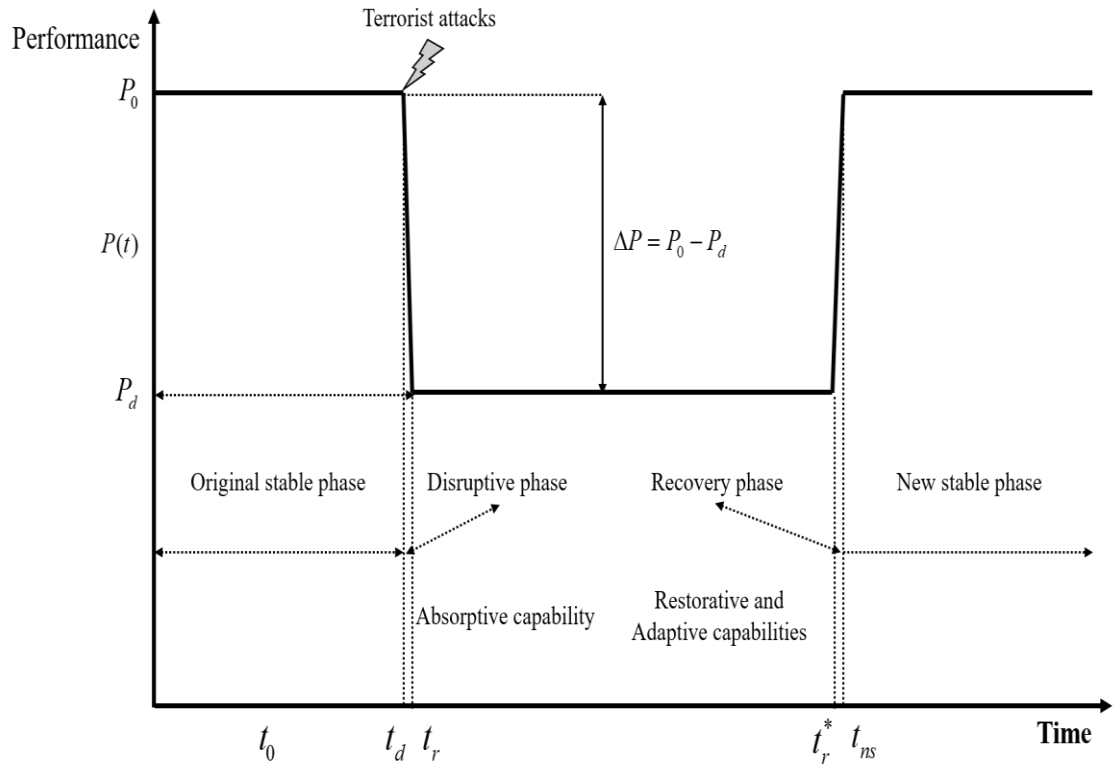



Figure 1.5: Different phases of network resilience when only considering terrorist attacks

Moreover, in this thesis, the resilience analysis on the ICE network is mainly used to compare the different implemented mathematical algorithms from the field of graph theory and conclude which algorithm is the most suitable and effective one for identifying the key stations (nodes) that have more potential to be attacked by terrorists.

Since one of the goals in our research is to reduce the information overflow for decision-makers, and network resilience can verify the effectiveness of the proposed comprehensive aggregation method; therefore, our research can help decision-makers understand the structural properties of the ICE network and provide proper advice for them to decide which spots or parts need more security resources in advance to protect them from being attacked by terrorists.

## 1.3 Scientific Approaches and Goals of Research

In the research activities, we first apply the existing network structure-based approaches like graph centrality measures to identify the critical spots in a network. However, we find that the results are not good enough in a certain sense; therefore, we have proposed two new vulnerability measures based on the existing methods.

But the more numbers of measures are applied (which will lead to more different results), the larger the information overflow for decision-makers, making it difficult to decide which result is more suitable and efficient.

In our research, based on TOPSIS (Hwang and Yoon 1981), considering the aggregation technique widely used in the field of Multi-criteria Decision Making, we propose a new weight estimation approach for this aggregation technique to properly aggregate multiple measures in the complex network field.

Nevertheless, another problem is that even though we have a more comprehensive measure that has considered more aspects and advantages of other multiple measures, we still cannot conclude that the comprehensive measure is the measure that we are looking for.

Therefore, considering the network resilience analysis and combining the network structure attributions, we propose a new network performance metric and use its changing percentages to compare different measures, then draw a conclusion which one is suitable and efficient to identify the critical nodes in a network. The details of our aimed contributions mainly include the following four parts:

(1) In order to determine the most critical and vulnerable spots (or points) that have more potential to be attacked by terrorists, first, we carry out network structure analyses by applying existing graph theory measures like centrality measures (Wang et al. 2011) or nodal efficiency measures (Nistor and Pickl 2017) on the German ICE network. So far, there have been many quantitative graph theory measures that can be used to analyze networks from different perspectives.

(2) In our research we mainly focus on a few basic centrality measures, like “degree centrality measure, closeness centrality measure , betweenness centrality measure and eigenvector centrality measure” (Freeman 1978, Boudin 2013, Tsiotas and Polyzos 2015, Maharani and Gozali 2014, Ruhnau 2000), which all have been widely used in complex networks, such as social networks or communication networks, for detecting the vital spots. The details of the aforementioned measures are systematically introduced in Chapter 3.

(3) Researchers have proposed many global vulnerability measures to compare different networks with diverse numbers of nodes and edges when analyzing the network vulnerability characteristics. In our research, based on the idea of existing global vulnerability measures and also inspired by betweenness centrality and classic efficiency measures, we propose two new nodal vulnerability measures to detect the key spots in a network and apply them in this thesis: One is named nodal betweenness-efficiency vulnerability measure (Wang et al. 2018); the other is called nodal residual closeness vulnerability measure; both are methodically explained in Chapter 3.

(4) Since the different graph measures analyze the network's structure properties from different points of view, this can lead to different results that further cause the information overflow problem for decision-makers. Therefore, in this thesis, we apply the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) (Lai et al. 1994) to aggregate the aforementioned graph measures into a new aggregation measure that considers multiple factors together. In the process of applying TOPSIS, the most important step is how to estimate and allocate the weights for different measures. Traditionally, in the field of Multi-criteria Decision Making (Borcherding and Winterfeldt 1991), there are some extant, well-known, and widely used estimating methods like AHP (Analytic Hierarchy Process) (Yoon and Hwang 1995), Simple Multi-Attribute Rating Technique (SMART) (Barron and Barrett 1996), Measuring Attractiveness by a Categorical-Based Evaluation Technique (MACBETH) (Bana et al. 2010), the Step-wise Weight Assessment Ratio Analysis (SWARA) method (Keršulienė et al. 2010,

Rezaei 2015), etc. However, the problem is that all of them need the experts' knowledge and experiences, but in graph theory, different researchers have different analysis criteria, which thus will lead to different results and draw distinct conclusions. Therefore, in order to eliminate these diversities and make experiments or computations repeatable, in our research projects we have introduced a new weight estimating method by conducting network global vulnerability analysis to quantify the process of estimating weights. The results show that the proposed aggregation measure is a promising one to identify the key points in a network. We gradually present the aggregation measure and the new weights estimation process in Chapter 3.

(5) In our research, when analyzing the network properties in our research activities, we mainly use the measures coming from the graph theory field; thus we will also combine some network structure characteristics to conduct the network resilience analysis. For the sake of carrying out the network resilience analysis while taking into account the network structure properties, we propose a new network performance metric considering three factors, namely traveling time, the number of people who can take advantage of the public transport systems and also the train flow, which means the least number of trains passing a given line. We also make use of the percentages of changes of the proposed network performance metric to compare the aforementioned centrality, efficiency, nodal vulnerability and the TOPSIS-based aggregation measures, coming to the conclusion which one is the most suitable and efficient measure to identify the key spots in a transportation network. The new network resilience performance metric is thoroughly discussed in Chapter 4, in which, among the aforementioned eight measures (betweenness centrality measure, closeness centrality measure, degree centrality measure, eigenvector centrality measure, nodal efficiency measure, nodal flow-weighted efficiency measure, nodal betweenness-efficiency vulnerability measure and nodal residual closeness vulnerability measure), we also compare and check which measures are the basic and necessary ones for the TOPSIS-based aggregation measure through resilience analysis.

## 1.4 Overview of the Thesis

The structure of this dissertation is organized as follows:

Chapter 1 is the introduction of this thesis. The fundamental issues concerning the research question on how to detect the critical spots in a mesh infrastructure system like train transport systems, while taking into account the terrorist attacks that are described here. The approaches and goals of our research are also addressed in this chapter.

Chapter 2 is the state of the art, in which the basic terms that are used in this dissertation are introduced, for example, what is *graph* and *graph theory* (West 2001) or what is *network* and *network theory* (Gaertler 2005). Moreover, many contributions regarding the network structure and vulnerability analysis using quantitative graph algorithms (which are called graph measures in graph theory) and the network quantitative resilience analysis (Hosseini et al. 2016) are presented.

For instance, in Chapter 2, we review the researches on centrality measures (Bavelas 1948, Tsiotas 2015), including degree centrality (Freeman 1978, Maharani and Gozali 2014), closeness centrality measure (Freeman 1978), betweenness centrality (Freeman 1978) and eigenvector centrality (Ruhnau 2000, Maharani and Gozali 2014), and their applications on the transportation networks (Wang et al. 2011, Li and Cai 2004, Chi et al. 2003, Sienkiewicz and Hołyst 2005, Mohmand and Wang 2013, Sen et al. 2003, Li and Cai 2007, Mohmand and Wang 2014, Derrible 2012, Mouronte and Benito 2012, Cheng et al. 2013). Furthermore, we also review the global efficiency measure (Latora and Marchiori 2003), nodal efficiency measure (Nistor and Pickl et al. 2017) and vulnerablility measures (Barefoot et al. 1987, Gao and Buldyrev 2011, Mishkovski et al. 2011, Vardi and Zhang 2007).

In Chapter 3, in order to identify the critical spots in a mesh system, we conduct a network structure analysis by applying the existing graph theory measures like centrality measures (namely degree centrality, closeness centrality measure, betweenness centrality and eigenvector centrality) and efficiency measures (namely global efficiency measure and node efficiency measure).

Based on the idea of vulnerability, in this chapter, we also propose two new nodal vulnerability measures based on global vulnerability measures and apply them to the German ICE network $G(V,E)$ to detect the critical spots. One nodal vulnerability measure is the nodal residual closeness vulnerability measure, which is based on the graph global residual closeness defined by Dangalchev (2006).

Another nodal vulnerability measure is the betweenness-efficiency vulnerability measure, which is based on the betweenness centrality measure (Freeman 1978) and global efficiency measure (Latora and Marchiori 2003), as well as taking into account the idea of the nodal residual closeness vulnerability measure.

For the sake of reducing the information overflow for decision-makers caused by implementing many different methods on the research object, the aggregation method called Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) (Hwang and Yoon 1981) from the Multi-criteria Decision Making field is introduced, and the TOPSIS-based aggregation approach is presented; here, we not only adapt this aggregation technique to our research, but more importantly, we also improve it by adding a new weighting approach to our study.

In Chapter 4, in order to compare different methods and conclude which measure is more suitable and efficient to detect the critical spots in a network and verify the effectiveness of the proposed new aggregation approach, we carry out a network resilience analysis. In this dissertation, when analyzing the resilience of the German ICE network, we mainly focus on quantitative methods. As it is well-known, when researchers conduct quantitative network resilience analysis, the network resilience is generally quantified using the changes of network performance metric, and thus, in Chapter 4, we develop a new network performance metric by considering traveling time, train flow and also the number of people who can use the system as usual, even under some disruptions.

Here, when roughly estimating the number of people, we also take into account network characters like the number of neighbors for each station (that is the degree of the given station).

In order to apply the idea of degree properly here, we also propose the concept of adjacency node-set level, whose definition is also introduced in detail in Chapter 4.

Furthermore, in that chapter, we also distinguish which measures are the basic and necessary ones for the TOPSIS-based aggregation measure through resilience analysis.

In Chapter 5, outlook and perspectives for future research works are presented. For instance, we are further investigating more extant graph measures with different information, such as mobility centrality (Tsiotas and Polyzos 2015), PageRank (Brin and Page 1998) or Clustering coefficient (Wang et al. 2011). In the future, based on linear algebra, we will also investigate a new algebraic aggregation measure and compare it with the aforementioned TOPSIS-based aggregation measure.

Finally, this dissertation is concluded in Chapter 6 and a summary for this thesis is presented in the end.

# 2 Literature Review on Graph Measures, Vulnerability Indices and Network Resilience Analysis

In this thesis, the main application field of our research is the intercity train system, which is the ICE train system. The data of the study at hand is obtained from Deutsche Bahn (2018). Regarding the problem on how to identify the key station on the ICE train system (here, each station on the ICE train system can also be called a city), in our research, we mainly focus on the quantitative analysis based on the mathematical approaches from graph theory, Multi-criteria Decision Making (MCDM) and network resilience fields.

Since the ICE train system has network characteristics (meaning it has stations and lines between pairs of stations), it can be abstracted into an ICE-network-based mathematical model (as introduced in Chapter 1), analyzed by using mathematical methods.

Based on graph theory, we can first apply the existing graph algorithms (called graph measures in graph theory) (Biggs 1986, West 2001) to detect the critical spots in a graph model (it is actually the aforementioned ICE-network-based mathematical model); based on the existing graph algorithms, we also propose some new approaches, which are presented in detail in Chapter 3.

As introduced in Chapter 1, when applying distinct methods to a graph model, it will lead to different results, which thus causes the information overflow problem for decision-makers. Therefore, to reduce the information overflow issues, we adapt the MCDM method to our research for aggregating multiple methods into a new promising approach by proposing and combining the methods from graph theory.

The new aggregation approach not only considers the advantages of other different methods, but it also compensates for the shortcomings of a single method and leads to a more comprehensive result to tell which node in a network will be the critical one. The proposed new aggregation method is introduced in Chapter 3.

Furthermore, in order to verify the effectiveness of the new aggregation method, we conduct the quantitative resilience analysis by developing and introducing a new network resilience performance metric. Before introducing the details of the applied algorithms, in this chapter, we make a brief literature review on the basic terms of graph theory and the related research history over decades, MCDM and some similar research work from other researchers and experts as well as the reviews on the relevant work of quantitative resilience analysis. So far, there has been a lot of literature (Freeman 1978, Landherr et al. 2010, Hosseini et al. 2016) including many approaches related to network analysis and network resilience analysis, which are reviewed in this chapter. However, to clarify ambiguities at the beginning, we introduce some basic terms that are used in this dissertation.

## 2.1 Basic Network and Graph Theory Concepts

Networks are all around us, including "technological networks (the internet, power grids, telephone networks, transportation networks, et al.), social networks (social graphs, affiliation networks, et al.), information networks (World Wide Web, citation graphs, patent networks, et al.), biological networks (biochemical networks, neural networks, food webs, et al.) and much more" (Aggarwal 2011, Gaertler 2005, Newman 2003, Newman 2008). Once a network has been mapped into a mathematical graph model, people can deduce some critical information by analyzing their structural characteristics using some methods from graph theory, for instance, which part or parts of a network are vital and how to reduce the vulnerability of the network in order to improve its robustness and resilience. In Chapter 1, the German ICE network has been mapped into Graph $G(V,E)$, but before applying some approaches from graph theory to it, we must first introduce some basic concepts regarding the network and graph theory in the following.

In mathematics, ***graph theory*** (Biggs 1986, West 2001) is studying the properties of graphs, which are "mathematical structures used to model pairwise relations between elements" (Rossetti 2015). Specifically, a ***graph*** is "a structure amounting to a set of elements" in which some pairs of elements are connected or interact. The elements corresponding to mathematical abstraction are called nodes (also called vertices or points), and each of the connected pairs of elements is called an edge (also called an arc or line) (Rossetti 2015, West 2001). Typically, a graph can be depicted in a diagrammatic form as a set of dots or circles for the nodes, joined by lines or curves for the edges.

***Network theory*** (Aggarwal 2011, Gaertler 2005, Newman 2003, Newman 2008) is studying the graphs as a representation of either symmetric relations or asymmetric relations between discrete elements. In computer science and network science, the network theory is a part of graph theory. A ***network*** is defined as a graph in which its nodes and edges have attributes (e.g. names or specific weighted values). In summary, the term ***network*** denotes the straightforward concept describing an object consisting of elements and connections between elements. The term ***graph*** is an abstract object composing of "a set of nodes and a set of edges that connect pairs of nodes" (Aggarwal 2011, Dinh 2010, Newman 2003, Rossetti 2015).

Most commonly, in graph theory, the term ***graph*** is defined as an ordered pair $G = (V, E)$, which consists of a set $V$ of nodes with a set $E$ of edges. Since in this dissertation we take the ICE network as an example, for the sake of uniformity and simplicity, we suppose there are no differences between graph and network, nodes and stations, and edges and links throughout this dissertation.

## 2.2 Graph Measures - Centrality, Efficiency and Vulnerability

The so-called ***centrality*** quantifies the intuitive feeling that some nodes or edges are more important than others in a network (Tsiotas 2015). The idea of ***centrality*** was firstly introduced by Bavelas in 1948 (Bavelas 1948) and applied to human communication networks.

Up to now, many researchers have studied this topic and have proposed lots of new different "centrality measures, such as degree centrality, closeness centrality, betweenness centrality and so forth" (Rueda 2017), for identifying the crucial nodes. In the beginning, these centrality measures were mainly applied on social networks (Freeman 1978, Wasserman and Faust 1994).

Afterward, researchers from different fields began to introduce and implement these centrality measures to other kinds of networks, for instance information networks, biological networks, technological networks, and so on (Gaertler 2005). Meanwhile, lots of different centrality measures are proposed.

Distinct centrality measures, which have different meanings and analyze the network from distinct perspectives, lead to different results. For example, degree centrality (Freeman 1978, Maharani and Gozali 2014), as the most simple and straightforward graph measure, can rather easily tell which nodes are the important ones based on the number of neighbors of these given nodes. While, according to closeness centrality measure (Freeman 1978), if one node has the shortest distance to the others and thus can reach other nodes very quickly on the network, the given node will be in the central position in the network. However, based on the prominent betweenness centrality (Freeman 1978), one node can be regarded as the most central one if lies on the shortest paths with largest frequencies between all pairs of other nodes. Another well-known centrality measure is eigenvector centrality (Ruhnau 2000, Maharani and Gozali 2014), according to which one node can be identified as the most important one if its directly connected nodes also have many well-connected neighbor nodes (Landherr et al. 2010).

In recent decades and years, researchers have begun to conduct network analyses for studying the structure properties and detecting the key nodes using the centrality measures in the transportation networks, which include the airport networks (Wang et al. 2011, Li and Cai 2004, Chi et al. 2003), urban road networks (Sienkiewicz and Hołyst 2005, Mohmand and Wang 2013), railway networks (Sen et al. 2003, Li and Cai 2007, Mohmand and Wang 2014), and city metro or subway networks (Derrible 2012, Mouronte and Benito 2012, Cheng et al. 2013).

Especially in order to adapt the centrality measure to the transportation networks efficiently, some new centrality measures were proposed, for instance, Tsiotas and Polyzos (2015) introduced a mobility centrality measure using "the anagogic method considering the kinetic energy of a particle in physics and adjusting its mathematical analog to the transportation network" (Tsiotas and Polyzos 2015). Moreover, a new DelayFlow centrality measure, which takes into account the travel time and commuter flow volume, was proposed by Cheng et al. (2013).

In this dissertation, we apply the centrality measures in German high-speed train networks for identifying these essential nodes to protect them from being attacked by terrorists; or if acts of terrorism do happen on these key nodes, the impacts can be at least reduced to a certain low extent by deploying some security resources in advance on these essential nodes.

For instance, when a node has been identified as the critical one, decision-makers can allot more police to protect it and install in advance some safety detection devices for detecting for example a dangerous chemical material or destructive weapons, and so on.

***Efficiency*** means how well information can spread over the network. Therefore, the nodal efficiency quantifies how fast the information can be propagated from a given node to the rest of the network. Based on Smith (1988), in Latora and Marchiori (2003), the global network efficiency is defined. Furthermore, on the basis of Latora and Marchiori (2003), Nistor and Pickl et al. (2017) defined the nodal efficiency measure to detect the critical nodes. Meanwhile, by considering the train flow information, the authors also proposed a new flow-weighted nodal efficiency measure that can be used not only to identify the critical nodes, but also to distinguish the vital edges.

When quantifying the vulnerability of a network under disruptions or attacks, there are commonly two types of methods (Boesch et al. 2009): one is probabilistic and based on models from reliability theory, the other method is graph invariants as deterministic measures, such as centrality-based measures, graph diameter, etc. (Holme et al. 2002, Albert and Nakarado 2004, Holmgren 2006, Johansson and Hassel 2013). In this dissertation, we only consider graph invariants-based measures.

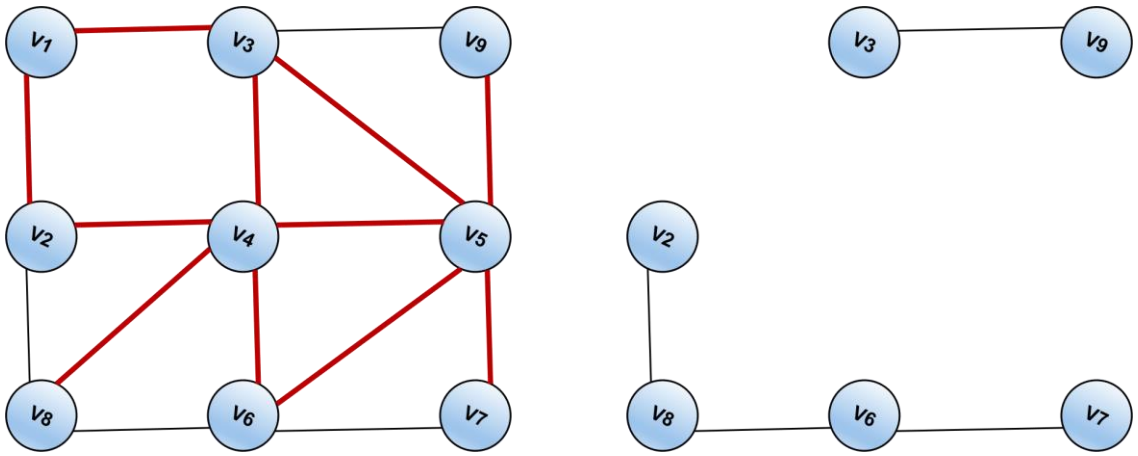
In graph theory, the term ***vulnerability*** can be understood as what percentage of the structural properties of network changes due to defunct or removed nodes (Barefoot et al. 1987, Gao and Buldyrev 2011, Mishkovski et al. 2011, Vardi and Zhang 2007). Based on the percentages of changes of network structure, one can tell which one or set of nodes is much more important among different nodes.

However, the existing traditional vulnerability measures like graph connectivity (Mamut and Vumar 2008), graph toughness (Bauer et al. 2013), graph scattering number (Zhang and Wang 2013, Kirlangiç 2002), graph integrity (Mishkovski et al. 2011), graph extreme tenacity (Cheng et al. 2014, Li et al. 2014) and graph domination number (Alanko et al. 2011), generally detect the same changes or damage the of network structure if the removed nodes are trivial ones, which therefore cannot distinguish between these different trivial nodes.

Here, we generally explain the formulas of "connectivity, toughness, scattering number, integrity, tenacity and domination number" (Aslan and Kirlangic 2011). For Graph $G$, $S \subseteq G$, $G-S$ signifies the remains of $G$ after removing the subset $S$ of vertices and its corresponding edges, $\omega(G-S)$ means the number of components in $G-S$, $\tau(G-S)$ denotes the order (i.e., the number of vertices) of the largest component in $G-S$, vertex subset $X$ ( $X \subset V(G)$, $V(G)$ is the vertex set of graph $G$ ) is the vertex set cut (whose removal will disconnect graph $G$ ) of graph $G$ ( Aslan and Kirlangic 2011, West 2001), $|X|$ means the number of vertices.

For example, in Figure 2.1, the left picture is graph $G$ ; here, we suppose one node subset $S=\{V_1,V_4,V_5\}$, then when deleting these three nodes and their corresponding edges (marked in red and bold), the remaining graph $G-S$ is shown on the right side of Figure 2.1. Apparently, $G-S$ has two components, one component contains nodes $\{V_3,V_9\}$, another component is the largest component including nodes $\{V_2,V_6,V_7,V_8\}$; then, we can say $\omega(G-S)=2$ and $\tau(G-S)=4$. Because removal of the subset $S=\{V_1,V_4,V_5\}$ can separate graph $G$, the subset $S=\{V_1,V_4,V_5\}$ can also be regarded as one of the vertex set cuts $X$ ; in such a case, $|X|=3$.

In Figure 2.1, $|X|=\{2,3,4,5,6,7\}$.




Graph G

Remaining graph $G-S$

Figure 2.1: Simple graph for explaining $S$, $\omega(G-S)$ and $\tau(G-S)$

The connectivity measure (Mamut and Vumar 2008) is a basic vulnerability measure and can be easily applied to a large complex network. It mainly measures how easily a network can be broken apart by counting the least numbers of nodes that need to be removed. Its definition is denoted as follows:

$$\kappa(G)=min\{|X|: X\subset V(G), \omega(G-X)>1\} \quad (2\text{-}1),$$

where $\kappa(G)$ denotes the connectivity of G; here, the reason of $\omega(G-X)>1$ is used to make sure that subset $X$ is the vertex set cut whose removal can separate graph $G$ into at least two components. The toughness measure (Bauer et al. 2013) is used as a more refined graph vulnerability measure to evaluate how heavily a network can be broken, based on the numbers of deleted nodes. The above-mentioned formula of toughness measure denotes that the smaller the toughness measure value is, the more vulnerable the network is, which means that more components will be generated by removing fewer nodes.

Specially, if the connectivity between two graphs is the same, the toughness measure can be applied to compare their vulnerabilities.

The formula of vertex toughness measure is shown as follows:

$$t(G) = min\{\frac{|X|}{\omega(G-X)} : X \subset V(G), \omega(G-X) > 1\} \quad (2\text{-}2),$$

where $t(G)$ denotes the toughness measure.

The scattering number (Zhang and Wang 2013, Kirlangiç 2002) shows "not only how difficult it is to break down the network, but also how badly the network is damaged" (Aslan and Kirlangic 2011). Its definition is given as follows:

$$s(G) = max\{\omega(G-X) - |X| : X \subset V(G), \omega(G-X) > 1\} \quad (2\text{-}3),$$

where $s(G)$ denotes the scattering number measure.

The integrity measure (Mishkovski et al. 2011) is used to judge how easy it is to keep both the number of destroyed nodes and the largest remaining component small. The integrity measure is defined as follows:

$$I(G) = min\{|X| + \tau(G-X) : X \subset V(G)\} \quad (2\text{-}4),$$

where $I(G)$ denotes the integrity measure.

The tenacity measure (Cheng et al. 2014, Li et al. 2014) mainly studies the intactness of a graph when some of its nodes are deleted. It means that the higher the tenacity value of a network, the more stable or less vulnerable it is considered to be. Its formula is shown as follows:

$$T(G) = min\{\frac{|X| + \tau(G-X)}{\omega(G-X)} : X \subset V(G), \omega(G-X) > 1\} \quad (2\text{-}5),$$

where $T(G)$ denotes the tenacity measure. Supposing a subset $S \subseteq G$ is the dominating set of graph G (such that every node not in $S$ is adjacent to at least one node in $S$), then the domination number (Alanko et al. 2011) of a network is the cardinality of a minimum dominating set. Its formula is defined as follows:

$$D(G) = min\{|S|\} \quad (2\text{-}6),$$

To quantify the vulnerability of a network, lots of researchers have proposed more new sensitive vulnerability measures which can detect the small change under the situation of even only removing one trivial node or edge; for instance, Boccaletti et al. (2007) proposed a new multiscale evaluation measure of vulnerability.

Based on closeness centrality, Dangalchev (2006) developed a new residual closeness vulnerability measure applied in complex networks.

Meanwhile, some researchers have also identified the important components or nodes in a network by analyzing the vulnerability of the network. Rodriguez-Nunez and Garcia-Palomares proposed vulnerability component importance measures for a public transportation network considering the travel time. The authors in Sullivan et al. (2010) and Jenelius and Petersen (2006) developed vulnerability component importance measures for road networks based on the cost of travel time. Ouyang et al. (2014) proposed and applied the flow-based vulnerability measure on train networks. In this dissertation, we now propose two new nodal vulnerability measures based on existing global graph vulnerability measure, centrality measure and efficiency measure. We explain them and their advantages in detail in Chapter 3.

### 2.2.1 Structural Properties

When a network is non-deterministic or we know nothing about its structures, through the structural analysis of network using some structural measures (such as degree distribution measures, clustering coefficient measures and centrality measures), we can derive some useful *structural properties* of the network and further infer what kinds of characters and functions the network has. For example, we could identify critical nodes through the network structural analysis, if transportation networks and the crucial stations with specific properties, that are more likely to become the attacked targets, can be detected, so the responding security measures can be deployed in advance to protect these vital stations against terrorist attacks. Here, we will do some specific reviews on the structural and vulnerability analysis of transportation networks. Starting with a paper authored by Meyer-Nieberg et al. (2014), in which, for the sake of evaluating the

vulnerabilities of public transportation systems, the authors propose a three-model-based approach which combines multi-agent systems, dynamical systems and graph models, where the multi-agent systems are mainly used to analyze the system behaviors in the most detailed level. By using difference or differential equations, the dynamical systems were used to describe the development of system behavior over time.

Moreover, based on the dynamical system model, the graph models could be constructed. Afterward, the complexity of the network-based systems was analyzed by using some quantitative network measures, such as distance-based graph measures, eigenvalue-based graph measures and entropic graph measures.

Emmert-Streib (2011) not only introduced some well-known network classes, such as simple networks, random networks, small-world networks, scale-free networks and trees, but Emmert-Streib (2011) also presented some useful methods for network structural analysis, for example degree distribution measures, clustering coefficient measures, path-based measures, centrality measures and a method for identifying the community structure of networks.

Ducruet and Lugo (2013) discussed the structures of transportation networks from the perspective of both network-level and node-level measures. To understand transportation networks better, the usefulness of these measures was also discussed. Regarding the problem of how transportation networks had been defined and analyzed, the authors did some reviews from four aspects concerning spatial structure, geometry, morphology and topology of transportation networks. Furthermore, the dynamics in transportation networks were explored by adopting the Agent-based Models (ABMs). In order to apply the ABMs on transportation networks for dynamic analysis, two distinct approaches including generative and degenerative processes were presented.

Derrible (2012) examined the network centrality of subway networks. The assessment of centrality was conducted by adopting betweenness centrality. In order to do research on the emergence of global trends with network size in the evolution of centrality, betweenness centrality was applied to 28 metro systems with different sizes around the world.

It was found out that betweenness becomes more uniformly distributed with size. Moreover, it was shown that the share of betweenness decreased with network size in a power law. However, the share of nodes with the most central properties decreased more slowly than those with the least central properties.

In the end, betweenness was demonstrated to be useful to locate stations for helping relieve pressure from overcrowded stations by analyzing the betweenness of individual stations in several systems.

It was found out that a Macroscopic Fundamental Diagram (MFD) could be presented in the urban transportation networks when meeting certain conditions. In order to analyze whether the MFD exists in heterogeneously congested transportation networks or not, Ji and Geroliminis (2012) mainly conducted research on the clustering problem of transportation networks. As one category of clustering algorithms, a partitional method was used in Ji and Geroliminis (2012). To minimize the variance of link densities as well as to preserve the spatial compactness of clusters, a new partitioning mechanism was proposed. The presented method consisted of the normalized cut algorithm, the merging algorithm and the boundary adjustment algorithm. In addition, density variance and shape smoothness metrics were also introduced to examine the proposed partitioning mechanism.

Mouronte and Benito (2012) studied the urban bus and subway networks of Madrid. Many characteristics of these two networks, such as stops, routes and densities of these two networks, were analyzed. The authors represented these two networks as a graph. Moreover, some structural parameters, including average distances between nodes, betweenness, robustness, sensitivity and communities of the graph were evaluated not only in the entire city, but also in its different districts. Furthermore, the singularity of one transport line in a district was also explored in Mouronte and Benito (2012). Moreover, many useful results were achieved through the aforementioned analysis.

According to betweenness centrality measures of complex networks which are based on the shortest paths, Puzis and Altshuler et al. (2013) proposed a new "betweenness-driven traffic assignment model for the optimal deployment of traffic monitoring units in transportation networks" (Puzis and Altshuler et al. 2013).

For the sake of coping with the problem of traffic assignment given an arbitrary travelling cost definition, the problem of how to augment the betweenness was discussed. In order to evaluate the proposed model used for generating efficient deployment schemes, a high-resolution Israeli transportation dataset was used for examination. Meanwhile, the correlation was analyzed between "betweenness centrality and traffic flow" (Puzis and Altshuler et al. 2013).

Finally, it was illustrated that "the group variant of the augmented betweenness centrality used to optimize the locations of traffic monitoring units could decrease the costs and enhance the effectiveness of traffic monitoring" (Puzis and Altshuler et al. 2013).

In order to improve the design of the transportation networks and to conceive the plans dealing with the problems of failures of transportation networks, the centrality measures identifying crucial nodes in a transportation network were explored by Cheng and Lee et al. (2013). In this thesis, a new centrality measure named DelayFlow is proposed.

Unlike common centrality measures, the new presented centrality measure does not only take the topological structure of network into account, but also considers two transportation factors, namely travel time delay and commuter flow volume. In the end, the proposed measure is compared with some common "centrality measures like degree centrality, closeness centrality and betweenness centrality" by using Singapore's Mass Rapid Transit network (Cheng and Lee et al. 2013).

Discovering the hub road sections is not only in favor of protecting urban infrastructure from being attacked, it is also useful to solve the design problem of a traffic network. Based on Girvan and Newman algorithm, Chen and Hu (2013) proposed a new algorithm used to detect community structure and uncover hub road sections in an urban traffic network. Also in Chen and Hu (2013), an improved modularity that determines the proper number of community structures was presented.

By studying the traffic network of Wuchang, it was validated that the characteristics of community structure existed in the urban traffic network; meanwhile, the hub road sections deduced by using the proposed algorithm were also demonstrated in accord with the actual situation.

When analyzing “the interregional transportation network in Greece”, Tsiotas and Polyzos (2015) proposed a new centrality measure called mobility centrality. It was assessed that the presented measure could be applied efficiently during the operational network analysis. Additionally, the Pearson’s Linear Bivariate Coefficient of Correlation and the Linear Regression Backward Elimination method were used to test the ability of the proposed measure.

Moreover, the presented centrality measure was compared with other four traditional “existing centrality measures, namely betweenness, closeness, straightness and degree centrality measures” (Tsiotas and Polyzos 2015).

Finally, it was shown that “the status of the Greek interregional commuting system could be described properly by the presented measure through the empirical analysis” (Tsiotas and Polyzos 2015).

In modern society, railways play a crucial role in establishing efficient complex transportation networks. The structural properties of the Pakistan Railway Network (PRN) were studied by Mohmand and Wang (2014). Especially the PRN was represented as an unweighted graph.

Through the network analysis it was found that the PRN clearly manifested the small world properties. Moreover, the betweenness and closeness centrality measures were also applied to detect critical stations with high traffic and potential congestion (Mohmand and Wang 2014).

## 2.3 Network Resilience Analysis

Although most people find it easy to grasp an intuitive and qualitative meaning for the concept of resilience, this notion proved to be one of the most difficult ones to be defined qualitatively in a general and comprehensive way (Wang et al. 2017). Numerous qualitative and quantitative definitions have been proposed in different fields, including psychology, social sciences, ecology and engineering. Some studies tried to differentiate between the meanings to be used in engineering and ecology (Holling 1996). Attempts have also been made to review this field; for instance, Martin-Breen et al. (2011) and Hosseini et al. (2016) have done relatively comprehensive reviews on the definitions of resilience.

Specifically in ecological systems, Holling (1996) was the first ecologist who introduced the concept of resilience. According to Holling (1996), resilience is defined as "the magnitude of disturbance that can be absorbed before the system changes its structure by changing the variables and processes that control behavior." Based on this definition, a *system* can be seen as *resilient* if its structure cannot be destroyed by the maximum amount of disturbances such as adverse events or natural disasters.

Here, the maximum amount of disruptions (the system structure will start to be destroyed if the disruptions exceed this maximum amount of disruptions) can be attained by adjusting the variables and processes.

The system resilience is defined by Vugrin et al. (2011) as "Given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels". Vugrin and Warren et al. (2011) qualitatively define system resilience by using three key factors, namely the disruptive event, the efficiency of system recovery and the system performance.

*Organizational resilience* is explicitly defined by Altintas and Royer (2009) as the "capacity of an organization to maintain or return to a dynamic stable state which allows it to continue its operations during and after a major incident or in the presence of continuous stress."

This definition is similar to the one of ecological resilience proposed by Holling (1996), which also only focuses on the capacity of a resilient organization to retain or bounce back to a dynamic stable state so that it can always operate normally. Here, the steady state or the stable performance of a system refers to a system which can work without any interruptions or stops, or within a tiny range of variations of performance.

Furthermore, taking more factors and abilities of an organization into account, Gilly and Kechidi (2014) describe organizational resilience as "a double capacity: that of resisting a shock or limiting its effects but also that of anticipating and thus adapting to this shock or to a rapid evolution in the economic context by creating new systems, particularly organizational ones." Two abilities of an organization in this definition are emphasized, which are the ability of absorbing disruption and recovering from it by resisting a shock or limiting its damage, and the ability of firstly anticipating and then adapting to this shock or rapid evolution (Gilly and Kechidi 2014, Wang et al. 2017). However, incarnated in the efficiency of recovery of the system resilience proposed by Vugrin et al. (2011), the needed recovery time and the amount of resources during the progress of recovery of an organization couldn't be explicitly considered in this organizational resilience, which can be used to quantify the resilience of an organization.

More generally, based on Cutter and Ahearn (2013) and specially British Standards (2014), the organizational resilience is defined as the "ability to anticipate, prepare for, respond and adapt to events – both sudden shocks and gradual change to survive and prosper." Different from the definitions of ecological resilience that only require the ability to absorb change and disturbance while maintaining the same state, the definition of the organizational resilience focuses on more aspects and splits the process of resilience into four parts (Seager et al. 2017, Wang et al. 2017): what potential events could happen and what damage would be induced by these adverse events (anticipating); how to prevent these events from happening or how to relieve the loss by preparing for some security measures ahead (preparing); how to respond to these adverse events including absorbing the disruptions and recovering from the damage caused by events (responding); and the last one, which is how to adapt to these adverse events in the future (adapting) (Seager et al. 2017, Wang et al. 2017).

### 2.3.1 Transportation Engineering Field

Regarding the resilience and definitions of the transportation engineering field, many pieces of research also have been pursued. For instance, the resilience of a transportation system as defined by Murray-Tuite (2006) is "a characteristic that indicates system performance under unusual conditions, recovery speed and the amount of outside assistance required for the restoration to its original functional state." Ten dimensions of resilience were identified by Murray-Tuite (2006), which are redundancy, diversity, efficiency, autonomous components, strength, collaboration, adaptability, mobility, safety and the ability to recover quickly.

Murray-Tuite (2006), through simulation, studied the influence of System Optimum and User Equilibrium traffic assignments on the last four dimensions of adaptability, mobility, safety and recovery. The traveling time for all vehicles in the network can be minimized based on System Optimum traffic assignment, while the traveling time for individual vehicles can be reduced by User Equilibrium traffic assignment.

Results showed that User Equilibrium traffic assignment performs better than System Optimum when considering adaptability and safety; however, System Optimum traffic assignment outperforms User Equilibrium under mobility and recovery.

Moreover, many other researchers, such as Gunderson and Pritchard (2002), Battelle (2007), Sudakov and Vu (2008), Mostashari et al. (2009), Heaslip et al. (2010), VTPI (2010b), Serulle et al. (2011), Nagurney and Qiang (2009), Litman (2011), Cox et al. (2011), Zhang et al. (2009), also define and evaluate the resilience of transportation systems from different perspectives.

When assessing network resilience, one of the convenient ways is to quantify resilience based on reliability and graph theory:

We consider a system or network and map it into an undirected graph $G(V,E)$, where $V=\{v_1,v_2,...,v_n\}$ denotes the set of nodes and $E=\{e_1,e_2,...,e_m\}$ represents the set of edges connecting the adjacent nodes with each other.

Before introducing the resilience of networks, the concept of passageway is defined as: "if a path set includes the paths connecting nodes $i$ and $j$ without any common edges with other paths between nodes $i$ and $j$, then the set is an independent passageway set of nodes $i$ and $j$". The element of the independent passageway set is called a passageway (Ip and Wang 2011). $L_k(i, j)$ denotes the $k^{th}$ passageway between nodes $i$ and $j$.

The operation reliability $q_l$ is represented as the normal operation reliability of one edge $l \in E$. Because one passageway consists of a series of edges, the reliability of a passageway $P_k(i, j)$ is defined as:

$$P_k(i, j) = \prod_{l \in L_k(i,j)} q_l \tag{2-7}$$

Based on equation (2-7), the reliability sum of all reliable passageways between the pair of nodes $i$ and $j$ is denoted as:

$$NP(i, j) = \sum_{k=1}^{N_p} P_k(i, j) \tag{2-8},$$

where $N_p$ is the number of independent passageways between nodes $i$ and $j$. According to Ip and Wang (2011), the resilience of a node in one network can be defined as "the weighted sum of the numbers of reliable passageways of all other nodes in the network"; its formula is shown as follows:

$$r_i = \sum_{j=1, j \neq i}^{n} sv_j NP(i, j) = \sum_{j=1, j \neq i}^{n} sv_j \sum_{k=1}^{N_p} \prod_{l \in L_k(i,j)} q_l \tag{2-9},$$

where $i = 1, 2, ..., n$. $sv_j = u_j / (\sum_{i=1}^{n} u_i - u_j)$ denotes the self-exhausted weight of a given node, which means that the connected nodes of a given node could not contain the given node itself when computing the resilience of the given node. Here, $u_i$ denotes the weight of a node $i \in V$.

For simplicity, we take graph $G$ in Figure 2.2 as an example to compute the resilience of one given node such as node $V_4$; here, we suppose that the weight of all nodes is $u_j = 1$, $j = 1,2,...,9$, and the normal operation reliability of all edges is $q_l = 0.5$. Then,

$$sv_j = u_j / (\sum_{i=1}^{9} u_i - u_j) = \frac{1}{8}, \quad j = 1,2,...,9$$

According to the definition of passageway, the passageways between nodes $V_4$ and $V_5$ only have three paths, which are $V_4 \to V_5$, $V_4 \to V_3 \to V_9 \to V_5$ and $V_4 \to V_6 \to V_7 \to V_5$. Therefore,

$$NP(V_4, V_5) = \sum_{k=1}^{N_p=3} P_k(4,5) = 0.5 + 0.5^3 + 0.5^3 = 0.75$$

Likewise, the numbers of passageways between nodes $(V_4, V_2)$, $(V_4, V_3)$ and $(V_4, V_6)$ are all only three paths, and $NP(V_4, V_2) = NP(V_4, V_3) = NP(V_4, V_6) = 0.75$. Moreover, the passageways between nodes $V_4$ and $V_1$ only have two paths, which are $V_4 \to V_2 \to V_1$ and $V_4 \to V_3 \to V_1$. Then,

$$NP(V_4, V_1) = \sum_{k=1}^{N_p=2} P_k(4,1) = 0.5^2 + 0.5^2 = 0.5$$

In the same way, the numbers of passageways between nodes $(V_4, V_7)$, $(V_4, V_8)$ and $(V_4, V_9)$ are all only two paths, and $NP(V_4, V_7) = NP(V_4, V_8) = NP(V_4, V_9) = 0.5$. Thus, based on Formula (2-9), the resilience of node $V_4$ is:

$$r_4 = \sum_{j=1, j\neq 4}^{9} sv_j NP(4, j) = \frac{1}{8} * (0.75 * 4 + 0.5 * 4) = 0.625.$$

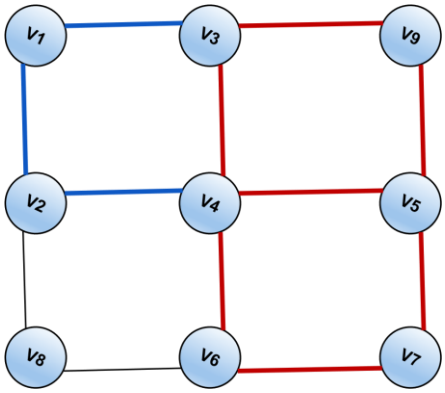



Figure 2.2: Simple graph $G$ for computing the resilience $r_i$ of one node in a network

Based on the resilience of a node shown in Formula (2-9), the global resilience of a network $G$ can be defined as "the weighted sum of the resilience of all nodes" presented as Formula (2-10) (Ip et al.., 2011):

$$R(G) = \sum_{i=1}^{n} \omega_i r_i \qquad (2\text{-}10),$$

where $\omega_i = u_i / \sum_{j=1}^{n} u_j$ represents the relative importance weight of a node $i \in V$. Based on graph theory and network resilience, as Ip and Wang (2011) pointed out, "if $H = \{V, E_H\}$ is a subgraph with the same node set $V$ of graph $G(V, E)$, subgraph $H$ has a lower or equal resilience to graph $G$, that is, if $E_H \subset E$, then $R(H) \leq R(G)$".

According to Formula (2-9), once a graph is defined because its number of nodes and the weight of each node are all determined, the parameter $sv_j$ is constant.

Therefore, the resilience of a node is monotonically increasing with values $q_l$ of reliability of all nodes. When computing network resilience, the vital steps are the estimations of the reliabilities of edges. That is, researchers need to calculate the probabilities of regular operation of edges in the system, which is difficult and based on the experience of experts.

As introduced in Chapter 1, one general and easily understandable way to assess network resilience is to represent resilience graphically by using special performance curves with time.

Bruneau et al. (2003) firstly defined the seismic resilience in civil infrastructure as "the ability of the system to reduce the chances of a shock, to absorb a shock if it occurs (abrupt reduction of performance) and to recover quickly after a shock (re-establish normal performance)."

To quantify the concept of resilience, Bruneau et al. (2003) proposed a well-known seismic resilience triangle model illustrated in Figure 2.3.

In another domain, the deterministic metric for measuring the earthquake-caused resilience loss of a community is mathematically defined using Formula (2-11).

$$R = \int_{t_0}^{t_1} \left[100 - Q(t)\right] dt \qquad (2\text{-}11),$$

where $t_0$ is the time at which the earthquake occurs, $t_1$ denotes the time that the community needs to restore to its pre-disruption level, $Q(t)$ means the quality of the infrastructure of a community, and its value range is $Q(t) \in [0,100]$; here, 100 means that the system recovers to 100% normal operation status.

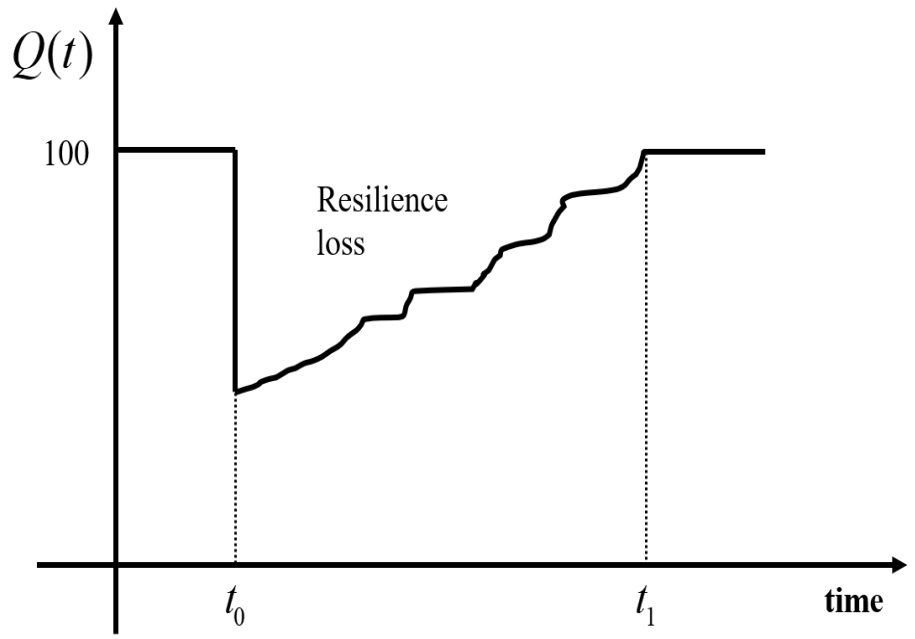



Figure 2.3: Measure of seismic resilience (adapted from Bruneau et al. 2003)

Furthermore, Bruneau et al. (2003) also specifically defined four properties of resilience as follows:

(i) Robustness: the ability of systems to withstand a given level of disruption without suffering degradation of function.

(ii) Redundancy: the extent to which systems exist that are capable of satisfying functional requirements in the event of disruption.

(iii) Resourcefulness: the capacity to identify problems, establish priorities and mobilize resources when conditions exist that threaten to disrupt the system; resourcefulness can be further conceptualized as consisting of the ability to apply material (i.e. monetary, physical, technological and informational) and human resources to meet established priorities and achieve goals.

(iv) Rapidity: the capacity to meet priorities and achieve goals in a timely manner in order to contain losses and avoid future disruption.

### 2.3.2 A New Interpretation of Resilience Triangle

Due to the general concept of quality and the general applicability of resilience triangle metric, the method proposed by Bruneau et al. (2003) can be implemented to many systems. For instance, Adams et al. (2012) extended the resilience triangle metric to freight transportation network for measuring resilience, while Sahebjamnia et al. (2015) applied it to measure organizational resilience.

Especially based on the resilience triangle model, Zobel (2011) proposed a new metric by "calculating the percentage of the total possible loss over some suitably long time interval $T^*$. The defined metric is shown in Formula (2-12).

$$R = \frac{T^* - X \cdot T/2}{T^*} = 1 - \frac{X \cdot T}{2T^*} \quad (2\text{-}12),$$

where $X \in [0,1]$ denotes the percentage of function loss after a disruption and $T \in [0, T^*]$ signifies the time that the system needs to fully recover.

The conceptual illustration of resilience is shown in Figure 2.4, from which, given a disruptive event, the entire possible loss can be computed using a triangular area ( $\frac{X \cdot T}{2}$ ). Comparing to the resilience metric proposed by Bruneau et al. (2003), this linear recovery metric developed by Zobel (2011) is more straightforward.

Therefore, it has the advantage of smooth understanding and application, especially meeting such circumstances without complex and accurate calculation.

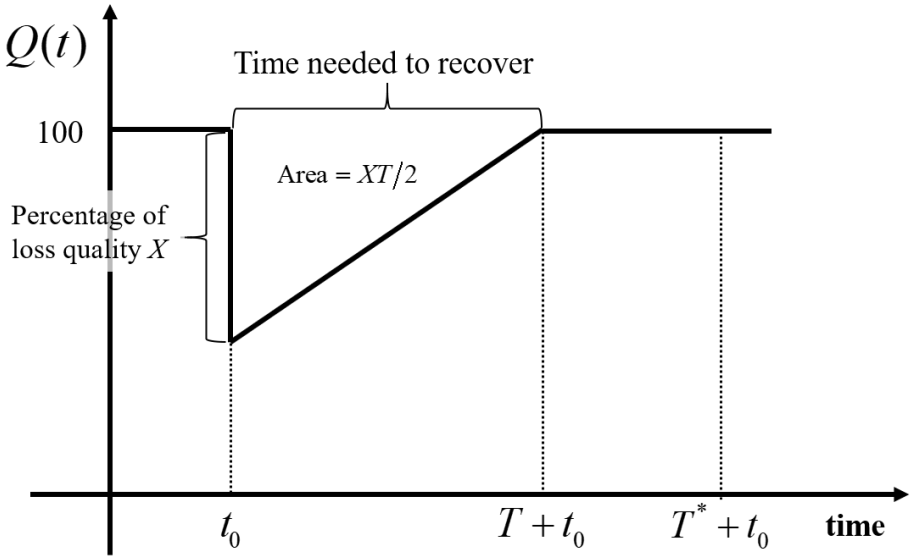



Figure 2.4: A new interpretation of resilience triangle (adapted from Zobel, 2011)

Similar to Bruneau et al. (2003) and Zobel (2011), but more generally based on Henry and Ramirez-Marquez (2012), as introduced in Chapter 1, Nan and Sansavini (2017) only split the resilience of the system into four different phases illustrated in Figure 1.4. Similar to dynamic resilience proposed by Francis and Bekera (2014), Nan and Sansavini (2017) also introduced the capabilities of resilience including absorptive, adaptive and restorative capabilities. Moreover, Nan and Sansavini (2017) quantified these capabilities by using some quantitative measures in different phases. In the first phase, which is the original steady phase ($t < t_d$, $t_d$ is the time when the adverse events happen), the original measurement of performance $P_0$ of the system is assumed as its target value, where $t_0$ denotes the time when the system is still in the first phase.

In the second phase (disruptive phase), the absorptive capability of the system begins to react. During this phase, the Robustness ( $R$ ), RAPIDITY ( $RAPI_{DP}$ ) and Time Averaged Performance Loss ( $TAPL_{DP}$ ) are used to assess the absorptive capability of the system. Nan and Sansavini (2017) quantify robustness as:

$$R = \min\{P(t)\} \quad t_d \le t < t_{ns} \tag{2-13},$$

where $t_{ns}$ denotes the time when the new steady phase is achieved. And rapidity can be calculated as follows:

$$RAPI_{DP} = \frac{\left| \sum_{i=1}^{K_{DP}} \frac{P(t_i) - P(t_i - \Delta t)}{\Delta t} \right|}{K_{DP}} \tag{2-14},$$

where $t_i \in [t_d, t_r)$ is the discrete time point, $P(t_i)$ means the system performance value at the $i-th$ detected ramp and $K_{DP}$ denotes the number of detected ramps during the second phase.

According to Kamath (2010) and Nan and Sansavini (2017), a ramp is assumed to be generated if the rate of change of the measured values within a time interval $\Delta t$ is larger than the predefined ramp threshold value ( $\Delta X_{ramp}$ ). It can be expressed as:

$$\frac{P(t + \Delta t) - P(t)}{\Delta t} > \Delta X_{ramp} \tag{2-15}.$$

Further, during the disruptive phase, the Time Averaged Performance Loss can be computed by:

$$TAPL_{DP} = \frac{\int_{t_d}^{t_r} \left[ P_0 - P(t) \right] dt}{t_r - t_d} \tag{2-16},$$

where $t_0$ denotes the time when the system is still in the first phase and $t_r$ is the time when the system starts to be in the third phase, that is the recovery phase.

According to Formula (2-16), the *Time Averaged Performance Loss* not only takes the amount of performance loss of the system into account, but it also considers the duration of the disruptive events.

In the third phase (recovery phase), the degraded system performance begins to increase up to a new steady level. Also, the adaptability and restorability of a system in this phase can be measured by the RAPIDITY ( $RAPI_{RP}$ ) and Time Averaged Performance Loss ( $TAPL_{RP}$ ). Accordingly, $RAPI_{RP}$ and $TAPL_{RP}$ are expressed by Formula (2-17) and Formula (2-18), respectively:

$$RAPI_{RP} = \frac{\left| \sum_{i=1}^{K_{RP}} \frac{P(t_i) - P(t_i - \Delta t)}{\Delta t} \right|}{K_{RP}} \tag{2-17}$$

$$TAPL_{RP} = \frac{\int_{t_r}^{t_{ns}} (P_0 - P(t))dt}{t_{ns} - t_r} \tag{2-18},$$

where $t_i \in [t_r, t_{ns})$, $K_{RP}$ denotes the number of detected ramps during the recovery phase. For example, based on Figure 1.4, here we only consider the recovery phase. In order to keep it simple, we suppose that there are only four different time intervals during which the rate of change of the measured performance values is linear but different, as shown in Figure 2.5. We also suppose the predefined ramp threshold value $\Delta X_{ramp} \approx 0$; therefore, according to Figure 2.5, we can say that there are four different detected ramps, i.e., $K_{RP} = 4$.

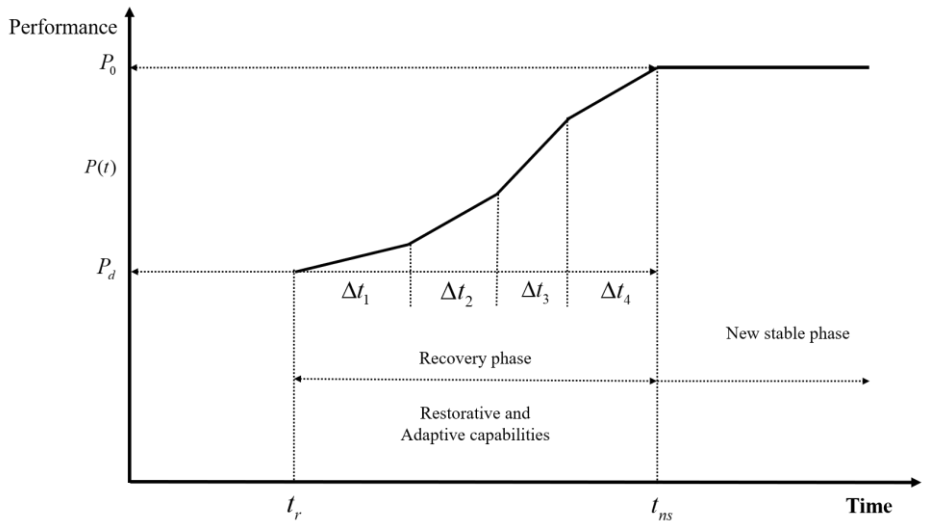



Figure 2.5: Recovery phase of resilience for computing $K_{RP}$

In the last phase (the new steady state), a new steady level is achieved and retained, which may be equal to the previous steady level, or a lower level, or even a higher level than the previous steady level (Seager et al. 2017). During this phase, according to Nan and Sansavini (2017), the recovery ability ($RA$) of a system can be assessed by:

$$RA = \left| \frac{P(t_{ns}) - P(t_r)}{P_0 - P(t_r)} \right| \tag{2-19}.$$

Based on Formula (2-13) - Formula (2-19), integrating the aforementioned measures, Nan and Sansavini (2017) defined resilience metric ($GR$) as follows:

$$\begin{aligned} GR &= f(R, RAPI_{DP}, RAPI_{RP}, TAPL, RA) \\ &= R \times \frac{RAPI_{RP}}{RAPI_{DP}} \times (TAPL)^{-1} \times RA \end{aligned} \tag{2-20},$$

where in order to contain effects of all performance loss during the second and third phases, combining measures $TAPL_{DP}$ and $TAPL_{RP}$ into one $TAPL$ measure is expressed as:

$$TAPL = \frac{\int_{t_d}^{t_{ns}} [P_0 - P(t)]dt}{t_{ns} - t_d} \tag{2-21}$$

As described in Nan and Sansavini (2017), based on Formula (2-20), Robustness ($R$), Recovery RAPIDITY ($RAPI_{RP}$) and Recovery Ability ($RA$) have a positive effect on resilience. Conversely, the negative effect on the resilience of a system is contributed by the Total Time Averaged Performance Loss ($TAPL$) and the Loss RAPIDITY ($RAPI_{DP}$). That is, the higher the robustness value, the faster the recovery speed and the stronger the recovery ability. Also, the less the performance loss and the slower the loss rapidity, the more resilient the system is (Wang et al. 2017).

Due to the fact that the proposed definition of resilience is not specifically domain-based, it only needs to calculate the system performances in different time series; it can thereby be applied in many domains and is suitable to varying modes if defining the system performance properly. In such case, the selection and computation of $P(t)$ are crucial (Wang et al. 2017).

In this thesis, we propose now a new resilience measure mainly based on the one presented by Nan and Sansavini (2017); the details are described in Chapter 4. Furthermore, it was also compared by the examination made in the project RE(H)STRAIN (RE(H)STRAIN 2021).

## 2.4 RE(H)STRAIN - A Testbed for Performance Management

Because of its location in the center of Europe, the Franco-German high-speed passenger train network forms the backbone of the European high-speed systems. It partially operates on the railroad network of neighboring countries in the EU and will develop further by offering services in an increasing number of European cities and capitals. It will also provide its track-network to additional high-speed train operators in other European countries to meet the requirements for more European competition.

Therefore, it is important that France and Germany set high standards of security against terrorist attacks to lead the way to maintain a secure European high-speed railway network, including a secure infrastructure for the future.

The project RE(H)STRAIN aims at investigating “preventive security and its impact on the resilience of the Franco-German high-speed rail network in case of terrorist attacks” (Amokrane et al. 2017, Ip and Wang 2011, Nan and Sansavini 2017). A view on historical terrorist impacts on high-speed trains provides lessons learned, behavioral patterns, means of attack and tactics applied for selection of means, development of attack plans, realization and execution of the attack. To reduce risks and to increase the resilience of transportation networks, prevention, mitigation and recovery strategies for the Franco-German high-speed passenger rail system have been developed and identified. Besides their efficiency, the societal and legal aspects of security measures have also been carefully considered.

The objectives of the project RE(H)STRAIN were "to investigate how the resilience of trains and related infrastructure of the German-French high-speed public passenger transport network can be increased against terrorist attack" (Amokrane et al. 2017, RE(H)STRAIN 2021).

In a *scenario-driven* holistic approach, the entire terrorist sphere of possible actions was considered. Security measures and systems aiming at prevention and mitigation were defined and evaluated against different terrorist scenarios derived from historic terrorist attacks, such as the sarin attack on the Tokyo subway in 1995, the 2004 Madrid train bombing, the 2005 London bombings, the 2008 Mumbai attacks and others.

Novel remote BCRE (biological, chemical, radiological, explosive) sensors and detectors were considered, assessed and combined with a system improving the resilience of the Franco-German high-speed passenger train system.

The project RE(H)STRAIN conducted research into innovative security solutions to improve the protection of the critical infrastructure "high-speed rail traffic" in Germany and France. Interdependencies between the two subsystems in France and Germany were considered and analyzed concerning risks resulting from the complexity of these interconnected systems. It is assumed that such risks can be exploited by intelligent and rationally acting terrorists applying BCRE weapons against specific vulnerabilities of the considered infrastructure.

Technological and organizational security measures were analyzed aiming at holistic solutions to increase the security of the infrastructure and its passengers against the highly sophisticated terrorist threat. The project analyzed and evaluated past incidents in order to investigate strategies and tactics of intelligent terrorists, tackle related new risks and threats, identify and research the capability of novel security measures (such as remote sensor combinations) and combine them with efficient security systems improving prevention, mitigation and resilience of the high-speed rail traffic without violating cross-cutting societal aspects like acceptance or privacy protection with respect to the security culture in Germany and France.

In the project RE(H)STRAIN, in order to describe and analyze the Franco-German high-speed passenger train system with respect to critical elements and requirements elicitation from the end-users, the quantity structure and functional representation of the Franco-German high-speed train system model were applied (Wang et al. 2018).

Based on the quantity structure (in this thesis, we only consider the German high-speed train system, and its quantity structure is shown in Figure 1.3), the most important elements of the high-speed system are identified through the algorithms from the graph theory field. Moreover, the most critical elements of the functional network are found through the interconnectedness interdependency analysis on the functional network.

To obtain a comprehensive understanding of the current, emerging and future nature of threat for passenger rail-based systems, a threat analysis is conducted, based on previous terrorist attacks (including details such as locations, casualties, infrastructure, impacts and effects) and emerging threats both in the physical and cyber security domains.

In the project RE(H)STRAIN, many complex scenarios were developed, addressing threats and risks for passengers and operators of high-speed trains (Zsifkovits and Pickl 2016a). Each scenario compiles and describes motivation and intention of potential terrorists, their potential means of attack from the BCRE arsenal (biological, chemical, radiological, explosive), the consequences (damage to infrastructure and railway traffic, the number of fatalities, injuries to persons, etc.) as well as the available intervention systems of the Franco-German systems.

Here, the intervention system describes the resilience capacity of the system and consists of measures reducing vulnerability, such as emergency management, preparedness and training of security staff as well as technological measures for prevention and mitigation of consequences.

In order to analyze the consequences of service disruption caused by terrorist attacks, risk assessment and impact analysis were implemented in the project RE(H)STRAIN (Zsifkovits and Pickl 2016b). Through risk assessment, a risk matrix was put out, which indicated where acceptable and inacceptable risks were located in the high-speed train system.

By conducting an impact analysis, a list of suitable security measures was achieved, serving as a basis for prevention (also the impact of sufficient detection methods for chemical detectors), mitigation and fast restoration strategies.

Meanwhile, in order to investigate the ability of the Franco-German high-speed train system to continue functioning in case of disruptions, a resilience analysis was carried out (Lotter et al. 2016). These special adaptive cycles in the system were studied in order to understand the system's vulnerability and its resilience capacity.

## 2.5 TOPSIS-based Aggregation Measure

In this chapter, we have introduced some basic terms which are used in the following chapters, including graph, network, graph theory and network theory. So far, we have introduced centrality, efficiency and also vulnerability measures, which can be used to identify the key nodes of a network from diverse perspectives.

In order to analyze the network comprehensively, TOPSIS, which can aggregate different measures, is also explained. Moreover, for the sake of adapting TOPSIS to transportation networks properly, we also introduce a new weight estimation approach, which is explained in detail in Chapter 3.

Finally, different quantitative resilience definitions are reviewed in this chapter; however, in our research, we only consider terrorist attacks as the disruptive events, and the resilience analysis here is mainly used to compare the aforementioned graph measures to verify whether the TOPSIS-based aggregation measure is a more suitable and effective measure than others to detect the key nodes. In this dissertation, we consider measuring resilience using graphical triangle representation based on network performance. In order to quantify network resilience properly, according to Nan et al. (2017), Martin-Breen et al. (2011) and Hosseini et al. (2016), we also propose a new network performance considering three factors, namely traveling time, the number of people who can use the transportation network and the train flow, that is how many trains pass through a given rail, which is presented in detail in Chapter 4.

In the following chapter, we therefore introduce relevant aggregation measures specifically for vulnerability indices.

The network resilience analysis from section 2.3 is based on the following publication:

*Wang, Z., Nistor, M. S., & Pickl, S. W. (2017). Analysis of the definitions of resilience. IFAC-PapersOnLine, 50(1), 10649-10657.*

# 3 Aggregation of Measures

## 3.1 Design and Characteristics of Network Structure and Vulnerability Measures

The understanding of network structures, functions, vulnerabilities and their relations can help decision-makers to reasonably allocate resources in order to protect networks from disturbances. As we know, there are many mechanisms, for instance cascading, spreading and synchronizing (Motter and Lai 2002, Pastor-Satorras and Vespignani 2002, Zhao et al. 2005, Zemanová et al. 2006), which are significantly affected by a small fraction of essential nodes. Therefore, how to identify these essential nodes is theoretically significant.

Furthermore, detecting important nodes has noteworthy practical value, which for instance can be used to control disease spreading and help decision-makers deploy security resources on a transportation network in advance to prevent terrorist attacks from happening, or at least it could reduce the impacts of terrorist attacks to a certain extent. In this chapter, we introduce and apply some graph measures to identify these essential nodes; moreover, to deeply explore the properties of the network, based on the idea of vulnerability and its dealing procedure, we have also developed two new nodal vulnerability measures to detect these critical nodes.

In this chapter, the network measures, such as centrality, efficiency and vulnerability measures, are presented as the central basis of the network analysis on the ICE network. Among the centrality measures in literature (Gómez and Figueira 2013), only four primary indices are considered in this thesis: degree centrality (Maharani and Gozali 2014), closeness centrality (Derrible 2012), eigenvector centrality (Maharani and Gozali 2014, Newman 2008) and betweenness centrality (Tsiotas and Polyzos 2015).

Meanwhile, “the classical network nodal efficiency” (Latora and Marchiori 2003, Nistor and Pickl et al. 2017) and “its improved version, i.e. flow-weighted network nodal efficiency” (Nistor and Pickl et al. 2017), are also described. When conducting the vulnerability analysis, we found that among the existing global vulnerability measures in literature (Mamut and Vumar 2008, Zhang and Wang 2013, Li et al. 2014, Zhang et al. 1999), most of them, for instance vertex connectivity (Mamut and Vumar 2008), vertex toughness (Bauer et al. 2013), vertex scattering (Kirlangiç 2002), vertex integrity (Mamut and Vumar 2008), vertex tenacity (Cheng et al. 2014) and vertex domination (Mishkovski et al. 2011, Alanko et al. 2011) can only detect trivial impacts due to the removal of one node or a group of nodes, but network residual closeness (Dangalchev 2006) is exceptional, according to which the relatively significant effects are caused by deleting one node or a small group of nodes.

Therefore, in this chapter, we propose two new *nodal vulnerability measures*: one is inspired by the betweenness centrality measure and efficiency measure, the other one is based on the network residual closeness.

### 3.1.1 Network Centrality Measures

The indicators of various centrality measures can be used to detect the key nodes in a graph. As reviewed in Chapter 2, many centrality measures have been developed and studied (Freeman 1978, Ruhnau 2000, Wang et al. 2011, Gómez and Figueira 2013, Tsiotas and Polyzos 2015). In this chapter, four of the most relevant existing centrality measures are implemented. They are degree centrality measure, closeness centrality measure, eigenvector centrality measure and betweenness centrality measure. In the following, we introduce these centrality measures in detail:

#### 3.1.1.1 Network Betweenness Centrality Measure (BetwCentr)

According to the betweenness centrality measure (Freeman 1978, Newman 2008, Boudin 2013), given one node in a graph, the more numbers of the shortest paths between all other pairs of nodes passing through the given node, the more critical the given node is.

In other words, a given node tends to be more crucial and has more potential to be attacked by terrorists, if it lies on the shortest paths connecting more pairs of nodes in a graph. Moreover, the nodal betweenness centrality also reflects the transitivity of a given node in a network. The formula of betweenness centrality $C_b(v_k)$ (Boudin 2013) for a node $v_k$ is defined as:

$$C_b(v_k) = \frac{2}{(n-1)(n-2)} \sum_{i \neq k}^{n} \sum_{j \neq i \neq k}^{n} \frac{\sigma_{ij}(v_k)}{\sigma_{ij}} \qquad (3\text{-}1),$$

where $\sigma_{ij}$ is the number of shortest paths between the nodes $v_i$ and $v_j$, and $\sigma_{ij}(v_k)$ is the number of the shortest paths between the nodes $v_i$ and $v_j$, which pass through the given node $v_k$.

### 3.1.1.2 Network Closeness Centrality Measure (CloCentr)

The closeness centrality (Freeman 1978, Boudin 2013, Tsiotas and Polyzos 2015) can be used to measure how close one node is to all the other nodes along the shortest paths, which means that a given node can be detected by this measure as the most critical one in a graph if the sum length of all the shortest paths from the given node to the remaining nodes of the graph is minimum, meaning the given node is closest to the remaining nodes in the graph. This can also reflect the accessibility of a given node in a graph. This measure is defined as "the reciprocal of the average distance from a given node $v_i$ to all other nodes" (Boudin 2013). As shown in Boudin (2013), the defined formula of the closeness centrality $C_c(v_i)$ of one node $v_i$ is shown as:

$$C_c(v_i) = \frac{n-1}{\sum_{j \neq i}^{n} d(v_i, v_j)} \qquad (3\text{-}2),$$

where $d(v_i, v_j)$ is the distance length (due to which we will apply this measure on the real German high speed network; therefore, we take 100 km as the unit of distance length) of the shortest path between node $v_i$ and node $v_j$.

### 3.1.1.3 Network Degree Centrality Measure (DegCentr)

The degree centrality measure (Freeman 1978, Boudin 2013) is defined as the number of edges that one node shares with the others. This is a simple indicator of whether one node is very connected (hub node) in a network or not. According to Freeman (1978) and Maharani and Gozali (2014), Formula $C_d(v_i)$ of the degree centrality of one node $v_i$ is defined as:

$$C_d(v_i) = \frac{|N(v_i)|}{n-1} \quad (3\text{-}3),$$

where $|N(v_i)|$ is the number of adjacent nodes of the node $v_i$; here, the nodes in this adjacent node set $N(v_i)$ are straightly connected to the node $v_i$.

### 3.1.1.4 Network Eigenvector Centrality Measure (EigenCentr)

The importance of a node in a network can be measured with the help of the eigenvector centrality measure (Maharani and Gozali 2014, Ruhnau 2000, Boudin 2013).

However, the importance of a central node depends not only on the number of its neighbors, but also on the importance of its neighbors. The eigenvector centrality $C_e(v_i)$ (Boudin 2013) for a node $v_i$ is defined as:

$$C_e(v_i) = \frac{1}{\lambda} \sum_{v_j \in N(v_i)} a_{ji} \times C_e(v_j) \quad (3\text{-}4),$$

where $N(v_i)$ is the set of nodes connected to $v_i$, and $\lambda$ is the maximum eigenvalue of the adjacency matrix.

Because these aforementioned four nodal network centrality measures are widely applied in different fields and networks to detect the important nodes (Freeman 1978, Boudin 2013, Chen et al. 2012, Chen and Hu 2013, Emmert-Streib 2011, Guimera et al. 2005), therefore, in this thesis, we take them as the basic measure to be applied on the German high speed network to identify the critical stations with higher potential risk of terrorist attacks. Meanwhile, based on these basic centrality measures, we also propose new measures and compare their effectiveness.

### 3.1.2 Network Efficiency Measures

Whether the information can be exchanged efficiently from one node to the rest of the network can be characterized with the support of efficiency measures. Based on the values of the efficiency measures, people can tell the differences among nodes and determine which ones are more critical than others. In this section, two types of efficiency measures are presented. These are the classical efficiency measures and their variation, for example the flow-weighted efficiency measure, which in addition computes the flow information between the nodes of a network.

#### 3.1.2.1 Network Classic Efficiency Measure (Effi)

According to Nistor and Pickl et al. (2017) and Latora and Marchiori (2003), the classical efficiency measure computes the distance length of the shortest paths from a given node to all the others. Its formula for a node $v_i$ in the graph $G$, $E_{V(G)}(v_i)$ (Latora and Marchiori 2003) is defined as:

$$E_{V(G)}(v_i) = \frac{1}{n-1}\sum_{j\neq i}^{n}\frac{1}{d(v_i,v_j)} \quad (3\text{-}5),$$

where $d(v_i,v_j)$ is defined as the distance length (unit of 100 km) of the shortest path between node $v_i$ and node $v_j$.

#### 3.1.2.2 Network Flow-Weighted Efficiency Measure (FWEffi)

Based on the classical efficiency measure (Latora and Marchiori 2003), the flow-weighted efficiency measure (Nistor and Pickl et al. 2017) considers not only the distance length of the shortest paths, but also the train flow information between the nodes of a network. The network flow-weighted efficiency measure $E_{F\_V(G)}(v_i)$ (Nistor and Pickl et al. 2017) for a node $v_i$ is defined as:

$$E_{F\_V(G)}(v_i) = \frac{1}{n-1}\sum_{j\neq i}^{n}\frac{w(v_i,v_j)}{d(v_i,v_j)} \quad (3\text{-}6),$$

where $w(v_i, v_j)$, which represents the lowest train flow of all edges along the shortest path between the nodes $v_i$ and $v_j$, and is defined as (Nistor and Pickl et al. 2017):

$$w(v_i, v_j) = \min_{(v_k, v_l) \in P_{ij}} \varpi_{kl} \quad (3\text{-}7),$$

where $P_{ij}$ represents the set of edges on the shortest path from node $v_i$ to node $v_j$, and $\varpi_{kl}$ denotes the train flow between the connected nodes $v_i$ and $v_j$. In this thesis, the train flow of the ICE network on the Tuesday to Thursday schedule (May 24 – 26, 2016) is considered.

### 3.1.3 The New Nodal Graph Vulnerability Measures

The objective of the RE(H)STRAIN project was to analyze the vulnerability of the rail-bound DE-FR high-speed train system (ICE, TGV) as part of the critical infrastructure "transport" in view of threats from terrorism as well as the derivation of measures for the improvement of their resilience; hence, the vulnerability of transportation networks is one of the central research focuses. Therefore, in this thesis, based on the aforementioned centrality measures and efficiency measures addressed in previous subsections of this chapter, we propose two nodal graph vulnerability measures, which are introduced in this subsection.

As it is well-known, "our daily lives are so dependent on the functioning of critical infrastructures" that they have become a significant target of terrorist attacks (Rinaldi 2004). Thereby, well-planned assaults on the most vital and vulnerable hubs or spots can damage a system very heavily. The protection of such infrastructures is a crucial challenge and essential. As one of the critical infrastructures, public transport plays a vital role in our society. One example of such a vulnerable public transport system is the German high-speed train system (ICE) (Deutsche Bahn 2018), on which the study of this thesis mainly focuses. In the future, many advanced security technologies can be applied to keep the ICE network safe. However, economic boundaries demand a highly efficient use of resources. Thus, before deploying security measures, decision-makers need to deeply understand the vulnerabilities of the ICE network.

The aim of the analysis in this subsection is to make full use of the quantitative graph theory to analyze the vulnerabilities of the graph and to detect the centers (or hubs) of the system. In this part, inspired by the idea of global residual closeness and the idea of vulnerability in graph theory, we have not only proposed a nodal residual closeness vulnerability measure, but based on the betweenness centrality measure and the efficiency measure we have also proposed a new vulnerability measure that we call betweenness-efficiency vulnerability measure. Both of them can be used to detect the most vulnerable nodes, which therefore have more potential to harm the overall system in case of disruption. The analysis of this subsection can help decision-makers understand the structure, behavior and vulnerabilities of the network more clearly from the quantitative graph theory's point of view.

#### 3.1.3.1 Nodal Residual Closeness Vulnerability Measure (ResiduCloVul)

In Dangalchev (2006), the graph global residual closeness is defined by Dangalchev (2006) as:

$$GRC(G) = \min_{k\in[1,n]}\left( \sum_{i}\sum_{j\neq j} \frac{1}{2^{d_{G\_k}(v_i,v_j)}} \right) \quad (3\text{-}8),$$

where $d_{G\_k}(v_i,v_j)$ denotes the distance of the shortest path between node $v_i$ and $v_j$, after node $v_k$ is removed from the original graph $G$. The author showed that global residual closeness was more sensitive than other well-known global vulnerability measures like vertex integrity, connectivity, toughness, binding number, and so on. Even deleting only one node from the original graph that can't lead to the disconnection of the remaining graph, the global residual closeness can still detect the apparent change between the original graph and the remaining graph.

In graph theory, when analyzing whether one given node in a graph is vulnerable (which means that once the given node is removed from the original graph, it will lead to a large change of graph structure), if in a real network (which has been mapped into a graph, for instance in this thesis the ICE network), it could lead to a huge loss, including economic losses and casualties if attacked.

Therefore, the given node will have more potential to be attacked by terrorists. Inspired by the idea of vulnerability in graph theory, here, we have proposed a nodal residual closeness vulnerability measure, which is defined as:

$$NRC(v_x) = \frac{|GRC(G) - GRC(G_x)|}{GRC(G)} \quad (3\text{-}9),$$

where $G_x$ denotes the remaining graph after node $x$ is removed from the original graph $G$, and similar to Formula (3-8), the global residual closeness of the remaining graph is defined as:

$$GRC(G_x) = \min_{k\in[1,n-1]}\left(\sum_i \sum_{j\neq i} \frac{1}{2^{d_{G_{x-k}}(v_i,v_j)}}\right) \quad (3\text{-}10),$$

where accordingly, $d_{G_{x-k}}(v_i, v_j)$ denotes the distance of the shortest path between node $v_i$ and $v_j$, after node $v_k$ is removed from the remaining graph $G_x$.

### 3.1.3.2 Betweenness-Efficiency Vulnerability Measure (BetwEffiVul)

Accordingly, based on betweenness centrality and efficiency measures, as well as taking into account the idea of nodal residual closeness vulnerability measure, here we propose a new vulnerability measure: the betweenness-efficiency vulnerability measure (Wang and Zsifkovits 2018). This measure is defined as

$$BEV(v_x) = \frac{|BEV^*(G) - BEV^*(G_x)|}{BEV^*(G)} \quad (3\text{-}11),$$

where $x = \{1, 2, ..., n\}$, and $BEV^*(G)$, which denotes the original graph measure value without removing any nodes, is defined as:

$$BEV^*(G) = \frac{\sum_{k=1}^{n}\left(\sum_{i\neq k}^{n}\sum_{j\neq i, j\neq k}^{n}\left(\frac{1}{2^{d_G(v_i,v_j)}} - \frac{1}{2^{d_{G(k)}(v_i,v_j)}}\right)\right)}{n(n-1)/2} \quad (3\text{-}12),$$

where $d_G(v_i, v_j)$ represents the distance length of the shortest path between node $i$ and $j$ in the original graph $G$. $d_{G(k)}(v_i, v_j)$ denotes the distance length of the

shortest path between node $i$ and $j$ in the original graph $G$; meanwhile, this shortest path will go through node $k$. In Formula (3-11), $G_x$ denotes the remaining graph after node $x$ is removed from the original graph. Therefore, $BEV^*(G)$, which denotes the remaining graph measure value after removing the $x^{th}$ node from the original graph, is defined as:

$$BEV^*(G_x) = \frac{\sum_{k=1}^{n-1}\left(\sum_{i\neq k}^{n-1}\sum_{j\neq i,j\neq k}^{n-1}\left(\frac{1}{2^{d_{G_x}(v_i,v_j)}} - \frac{1}{2^{d_{G_x(k)}(v_i,v_j)}}\right)\right)}{(n-1)(n-2)/2} \qquad (3\text{-}13),$$

where $d_{G_x}(v_i, v_j)$ denotes the distance length of the shortest path between nodes $i$ and $j$ in the remaining graph $G_x$; $d_{G_x(k)}(v_i, v_j)$ represents the distance length of the shortest path between nodes $i$ and $j$ passing through node $k$ in the residual graph $G_x$. The reason to choose $2^{d_x(v_i,v_j)}$ in the definition of the proposed measure is that it doesn't need to judge whether node $i$ and node $j$ are the same ones when computing this measure in order to save calculating time and also to be convenient for matrix calculations. Because when they are the same, the distance will be zero, that is nullity, if it is the denominator.

Since this proposed measure is used to quantify the significance of the influence it will have on a graph after removing one node from the graph, it is apparent that the corresponding node needs to be removed when calculating the measure of value of a given node. However, no matter how the order of the deleting nodes is changed, this measure cannot be affected. Therefore, the measuring results of every node will not vary.

### 3.1.4 Implementations and Discussions

The results based on the aforementioned centrality, nodal efficiency and also the proposed nodal vulnerability measures in this chapter are shown in the Appendix from Table A-1 to Table A-8. As an example, we show one of the tables in the Appendix, such as Table A-1, in the following:

Table A-1: The results based on betweenness centrality measure

| ID | Betweenness | ID | Betweenness | ID | Betweenness | ID | Betweenness |
|---|---|---|---|---|---|---|---|
| 1 | 0.284033613 | 32 | 0.034173669 | 63 | 0.092156863 | 94 | 0.033053221 |
| 2 | 0.196778711 | 33 | 0.038795518 | 64 | 0.102941176 | 95 | 0.016666667 |
| 3 | 0 | 34 | 0.131092437 | 65 | 0 | 96 | 0 |
| 4 | 0.165266106 | 35 | 0.087955182 | 66 | 0.158823529 | 97 | 0.016666667 |
| 5 | 0.049159664 | 36 | 0 | 67 | 0.033613445 | 98 | 0.016666667 |
| 6 | 0.033053221 | 37 | 0.037114846 | 68 | 0.034313725 | 99 | 0 |
| 7 | 0 | 38 | 0.02394958 | 69 | 0.041736695 | 100 | 0.094677871 |
| 8 | 0 | 39 | 0 | 70 | 0 | 101 | 0 |
| 9 | 0.04929972 | 40 | 0.042857143 | 71 | 0.131512605 | 102 | 0.144257703 |
| 10 | 0 | 41 | 0.104761905 | 72 | 0.033053221 | 103 | 0.280392157 |
| 11 | 0.016526611 | 42 | 0.008683473 | 73 | 0.016666667 | 104 | 0.17464986 |
| 12 | 0 | 43 | 0.010644258 | 74 | 0 | 105 | 0.091316527 |
| 13 | 0 | 44 | 0.030812325 | 75 | 0 | 106 | 0 |
| 14 | 0.034313725 | 45 | 0.000840336 | 76 | 0.078571429 | 107 | 0.064985994 |
| 15 | 0.024229692 | 46 | 0.029551821 | 77 | 0.064985994 | 108 | 0.139915966 |
| 16 | 0.033473389 | 47 | 0.02394958 | 78 | 0.049159664 | 109 | 0.125490196 |
| 17 | 0 | 48 | 0.013865546 | 79 | 0.033053221 | 110 | 0.110784314 |
| 18 | 0.118627451 | 49 | 0 | 80 | 0.026190476 | 111 | 0.095798319 |
| 19 | 0.016666667 | 50 | 0.066666667 | 81 | 0.027310924 | 112 | 0.080532213 |
| 20 | 0 | 51 | 0.043557423 | 82 | 0.181652661 | 113 | 0.064985994 |
| 21 | 0.10952381 | 52 | 0.114845938 | 83 | 0.007282913 | 114 | 0.049159664 |
| 22 | 0.201960784 | 53 | 0.114145658 | 84 | 0.006162465 | 115 | 0.033053221 |
| 23 | 0.090616246 | 54 | 0.041736695 | 85 | 0.090616246 | 116 | 0.016666667 |
| 24 | 0.149019608 | 55 | 0.032492997 | 86 | 0.037885154 | 117 | 0 |
| 25 | 0 | 56 | 0.033053221 | 87 | 0.047478992 | 118 | 0.049159664 |
| 26 | 0.114565826 | 57 | 0.016666667 | 88 | 0 | 119 | 0.033053221 |
| 27 | 0.163585434 | 58 | 0 | 89 | 0.113165266 | 120 | 0.016666667 |
| 28 | 0.116526611 | 59 | 0.088935574 | 90 | 0.025770308 | 121 | 0 |
| 29 | 0.050280112 | 60 | 0.082913165 | 91 | 0.116946779 | | |
| 30 | 0.041736695 | 61 | 0.078291317 | 92 | 0.049439776 | | |
| 31 | 0.03487395 | 62 | 0.081372549 | 93 | 0 | | |

According to Table A-1 to Table A-8, the top ten stations that are identified by these different measures are presented in Table 3-1 and highlighted in Figure 3.1 to Figure 3.8.

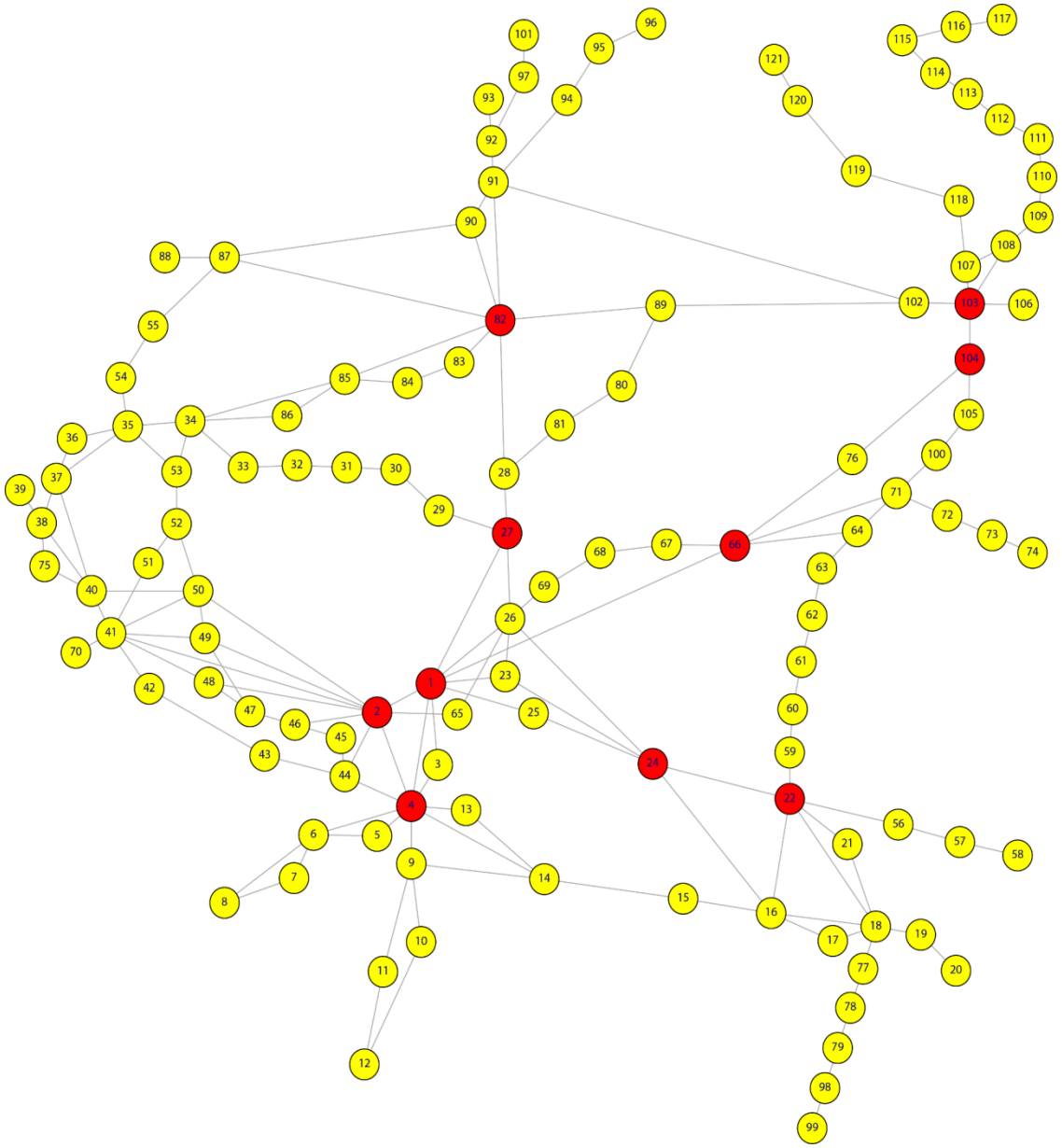



Figure 3.1: Top ten stations identified by betweenness centrality measure are highlighted in red color

From Figure 3.2 we can see that these top ten stations detected by betweenness centrality measure are mainly the important transferring stations; if removing them, the network will be disconnected and separated into eleven parts, which means that the cost and time of transport will significantly increase.

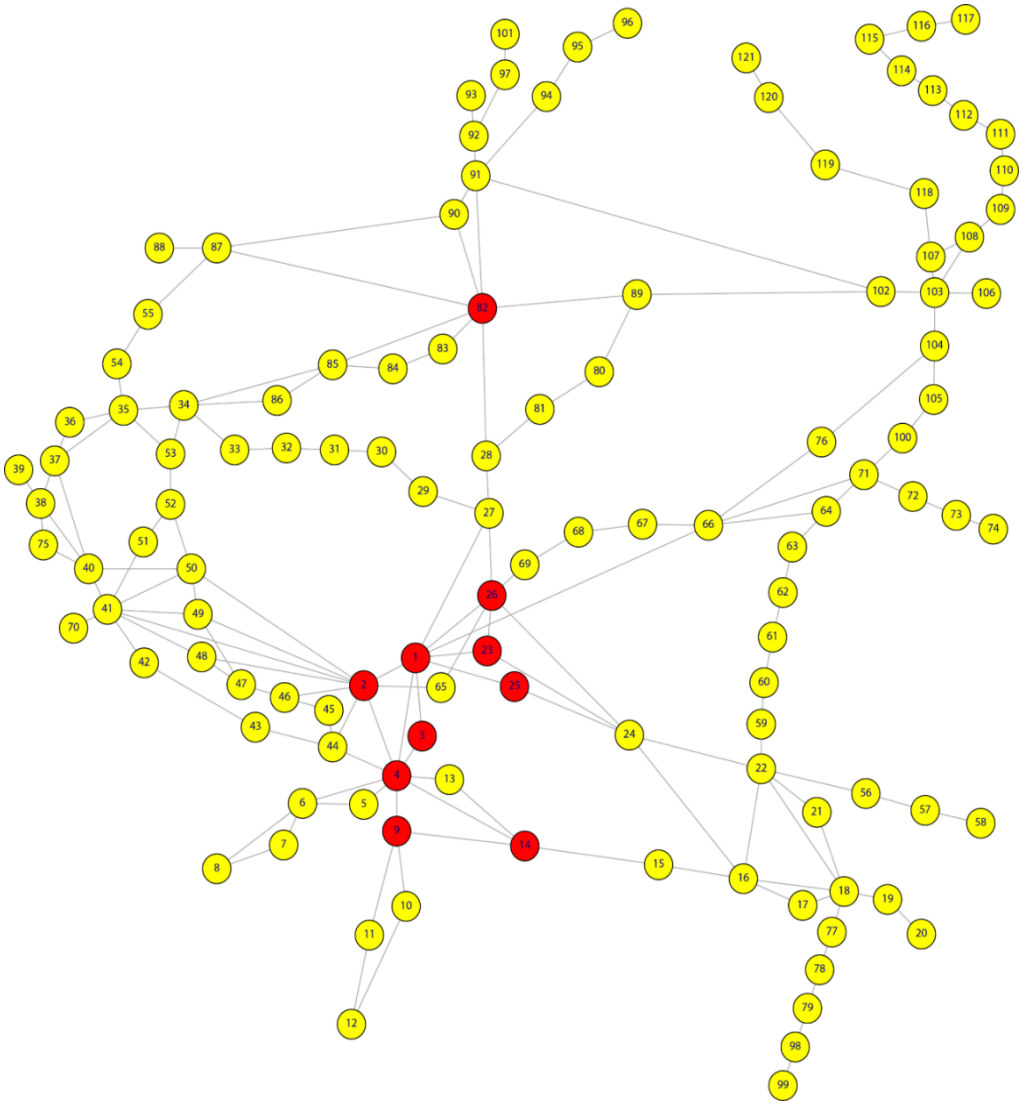



Figure 3.2: Top ten stations identified by closeness centrality measure are highlighted in red color

Different from Figure 3.1, according to Figure 3.2, except for station 82, the rest of the top ten stations detected by closeness centrality measure focuses on one zone. If deleting these top ten stations, the network will also be disconnected but only divided into five parts, and four parts of them are just very small components (part one only contains station 13; part two only has station 65; part three consists of stations 5, 6 ,7 and 8; stations 10, 11 and 12 belong to part four; and part five includes the remaining stations). Therefore, compared to Figure 3.1, the cost and time of transport will increase less.

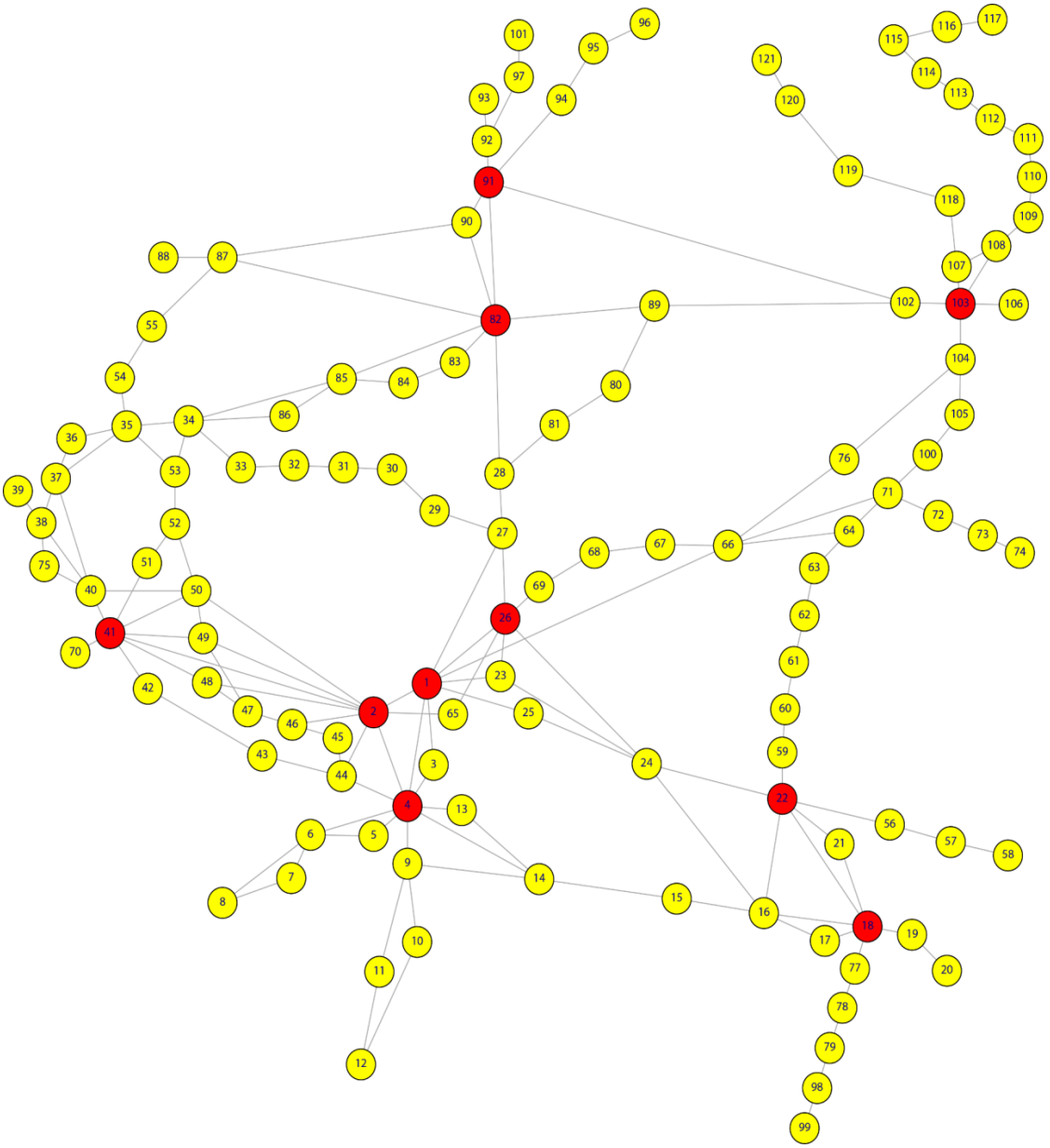



Figure 3.3: Top ten stations identified by degree centrality measure are highlighted in red color

Similar to Figure 3.1, but different from Figure 3.2, in Figure 3.3, the top ten stations detected by degree centrality measure are also at the important transferring stations. When these critical stations are shut down, the network will be separated into fifteen parts; therefore, the transit efficiency of the network will significantly decrease, and the cost and time of transport will increase to a more apparent extent than it is the case in Figure 3.1.

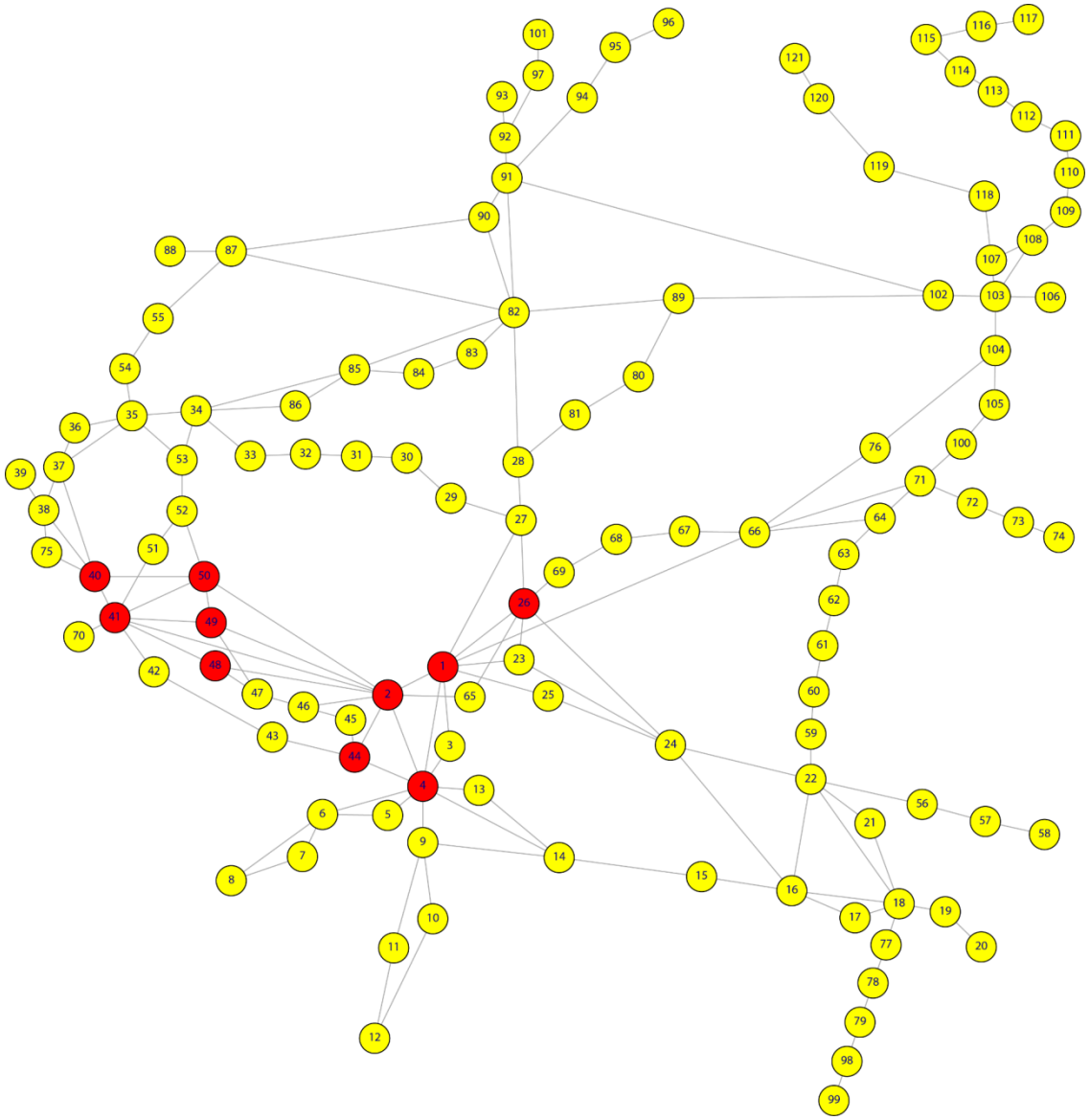



Figure 3.4: Top ten stations identified by eigenvector centrality measure are highlighted in red color

Apparently, according to Figure 3.4, the top ten stations identified by the eigenvector centrality measure mainly focus on one zone and most of them are directly connected to station 2. Therefore, based on the eigenvector centrality measure, station 2 is the most important one. Furthermore, when removing these top ten stations, the network will be divided into seven parts, but six of which only contain stations 1 to 4. Thus, in such a case, the influence will be lower than in Figure 3.1 and Figure 3.3.

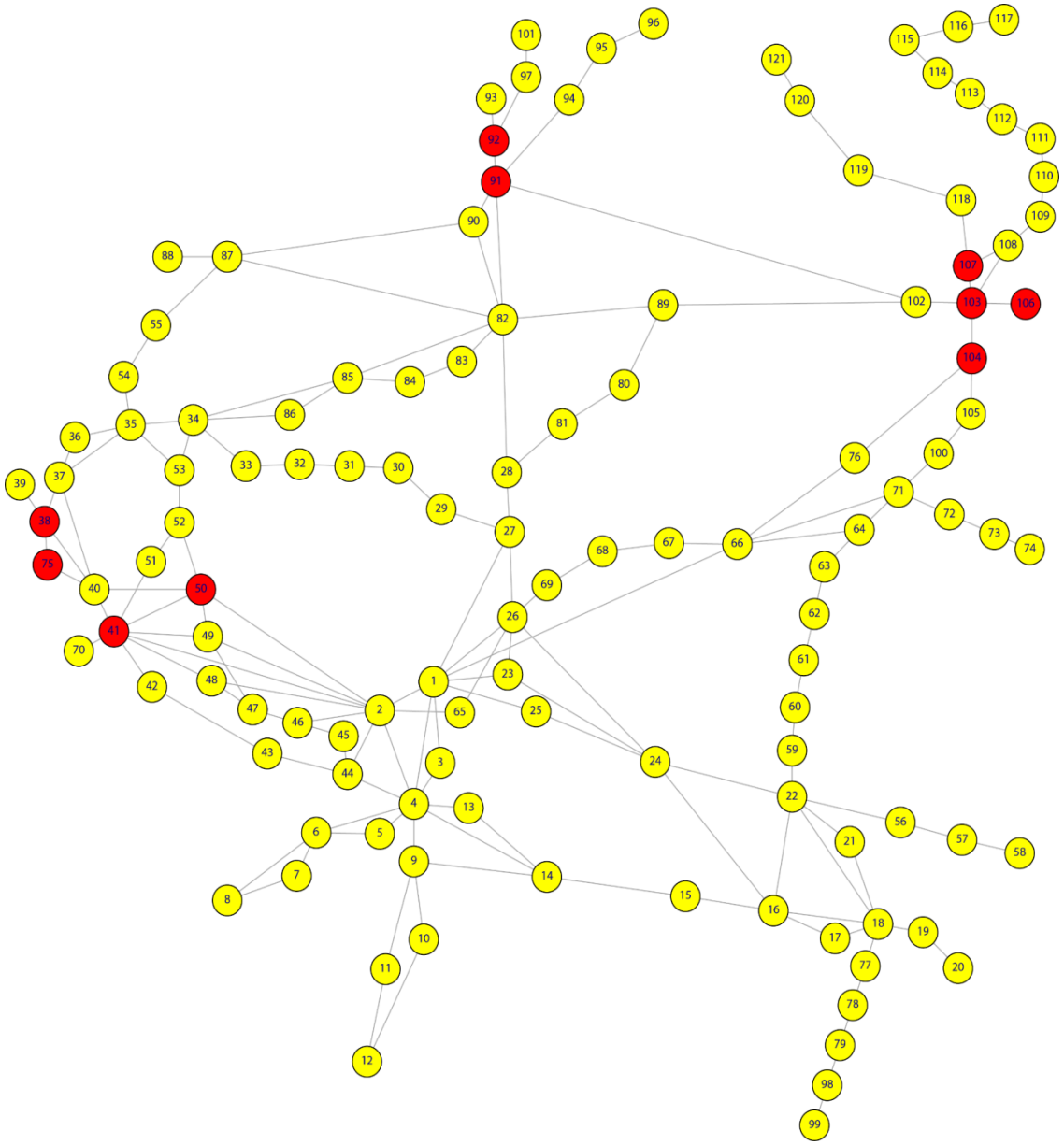



Figure 3.5: Top ten stations identified by nodal efficiency measure are highlighted in red color

According to Figure 3.5, the top ten stations are mainly located in three zones. However, the important stations 1 and 2, which are marked as the top ten stations in Figure 3.1 - Figure 3.4, are not highlighted as the top ten stations by nodal efficiency measure, but the end station 106 is identified as one of the top ten stations. In a certain sense this is abnormal.

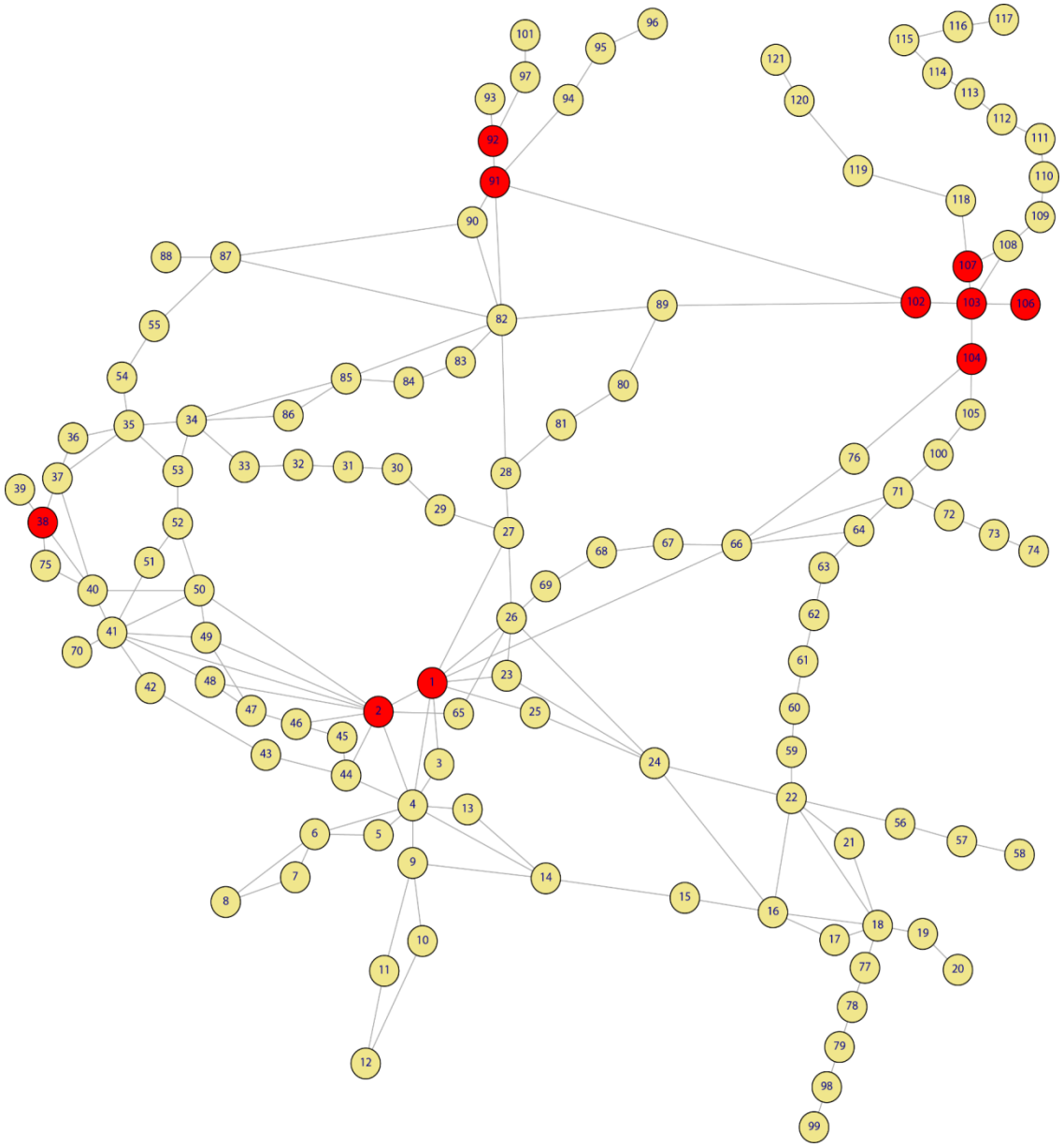



Figure 3.6: Top ten stations identified by flow-weighted efficiency measure are highlighted in red color

Similar to Figure 3.5, the top ten stations highlighted in Figure 3.6 are distributed in four zones. Based on the nodal efficiency measure, when considering the factor train flow, the improved flow-weighted efficiency measure can also identify the stations 1 and 2 as part of the top ten critical stations. However, the only problem is that station 106 with only one neighbor station is still detected as one of the top ten stations.

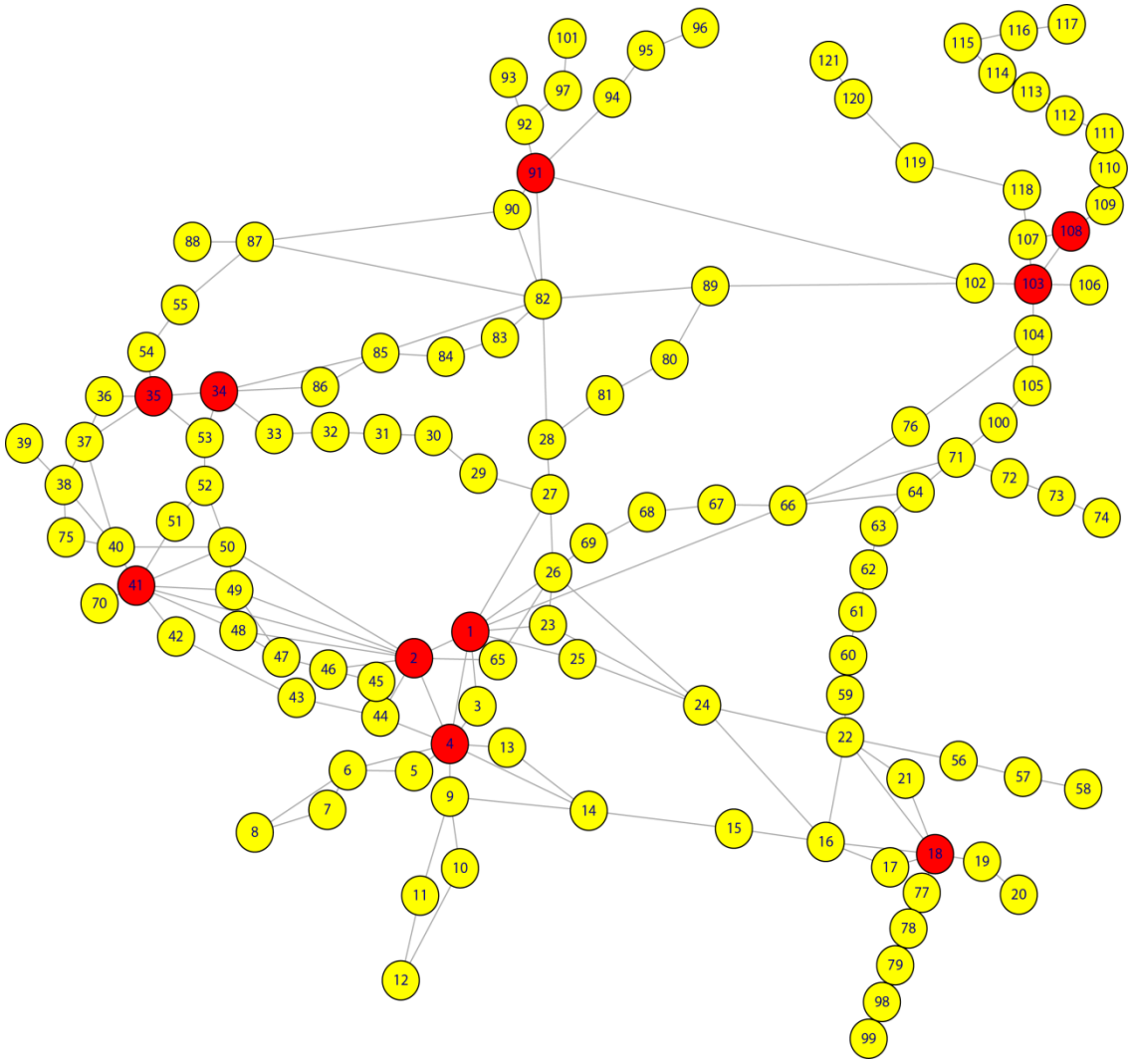



Figure 3.7: Top ten stations identified by nodal betweenness-efficiency vulnerability measure are highlighted in red color

As introduced before, the proposed nodal betweenness-efficiency vulnerability is based on the betweenness centrality measure and the efficiency measure; thus, the proposed measure can be seen as an aggregation measure. Comparing Figure 3.7 with Figure 3.1 and Figure 3.5, it is found that some of the top ten stations highlighted in Figure 3.7 can be found in Figure 3.1 and some of the top ten stations marked in Figure 3.7 only appear in Figure 3.5; however, it is interesting that there are also four new stations (stations 18, 34, 35 and 108) marked as part of the top ten critical stations in Figure 3.7. In such a case, this aggregation measure can not only compensate the disadvantages of a single measure, but it can also mine new information.

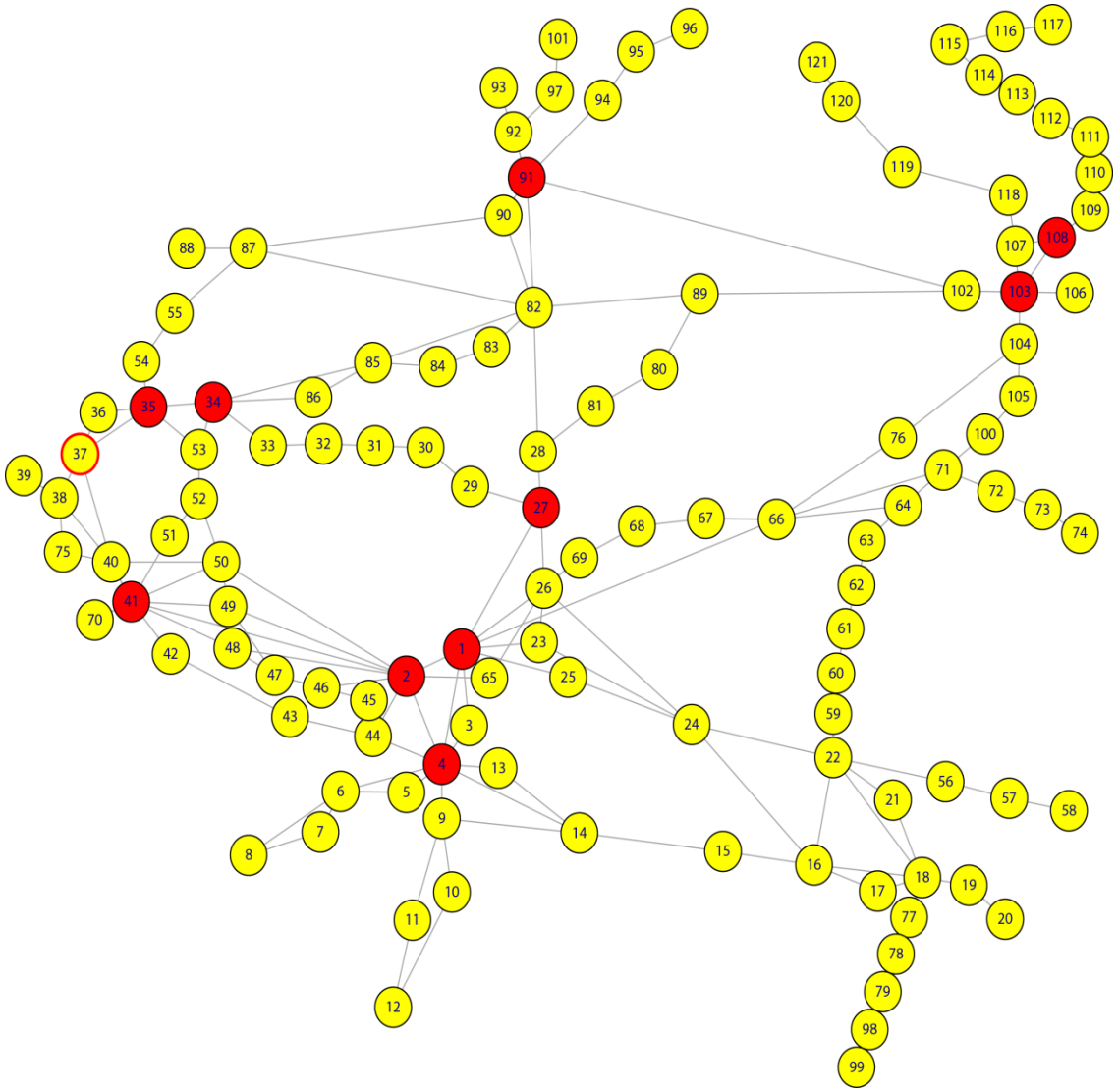



Figure 3.8: Top ten stations identified by nodal residual closeness vulnerability measure are highlighted in red color

Intuitively, according to Figure 3.1 - Figure 3.8, the different characteristics of distinct graph measures can be found from diverse graph structure perspectives. For instance, in Figure 3.1, resulting from betweenness centrality measure, most of these key stations lie on the very important transferable points, which means most of the shortest paths between other pairs of stations will pass them; thus, once they are attacked and shut down, the transit efficiency of the network will decrease to a rather apparent extent.

As shown in Figure 3.2, based on closeness centrality measure, although it can detect the key stations, most of them are in the same zone, and with this figure one cannot tell the differences among these key stations. The degree centrality is a very simple and basic measure that only considers how many neighbors a given node has. It also has a network transferring character like the betweenness centrality measure.

Therefore, most of the top ten stations detected by the degree centrality measure and the betweenness centrality measure are the same. Comparing Figure 3.1 and Figure 3.3, the degree centrality can be seen as a complement of betweenness centrality measures due to the fact that the stations 18, 41 and 91 in this network are also identified as key stations, which are located in very important cities in Germany, like Munich, Cologne and Hamburg; the details regarding the stations' ID versus their corresponding station names are listed in Appendix Table A-15.

Based on eigenvector centrality measure, one node can be detected as an important point not only because of its own significance but also because of the importance of its neighbors. Therefore, as highlighted in Figure 3.4, the top ten stations based on eigenvector centrality measure are basic only in the same small region; in this case, it is similar to closeness centrality measure.

Originated from closeness centrality, the nodal efficiency measure can also be applied in a disconnected network in which two stations cannot reach each other, but unlike the results based on closeness centrality, most of the top ten stations highlighted in Figure 3.5 are scattered in three different zones.

Moreover, based on the nodal efficiency measure, the flow weighted efficiency measure further considers the train flow between pairs of straightly connected stations. In such a case, the results shown in Figure 3.6 are a little different and a few improvements by comparing the results of the nodal efficiency measure can be achieved.

Furthermore, inspired by the betweenness and nodal efficiency measure, the developed nodal betweenness-efficiency vulnerability measure combines advantages of these two measures, and the top ten stations are shown in Figure 3.7.

Comparing Figure 3.7 with Figure 3.1 and Figure 3.5, we can find that only node 103 is the shared node in the top ten stations identified by both the betweenness centrality and nodal efficiency measure, and more stations could be found in the top ten stations based on the betweenness centrality measure; meanwhile, four stations do not belong to any top ten stations sets based on both betweenness centrality and nodal efficiency measures. However, according to the distribution of the top ten stations in Figure 3.7, the nodal betweenness-efficiency vulnerability measure is a promising measure for identifying the key stations, because the detected top ten stations are all located in the most important cities in Germany; the corresponding cities' names of these stations are shown in Table A-15.

Interestingly, originated from closeness centrality, but also taking into account nodal efficiency and the idea of global residual vulnerability, the top ten stations highlighted in Figure 3.8 detected by the proposed nodal residual closeness vulnerability are almost the same, even the order of them presented in Table 3-1 are similar.

Now let us come back to Table 3-1. It is apparent that the orders of most key stations identified by different measures are entirely distinctive. What can be noticed is that the top one station 92 detected by the nodal flow-weighted efficiency measure only appears in the top ten stations determined by the nodal classical efficiency measure in the top-five ranks.

However, also based on Table 3-1, if taking into account the frequencies of each station appearing in the top one lists (which means that we only consider the stations that appear in the first ranking position in each list based on different measures), it is easy to find that the stations 1, 2 and 103 have the same frequencies. Therefore, it is impossible to distinguish which one is the most important station.

Nevertheless, if considering the frequencies of each station appearing in the top two lists, here we count the frequencies of how many times the stations appear in the ranking in the first and second ranking positions in each list based on different measures. Thereby, we can find that station 4 has the highest frequencies and the second one is station 103; in such a case, we can only conclude that the most crucial station is station 4, *but we can still not rank other stations*.

#### 3.1.4.1 Ranking and Rank Order

When taking into account the frequencies of each station appearing in the lists within the top three positions, stations 4 and 103 have the same frequencies. Likewise, it is the same situation between stations 1 and 2. Thus, most key stations cannot be identified in such a case.

Moreover, if considering the frequencies of each station appearing in the lists within the top four, five or six positions, station 1 with the highest frequency can be regarded as the most important station. When taking into account the frequencies of each station appearing in the top seven lists, we can find that the stations 1, 2 and 4 have the same frequencies, according to which we can't come to a conclusion which one is the most important station.

Nevertheless, when further considering the rank order of each station in every list, we can find that station 4 mostly appears in the top two positions, thus station 4 can be regarded as the most important one. Comparing stations 1 and 2 based on their rank orders in every list, they always have the same frequencies before the top three ranks, but when reaching top four positions, station 1 has a higher frequency; in such a case, we can say that station 1 is more important than station 2, so the top three stations could be station 4, station 1 and station 2.

When thoroughly taking into account the frequencies of each station's appearing in these lists within the top ten positions, only nine stations can be distinguished, which are stations 1, 2, 4, 41, 103, 91, 26, 82 and 104, and the frequencies of most other stations are mainly 2 or 1. Yet, among these nine stations, we still cannot tell the difference between them, because station 1 and 2 for instance have the same frequencies; likewise, the same frequencies can be found between stations 41 and 103, and even the three stations 26, 82 and 104 also have the same frequencies. Nonetheless, as aforementioned, taking into account the rank order of each station in every list, we can find that station 1 is more important that station 2. Comparing stations 41 and 103, we can see that station 103 mostly appears in the top two positions, while station 41 only appears after top two positions, so it is easy to tell the difference between them.

Furthermore, among stations 26, 82 and 104, we can notice that station 26 mainly appears between the top ranks eight and nine, station 82 appears twice in the top five ranks, while station 104 only appears in the top positions five, six and eight. Therefore, combining the frequencies of each station's appearing in these lists with top ten positions and the rank order of each station in every list, we can rank these top nine stations as follows: 1, 2, 4, 103, 41, 91, 82, 104, 26.

Even though nine stations can be ranked based on the frequencies and their corresponding rank order in every list, it is difficult to rank all of the stations based on this idea, especially since it will be more difficult once the number of stations increases. Since so far there hasn´t been any unified standard criterion to tell the difference of various graph measures from each other and to compare them in order to find out which one is more suitable and efficient to detect the most critical nodes in graph theory, when applying different graph measures on a graph (or network), it can therefore certainly lead to different results, which will cause the problem of information overload for decision-makers, who, based on these results, still can't know which measure is the more efficient one to identify the most suitable and practical essential nodes in a graph.

#### 3.1.4.2 Graph Measures and Multi-criteria Decision Making

Since different graph measures analyze the graph from different perspectives, every graph measure is a special one, which can lead to meaningful results based on its typical analysis´ perspective of view. Therefore, it will be helpful to resolve the information overflow problem for decision-makers if there is one method that does not only consider multitude measures and combines their advantages, but also yield more efficient and meaningful results.

In the Multi-criteria Decision Making field, we found one approach called Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), which could combine many criteria and also take the advantages of each criterion into account, giving comprehensive decision-making advice for decision-makers.

In the next subsection of this chapter, we introduce this kind of approach in detail, while adapting this approach to graph measures and especially to our research problem.

We also present a new parameter evaluation approach based on global graph vulnerability analysis.

Table 3-1: Top ten stations based on different measures

| Rank | Centrality | | | | Nodal Efficiency | | Nodal Vulnerability | |
|---|---|---|---|---|---|---|---|---|
| | BetwCentr | CloCentr | DegCentr | EigenCentr | Effi | FWEffi | BetwEffiVul | ResiduCloVul |
| 1 | 1 | 1 | 2 | 2 | 103 | 92 | 103 | 4 |
| 2 | 103 | 4 | 4 | 4 | 106 | 91 | 4 | 103 |
| 3 | 22 | 2 | 1 | 41 | 41 | 103 | 34 | 34 |
| 4 | 2 | 23 | 41 | 1 | 50 | 107 | 1 | 1 |
| 5 | 82 | 25 | 82 | 50 | 91 | 104 | 35 | 2 |
| 6 | 104 | 3 | 18 | 49 | 92 | 102 | 41 | 35 |
| 7 | 4 | 82 | 22 | 44 | 107 | 106 | 2 | 41 |
| 8 | 27 | 14 | 26 | 48 | 104 | 1 | 91 | 27 |
| 9 | 66 | 26 | 91 | 26 | 38 | 2 | 108 | 108 |
| 10 | 24 | 9 | 103 | 40 | 75 | 38 | 18 | 91 |

From Table 3-1 we can see that the top ten stations identified by different measures are mainly distinctive; even though there are some common stations, their ranking orders based on diverse measures are also different. Comparing the top ten stations detected by Effi and FWEffi (because the latter one considers one more factor, which is train flow), the improved nodal flow-weighted efficiency can also identify the critical stations 1 and 2, which can be detected by all other measures as the top ten stations.

Furthermore, comparing CloCentr with ResiduCloVul and also comparing BetwCentr and Effi with BetwEffiVul, as introduced before, the latter one in every comparative group combines the information of former one and aggregates new factors.

Therefore, from Table 3-1, we can see that the aggregation measures (ResiduCloVul and BetwEffiVul) can not only inherit the advantage of a single measure, but they can also compensate the disadvantage of a single measure and give us some additional new information. Thus, in this thesis, one of the research focuses is to look for a suitable aggregation approach, which can combine much more information and lead to more comprehensive results. The detailed information regarding the aggregation method is introduced in the next subsection of this chapter.

## 3.2 New Aspect: Multi-criteria Decision Making (MCDM) in RE(H)STRAIN as a Comprehensive Approach

When evaluating and ranking alternatives across distinctive application fields, the Multi-Criteria Decision Making (MCDM) approaches have drawn lots of attention from researchers and experts. Among copious MCDM approaches that can be used to deal with real-world decision-making problems, the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) continues to work suitably across diverse application fields. Hwang and Yoon (1981) initially developed TOPSIS to help find the best alternative within a finite number of criteria. As a well-known MCDM approach, the global interest of the TOPSIS method has exponentially grown since the 1980s.

### 3.2.1 TOPSIS as Possible Ranking Approach

The so-called TOPSIS method is a simple ranking approach in the application (Roszkowska 2011). The TOPSIS method aims “to select the best alternative that simultaneously has the shortest distance from the positive ideal solution and furthest distance from the negative ideal solution” (Roszkowska 2015). Here the positive ideal solution means maximum alternative value based on benefit criteria and minimum alternative value based on cost criteria; however, the negative ideal solution represents the minimum alternative value according to benefit criteria and maximum alternative value according to cost criteria.

TOPSIS offers a cardinal ranking of finite distinctive alternatives by making full use of attribute information but without considering the attribute preferences to be independent (Chen and Hwang 1992, Yoon and Hwang 1995). So far, TOPSIS has been applied in a lot of different fields, such as supply chain management and logistics, engineering and manufacturing systems, business and marketing management, human resources management, energy management, and so on (Behzadian and Otaghsara 2012). In order to apply the TOPSIS method in a specific area, the attribute values of different criteria must be numeric, monotonically increasing or decreasing and have commensurable units (Behzadian and Otaghsara 2012).

Mainly, there are seven steps when implementing TOPSIS in a specific application area (Chen and Hwang 1992, Yoon and Hwang 1995):

(1) In the first step, an initial decision matrix needs to be created. The number of columns is the number of criteria (or measures) we will apply, and the number of rows denotes the number of alternatives (or nodes) we will rank and distinguish which one is critical based on the criteria. The values of the distinct columns are deduced according to different measures.

(2) In order to transform the values resulting from each measure into dimensionless ones, the second step is to normalize the decision matrix using the same normalized approach.

(3) Based on the normalized decision matrix from step 2, a new weighted normalized decision matrix is needed to be built in the third step. How to estimate the weights for different criteria is also presented in this chapter.

(4) In the fourth step, the positive and negative ideal solutions are determined according to the weighted normalized decision matrix.

(5) In this stage, the Euclidean distances from positive and negative ideal solutions of each alternative need to be calculated.

(6) Based on the Euclidean distances, in this step, the relative closeness for each alternative with respect to the ideal solutions is computed.

(7) In the final step, the set of alternatives according to the descending order of the values of relative closeness can be achieved. Here the order can show the importance of each alternative. In this dissertation, the top one alternative in a rank order denotes the given alternative and is the most important one, and so on.

The details of each step are introduced in the following subsection of this chapter. Among these 7 steps when implementing TOPSIS, the most important step is step 3, during which the problem of how to evaluate different criteria and allocate them different weights is far more critical. So far, commonly and widely used weighting methods are the Analytic Hierarchy Process (AHP) (Yoon and Hwang 1995), Simple Multi-Attribute Rating Technique (SMART) (Barron and Barrett 1996), Measuring Attractiveness by a Categorical Based Evaluation Technique (MACBETH) (Bana et al. 2010), the Step-wise Weight Assessment Ratio Analysis (SWARA) method (Keršuliene et al. 2010), and so forth.

These weighting approaches need to compare different criteria and then allocate their weights based on the experts' experiences. However, different experts will have distinctive standards to determine the weights that further lead to different results, which means the process is not repeatable if researchers don´t communicate their determining criteria with each other. Taking into account the global vulnerability analysis, in our research, we introduce a new objective weighting method to estimate the weights when implementing TOPSIS in a specific transportation network to identify the important stations. The detailed process of the *new weighting method* are also explained later in this chapter.

So far, when carrying out network analysis for detecting the key nodes, most researchers have applied some existing graph measures, like centrality measures or their variants, to certain specific fields. Since there are hardly any graph measures which can effectively be applied to most application fields, the approaches that can consider many factors to identify the key nodes are even fewer.

As we know, most graph measures like degree centrality or betweenness centrality only consider a single or a few very finite perspectives of network structure.

However, in real-world networks, nodes might be important for multiple reasons, for instance, one node is very important maybe because it is not only close to its many other nodes, but it also has more neighbors than others and it lies on most of the shortest paths between other pairs of nodes. Meanwhile, different measures detecting the important nodes will lead to the distinctive ranking orders of nodes.

Therefore, this could result in information overflow for decision-makers, who cannot decide which measure is more suitable and effective to identify the important nodes; thus, they cannot know which nodes are so important that more security resources are needed to be deployed in advance around those important nodes in order to prevent them from being attacked by terrorists, or at least it will reduce the impacts caused by *terrorist attacks* to a lower extent.

In order to resolve the information overflow issue for decision-makers, it is necessary and essential to develop a comprehensive method that can not only consider multiple advantage aspects from other different approaches, but can also aggregate them into only a new one to identify the key spots in a network.

As introduced before, in the multiple decision-making field, as a well-known Multi-criteria Decision Making method, TOPSIS can consider many criteria together, which has been applied to many areas, such as supply chain management and logistics, design and engineering, manufacturing systems, business and marketing management, health and safety, environment management, human resources management, energy management, chemical engineering, water resources management, and so on.

In recent years, researchers have started to apply TOPSIS to complex networks (Yu et al. 2013), specifically the social network (Mesgari et al. 2015, Muruganantham and Gandhi 2016), to identify the critical nodes by aggregating different graph measures. Nevertheless, they estimate and allocate the weights for each criterion using the traditional subjective weighting approaches like AHP, SMART, MACBETH, SWARA, and so on, which need experts' knowledge and experiences to compare the criteria with each other and then allocate different weights according to their importance.

But in graph theory, since there is no unified standard to compare different graph measures with each other (one standard method can determine which measure is more efficient than other measures to detect the critical nodes, then allocate a higher weight to that measure), the experts' knowledge and experiences are thus not that significant to be used to evaluate the weights for criteria. Thereby, in our research, we have introduced a new objective weight estimating method by considering the global vulnerability analysis to allocate the weights for different graph measures. In comparison to Yoon and Hwang (1995), Barron and Barrett (1996), Bana et al. (2010) and Keršulienė et al. (2010), the exact weight determining approach and its procedure of calculation are explained in the following subsection of this chapter.

## 3.3 TOPSIS as a Framework for MCDM

TOPSIS is a kind of ranking method based on the closeness between a limited number of evaluation objects and the ideal solutions. It is used to evaluate the relative merits of the existing objects. There are two ideal solutions, one is the *positive ideal solution* or the optimal target; the other one is the negative ideal solution or the worst target.

The best object should have the closest distance to the positive ideal solution and the furthest distance from the negative ideal solution (Rezaei 2015). Both optimal and worst targets among multiple targets can be found based on the normalization matrix. Then the closeness between each target and the ideal solution can be obtained by calculating the distance between each evaluated target and the positive (negative) ideal solution. Afterward, according to the value of the closeness, we can obtain a ranking order serving as the basis for evaluating the pros and cons of the target. Here, the closeness value is between 0 and 1. The closer the value is to 1, the closer the corresponding evaluated target is to the optimal level; otherwise, if the value is closer to 0, the evaluated target is closer to the worst level. In summary, TOPSIS consists of the following seven steps (Chen and Hwang 1992, Yoon and Hwang 1995):

# TOPSIS Procedure:

***First Step:*** The decision matrix $X$ is created with $n$ rows and $m$ columns; here, $n$ is the number of nodes and $m$ is the number of graph measures. The matrix is shown as follows:

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1m} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nm} \end{pmatrix} \quad (3\text{-}14),$$

where $x_{ij}$ denotes the measure value of $i^{th}$ node according to the $j^{th}$ graph measure.

***Second Step:*** Since the decision matrix is composed of values with different scales resulting from distinct graph measures, in this step the decision matrix $X$ needs to be normalized and transformed into a dimensionless matrix $\Gamma$, which allows the comparison of the various graph measures; its normalized decision matrix with a notionally common scale is shown as follows:

$$\Gamma = \begin{pmatrix} r_{11} & \cdots & r_{1m} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nm} \end{pmatrix} \quad (3\text{-}15),$$

where the element $r_{ij}$ is: c

$$r_{ij} = \frac{x_{ij}}{max\{x_{ij}\}_{i=1}^{n}}$$

***Third Step:*** In this step, based on the normalized evaluation matrix $\Gamma$, we create the weighted normalized evaluation matrix, which is shown in the following formula:

$$T = \begin{pmatrix} t_{11} & \cdots & t_{1m} \\ \vdots & \ddots & \vdots \\ t_{n1} & \cdots & t_{nm} \end{pmatrix} \quad (3\text{-}16),$$

where

$$\begin{cases} t_{ij} = \varepsilon_j r_{ij} \\ \sum_{j=1}^{m} \varepsilon_j = 1 \end{cases}$$

Here, $\varepsilon_j$ is the weight for each graph measure, and we will explain how to determine and allocate the weights for different measures after introducing the computing steps of TOPSIS.

***Fourth Step:*** After we have weighted the normalized-evaluation-matrix, in this step, we can derive the positive ideal solution $t^+$ and the negative ideal solution $t^-$, since in our research, every graph measure (i.e. criterion) has the benefit attribute, which means one given node (i.e. choice) is much more important if its corresponding graph measure value is higher. In such a case, these positive and negative ideal solutions can be achieved based on the following Formulas (3-17):

$$\begin{cases} t^+ = \left\{ \max_i \left( t_{ij} \right) \middle| i = 1,2,\ldots,n;\ j = 1,2,...,m \right\} = \left\{ t_j^+ \middle| j = 1,2,...,m \right\} \\ t^- = \left\{ \min_i \left( t_{ij} \right) \middle| i = 1,2,\ldots,n;\ j = 1,2,...,m \right\} = \left\{ t_j^- \middle| j = 1,2,...,m \right\} \end{cases} \quad (3\text{-}17)$$

However, when applying TOPSIS to different fields, (for instance, threat analysis), if every criterion has the cost attribute (which means that one given choice is of higher importance if its corresponding criterion value is smaller), one can obtain positive and negative ideal solutions using the following Formulas (3-18):

$$\begin{cases} t^+ = \left\{ \min_i \left( t_{ij} \right) \middle| i = 1,2,\ldots,n;\ j = 1,2,...,m \right\} = \left\{ t_j^+ \middle| j = 1,2,...,m \right\} \\ t^- = \left\{ \max_i \left( t_{ij} \right) \middle| i = 1,2,\ldots,n;\ j = 1,2,...,m \right\} = \left\{ t_j^- \middle| j = 1,2,...,m \right\} \end{cases} \quad (3\text{-}18)$$

***Fifth Step:*** In this step, we calculate the Euclidean distances from each node to the positive ideal solution and negative ideal solution. The Euclidean distances from each node to positive ideal solution can be calculated according to Formula (3-19):

$$S_i^+ = \sqrt{\sum_{j=1}^{m}\left(t_{ij} - t_j^+\right)^2} \qquad i = 1,\ldots,n \tag{3-19}$$

And the Euclidean distances from each node to negative ideal solution can be computed using Formula (3-20):

$$S_i^- = \sqrt{\sum_{j=1}^{m}\left(t_{ij} - t_j^-\right)^2} \qquad i = 1,\ldots,n \tag{3-20}$$

***Sixth Step:*** Based on the Euclidean distances $S_i^+$ and $S_i^-$ from each node to every positive and negative ideal solution, in this step, we can calculate the relative closeness $Z_i$ to the ideal solution. Its computing formula is defined as follows:

$$Z_i = \frac{S_i^-}{S_i^- + S_i^+} \tag{3-21}$$

***Seventh Step:*** In the last step, we rank the nodes based on the values of $Z_i$ and get a new node order which considers and aggregates multiple perspectives from different graph measures.

### 3.3.1 Illustration of Determining Weight in Third Step of TOPSIS Procedure

Now we will introduce how to determine and allocate the weight for each graph measure. Since, in graph theory, so far there hasn´t been any unified standard criterion to compare different graph measures to tell which one is more suitable and efficient to identify the key nodes, the experiences of experts might be meaningful in some application fields, but not always possible.

However, when researchers analyze the vulnerability of a graph from a graph theory point of view, the general approach is first to conduct some attack scenarios, for instance, the nodal level graph centrality-based attack scenarios and the nodal level graph vulnerability-based attack scenarios, which can be carried out by removing some numbers of nodes or edges from a graph.

Then, regarding the remaining graph, its certain global graph vulnerability evaluation model value needs to be calculated, which can be used to compare which node or group of nodes are more vulnerable than other nodes or other groups of nodes under these kinds of attack scenarios. Based on this idea, we have proposed two new nodal graph vulnerability measures. Accordingly, in order to allocate the weights for different graph measures when implementing TOPSIS, in our research we also take into account this idea of introducing a new weights determination approach into the computing process of TOPSIS. In total, regarding the procedure of how to determine and allocate the weights for different graph measures, there are six steps, presented as follows:

**Step one:**

Supposing $M_i$ denotes the $i^{th}$ graph measure and having completed the calculations of each graph measure for every node in a given graph, in this step we rank the nodes based on the graph measure values of nodes. Therefore, different graph measures will lead to different rank orders. For instance, we take a simple graph as an example shown in Figure 3.9, in which the numbers near every edge denote the distance between two adjacent straightly connected nodes; here, supposing we have two graph measures $M_1$ and $M_2$, the rank order 1 will be V5, V3, V4, V6, V2, V7, V1, according to graph measure $M_1$, whereas the rank order 2 will be V4, V6, V3, V5, V2, V1, V7, based on graph measure $M_2$.

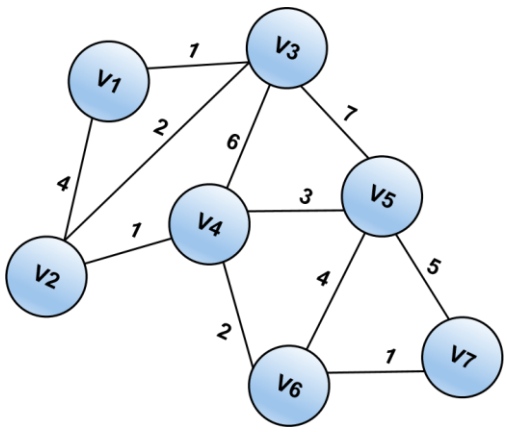



Figure 3.9: A simple graph example

**Step two:**

In this step, we delete the same numbers of nodes, but maybe different nodes from the graph based on the different rank orders. For example, if we only delete the top one node, then node V5 will be removed from the graph based on rank order 1; however, node V4 will be removed from the graph according to rank order 2. Likewise, if deleting the top two nodes, then the two nodes V5 and V3 will be removed simultaneously, based on rank order 1, while nodes V4 and V6 will be removed at the same time, according to rank order 2.

**Step three:**

In this step, first we need to compute the global graph vulnerability evaluation model of the original graph without deleting any nodes $I_{original}$, then after deleting the same number of top nodes, based on graph measure $M_i$, we also need to calculate the global graph vulnerability evaluation model $I_{M_i - S_{N_d}}$ of the remaining graph. Here, $S_{N_d}$ denotes the node set which contains top $N_d$ nodes that will be removed from the original graph. For instance, if deleting top two nodes ( $N_d = 2$ ) from the given original graph $S_{N_d} = \{V5, V3\}$, based on rank order 1, its remaining graph is like Figure 3.10, and so on.

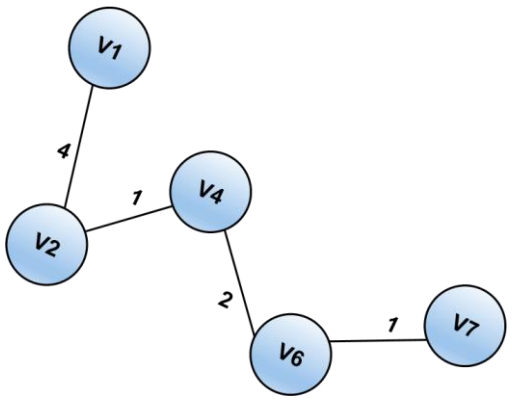



Figure 3.10: The residual graph of the given simple graph after removing nodes V5 and V3

In graph theory, there are three kinds of commonly and widely used global graph vulnerability evaluation models when conducting the global vulnerability analysis, which include the giant connected component, origin-destination connected ratio and global graph efficiency. The so-called giant connected component means that after removing some numbers of nodes from the graph, if the remaining graph is split into different small connected parts, then the part with the largest number of nodes is the giant connected component. In this case, the removed nodes will cause larger influences on the given graph if its giant connected component is smaller.

While the origin-destination connected ratio (ODCR) shows the percentage of pairs of nodes that are still connected in the remaining graph, its formula is defined as follows:

$$ODCR = \frac{2E_{N_d}}{(n - N_d)(n - N_d - 1)} \quad (3\text{-}22),$$

where $E_{N_d}$ denotes the number of edges in the remaining graph, according to the sense of the origin-destination connected ratio, and the bigger the values of the origin-destination connected ratio, the less influence the removed nodes will have.

Moreover, another evaluation model called Global Graph Efficiency (GGE) is a measure which can be used to quantify how fast the information can be propagated within the graph. Its computing formula is shown as follows:

$$GGE = \frac{1}{n_r(n_r - 1)} \sum_{i}^{n_r} \sum_{j \neq i}^{n_r} \frac{1}{d(v_i, v_j)} \quad (3\text{-}23),$$

where $n_r = n - N_d$ is the number of nodes in the remaining graph and $d(v_i, v_j)$ is the distance of the shortest path between node $v_i$ and node $v_j$ in the remaining graph. Based on this evaluation model, the removed nodes will result in a larger influence on the graph if its evaluation model value of the remaining graph is bigger. However, when deleting the same number of nodes from maybe different nodes, the remaining graphs are still connected. For instance, taking the simple graph in Figure 3.9 as an example, according to the aforementioned rank orders 1 and 2 derived from its corresponding graph measure $M_1$ and $M_2$ after deleting the top one node, namely node V5 and node V4, the two remaining graphs are still connected.

Furthermore, after deleting the top two nodes, namely nodes {V5, V3} and nodes {V4, V6}, two other remaining graphs are still connected. In these cases, based on the giant connected component and the origin-destination connected ratio, we cannot tell the differences between node V5 and node V4, and cannot distinguish the importance between the group nodes {V5, V3} and group nodes {V4, V6}. Yet, due to the fact that the simple graph is a distance weighted graph and most of the distances between two straightly connected adjacent nodes are different, the value of global graph efficiency will be different, which can be used to tell the difference between different nodes and also groups of nodes. Meanwhile, since in our research, we have mapped the research object ICE network into a distance weighted graph, in this dissertation, we take the global graph efficiency as the global graph vulnerability evaluation model, which is $I = GGE$.

**Step four:**

In this step, we use the following Formula (3-24) to compute the damage to the structure of the original graph after removing top $N_d$ nodes of the ranked order based on graph measure $M_i$.

$$D_{M_i - S_{N_d}} = I_{original} - I_{M_i - S_{N_d}} \tag{3-24}$$

According to the definition of damage degree, the removed nodes will lead to larger damage to the structure of the original graph if its value is bigger.

**Step five:**

For this step, based on graph measure $M_i$, we need to calculate the cumulative damage to the structure of the original graph after deleting the node sets from $S_1$ to $S_{N_d}$, using the following formula:

$$SD_{M_i - S_1 \sim S_{N_d}} = \sum_{N_d} D_{M_i - S_{N_d}} \tag{3-25},$$

where $N_d \in [1, n * 26\%]$.

The reason for taking 26 percent of nodes in the graph is that in this dissertation, regarding the research object ICE network and after having removed these nodes, the remaining graphs are almost unconnected, which means the structure of the original graph has almost or already been destroyed.

**Step six:**

In the final step, we use the following formula to determine the weights of graph measures when applying TOPSIS in ICE network in order to detect the key nodes which have more potential to be attacked by terrorists.

$$\varepsilon_j = \frac{SD_{M_j - S_1 \sim S_{N_d}}}{\sum_i SD_{M_i - S_1 \sim S_{N_d}}} \tag{3-26}$$

## 3.4 Implementation of the New TOPSIS-based Aggregation Measure

Before implementing the TOPSIS-based aggregation measure, here we first implement the method on how to allocate the weights for the third step of TOPSIS.

***Step one:***

In this step, $\{ M_1, M_2, M_3, M_4, M_5, M_6, M_7, M_8 \}$ denote {BetwCentr, CloCentr, DegCentr, EigenCentr, Effi, FWEffi, BetwEffiVul, ResiduCloVul} measures respectively. Based on the results shown from Table A-1 to Table A-8 in the Appendix, according to $\{ M_1, M_2, ..., M_8 \}$, since we take $N_d \in [1, n*26\%] = [1, 31]$ in the fifth step of the procedure of the weights determination approach, in this step, we therefore only consider the top 31 nodes, and the results are shown in Appendix Table A-9.

***Step two:***

In this step, we delete some numbers of nodes from the top one node to the top third nodes from the graph step by step. For instance, if we delete the top five nodes, then based on Appendix Table A-9, different groups of nodes, like {1, 103, 22, 2, 82}, {1, 4, 2, 23, 25}, {2, 4, 1, 41, 82}, {2, 4, 41, 1, 50}, {103, 106, 41, 50, 91}, {92, 91, 103, 107, 104}, {103, 4, 34, 1, 35} and {4, 103, 34, 1, 2}, according to $\{M_1, M_2, ..., M_8\}$ respectively, will be removed from the graph, just like groups of nodes based on certain other top numbers of nodes.

***Step three:***

Since we take $I_{M_i - S_{N_d}} = GGE$ shown in Formula (3-23) as the global graph vulnerability evaluation model, firstly, in this step, we can compute $I_{original} = 0.3905928$. Then, based on different $M_i$, $I_{M_i - S_{N_d}}$ is calculated, the results are shown in Appendix Table A-10.

***Step four:***

According to the results of $I_{original}$ and $I_{M_i - S_{N_d}}$ shown in Appendix Table A-10 and Formula (3-24), we can obtain the damage to the structure of the original graph after removing top $N_d$ nodes of the ranked order based on graph measure $M_i$, and the results are shown in Appendix **Table A-11**.

***Step five:***

In this step, based on Formula (3-25) and the values of $D_{M_i - S_{N_d}}$, we can calculate the cumulative damage $SD_{M_i - S_1 \sim S_{31}}$ to the structure of the original graph after deleting the nodes sets from $S_1$ to $S_{N_d}$. The results are shown in Table 3-2.

Table 3-2: The values of $SD_{M_i-S_1\sim S_{31}}$

| $SD_{M_1-S_1\sim S_{31}}$ | $SD_{M_2-S_1\sim S_{31}}$ | $SD_{M_3-S_1\sim S_{31}}$ | $SD_{M_4-S_1\sim S_{31}}$ | $SD_{M_5-S_1\sim S_{31}}$ | $SD_{M_6-S_1\sim S_{31}}$ | $SD_{M_7-S_1\sim S_{31}}$ | $SD_{M_8-S_1\sim S_{31}}$ |
|---|---|---|---|---|---|---|---|
| 7.6125265 | 4.4568082 | 7.7034144 | 4.6344502 | 6.7014747 | 6.1768206 | 8.44332 | 8.4979834 |

***Step six:***

According to the values of cumulative damage $SD_{M_i-S_1\sim S_{31}}$ in

Table 3-2, based on Formula (3-26), we can obtain the weights of graph measures when implementing TOPSIS as shown in Table 3-3.

Table 3-3: The weight values $\{\varepsilon_1,\varepsilon_2,...,\varepsilon_8\}$ of measures $\{M_1,M_2,...,M_8\}$ when implementing TOPSIS

| $\varepsilon_1$ | $\varepsilon_2$ | $\varepsilon_3$ | $\varepsilon_4$ | $\varepsilon_5$ | $\varepsilon_6$ | $\varepsilon_7$ | $\varepsilon_8$ |
|---|---|---|---|---|---|---|---|
| 0.1403831 | 0.0821883 | 0.1420592 | 0.0854642 | 0.1235823 | 0.1139072 | 0.1557038 | 0.1567119 |

The procedure of implementing the TOPSIS-based aggregation measure is described as follows:

***First step:***

As described before, $\{M_1,M_2,M_3,M_4,M_5,M_6,M_7,M_8\}$ denote BetwCentr, CloCentr, DegCentr, EigenCentr, Effi, FWEffi, BetwEffiVul, ResiduCloVul measures respectively. Supposing that $V_{M_i}$, which is a $121\times1$ vector, denotes the values of measure $M_i$, its value is corresponding to Table A-1 to Table A-8 in the Appendix. Thus, the evaluation matrix $X$ with size $121\times8$ can be expressed as $X=(V_{M_1},V_{M_2},...,V_{M_8})$.

***Second step:***

Based on the first step, in this step we can attain the normalized evaluation matrix with the same scale column with the following formula:

$$\Gamma = (\frac{V_{M_1}}{\max(V_{M_1})}, \frac{V_{M_2}}{\max(V_{M_2})}, ..., \frac{V_{M_8}}{\max(V_{M_8})})$$

***Third step:***

According to Table 3-3, we have the weights for each measure; thereby, we can obtain the weighted normalized evaluation matrix shown as the following formula here:

$$T = (\varepsilon_i * \Gamma_i) = (\varepsilon_1\Gamma_1, \varepsilon_2\Gamma_2, ..., \varepsilon_8\Gamma_8)$$

$$= (0.140383109 \times \Gamma_1, 0.082188298 \times \Gamma_2, ..., 0.156711879 \times \Gamma_8)$$

***Fourth step:***

In our research, each graph measure has the benefit attribute, which means one given node is much more important if its corresponding measure value is higher. Therefore, based on Formula (3-17), we can compute the positive and negative ideal solution like in the following formulas:

$$\begin{cases} t^+ = \left\{\max(T_1), \max(T_2), ..., \max(T_8)\right\} = \left\{t_1^+, \ldots, t_m^+\right\} \\ t^- = \left\{\min(T_1), \min(T_2), ..., \min(T_8)\right\} = \left\{t_1^-, \ldots, t_m^-\right\} \end{cases}$$

$$= \begin{cases} \{0.140383109 & 0.082188298 & 0.142059179 & 0.085464205 \\ 0.123582342 & 0.113907161 & 0.155703828 & 0.156711879\} \\ \{0.000000000 & 0.040484861 & 0.015784353 & 8.2313E-17 \\ 0.022937713 & 0.000000000 & 0.000889826 & 0.00503244\} \end{cases}$$

***Fifth step:***

Based on Formula (3-19) and Formula (3-20), we can calculate the separation distance from each node to every positive and negative ideal solution. Their results are shown in Table A-12 and Table A-13 in the Appendix.

***Sixth step:***

Based on the values of separation distances $S_{ID}^{+}$ and $S_{ID}^{-}$ shown in Table A-12 and Table A-13 in the Appendix, and according to Formula (3-21), we can obtain results of the relative closeness $Z_i$ to the ideal solutions shown in Appendix Table A-14.

***Seventh step:***

Based on the values of $Z_i$ in Appendix Table A-14, we rank the nodes and get a new node order, which takes into account and aggregates all the multiple advantage perspectives of different graph measures. Here, we list the top ten nodes and compare them to other top ten nodes based on other graph measures in Table 3-4.

Table 3-4: Top ten stations identified by different measures

| Rank | Centrality | | | | Nodal Efficiency | | Nodal Vulnerability | | AggregTOPSIS |
|---|---|---|---|---|---|---|---|---|---|
| | BetwCentr | CloCentr | DegCentr | EigenCentr | Effi | FWEffi | BetwEffiVul | ResiduCloVul | |
| 1 | 1 | 1 | 2 | 2 | 103 | 92 | 103 | 4 | 103 |
| 2 | 103 | 4 | 4 | 4 | 106 | 91 | 4 | 103 | 1 |
| 3 | 22 | 2 | 1 | 41 | 41 | 103 | 34 | 34 | 4 |
| 4 | 2 | 23 | 41 | 1 | 50 | 107 | 1 | 1 | 2 |
| 5 | 82 | 25 | 82 | 50 | 91 | 104 | 35 | 2 | 34 |
| 6 | 104 | 3 | 18 | 49 | 92 | 102 | 41 | 35 | 91 |
| 7 | 4 | 82 | 22 | 44 | 107 | 106 | 2 | 41 | 41 |
| 8 | 27 | 14 | 26 | 48 | 104 | 1 | 91 | 27 | 22 |
| 9 | 66 | 26 | 91 | 26 | 38 | 2 | 108 | 108 | 104 |
| 10 | 24 | 9 | 103 | 40 | 75 | 38 | 18 | 91 | 18 |

According to Table 3-4, the top ten stations identified by the TOPSIS-based approach are stations 103, 1, 4, 2, 34, 91, 41, 22, 104 and 18, highlighted in red color in the graph shown in Figure 3.11. In this figure, we can see that most of them are in critical positions, and once they are removed from the network, the network will be disconnected, or the network efficiency will be reduced a lot.

Furthermore, based on Table 3-4, all of these top ten stations detected by the TOPSIS-based aggregation measure appearing from column 2 to column 9 (identified by BetwCentr, CloCentr, DegCentr, EigenCentr, Effi, FWEffi, BetwEffiVul, and ResiduCloVul measures respectively), most of them, except stations 34, 22 and 18, appear in the top nine nodes (which are stations 1, 2, 4, 103, 41, 91, 82, 104 and 26), based on the frequencies of each station's appearing in the lists within top ten positions shown in Table 3-4 from column 2 to column 9, and also in the rank order in each top ten station list.

Because this aggregation measure considers and aggregates the advantages of different graph measures and also compensates their disadvantages to each other, we can say the aggregation measure is promising and maybe more efficient for detecting the critical nodes in a graph. Considering Figure 3.11 again, we can find that most of them are very important. For instance, if removing stations 4, 18, 22, 41, 91, 103 from the network, the remaining network will be disconnected, which apparently will affect people's lives.

Although after deleting stations 1, 4, 34, 104, the remaining network is still connected; this will however largely increase the costs for transport, time and the economy. Thus, from an intuitive point of view, the TOPSIS-based approach can be a promising, suitable and effective measure.

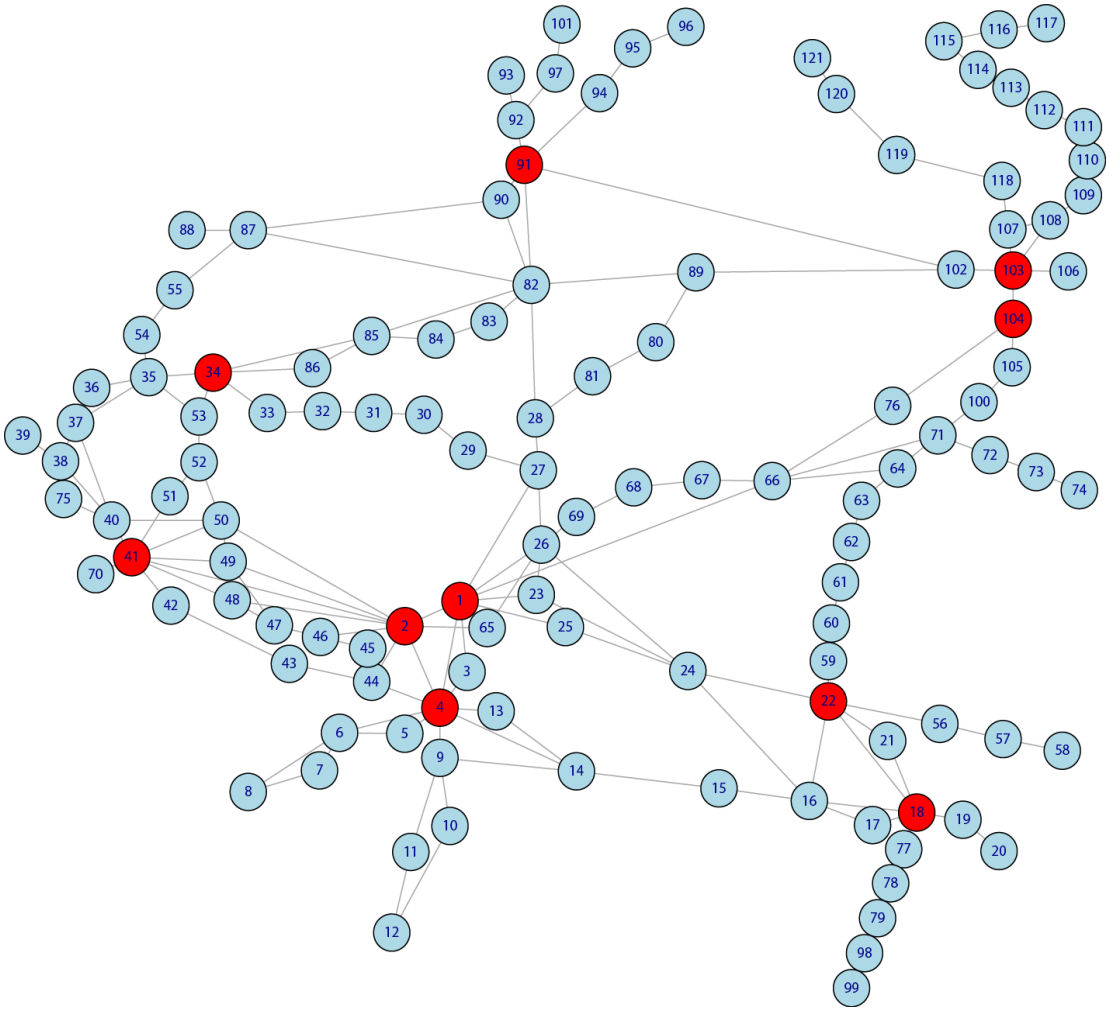



Figure 3.11: Top ten stations identified by TOPSIS-based measure are highlighted in red color

When comparing Figure 3.11 with Figure 3.1 and Figure 3.8, it is found that Figure 3.11 is similar to Figure 3.3 (based on DegCentr) and Figure 3.7 (based on BetwEffiVul), and there are only two different highlighted top ten stations. But from Table 3-4, we can see that their ranking orders are different.

According to Figure 3.11, station 82 connects lines going into four different directions; from an intuitive point of view, it should be one of the top ten critical stations. Although station 82 is not highlighted as one of the top ten critical stations, it doesn't mean that this station is not important according to the TOPSIS-based aggregation measure.

Based on Appendix Table A-14, the rank order of station 82 is 12, which means that station 82 is still very critical based on the TOPSIS-based aggregation measure; therefore, the results, which are deduced from the TOPSIS-based aggregation measure combining information of eight different measures, are comprehensive and suitable.

## 3.5 Summary

In this chapter, we first introduce four centrality measures like degree centrality (Maharani and Gozali 2014), closeness centrality (Derrible 2012), eigenvector centrality (Maharani and Gozali 2014, Newman 2008) and betweenness centrality (Tsiotas and Polyzos 2015). Then, the classical network nodal efficiency (Latora and Marchiori 2003) and its improved version, i.e. the flow-weighted network nodal efficiency (Nistor and Pickl et al. 2017) are also introduced. Based on the network residual closeness, we propose a new nodal residual closeness vulnerability measure. Inspired by the betweenness centrality and efficiency measures, we also propose a new betweenness-efficiency vulnerability measure. Afterward, the aforementioned measures are applied to the ICE network. However, different measures lead to distinctive results, which can cause information overflow and confusion for decision-makers, who cannot judge which measures are the most effective ones to identify the key stations in the ICE network.

In order to decrease the information overflow for decision-makers, we introduce TOPSIS from Multi-criteria Decision Making field to aggregate different measures into a new comprehensive measure. And the results, from an intuitive point of view, show that the new TOPSIS-based approach is a promising, suitable and effective measure. However, as stated before, since so far, there has not been a unified standard criterion to tell the difference between various graph measures and to compare them to find out which one is more suitable and efficient to detect a group of most critical nodes in graph theory, now we are introducing an aggregation measure which to a certain extent resolves the problem of information overload for decision-makers (who, based on different results, couldn't make a reasonable judgment which measure is the more efficient one to identify more suitable and practical vital nodes in a graph before).

Therefore, to compare different approaches and to tell which one is more suitable and efficient to detect the key nodes in a network, and in order to validate the effectiveness of the new proposed aggregation approach in the meantime, in the next Chapter 4 we conduct a quantitative network resilience analysis, which can analyze the network from different perspectives and views considering some real information, for instance, how many people could be injured or killed in terrorist attacks, how much economic loss it might cause, how many people's lives would be affected by and after the attacks, and so on.

As it is known, when researchers carry out quantitative network resilience analysis, the network resilience is usually quantified by the changes in network performance metrics. And due to the fact that the safety of people is of highest importance, in the next chapter, we therefore propose and present a new resilience measure by introducing a new network performance metric which mainly considers the factor of how many people can generally take advantage of the system, even under some disturbances. Meanwhile, we also take into account the traveling time and train flow. Furthermore, in another critical aspect, we also propose a concept of an adjacency node-set level when appropriately adapting the idea of degree centrality from graph theory. The details are presented in the following Chapter 4, where we introduce and characterize a new quantitative resilience measure.

In Chapter 3, the contents from section 3.1, section 3.2 and section 3.3 are based on the following publications (in order of appearance):

*Wang, Z., Zsifkovits, M., & Pickl, S. W. (2018). Analyzing vulnerabilities of the German high-speed train network using quantitative graph theory. International Journal of Safety and Security Engineering, 8(1), 59-64.*

*Zsifkovits, M., Wang, Z., Nistor, M. S., & Pickl, S. W. (2016). Complex System Analysis using Graph Theory - Identifying Criticality in Transportation Networks. Security Research Conference.*

*Wang, Z., Nistor, M. S., & Pickl, S. W. (2020). Introducing a TOPSIS based quantitative resilience measure for railway systems. The international conference on railway technology. (submitted)*

# 4 A New Quantitative Resilience Measure

As described in Chapter 3, it is found that the proposed TOPSIS-based aggregation measure can reduce information overflow for decision-makers, and the results also show that it is a promising approach to identify the critical nodes of networks. The TOPSIS-based aggregation measure considers many advantage factors of different measures, and the various advantage factors can compensate for the disadvantages of various measures. Thereby, the TOPSIS-based aggregation measure can be regarded as a much more comprehensive method than other centrality, efficiency and nodal vulnerability measures, which only consider one or two aspects.

However, in graph theory, because there is no unified standard to compare distinct measures and tell the difference from each other, the effectiveness of the developed TOPSIS-based aggregation measure can therefore not be verified, and it certainly cannot conclude which one is more suitable and effective to detect the critical nodes for network. Therefore, in this chapter, we conduct the network resilience analysis mainly in order to compare different measures from distinct perspectives. In order to achieve this aim we also develop a new network performance metric based on network structure properties from the graph theory field and combine them with other information like the precise number of people and trains in the German high-speed train network (ICE network).

Regarding resilience analysis, several studies proposed different definitions of resilience during the past two decades (Ip and Wang 2011, Wang et al. 2017). While most people find it easy to grasp an intuitive and qualitative meaning for the concept of resilience, this notion proved to be one of the most difficult ones to define qualitative terms in a general and comprehensive way (Wang et al. 2017). Numerous qualitative and quantitative definitions have been proposed in different fields, for example in psychology and social sciences as well as in ecology and engineering.

Some studies, for example in Holling (1996), tried to differentiate between the meanings to be used in engineering and ecology. Attempts have also been made to review the field; for instance, Martin-Breen and Anderies (2011), as well as Hosseini and Barker (2016) have made a relatively comprehensive review of resilience and its applications.

In Chapter 2, we have also reviewed in detail some resilience definitions and found that the approach representing resilience graphically using performance curves is promising and adaptable in our research. As described in Chapter 1, the graphical network performance curve method has four phases containing (i) original steady phase, (ii) disruptive phase, (iii) recovery phase, and (iv) new steady phase. Here, we only focus on the disruptive phase by considering the time consumed, because in our research, we merely take terrorist attacks into account, and, assuming once these terrorist events have happened, the network will be shut down immediately.

## 4.1 Network Performance Metric

In our research, due to the fact that the German high-speed train network is not a local transportation network, if one station is attacked by terrorists, it only affects a few neighboring stations in the network. Let´s take the graph in Figure 4.1 as an example:

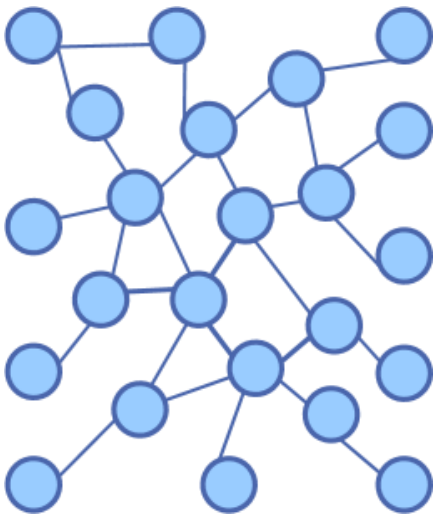


Figure 4.1: A simple example of transportation network

As described in Chapter 1, when assessing the resilience, we present it graphically.

In this thesis, we only focus on disruptive events caused by terrorists, thus the different phases of network resilience are presented in Figure 1.5. In such a case, we suppose that one station marked black is attacked at the time $t_d$, and every stage of network resilience is shown in Figure 4.2. Furthermore, as stated in Chapter 1, the time consumption of disruptive and recovery phases is not necessary under terrorist attacks, therefore, here we suppose that the disruptive and recovery phases will immediately happen almost without time consumption as shown in Figure 4.2; the duration time of disruptive and recovery phases then can be written as $\Delta t_d = t_r - t_d \to 0$ and $\Delta t_r = t_{ns} - t_r^* \to 0$ and $\Delta t_d = \Delta t_r$.

According to Figure 4.2, after the given station is attacked, its neighboring stations are affected quickly. The stations marked in red, which are straightly connected to the given station, will be profoundly affected. Compared to the stations marked in red, there are fewer impacts on the stations with yellow marks, which are straightly connected to the neighbors of the given station marked in black. And other stations marked in green are much less affected. As for how long the network will be affected, it depends on how long the decision-makers need to take some measures to resolve such a dangerous situation of terrorist attacks, then issuing the order that the network can be recovered to its normal status.

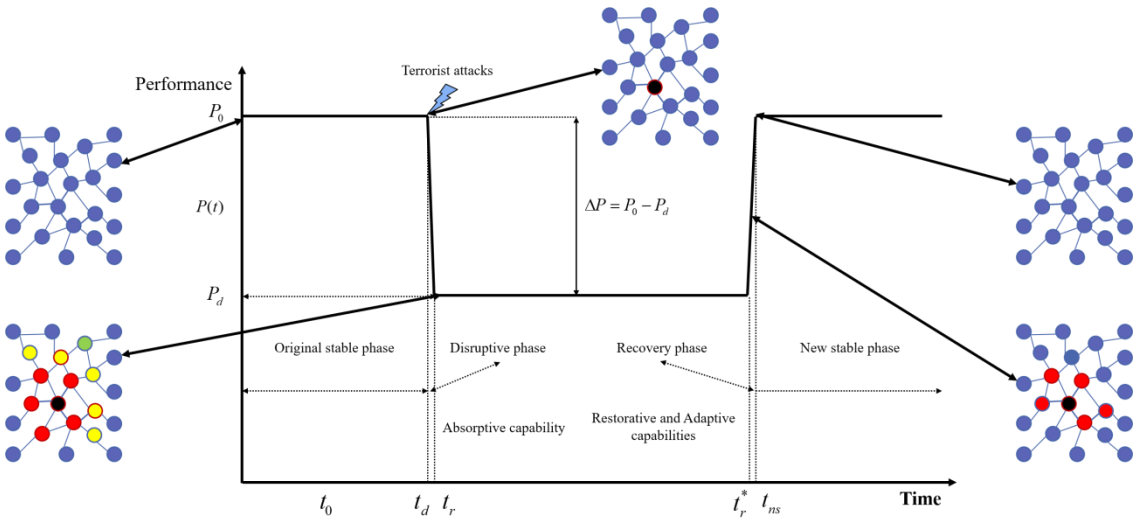



Figure 4.2: Different phases of network resilience and their different network status when considering terrorist attacks

### 4.1.1 The New Robustness-based Resilience Measure of the Network

In this thesis, based on the resilience assessment approach presented by Nan and based on Formula (2-13), and combined with Figure 4.2, we can derive the robustness of the network as follows:

$$Robustness = \min_{t}\{P(t)\} = P_d$$

Supposing the duration time of disruptive and recovery phases is equal and $\Delta t_d = \Delta t_r \to 0$, according to Formula (2-15), we can say that the number of ramps in both disruptive and recovery phases is one , namely, $K_{DP} = K_{RP} = 1$. In such a case, based on Formula (2-14) and Formula (2-17), the RAPIDITY of Disruptive Phase ( $RAPI_{DP}$ ) and the RAPIDITY of Recovery Phase ( $RAPI_{RP}$ ) can be calculated as follows:

$$RAPI_{DP} = \frac{\left|\sum_{i=1}^{K_{DP}} \frac{P(t_i) - P(t_i - \Delta t)}{\Delta t}\right|}{K_{DP}} = \left|\frac{P(t_d + \Delta t_d) - P(t_d)}{\Delta t_d}\right| = \frac{P_0 - P_d}{\Delta t_d}$$

$$RAPI_{RP} = \frac{\left|\sum_{i=1}^{K_{RP}} \frac{P(t_i) - P(t_i - \Delta t)}{\Delta t}\right|}{K_{RP}} = \left|\frac{P(t_{ns}) - P(t_{ns} - \Delta t_d)}{\Delta t_r}\right| = \frac{P_0 - P_d}{\Delta t_r}$$

Thus, $RAPI_{DP} = RAPI_{RP}$, according to Formula (2-19), and combining Figure 1.4 and Figure 1.5 or Figure 4.2, the recovery ability of a network can be computed as follows:

$$RA = \left|\frac{P(t_{ns}) - P(t_r)}{P_0 - P(t_r)}\right| = \left|\frac{P(t_{ns}) - P(t_r^*)}{P_0 - P(t_r)}\right| = \frac{P_0 - P_d}{P_0 - P_d} = 1$$

Based on Formula (2-21), the Time Averaged Performance Loss during the disruptive phase and the recovery phase can be obtained as follows:

$$TAPL = \frac{\int_{t_d}^{t_{ns}} [P_0 - P(t)]dt}{t_{ns} - t_d} = \frac{(P_0 - P_d)\int_{t_d}^{t_{ns}} dt}{t_{ns} - t_d} = P_0 - P_d ;$$

here, we suppose the duration time of disruptive and recovery phases is equal and $\Delta t_d = t_r - t_d = \Delta t_r = t_{ns} - t_r^* \to 0$, therefore, $P(t) = P_d$.

Hence, under the circumstance of terrorist attacks, according to Formula (2-20), the resilience of a network can be measured by the following formula:

$$\begin{aligned} Resilience &= Robustness \times \frac{RAPI_{RP}}{RAPI_{DP}} \times (TAPL)^{-1} \times RA \\ &= P_d \cdot 1 \cdot \frac{1}{P_0 - P_d} \cdot 1 \\ &= \frac{P_d}{P_0 - P_d} \end{aligned} \quad (4\text{-}1)$$

Based on Formula (4-1), we can find that network resilience is only related to the network performances before and after disruptive events if only considering terrorist attacks. Because $P_0 \geq P_d$, for the sake of avoiding the situation of $P_0 = P_d$ and limiting the value of resilience within the range $[0,1]$, we redefine and quantify network resilience using the network performance drop percentage without considering the time factor shown in the following formula:

$$Resilience(G_k) = \frac{\Delta P}{P_0} = \frac{P_0 - P_d}{P_0} \quad (4\text{-}2),$$

where $G_k$ means the remaining network after station $k$ or a group of stations $\{k = k_i \mid i = 1, 2, ..., j, j < n\}$ are deleted from the original network $G$. $Resilience(G_k)$ denotes the resilience of the remaining network $G_k$.

**According to such resilience definition, if the value of Formula (4-2) is higher, the resilience of a network is lower. That means, we need to make more efforts to help the network recover to its normal level, or to protect the network from attacks. For instance, we should deploy in advance more security resources, including security detection devices, more police, and so on.**

In order to quantify the resilience, first, we need to define a proper network performance. In this dissertation, when considering the three factors train flow, traveling time and the number of people, we define a new network performance as follows:

$$FTP(G_k) = \frac{Q_k}{n(n-1)} \sum_{i \neq j \in V(G_k)} \frac{f_{ij}}{\tau_{ij}} \quad (4\text{-}3),$$

where $n$ is the number of stations of the network $G$. $FTP(G_k)$ is the network performance of the remaining network $G_k$, $f_{ij}$ is the train flow on the edge with the lowest train flow along the shortest path between stations $i$ and $j$. $\tau_{ij}$ denotes the total traveling time along the shortest path between stations $i$ and $j$. $Q_k$ denotes the number of people who can still normally use the network when station $k$ is attacked by terrorists, and its formula is defined as:

$$Q_k = \sum_{i=1}^{n} Q_i^* - Q_{k\_a}^* \quad (4\text{-}4),$$

where $Q_{k\_a}^*$ represents the number of people that will be affected when station $k$ is attacked, and its definition formula is shown as follows:

$$Q_{k\_a}^* = Q_k^* + \sum_{j \in A_k^1} \rho_j Q_j^* + \sum_{j \in A_k^2} \rho_j^2 Q_j^* + \cdots + \sum_{j \in A_k^L} \rho_j^L Q_j^* \quad (4\text{-}5),$$

where, $\rho < 1$, $L \geq 1$, thus, $\rho_j^L Q_j^*$ means that station $j$ is further away from the attacked station $k$, and a smaller number of people in the city where station $j$ belongs to would be affected. Here,

$$\rho_j = \frac{Q_j^*}{\sum_{i=1}^{n} Q_i^*}$$

Since we are going to publish our research results in the future and we do not want any malicious persons to take advantage of it to harm other innocent people, we don't use the somewhat accurate statistic data to calculate $Q_{k\_a}^*$ here. Therefore, instead of statistic data, in this dissertation we use the population of every city to estimate it. In Formula (4-5), $Q_k^*$ denotes the population of the city to which station $k$ belongs to. $L$ represents the maximum depth level of adjacent stations sets of a given station in a network, and $A_k^i$ denotes the $i_{th}$ depth level of adjacent stations sets of station $k$.

In order to make the different depth levels of adjacent stations sets understandable, we take the simple graph shown in Figure 4.3 as an example, in which, supposing that node $V_4$ marked in yellow is attacked, then $A_4^1 = \{V_2, V_3, V_6\}$ highlighted in red is the first depth level adjacency node-set of node $V_4$, and its second depth level adjacency node-set is $A_4^2 = \{V_1, V_5, V_7, V_8\}$ marked in light blue. Moreover, its third depth level adjacency node-set is $A_4^3 = \{V_9\}$ marked in green; likewise, if the attacked node is different, it's the same way to look for the different depth level adjacency node-sets.

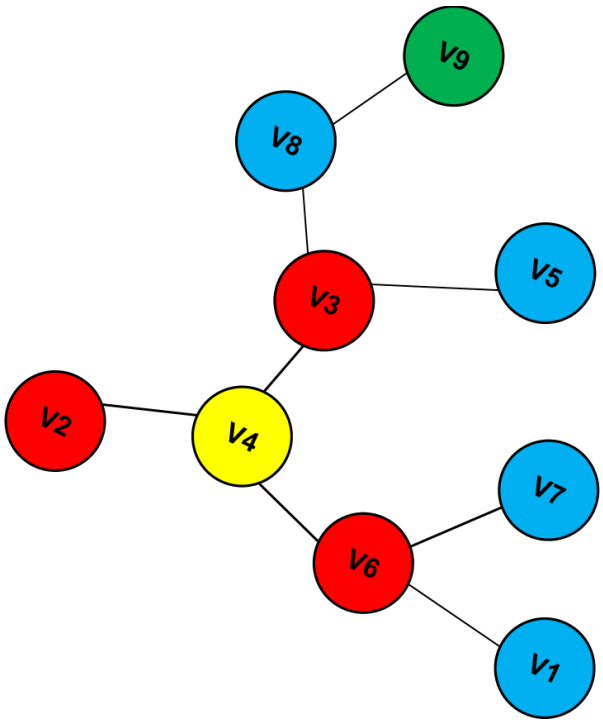



Figure 4.3: A simple graph with different depth level adjacency node-sets

According to Formula (4-3), the network performance of the original network $G$ without any disruptive events can be obtained by calculating the following Formula (4-6):

$$FTP(G) = \frac{Q}{n(n-1)} \sum_{i \neq j \in V(G)} \frac{f_{ij}}{\tau_{ij}} \qquad (4\text{-}6),$$

where the number of people $Q$ who can still normally make use of the network is defined as follows:

$$Q = \sum_{i=1}^{n} Q_i^* \tag{4-7}$$

Combining Formula (4-2), Formula (4-3) and Formula (4-6), the definition of resilience can be rewritten as follows:

$$Resilience(G_k) = \frac{\Delta P}{P_0} = \frac{P_0 - P_d}{P_0} = \frac{FTP(G) - FTP(G_k)}{FTP(G)} \tag{4-8}$$

## 4.2 Implementation of the New Resilience Measure and Application to RE(H)STRAIN-related Aspects

So far, in this dissertation we have applied nine measures: betweenness centrality measure (BetwCentr), closeness centrality measure (CloCentr), degree centrality measure (DegCentr), eigenvector centrality measure (EigenCentr), nodal efficiency measure (Effi), nodal flow-weighted efficiency measure (FWEffi), nodal betweenness-efficiency vulnerability measure (BetwEffiVul), nodal residual closeness vulnerability measure (ResiduCloVul) and the TOPSIS-based aggregation measure (AggregTOPSIS), to identify the key nodes in a graph. In order to compare and evaluate them and then tell the differences which one is more suitable and efficient to identify the key nodes, in this chapter, we propose a new network performance to define the resilience. However, before conducting the resilience analysis, we first need to design different attack scenarios based on these distinguished measures. In the RE(H)STRAIN project, when considering the terrorist attacks, many aspects need to be taken into account, including the motivation and intention of potential terrorists, the possible means of attack from the BCRE (biological, chemical, radiological, explosive) arsenal, the damage to infrastructure and railway traffic, the number of fatalities and injured persons, economic loss, etc. But, in this dissertation, the so-called attack means that when we attack one node in a graph, we will remove the given node and its corresponding edges from the original graph. Therefore, the procedure to conduct resilience analysis is like the process of how to determine and allocate the weights for each measure during the calculation of TOPSIS. In summary, there are four steps to follow:

**Firstly,** based on each measure, we rank the nodes of a graph to prepare each attack scenario.

**Secondly**, we delete the same top number of key nodes from the graph based on the order derived from the first step. For instance, if we remove the top one node, then according to Table 3-1, node 1 should be removed based on the betweenness centrality measure, while according to the nodal betweenness-efficiency vulnerability measure, node 103 needs to be removed. Likewise, if removing the top two nodes, then nodes 1 and 103 should be removed based on the former measure, and nodes 103 and 4 need to be removed according to the latter measure, and so on.

**Thirdly**, in this step, we should also stepwise calculate the resilience of a network based on Formula (4-3)～Formula (4-8). For example, when deleting the top one node from the graph, we compute the first group of network resilience values based on different measures. If removing the top two nodes, then we need to calculate the second group of network resilience values also based on these measures, and so on. That means, when deleting top $i$ nodes, we should calculate and get the $i_{th}$ group of network resilience values.

**Fourthly**, based on the network resilience values within $i_{th}$ group, i.e., after we have removed top $i$ nodes from the network, we can compare and conclude which measure is more suitable and efficient to identify the key nodes. The specific numerical results are shown in Figure 4.4. According to this figure, we can find that with the largest frequencies, the attacks based on aggregation measure can almost always lead to lower resilience. For example, in the square zone of Figure 4.4, its zoom-in picture is shown in Figure 4.5, based on which we can see there are only six cases that the TOPSIS-based aggregation measure cannot lead to lower resilience from the numbers of removed stations 10 to 30; in such a case, the TOPSIS-based aggregation measure can be seen as a promising and suitable measure.

However, in practice, for terrorists it is impossible to attack many stations simultaneously. Therefore, the most likely situation is that they might attack the most essential stations.

Thus, if one measure can lead to lower resilience when deleting a small number of nodes from the network, we can say this measure is more suitable and effective to identify the critical stations in transportation network.

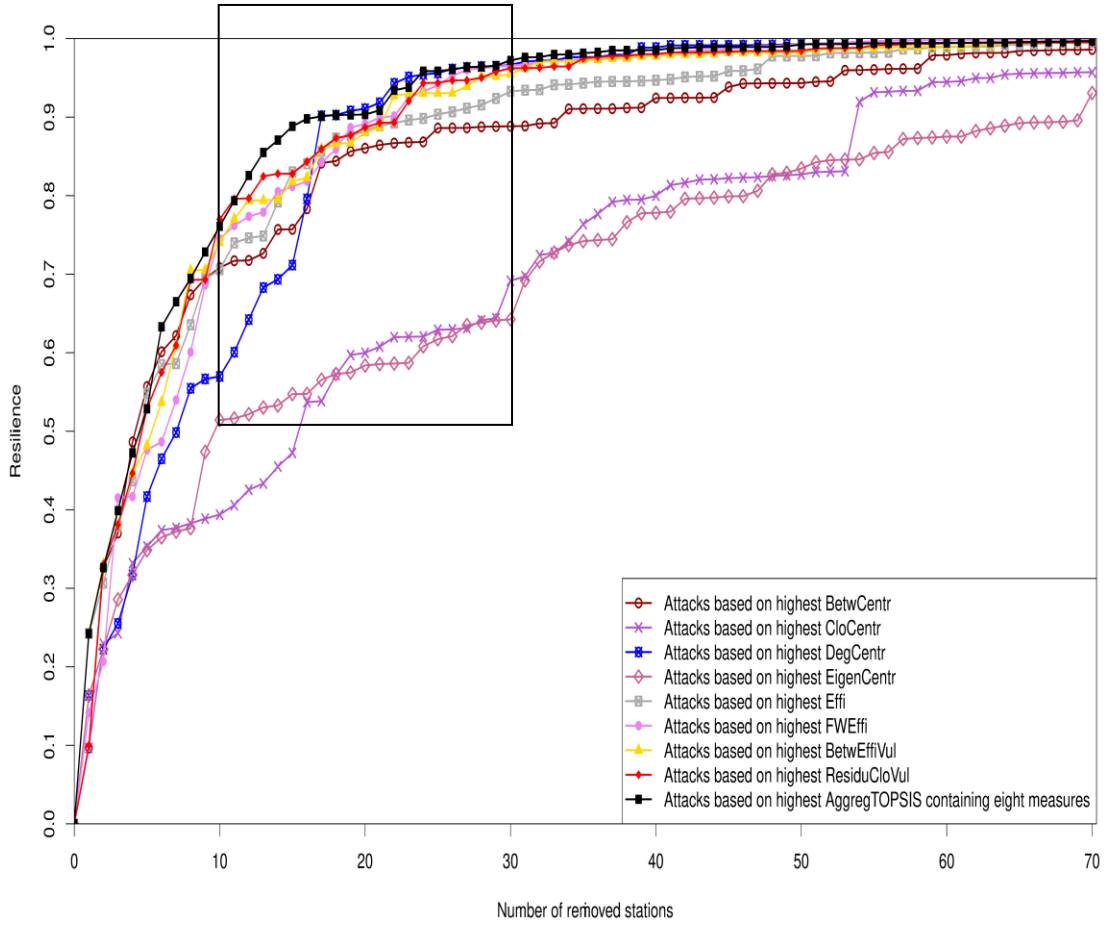



Figure 4.4: Results of resilience analysis under different targeted attacks

When only focusing on the small number of nodes deleted from networks, the results are shown in Figure 4.6, based on which, although the *aggregation measure* can almost always lead to lower resilience, it can´t always lead to lower resilience when deleting a small number of nodes. For instance, when deleting the top 3 nodes, the attacks based on flow-weighted efficiency can lead to lower resilience, whereas if deleting the top 4 or 5 nodes, the attacks based on betweenness centrality can lead to lower resilience.

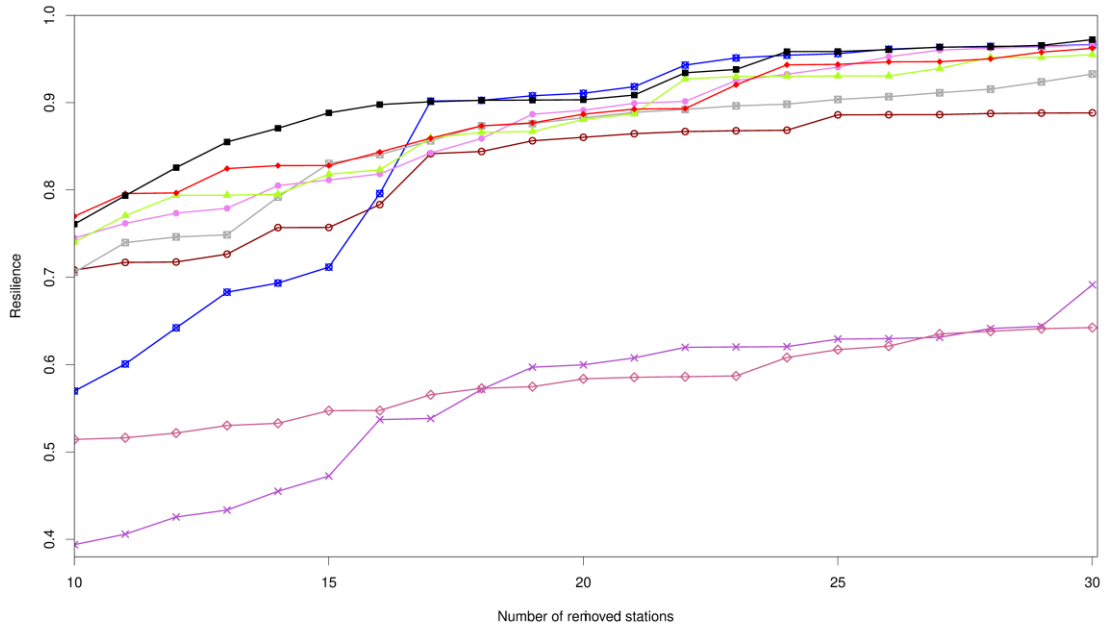



Figure 4.5: Zoom-in of the square zone in Figure 4.4

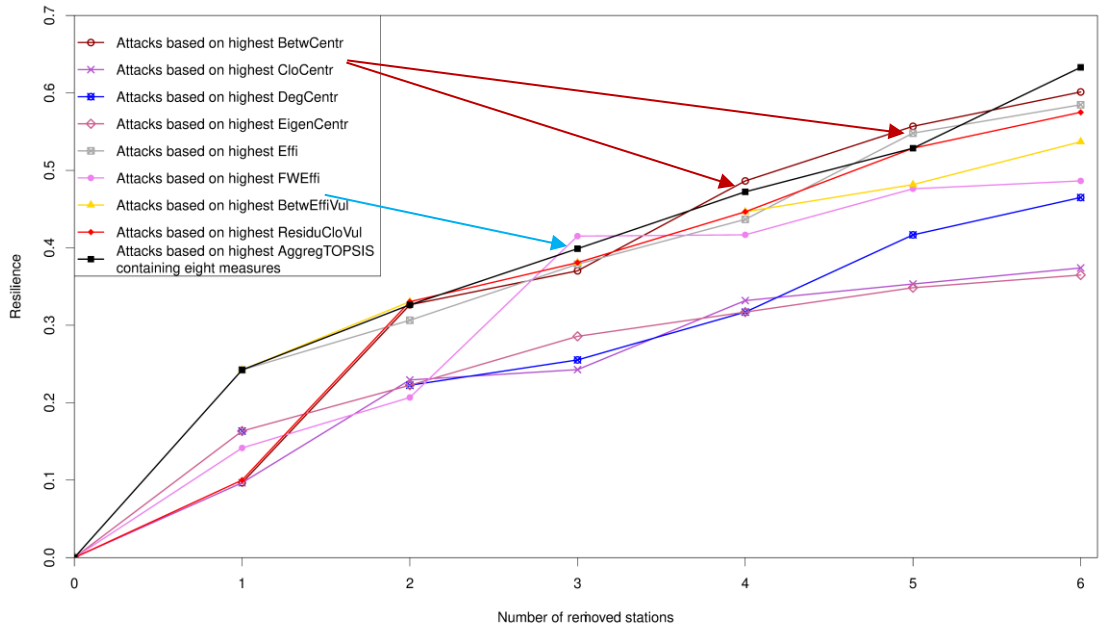



Figure 4.6: Results of resilience analysis under different targeted attacks focusing on deleting top small numbers of nodes

Furthermore, according to Figure 4.4, we find that with larger frequencies, the attacks based on closeness and eigenvector centrality measures can almost always lead to larger resilience, which means that these two measures will contribute less to the TOPSIS-based aggregation measure, and the attacks based on other measures result in different resilience, but the differences are not too many, not like the aforementioned closeness and eigenvector measures with larger deviation.

Therefore, among these eight measures BetwCentr, CloCentr, DegCentr, EigenCentr, Effi, FWEffi, BetwEffiVul and ResiduCloVul, we further consider what situation will happen if only aggregating seven of them and whether the new simplified TOPSIS-based aggregation measure can lead to lower resilience with higher frequencies when deleting even just a small number of nodes.

## 4.3 Comparison

Here, when aggregating different measures but without considering a certain single measure, the results compared to the TOPSIS-based aggregation measure considering all eight measures (in the following we call it “original aggregation measure”) display distinguished situations, which are shown in Figure 4.7 to Figure 4.14.

According to Figure 4.4, when the top thirty stations based on the TOPSIS-based aggregation measure are removed (i.e. attacked), network resilience decreases to over 95%; therefore, in the following comparison figures, we only plot resilience under the range of the number of removed stations from 0 to 40.

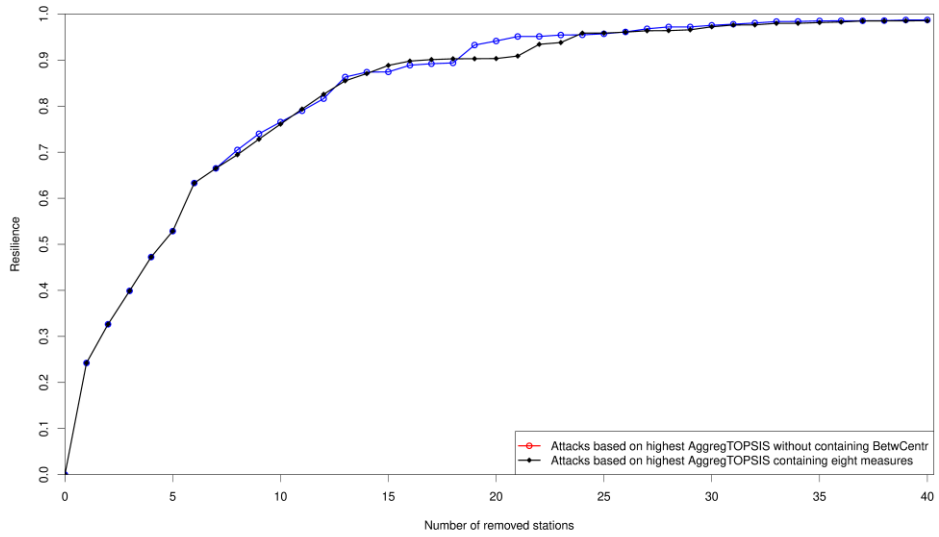



Figure 4.7: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwCentr

According to Figure 4.7, we find that with larger frequencies, the attacks based on AggregTOPSIS without containing BetwCentr can lead to lower resilience, which means that BetwCentr contributes negative influence to the TOPSIS-based aggregation measure.

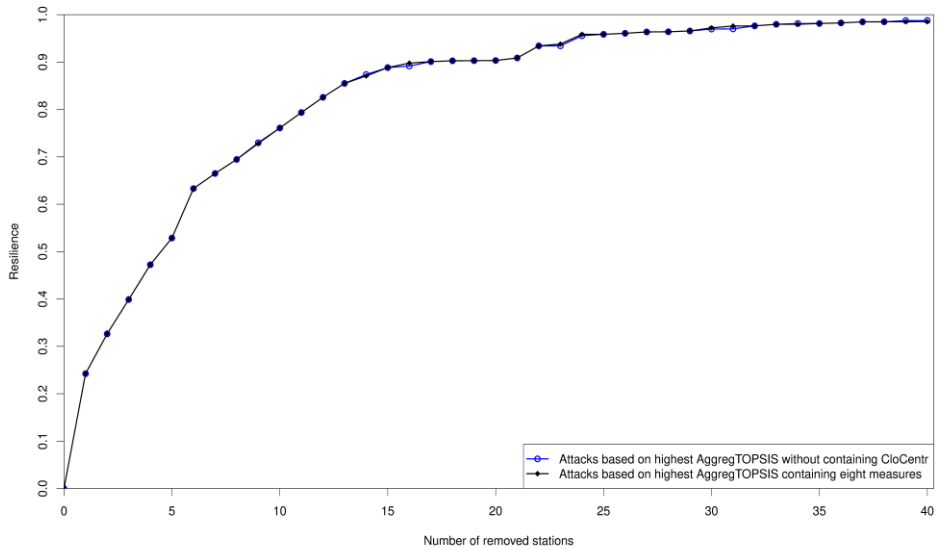



Figure 4.8: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing CloCentr

In Figure 4.8, it is found that the attacks based on AggregTOPSIS without containing CloCentr can only lead to a very slight fluctuation of resilience, meaning that Clocentr has almost no effect on AggregTOPSIS. Therefore, in such a case, we can say that Clocentr make slight (or almost not any) contribution to AggregTOPSIS.

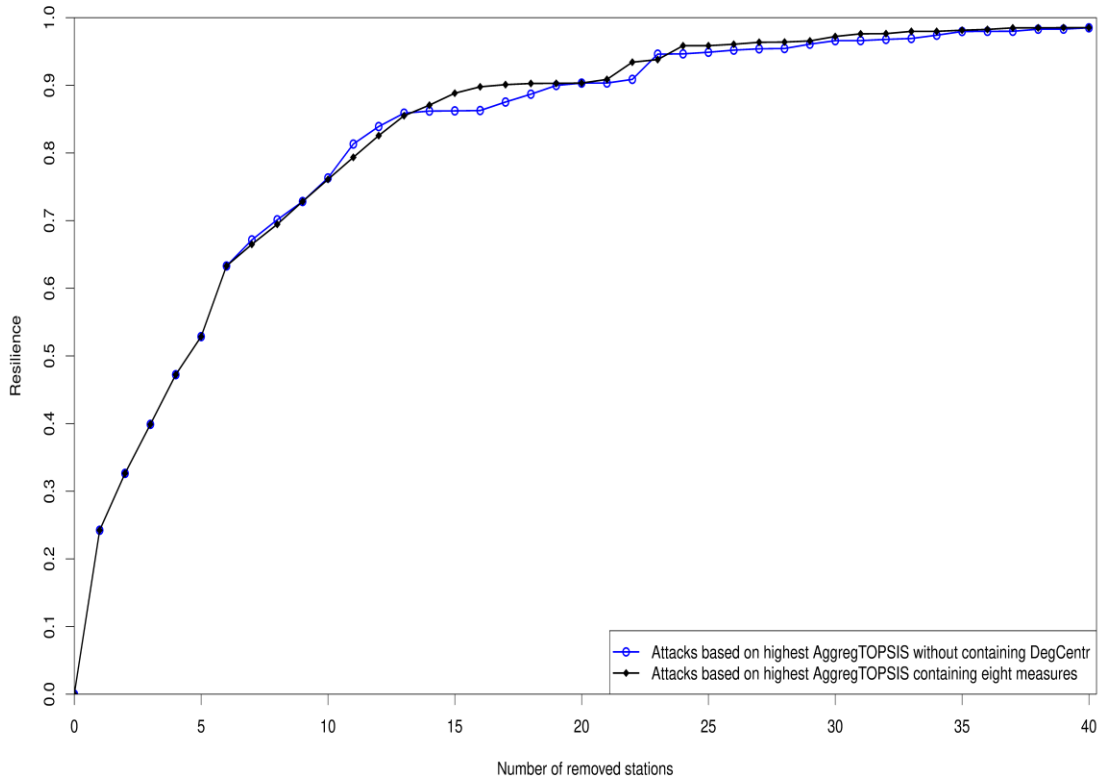



Figure 4.9: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing DegCentr

From Figure 4.9 we can see that, if AggregTOPSIS doesn't include DegCentr, the attacks based on AggregTOPSIS will, with larger frequencies, lead to higher resilience and result in lower resilience in only six cases. Therefore, in such case, we can say that DegCentr will positively affect the AggregTOPSIS.

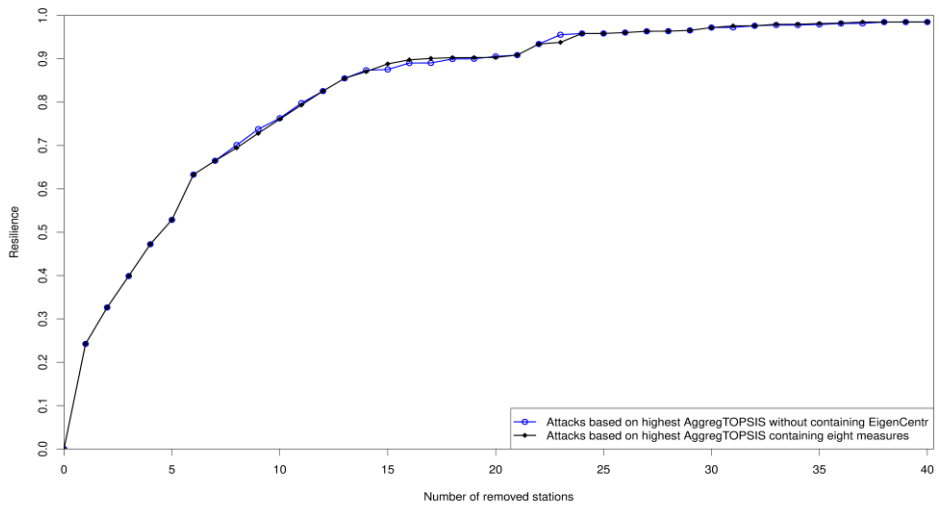



Figure 4.10: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing EigenCentr

Based on Figure 4.10, we can find that the attacks based on AggregTOPSIS without containing EigenCentr, can cause a small (but larger than it is the case in Figure 4.8) fluctuation of resilience in a few situations. Thus, we can say that EigenCentr will only affect AggregTOPSIS to a certain small extent.

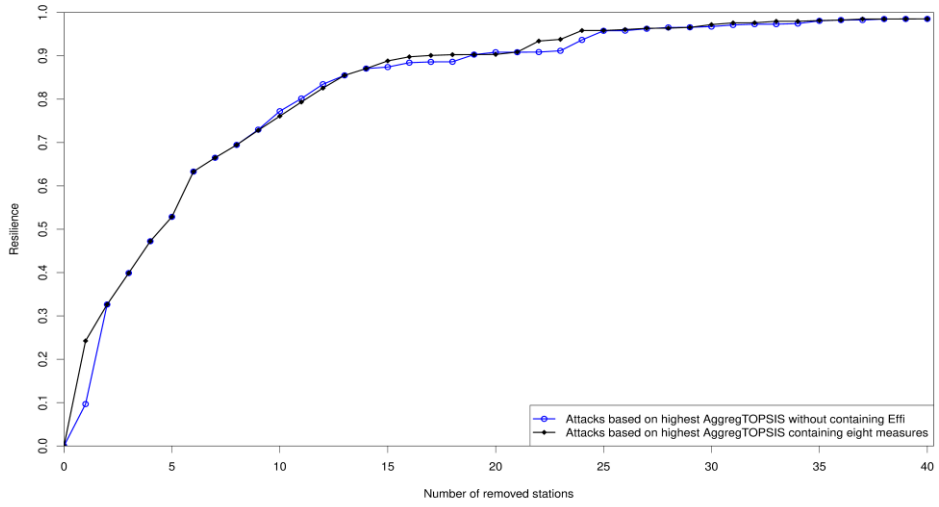



Figure 4.11: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing Effi

In Figure 4.11, we find that with larger frequencies, the attacks based on AggregTOPSIS without containing Effi can result in higher resilience, and especially in the case when only the top one station is attacked, the resilience becomes apparently much higher. Therefore, we can say that Effi has a very positive influence on AggregTOPSIS.

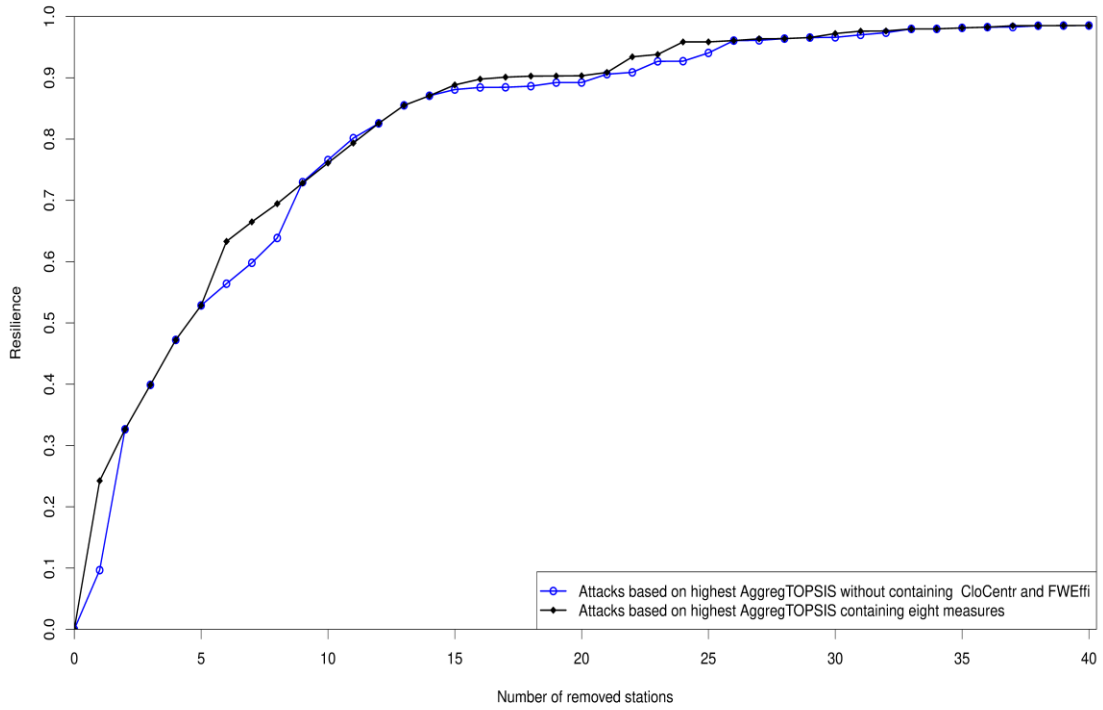



Figure 4.12: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing FWEffi

In Figure 4.12, the picture shows that with larger frequencies, the attacks based on AggregTOPSIS without containing FWEffi can lead to higher resilience. Especially when the top ten stations are attacked, there are four cases that the resilience of the network becomes apparently higher. That is, the network will easily and quickly recover to a normal level under the attacks based on AggregTOPSIS without containing FWEffi. Therefore, in such case, we can say that FWEffi has a very positive effect on AggregTOPSIS.

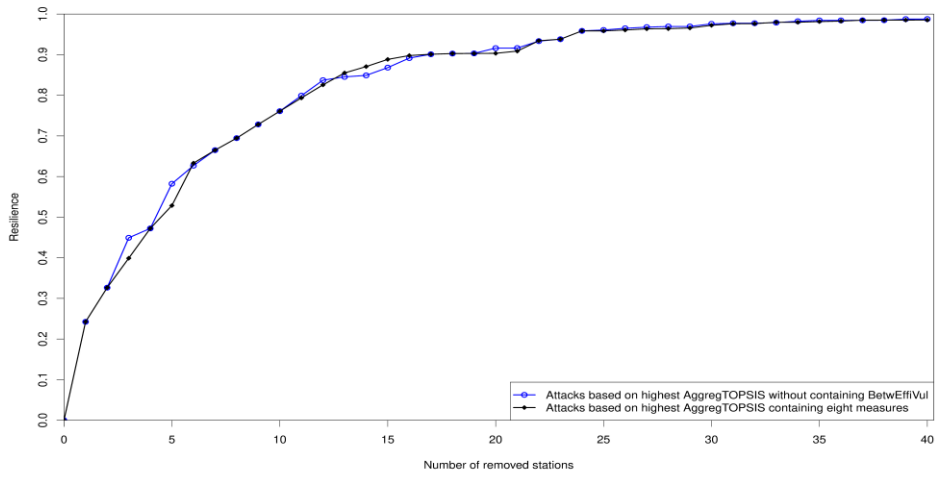



Figure 4.13: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwEffiVul

In Figure 4.13 we can see that with only four cases, the attacks according to AggregTOPSIS without containing BetwEffiVul can cause a little higher resilience. Specially, when the top three and top five stations (identified by AggregTOPSIS without containing BetwEffiVul) are attacked, the resilience of the remaining network apparently decreases. Thus, in such a case, we can say that BetwEffiVul mainly contributes negatively to AggregTOPSIS.

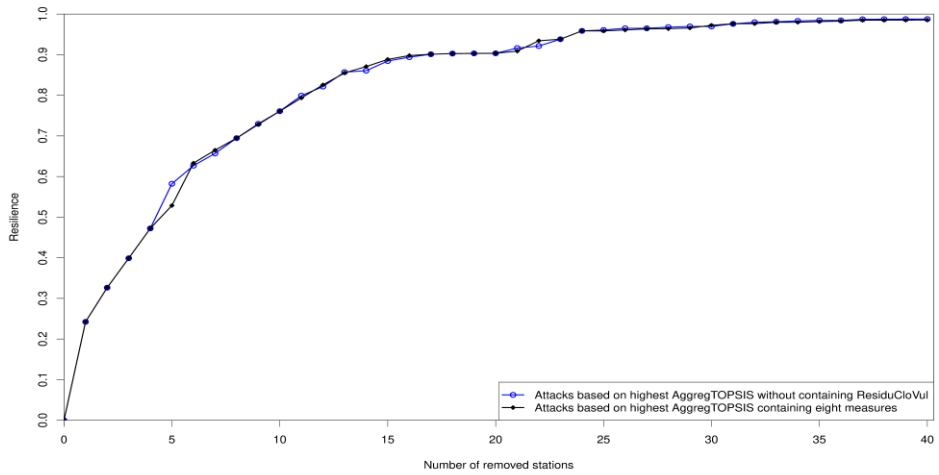



Figure 4.14: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing ResiduCloVul

From Figure 4.14, it can be found that with larger frequencies, the attacks according to AggregTOPSIS without containing ResiduCloVul can result in lower resilience. Especially, when the top five stations (identified by AggregTOPSIS without containing ResiduCloVul) are attacked, the resilience of the remaining network apparently decreases. Thus, in such a case, we can say that ResiduCloVul mainly affects AggregTOPSIS in a negative way.

According to Figure 4.8 and Figure 4.10, we can find that the changes of resilience caused by the aggregation measures without considering closeness or eigenvector centrality measure (compared to the original aggregation measure) are very slight, which is conforming to the situation shown in Figure 4.4, that they don't contribute too much to the aggregation measure; therefore, the aggregation measure is not affected too much, even without considering closeness or eigenvector.

Based on Figure 4.9, Figure 4.11 and Figure 4.12, the resilience caused by the attacks according to the TOPSIS-based aggregation measures (without considering degree, node efficiency or flow-weighted efficiency) will mainly increase. However, as we can find from Figure 4.7, the resilience caused by the attacks according to the TOPSIS-based aggregation measure without considering betweenness becomes a little lower when removing the top nineteen to twenty-three nodes.

From Figure 4.13 we can see that the resilience caused by the attacks according to the TOPSIS-based aggregation measures without considering nodal betweenness-efficiency vulnerability decreases, when deleting the top three or five nodes from the network, but increases when removing nodes thirteen to sixteen. Moreover, based on Figure 4.14, it can be found that the resilience caused by the attacks according to the TOPSIS-based aggregation measures without considering the nodal residual closeness measure becomes somewhat lower when deleting the top five nodes.

Therefore, in this case, we can conclude that the degree centrality measure, node efficiency measure and also the flow-weighted efficiency measure can usually make a positive contribution to the original TOPSIS-based aggregation measure.

The closeness centrality measure and the eigenvector centrality measure make a slight contribution to the original TOPSIS-based aggregation measure; but the betweenness centrality measure will make a negative contribution to the nodes ranking nineteenth to twenty-third based on the original TOPSIS-based aggregation measure, and the nodal betweenness-efficiency vulnerability measure will make a negative contribution to the third and fifth nodes based on the original TOPSIS-based aggregation measure.

Nevertheless, it makes a positive contribution to the nodes ranking thirteenth to sixteenth based on the original TOPSIS-based aggregation measure; the nodal residual closeness measure will mainly make a slight contribution to the original TOPSIS-based aggregation measure, but a negative contribution to the fifth node based on the original TOPSIS-based aggregation measure.

Furthermore, we can say that the degree centrality measure, nodal efficiency measure and the flow-weighted efficiency measure are the basic measures to the TOPSIS-based aggregation measure, but we still cannot conclude whether the closeness and eigenvector centrality measures are not the basic measures to the TOPSIS-based aggregation measure.

However, we can conclude that betweenness centrality measure, nodal betweenness-efficiency vulnerability measure and nodal residual closeness measure are not the basic and necessary measures to the TOPSIS-based aggregation measure since sometimes they make negative contributions to the TOPSIS-based aggregation measure.

In order to verify these conclusions, in the following we will aggregate measures without considering two certain measures compared to the original TOPSIS-based aggregation measure and also the TOPSIS-based aggregation measure without considering one certain measure, and the results are shown in Figure 4.15 to Figure 4.41.

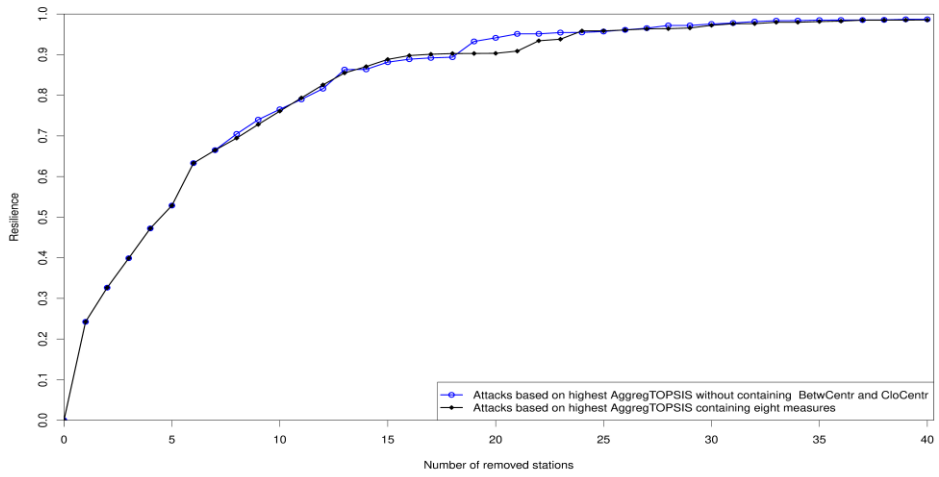



Figure 4.15: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwCentr and CloCentr

Comparing Figure 4.7 and Figure 4.8 with Figure 4.15, we can find that Figure 4.15 is almost the same as Figure 4.7. In such a case, when aggregating measures based on TOPSIS, whether CloCentr is considered or not, it doesn't affect AggregTOPSIS. As stated before in this chapter, BetwCentr is not the basic measure; thus, to a certain extent, here we can say that CloCentr cannot be seen as the basic measure either.

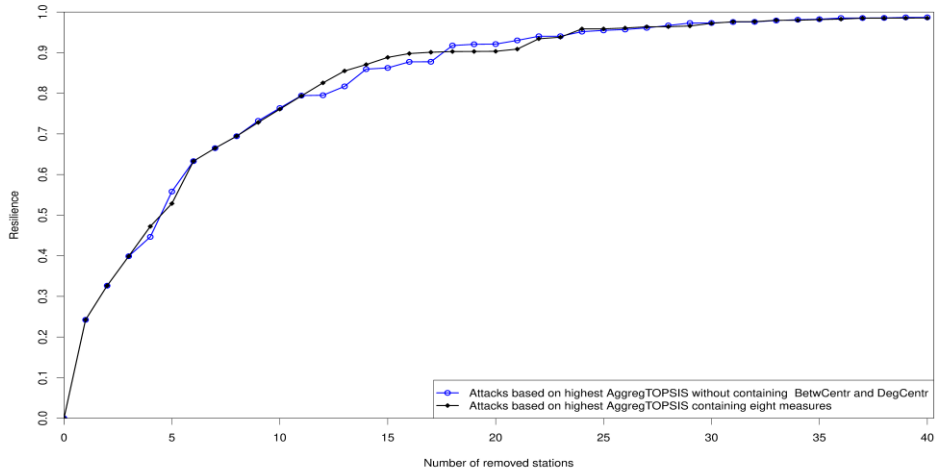



Figure 4.16: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwCentr and DegCentr

Comparing Figure 4.16 (AggregTOPSIS without containing BetwCentr and DegCentr) with Figure 4.7 (AggregTOPSIS without containing BetwCentr), it is found the resilience increases under an increased number of cases; but when comparing Figure 4.16 with Figure 4.9 (AggregTOPSIS without containing DegCentr), we can find that the resilience decreases under an increased number of situations. Therefore, it is further demonstrated that DegCentr is a basic measure but BetwCentr is not.

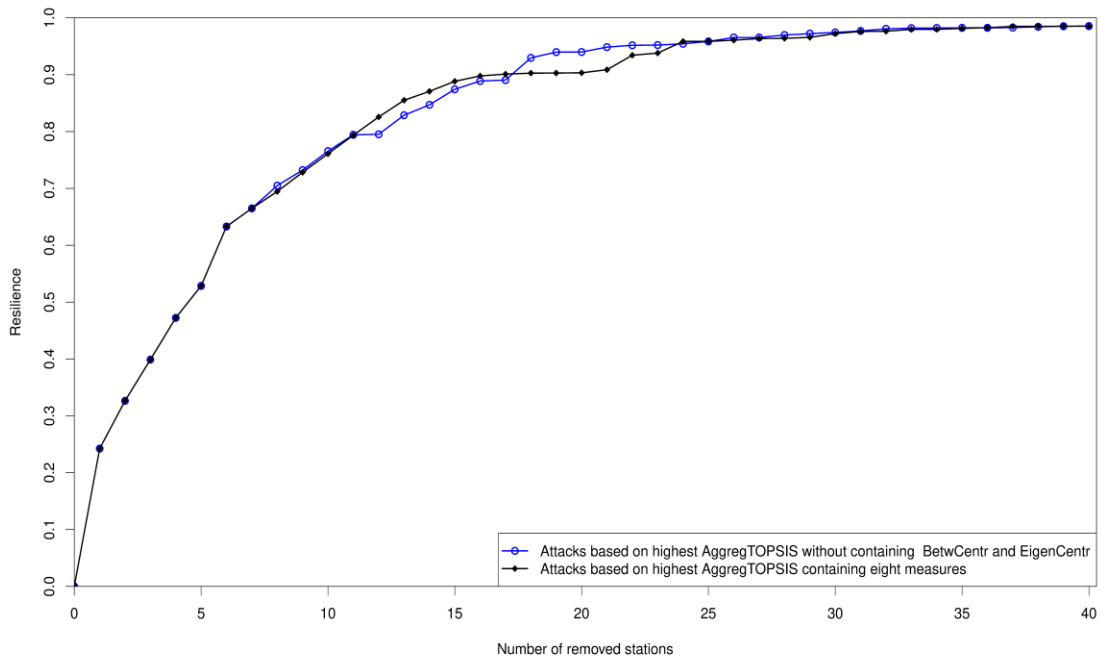



Figure 4.17: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwCentr and EigenCentr

Comparing Figure 4.17 (AggregTOPSIS without containing BetwCentr and EigenCentr) with Figure 4.7 (AggregTOPSIS without containing BetwCentr), we can see that the resilience decreases with an increased number of cases; however, when comparing Figure 4.17 with Figure 4.10 (AggregTOPSIS without containing EigenCentr), we can find that the resilience increases under a raised number of situations. Therefore, it is further demonstrated that BetwCentr is not a basic measure, but EigenCentr might be seen as a basic one.

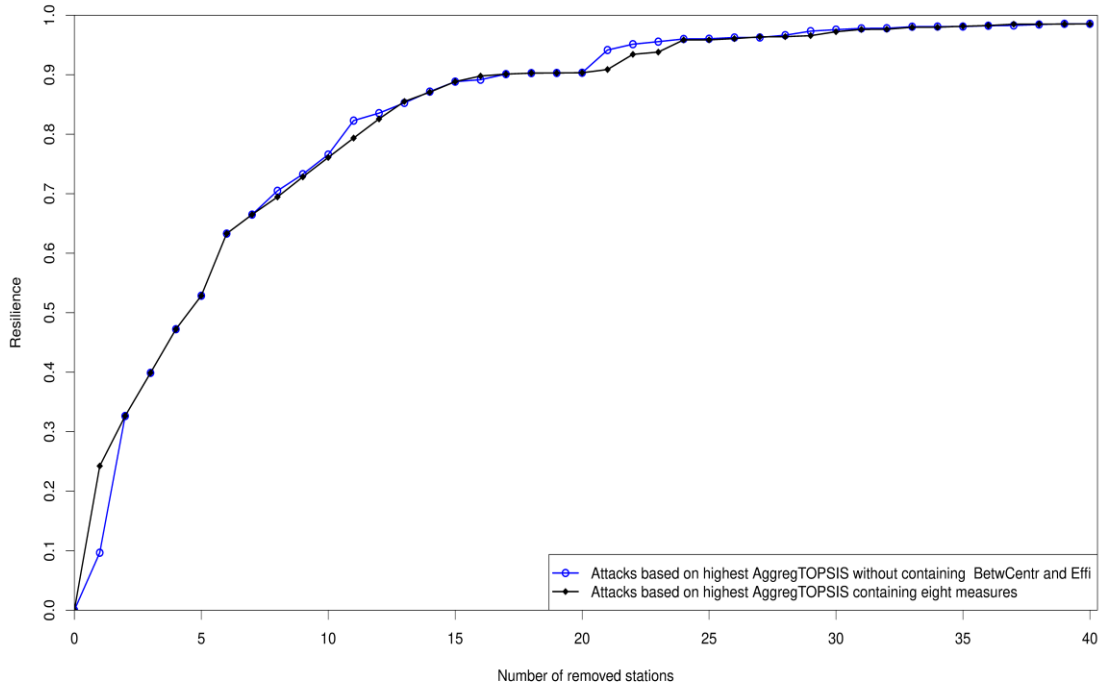



Figure 4.18: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwCentr and Effi

From Figure 4.18 and Figure 4.7, comparing AggregTOPSIS without containing BetwCentr, it can be found that with larger frequencies, the attacks based on AggregTOPSIS without containing BetwCentr and Effi can lead to higher resilience; it is especially obvious that the resilience is much higher when the top one station is attacked based on the latter one.

Moreover, comparing AggregTOPSIS without containing Effi in Figure 4.11 with AggregTOPSIS without containing BetwCentr and Effi in Figure 4.18, we can see that with larger frequencies, the resilience based on the attacking strategies according to the latter one decreases. Therefore, in these two cases, it is validated that BetwCentr has a negative influence on AggregTOPSIS, and Effi positively affects AggregTOPSIS; as stated before in this chapter, here, Effi is validated as a basic measure while BetwCentr is not.

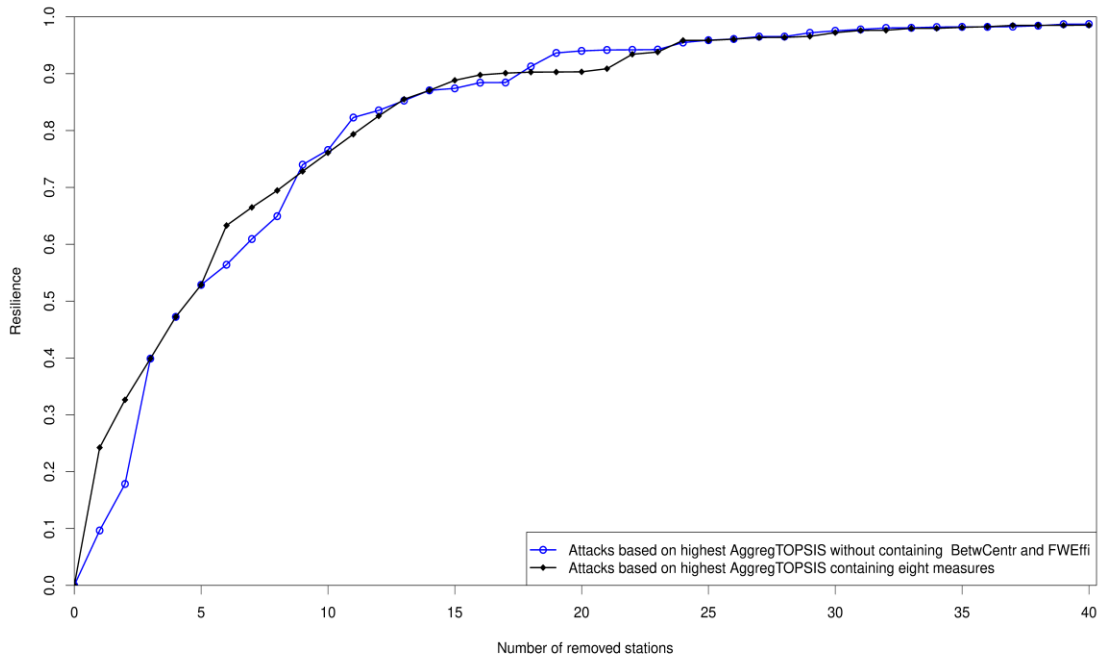



Figure 4.19: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwCentr and FWEffi

According to Figure 4.19 and Figure 4.7, comparing AggregTOPSIS without containing BetwCentr, we can find that with larger frequencies, the attacks based on AggregTOPSIS without containing BetwCentr and FWEffi can lead to higher resilience; apparently, the resilience is much higher when the small top numbers (such as one, two, six, seven and eight) of the stations are attacked based on the latter one. Moreover, comparing AggregTOPSIS without containing FWEffi in Figure 4.12 with AggregTOPSIS without containing BetwCentr and FWEffi in Figure 4.19, we can see that with larger frequencies, the resilience based on the attacks according to the latter one decreases.

Therefore, in these two cases, it is verified that BetwCentr has a negative influence on AggregTOPSIS, and FWEffi positively affects AggregTOPSIS, which means that FWEffi is a basic measure but BetwCentr cannot be seen as the basic one.

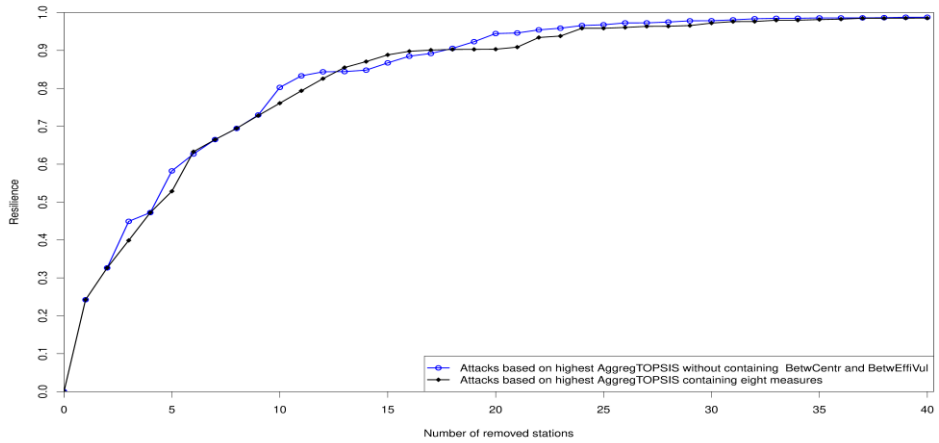



Figure 4.20: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwCentr and BetwEffiVul

According to Figure 4.7, Figure 4.13 and Figure 4.20, we can find that with larger frequencies, the attacks based on AggregTOPSIS without containing BetwCentr and BetwEffiVul can result in lower resilience compared to AggregTOPSIS without containing BetwCentr in Figure 4.7 and AggregTOPSIS without containing BetwEffiVul in Figure 4.13. Thus, both of BetwCentr and BetwEffiVul contribute negatively to AggregTOPSIS; that is, neither of them can be regarded as the basic measures.

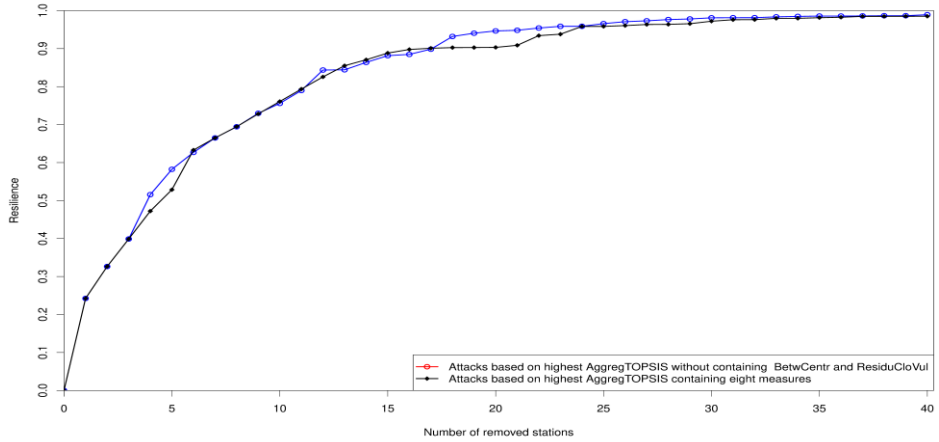



Figure 4.21: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwCentr and ResiduCloVul

Based on Figure 4.7, Figure 4.14 and Figure 4.21, similar to the situation in Figure 4.21, also with larger frequencies, the attacks based on AggregTOPSIS without containing BetwCentr and ResiduCloVul can lead to lower resilience compared with AggregTOPSIS without containing BetwCentr in Figure 4.7 and AggregTOPSIS without containing ResiduCloVul in Figure 4.14. Therefore, both BetwCentr and ResiduCloVul negatively affect AggregTOPSIS, which means that neither of these two can be seen as the basic measures.

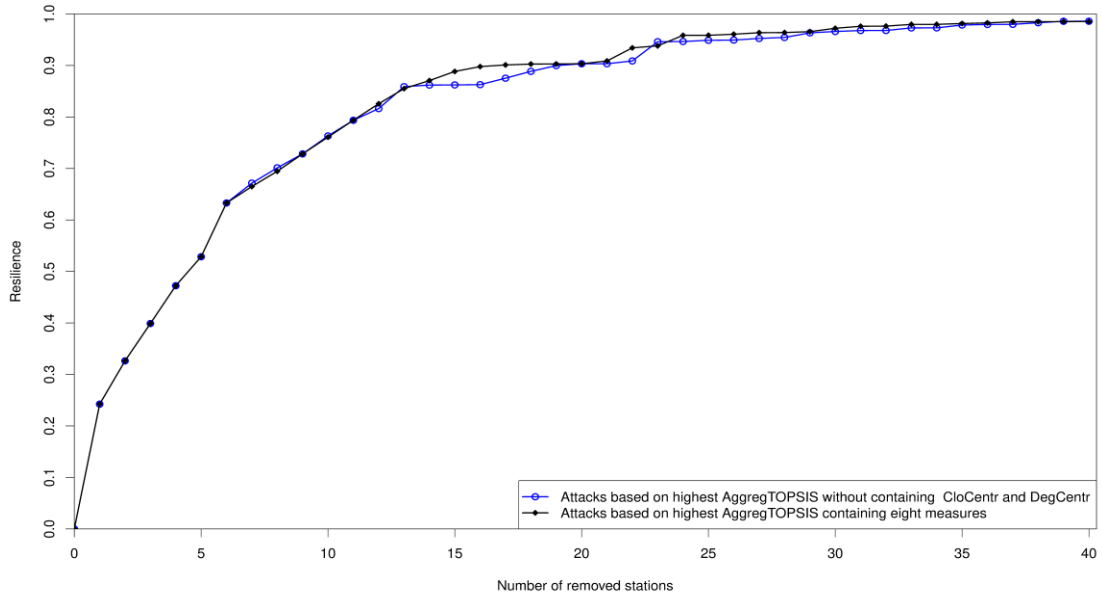



Figure 4.22: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing CloCentr and DegCentr

As stated before in Figure 4.8, CloCentr nearly doesn't affect AggregTOPSIS. From Figure 4.9 and Figure 4.22, it can be found that both of them are almost the same, there are only a few small differences between them. That means, based on AggregTOPSIS without containing CloCentr and DegCentr in Figure 4.22, when top eleven, twelve and thirteen stations are attacked, the resilience is a little higher compared to the case based on AggregTOPSIS without containing DegCentr in Figure 4.9. In such a case, we can say that CloCentr makes a positive contribution to AggregTOPSIS, but only a little; therefore, it cannot be concluded that CloCentr is a basic measure.

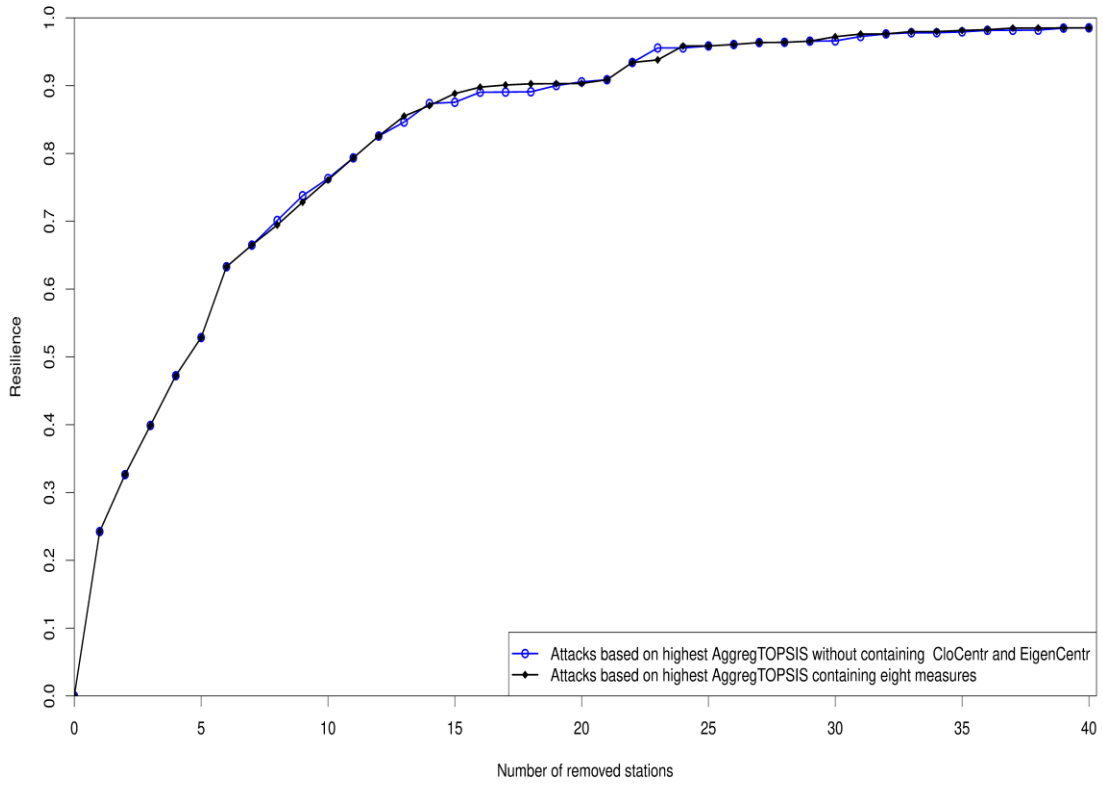



Figure 4.23: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing CloCentr and EigenCentr

Like the case in Figure 4.22, according to Figure 4.10 and Figure 4.23, we can see that both of them are almost the same, and even the differences between them are very slight.

However, comparing Figure 4.8 with Figure 4.23, it is found that with larger frequencies, the attacks based on AggregTOPSIS without containing CloCentr and EigenCentr can lead to higher resilience compared to AggregTOPSIS without containing CloCentr; thus, we can say that EigenCentr makes a positive contribution to AggregTOPSIS. Therefore, in such a case, EigenCentr might be seen as a basic measure.

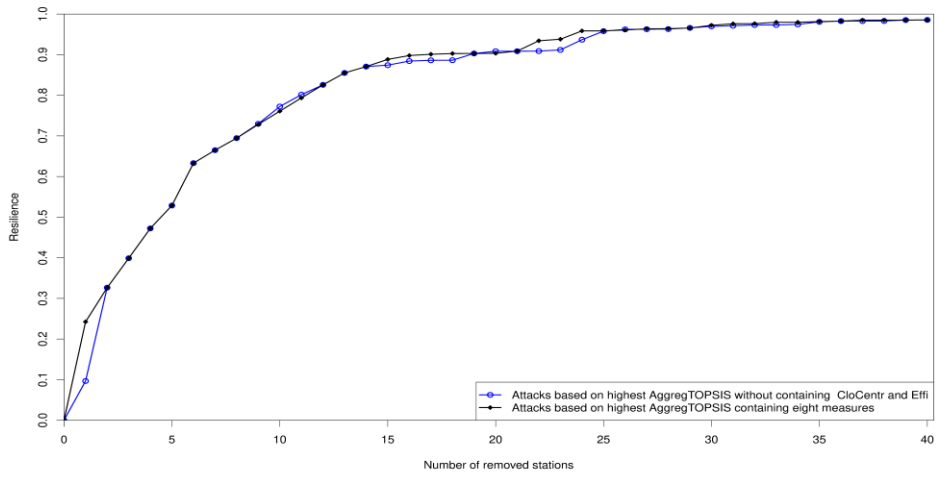



Figure 4.24: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing CloCentr and Effi

Also similar to the situation in Figure 4.22, we can see that Figure 4.24 is almost the same as Figure 4.11 but different from Figure 4.8. Therefore, these three figures can validate that Effi is the basic measure; but because CloCentr doesn't make apparent positive or negative contributions to AggregTOPSIS, it cannot be concluded whether CloCentr is a basic measure or not.

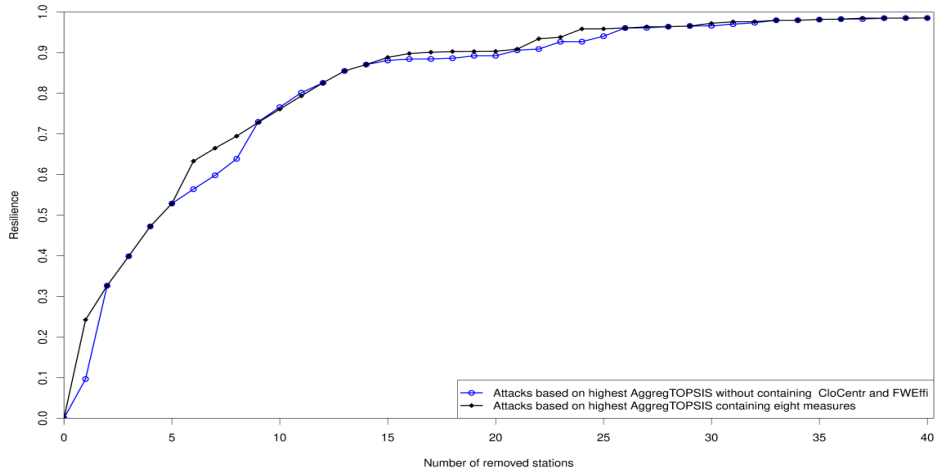



Figure 4.25: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing CloCentr and FWEffi

The same case applies in Figure 4.24, where Figure 4.25 is almost like Figure 4.12 but different from Figure 4.8; thus, based on those, it is demonstrated that FWEffi is the basic measure; however, it is still unknown whether CloCentr is a basic measure or not.

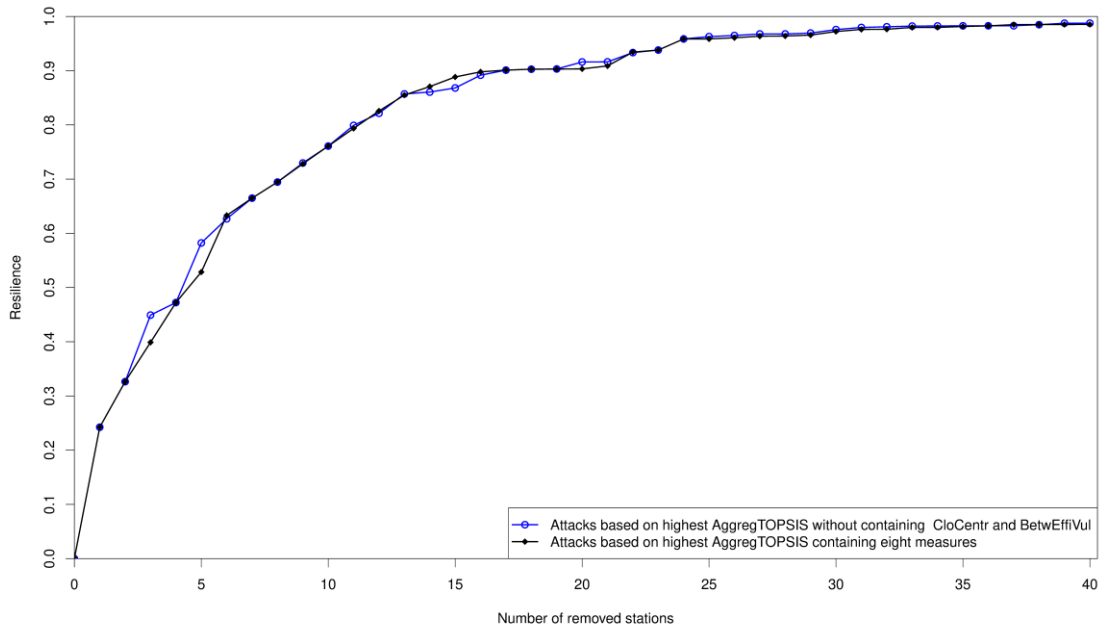



Figure 4.26: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing CloCentr and BetwEffiVul

From Figure 4.26 and Figure 4.8, we can find that with larger frequencies, the attacks based on AggregTOPSIS without containing CloCentr and BetwEffiVul can lead to lower resilience compared to AggregTOPSIS without containing CloCentr. What is especially obvious is that the resilience is much lower when the top three and five stations (identified by the AggregTOPSIS without containing CloCentr and BetwEffiVul) are attacked; thus, in this case, it is validated that BetwEffiVul has a negative influence on AggregTOPSIS and cannot be seen as a basic measure.

When comparing Figure 4.26 with Figure 4.13, it is found that they are similar but still have some differences, i.e., in contrast to AggregTOPSIS without containing BetwEffiVul, although not apparent, but still with larger frequencies, the attacks based on AggregTOPSIS without containing CloCentr and BetwEffiVul can lead to a little lower resilience.

Therefore, in such a situation, we can say that CloCentr makes a few negative contributions to AggregTOPSIS and cannot be regarded as a basic measure.

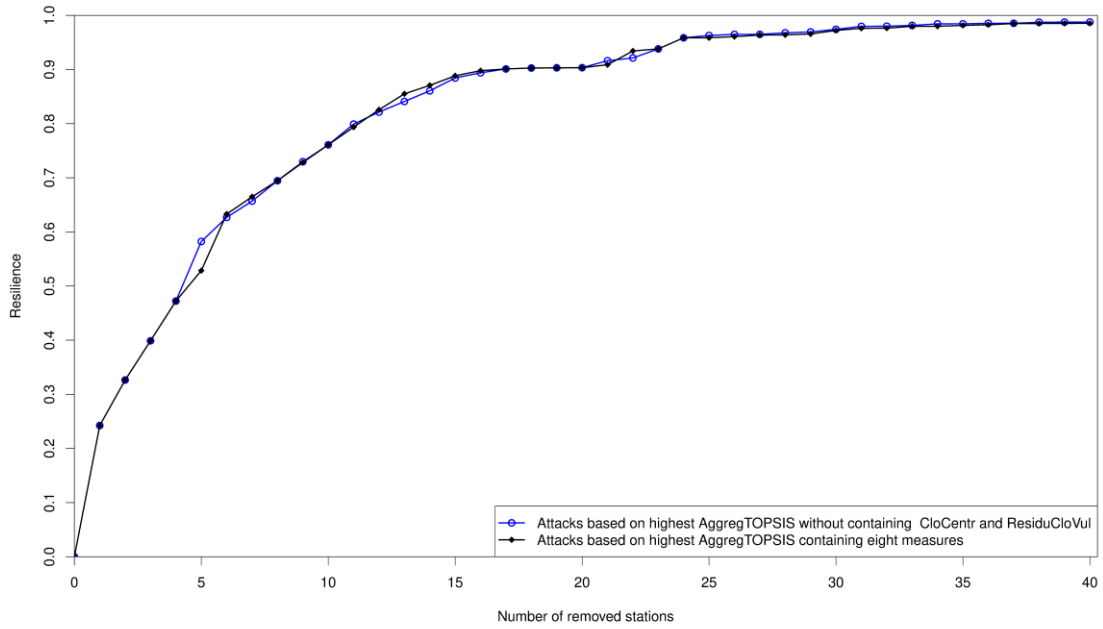



Figure 4.27: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing CloCentr and ResiduCloVul

According to Figure 4.27 and Figure 4.8, we can find that there are only seven cases in which the attacks based on AggregTOPSIS without containing CloCentr and ResiduCloVul result in higher resilience compared to AggregTOPSIS without containing CloCentr; however, with larger frequencies, the resilience caused by the attacks based on AggregTOPSIS without containing CloCentr and ResiduCloVul is lower; thus, in this case, we can say that ResiduCloVul can mainly affect AggregTOPSIS in a negative way, which means that it cannot be seen as a basic measure.

Here, when comparing Figure 4.27 with Figure 4.14, it is found that they are similar and there is only one obvious situation in which the resilience is a little higher compared to AggregTOPSIS without containing ResiduCloVul, namely when the top thirteen stations are attacked based on AggregTOPSIS without containing CloCentr and ResiduCloVul.

Therefore, in such a case, we can say that CloCentr makes a little but slightly positive contribution to AggregTOPSIS, which means that CloCentr might be a basic measure, but so far, we cannot be sure.

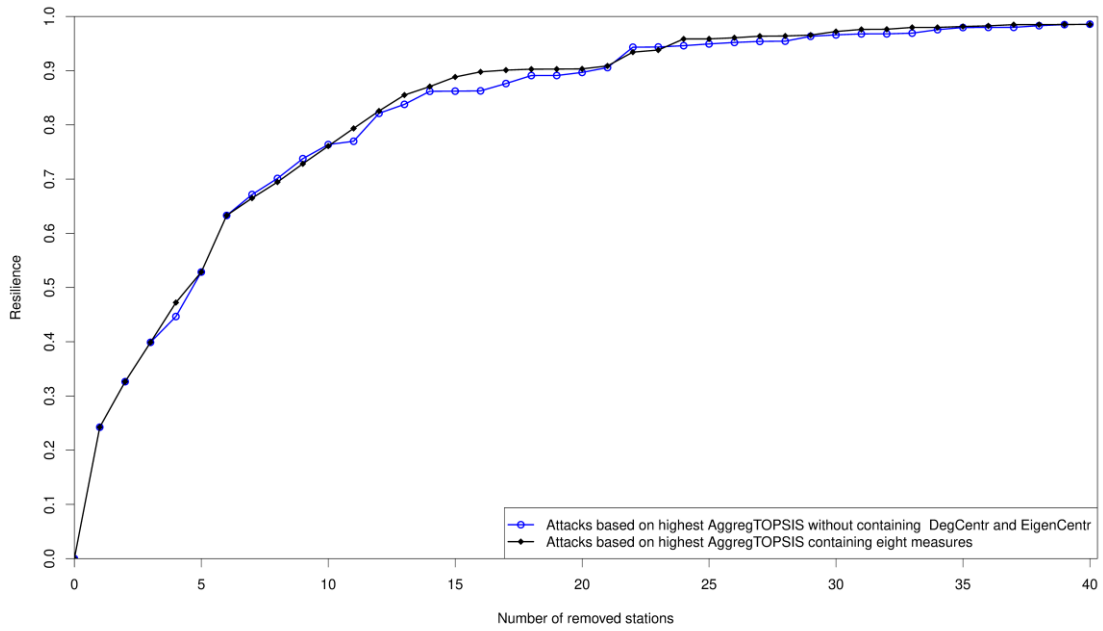



Figure 4.28: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing DegCentr and EigenCentr

From Figure 4.28 and Figure 4.9, we can see that with larger frequencies, the resilience caused by the attacks based on AggregTOPSIS without containing DegCentr and EigenCentr is higher compared to AggregTOPSIS without containing DegCentr.

Moreover, according to Figure 4.28 and Figure 4.10, we can find that with larger frequencies, the attacks based on AggregTOPSIS without containing DegCentr and EigenCentr can lead to higher resilience compared to AggregTOPSIS without containing EigenCentr.

Therefore, in these two situations, we can conclude that both DegCentr and EigenCentr make positive contributions to AggregTOPSIS and can be seen as the basic measures.

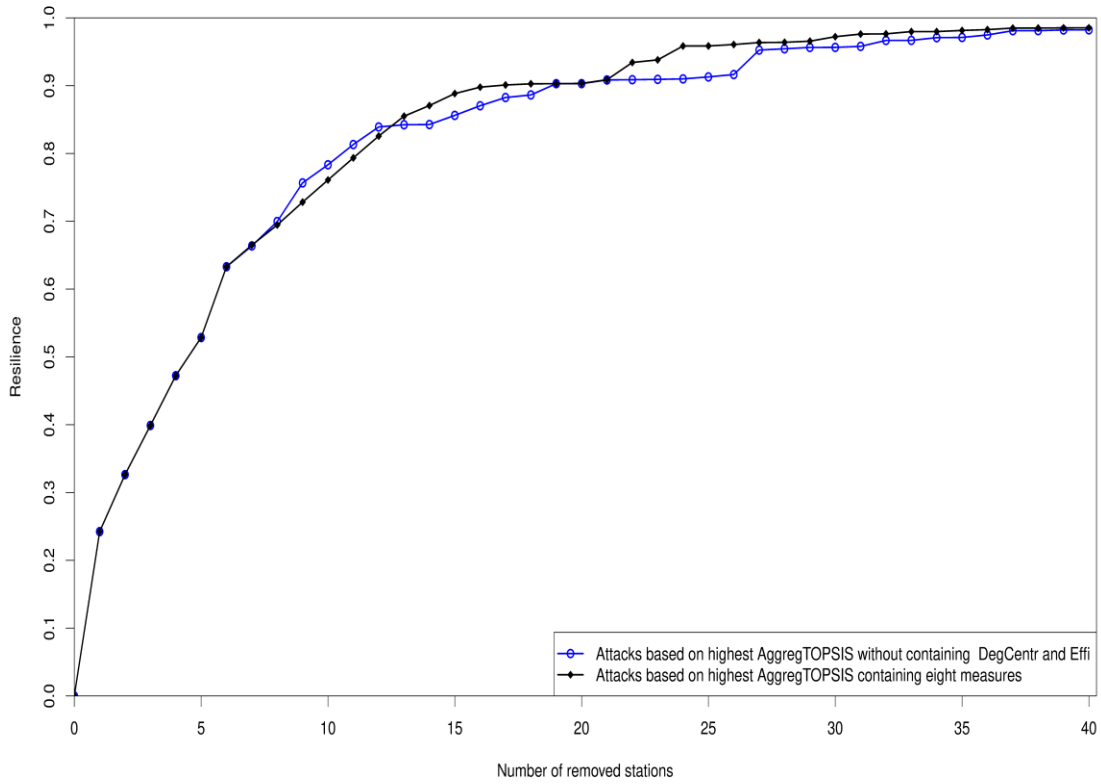



Figure 4.29: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing DegCentr and Effi

According to Figure 4.29 and Figure 4.9, we can see that with larger frequencies, the resilience caused by the attacks based on AggregTOPSIS without containing DegCentr and Effi is higher compared to AggregTOPSIS without containing DegCentr.

Furthermore, from Figure 4.29 and Figure 4.11, it can be found that with larger frequencies, the attacks based on AggregTOPSIS without containing DegCentr and Effi can lead to higher resilience compared to AggregTOPSIS without containing Effi. Therefore, these two cases demonstrate that both DegCentr and Effi make positive contributions to AggregTOPSIS and can be seen as the basic measures.

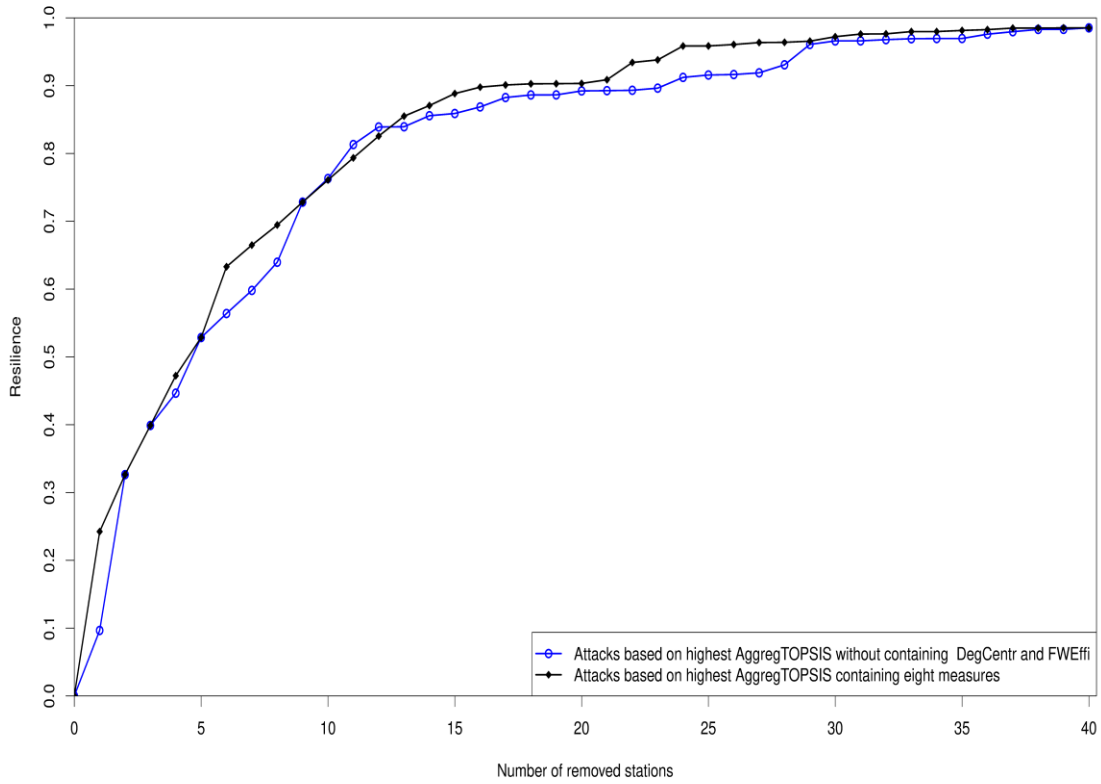



Figure 4.30: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing DegCentr and FWEffi

Similar to the case in Figure 4.29, from Figure 4.30 and Figure 4.9 we can find that with larger frequencies, the resilience caused by the attacks based on AggregTOPSIS without containing DegCentr and FWEffi is higher compared to AggregTOPSIS without containing DegCentr.

And based on Figure 4.30 and Figure 4.12, we can see that with larger frequencies, the attacks based on AggregTOPSIS without containing DegCentr and FWEffi can result in higher resilience compared to AggregTOPSIS without containing FWEffi. Thus, based on these two cases, we can conclude that both DegCentr and FWEffi positively affect AggregTOPSIS and can be seen as the basic measures.

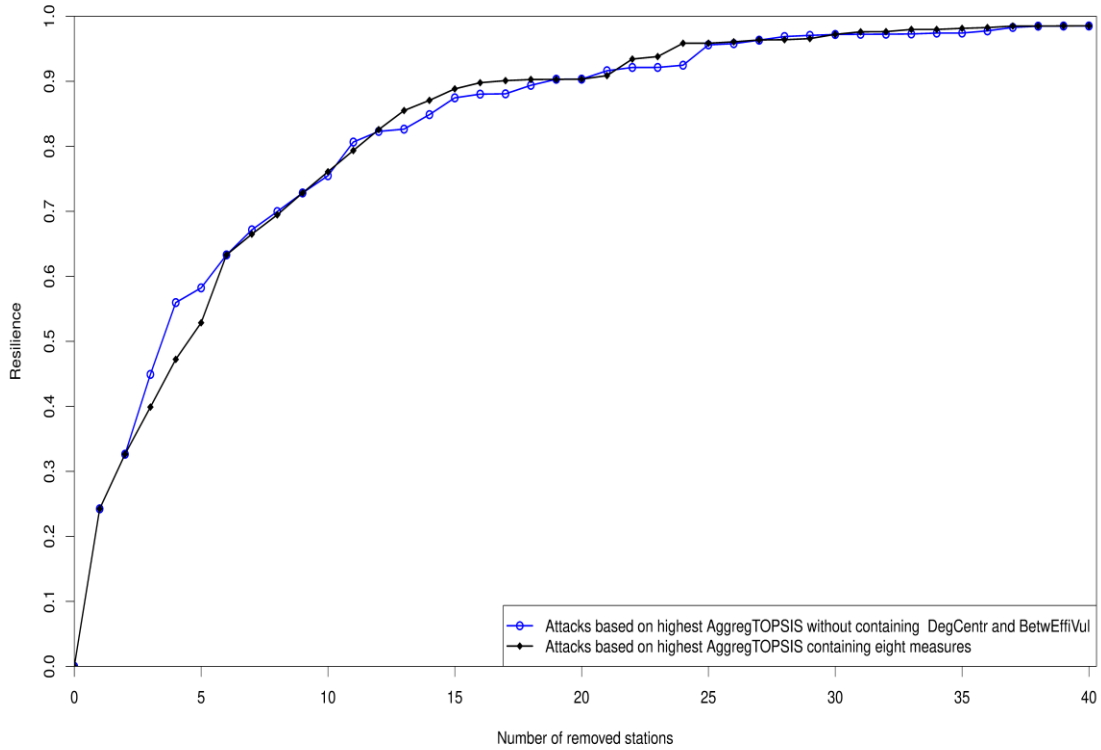



Figure 4.31: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing DegCentr and BetwEffiVul

From Figure 4.31 and Figure 4.9 we can find that with larger frequencies, the resilience caused by the attacks based on AggregTOPSIS without containing DegCentr and BetwEffiVul is apparently lower compared to AggregTOPSIS without containing DegCentr.

However, from Figure 4.31 and Figure 4.13 we can see that with larger frequencies, the attacks based on AggregTOPSIS without containing DegCentr and BetwEffiVul can lead to higher resilience compared to AggregTOPSIS without containing BetwEffiVul. Thus, based on these two cases, we can conclude that DegCentr positively affects AggregTOPSIS and can be seen as the basic measure, but BetwEffiVul has a negative influence on AggregTOPSIS and cannot be regarded as the basic measure.

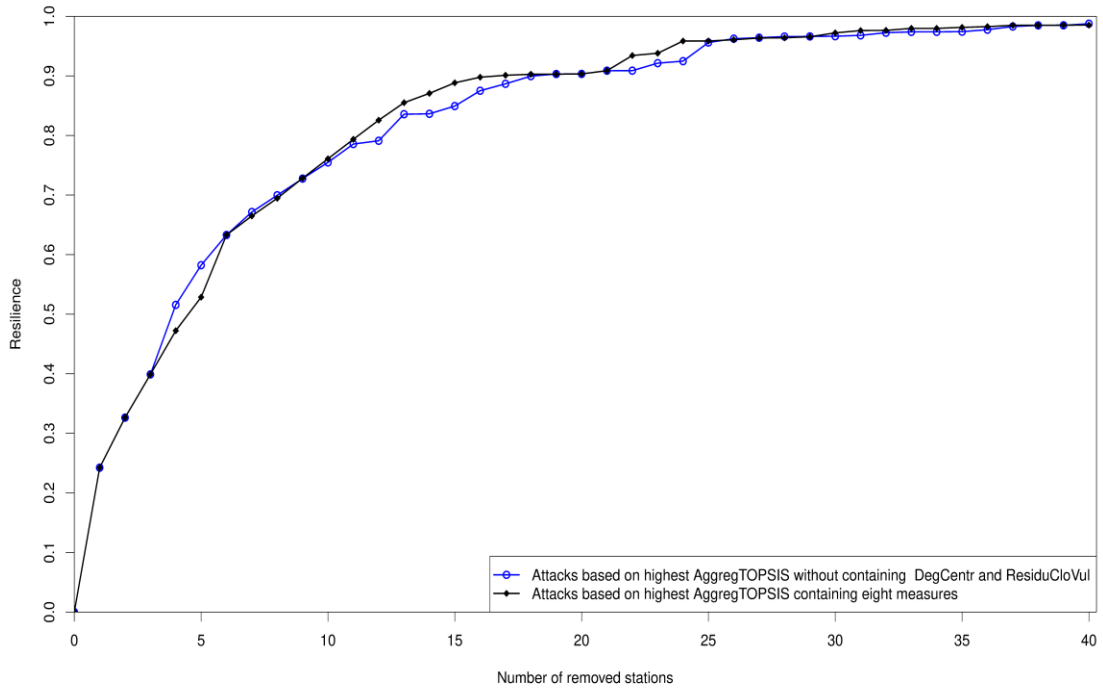



Figure 4.32: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing DegCentr and ResiduCloVul

According to Figure 4.32 and Figure 4.9, it can be found that with larger frequencies, the resilience caused by the attacks based on AggregTOPSIS without containing DegCentr and ResiduCloVul is lower compared to AggregTOPSIS without containing DegCentr, especially, when top four and five stations (detected on the basis of AggregTOPSIS without containing DegCentr and ResiduCloVul) are attacked.

However, from Figure 4.32 and Figure 4.14, we can see that with larger frequencies, the attacks based on AggregTOPSIS without containing DegCentr and ResiduCloVul can apparently lead to higher resilience compared to AggregTOPSIS without containing ResiduCloVul. Therefore, we can say that DegCentr affects AggregTOPSIS in a positive way and can be seen as the basic measure, but ResiduCloVul makes negative contributions to AggregTOPSIS and cannot be regarded as the basic measure.

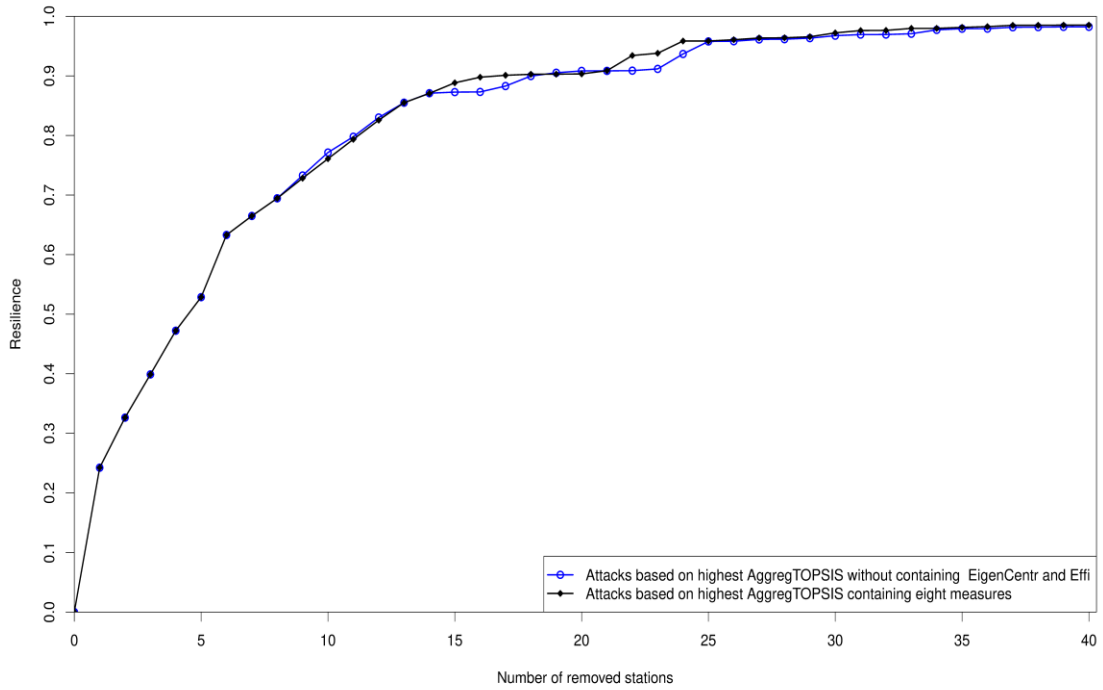



Figure 4.33: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing EigenCentr and Effi

Based on Figure 4.33 and Figure 4.10, it can be found that with larger frequencies, the resilience caused by the attacks based on AggregTOPSIS without containing EigenCentr and Effi is higher compared to AggregTOPSIS without containing EigenCentr. From Figure 4.33 and Figure 4.11, we can find that even if the top one station is attacked, the resilience based on AggregTOPSIS without containing EigenCentr and Effi is lower, but with larger frequencies, the attacks based on AggregTOPSIS without containing EigenCentr and Effi can result in higher resilience compared to AggregTOPSIS without containing Effi.

Therefore, we can say that Effi can positively affect AggregTOPSIS and can be seen as the basic measure; EigenCentr can also make a slightly positive contribution to AggregTOPSIS and can be regarded as the basic measure.

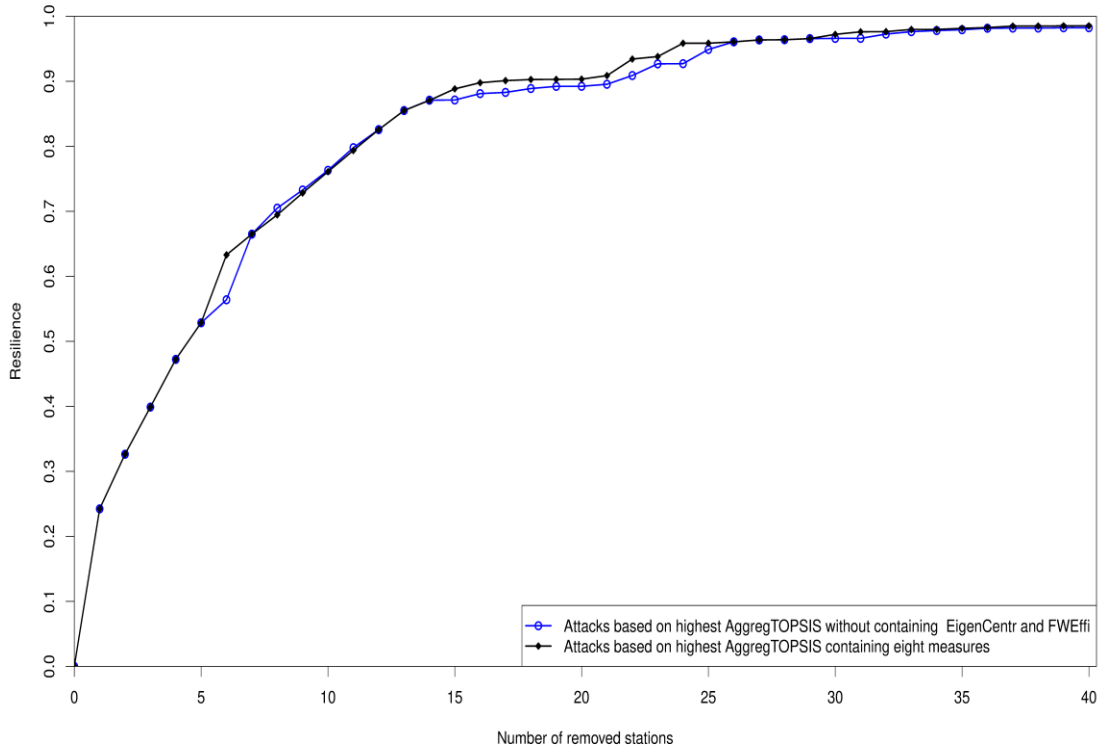



Figure 4.34: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing EigenCentr and FWEffi

From Figure 4.34 and Figure 4.10, it can be found that with larger frequencies, the resilience caused by the attacks based on AggregTOPSIS without containing EigenCentr and FWEffi is higher compared to AggregTOPSIS without containing EigenCentr.

From Figure 4.34 and Figure 4.12, we can see that even with larger frequencies, the attacks based on AggregTOPSIS without containing EigenCentr and FWEffi can result in a slightly higher resilience compared to AggregTOPSIS without containing FWEffi, but we can also find that when the top one, top seven and top eight stations are attacked, it is obvious that the resilience based on AggregTOPSIS without containing EigenCentr and FWEffi is lower. Therefore, we can say that FWEffi can positively affect AggregTOPSIS and can be seen as the basic measure; but here we cannot conclude whether EigenCentr can also be regarded as the basic measure or not.

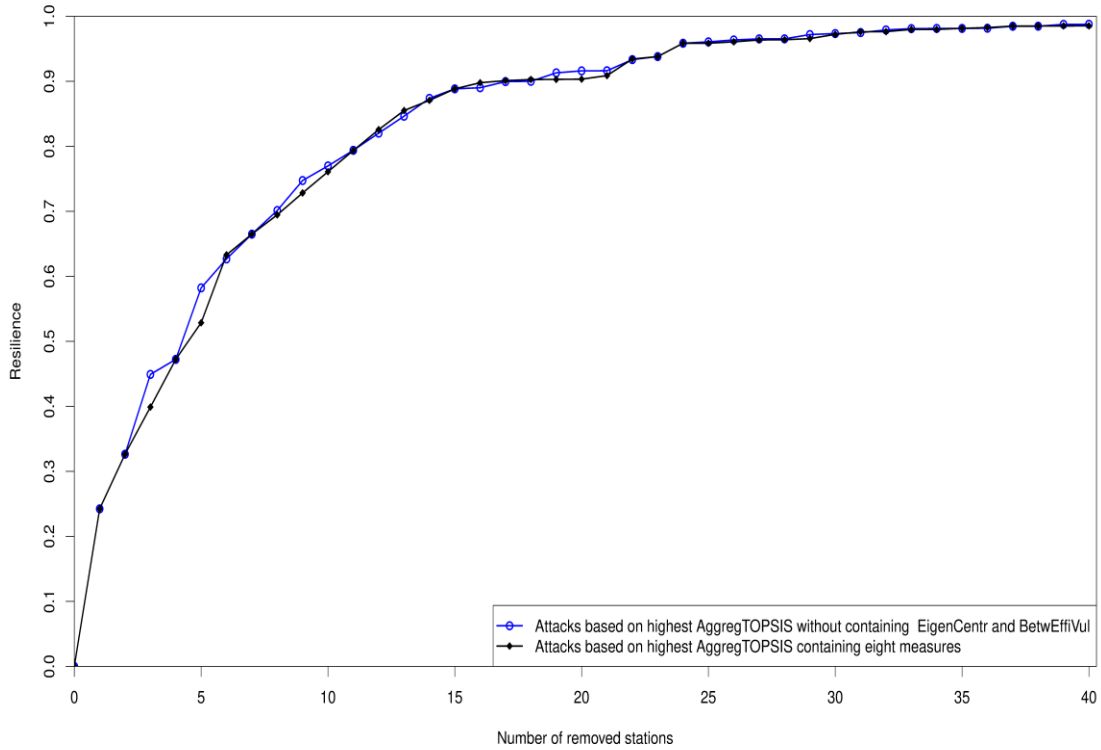



Figure 4.35: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing EigenCentr and BetwEffiVul

From Figure 4.35 and Figure 4.10 we can find that with larger frequencies, the attacks based on AggregTOPSIS without containing EigenCentr and BetwEffiVul can lead to lower resilience compared to AggregTOPSIS without containing EigenCentr.

According to Figure 4.35 and Figure 4.13, we can see that even with larger frequencies, the attacks based on AggregTOPSIS without containing EigenCentr and BetwEffiVul can also result in lower resilience compared to AggregTOPSIS without containing BetwEffiVul.

Therefore, here we can say that both EigenCentr and BetwEffiVul negatively affect AggregTOPSIS and cannot be regarded as the basic measure.

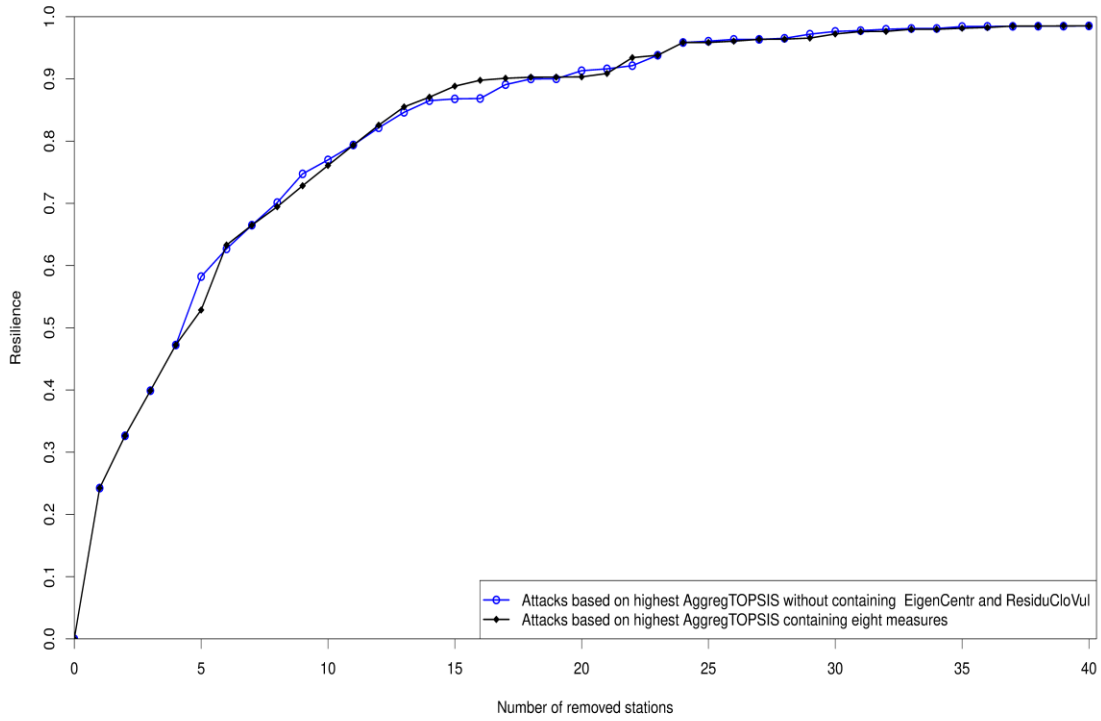



Figure 4.36: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing EigenCentr and ResiduCloVul

From Figure 4.36 and Figure 4.10 we can find that with larger frequencies, the attacks based on AggregTOPSIS without containing EigenCentr and ResiduCloVul can lead to lower resilience compared to AggregTOPSIS without containing EigenCentr.

From Figure 4.36 and Figure 4.13 we can see that some of the attacks based on AggregTOPSIS without containing EigenCentr and ResiduCloVul can also result in lower resilience compared to AggregTOPSIS without containing ResiduCloVul, but the resilience is higher under some other attacks based on AggregTOPSIS without containing EigenCentr and ResiduCloVul.

Therefore, we can conclude that ResiduCloVul negatively affects AggregTOPSIS and cannot be regarded as the basic measure, but regarding EigenCentr we do not know if it can be seen as the basic measure.

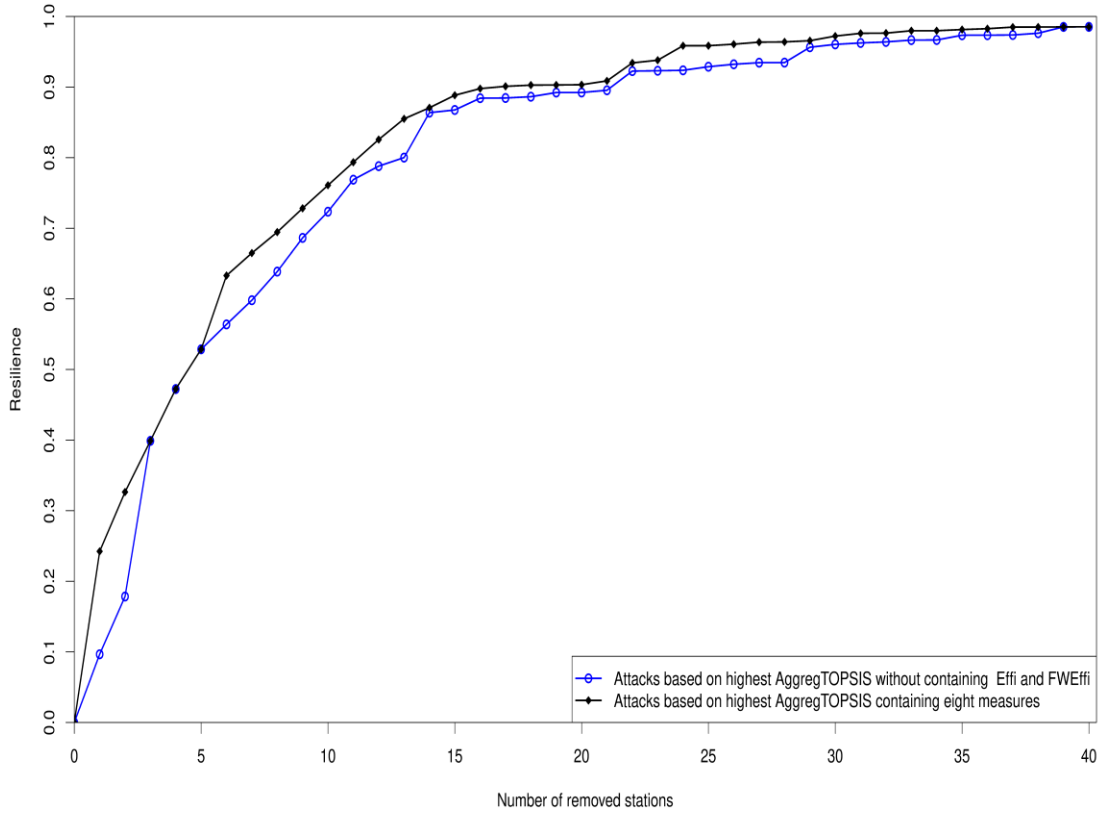



Figure 4.37: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing Effi and FWEffi

Comparing Figure 4.37 with Figure 4.11, we can find that with larger frequencies, the attacks based on AggregTOPSIS without containing Effi and FWEffi can apparently lead to higher resilience compared to AggregTOPSIS without containing Effi.

The situation is the same when comparing Figure 4.37 (AggregTOPSIS without containing Effi and FWEffi) with Figure 4.12 (AggregTOPSIS without containing FWEffi). Therefore, in these two cases it is demonstrated that both Effi and FWEffi contribute positively to AggregTOPSIS and can be seen as the basic measures.

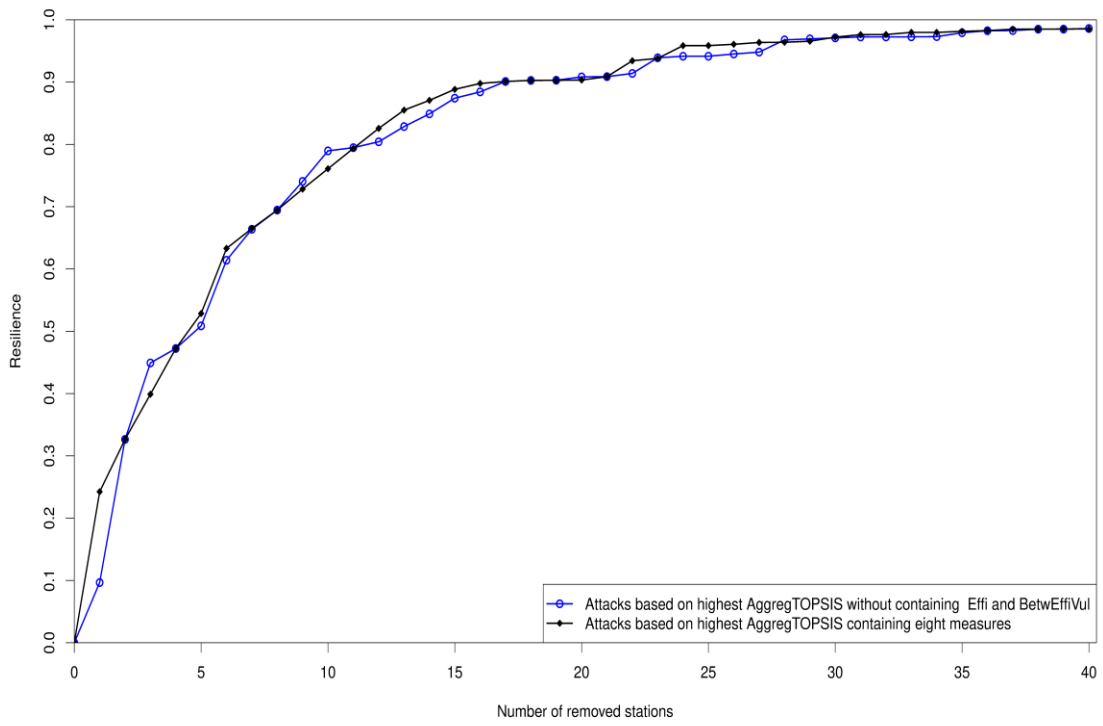



Figure 4.38: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing Effi and BetwEffiVul

From Figure 4.38 and Figure 4.11, we can see that with slightly larger frequencies, the attacks based on AggregTOPSIS without containing Effi and BetwEffiVul can result in higher resilience compared to AggregTOPSIS without containing Effi, but with some frequencies, the resilience caused by the attacks (based on AggregTOPSIS without containing Effi and BetwEffiVul ) is lower; therefore, in such a case, we cannot say if BetwEffiVul can make a positive contribution and can be seen as the basic measure or not.

When comparing Figure 4.38 with Figure 4.13 with apparently larger frequencies, the attacks based on AggregTOPSIS without containing Effi and BetwEffiVul can lead to higher resilience compared to AggregTOPSIS without containing BetwEffiVul, which validates that Effi can positively affect AggregTOPSIS and can be the basic measure.

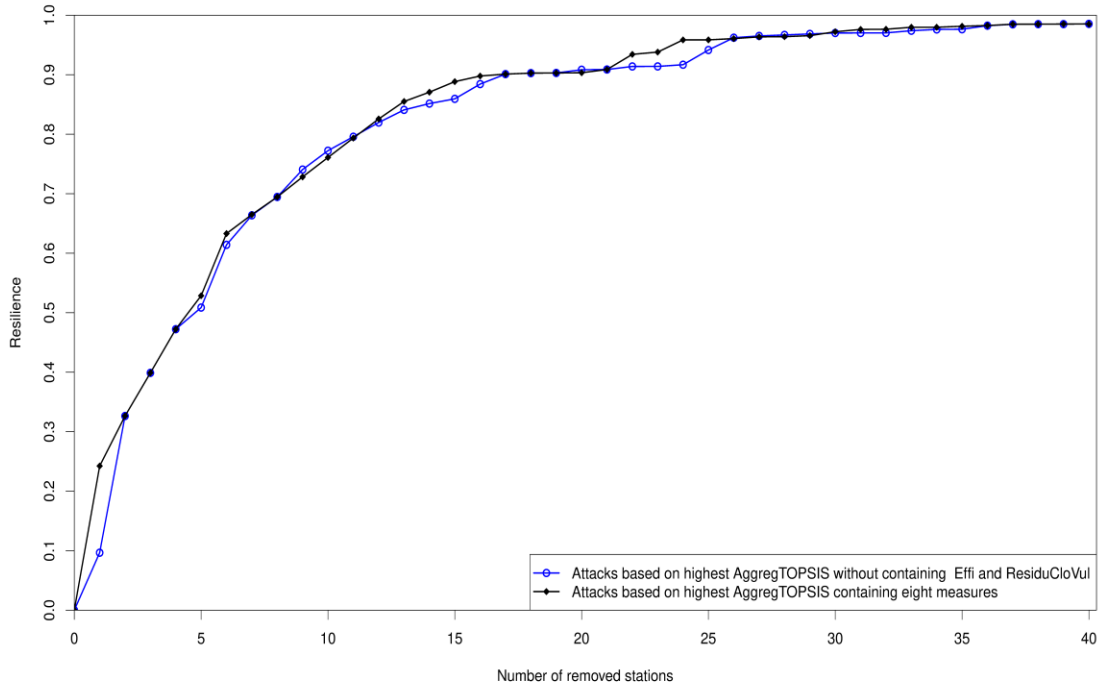



Figure 4.39: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing Effi and ResiduCloVul

From Figure 4.39 and Figure 4.11, we can see that with slightly larger frequencies, the attacks (especially when the top five and top six stations are attacked) based on AggregTOPSIS without containing Effi and ResiduCloVul can result in higher resilience compared to AggregTOPSIS without containing Effi; but with some frequencies, the resilience caused by the attacks (based on AggregTOPSIS without containing Effi and ResiduCloVul) is lower; therefore, in such a case, we can say that ResiduCloVul can make a slightly positive contribution. However, it cannot demonstrate that ResiduCloVul can be seen as the basic measure.

When comparing Figure 4.39 with Figure 4.14 with apparently larger frequencies, the attacks based on AggregTOPSIS without containing Effi and ResiduCloVul can lead to higher resilience compared to AggregTOPSIS without containing ResiduCloVul, which thus validates that Effi can positively affect AggregTOPSIS and can be the basic measure.

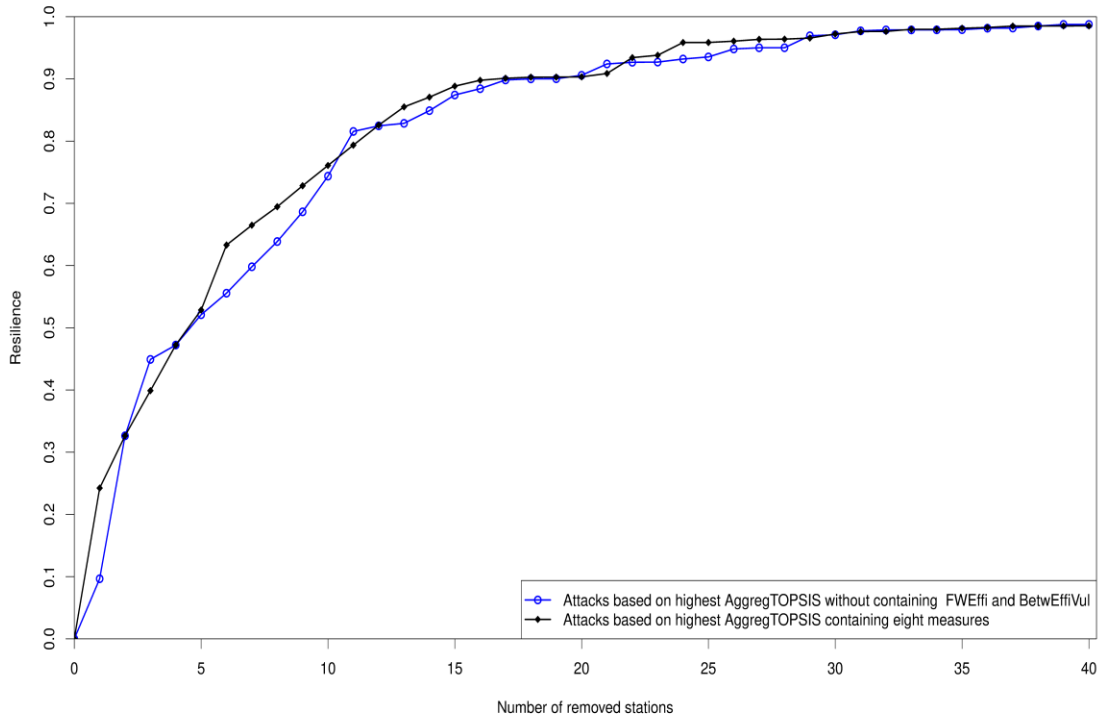



Figure 4.40: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing FWEffi and BetwEffiVul

From Figure 4.40 and Figure 4.12 we can see that with sightly larger frequencies, the attacks (especially when top three stations are attacked) based on AggregTOPSIS without containing FWEffi and BetwEffiVul can result in lower resilience compared to AggregTOPSIS without containing FWEffi; but with some frequencies, the resilience caused by the attacks (based on AggregTOPSIS without containing FWEffi and BetwEffiVul) is lower; therefore, in this case, we can say that ResiduCloVul can make a slightly negative contribution; thus it cannot be seen as the basic measure.

When comparing Figure 4.40 with Figure 4.13 with apparently larger frequencies, the attacks based on AggregTOPSIS without containing FWEffi and BetwEffiVul can lead to higher resilience compared to AggregTOPSIS without containing BetwEffiVul, which thus validates that FWEffi can positively affect AggregTOPSIS and can be the basic measure.

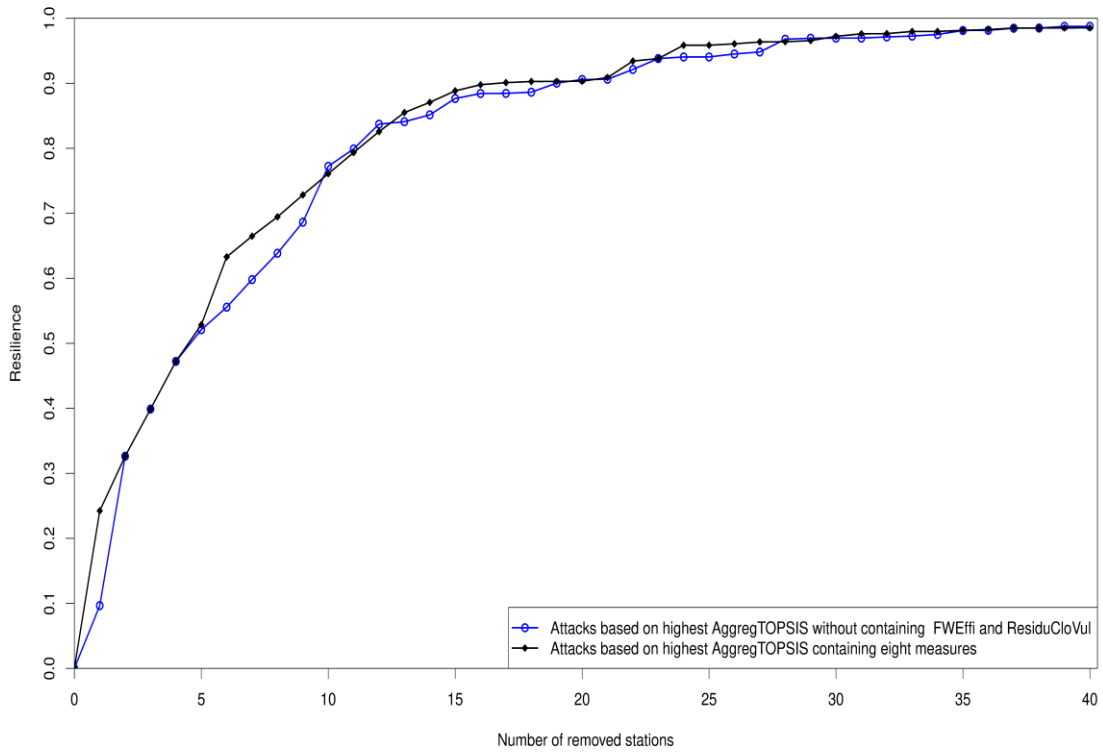



Figure 4.41: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing FWEffi and ResiduCloVul

According to Figure 4.41 and Figure 4.12, we can see that with slightly larger frequencies, the attacks (especially when top three stations are attacked) based on AggregTOPSIS without containing FWEffi and ResiduCloVul can result in higher resilience compared to AggregTOPSIS without containing FWEffi; therefore, in such a case, we can say that ResiduCloVul can positively affect AggregTOPSIS; thus, here it might be seen as the basic measure.

When comparing Figure 4.41 with Figure 4.14, the attacks based on AggregTOPSIS without containing FWEffi and ResiduCloVul can, with apparently larger frequencies, lead to higher resilience compared to AggregTOPSIS without containing ResiduCloVul, which thus demonstrates that FWEffi can make positive contributions to AggregTOPSIS and can be the basic measure.

### 4.3.1 Detailed Explanation

From Figure 4.15 to Figure 4.41 and comparing with Figure 4.7 ~ Figure 4.14, it can be found that to a certain extent the resilience caused by the attacks according to the TOPSIS-based aggregation measures without considering two certain measures is the overlap of resilience caused by the attacks according to two TOPSIS-based aggregation measures without considering the certain single measure.

According to Figure 4.29, Figure 4.30, and Figure 4.37, we can see the resilience (that is caused by the attacks according to the TOPSIS-based aggregation measures without considering degree centrality measure and nodal efficiency measure, or without considering degree centrality measure and nodal flow-weighed efficiency measure, or without considering nodal efficiency measure and nodal flow-weighed efficiency measure) increases even more compared to the original TOPSIS-based aggregation measure containing all eight measures and also compared to the TOPSIS-based aggregation measure without considering single degree centrality measure, nodal efficiency measure or nodal flow-weighted efficiency measure shown in Figure 4.9, Figure 4.11 and Figure 4.12.

In Figure 4.23, compared to the original TOPSIS-based aggregation measure containing all eight measures, the resilience caused by the attacks according to the TOPSIS-based aggregation measures without considering closeness centrality measure and eigenvector centrality measure still changes very slightly, like in the situations shown in Figure 4.8 and Figure 4.10, which are the TOPSIS-based aggregation measures without individually considering single closeness centrality measure or eigenvector centrality measure.

In Figure 4.20, the resilience caused by the attacks according to the TOPSIS-based aggregation measures (without considering betweenness centrality measure and nodal betweenness-efficiency vulnerability measure) not only decreases when deleting the top three or five nodes from the network like in Figure 4.13, but it also becomes lower when removing the range of around twenty nodes like in Figure 4.7.

According to Figure 4.21, it can be found that the resilience caused by the attacks according to the TOPSIS-based aggregation measures (without considering betweenness centrality measure and nodal residual closeness vulnerability measure) even decreases when deleting the top four or five nodes.

However, in Figure 4.14, there is only one situation where the top five nodes are deleted and the situation when removing the range of around top twenty nodes is similar to the situation in Figure 4.7.

So far, it has been verified that betweenness centrality measure, nodal betweenness-efficiency vulnerability measure and nodal residual closeness measure are not the basic and necessary measures to the TOPSIS-based aggregation measure. Meanwhile, it has also been demonstrated that the degree centrality measure, nodal efficiency measure and the flow-weighted efficiency measure are the basic measures to the TOPSIS-based aggregation measure.

When comparing EigenCentr with BetwCentr in Figure 4.17, CloCentr in Figure 4.23, Degcentr in Figure 4.28 and Effi in Figure 4.33, the results show that the eigenvector centrality measure can be seen as the basic measure; when comparing EigenCentr with FWEffi in Figure 4.34 and ResiduCloVul in Figure 4.36, the results only show that EigenCentr can affect the TOPSIS-based aggregation measure to a certain extent and cannot make sure whether it can be regarded as the basic measure; furthermore, only when comparing EigenCentr with BetwEffiVul in Figure 4.35, the results show that EigenCentr cannot be seen as the basic measure.

Therefore, based on these cases, we can conclude that the eigenvector centrality can also be a basic measure. However, so far, we still cannot be sure if the closeness centrality measure is the basic measure to the TOPSIS-based aggregation measure or not.

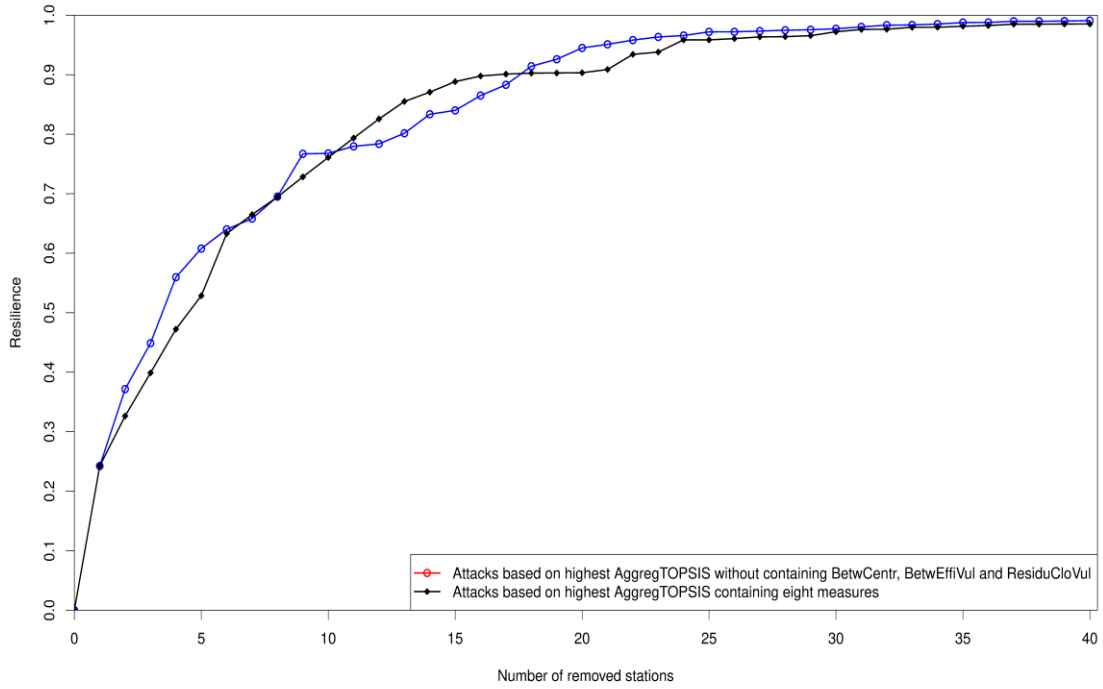



Figure 4.42: Comparison between AggregTOPSIS containing all eight measures and AggregTOPSIS without containing BetwCentr, BetwEffiVul and ResiduCloVul

When aggregating measures without considering the non-basic and unnecessary measures, as shown in Figure 4.42, we can find that the resilience caused by the attacks according to the TOPSIS-based aggregation measures (without considering betweenness centrality measure, nodal betweenness-efficiency vulnerability measure and the nodal residual closeness vulnerability measure) increases only a bit when deleting the top nodes from eleven to seventeen.

But it becomes lower when deleting the top ten nodes and top nodes from over eighteen; namely, comparing with AggregTOPSIS containing all eight measures, the attacks based on AggregTOPSIS without containing BetwCentr, BetwEffiVul and ResiduCloVul can result in larger destruction of network structure; this also means that the ranking order according to AggregTOPSIS without containing BetwCentr, BetwEffiVul and ResiduCloVul is a lot more reasonable, because it still leads to larger destruction of network structure even when removing a small number of nodes from the network.

Then decision-makers can decide, allot and deploy in advance the necessary resources to protect those key stations based on their importance according to this ranking order; and this is also our goal because the aim of our research is to focus on how to optimize the TOPSIS-based aggregation measure to result in a meaningful ranking order, which can help decision-makers to make timely, suitable and reasonable decisions in advance.

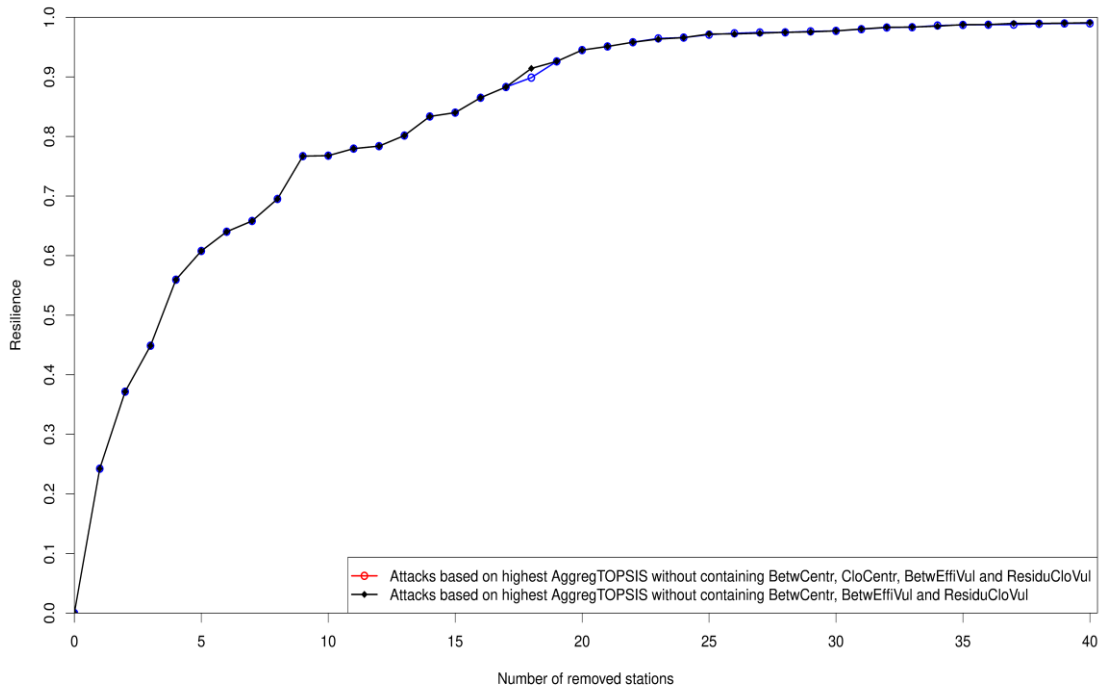



Figure 4.43: Comparison between AggregTOPSIS without containing BetwCentr, BetwEffiVul and ResiduCloVul and AggregTOPSIS without containing BetwCentr, CloCentr, BetwEffiVul and ResiduCloVul

In order to verify whether the closeness centrality measure is the basic measure to the TOPSIS-based aggregation measure or not, compared to the TOPSIS-based aggregation measure without considering betweenness centrality measure, nodal betweenness-efficiency vulnerability measure and the nodal residual closeness vulnerability measure, here we take one situation into account, meaning we do not aggregate the closeness centrality measure either.

The results are shown in Figure 4.43, according to which we can see that the closeness centrality measure just makes a very slight contribution to the TOPSIS-based aggregation measure without considering betweenness centrality measure, nodal betweenness-efficiency vulnerability measure and nodal residual closeness vulnerability measure.

Therefore, in such a case, we could conclude that the closeness centrality measure is not the basic and necessary measure for the TOPSIS-based aggregation measure.

When we compare the TOPSIS-based aggregation measure containing the basic measures DegCentr, EigenCentr, Effi and FWEffi to other individual measures, the results are shown in Figure 4.44, where we can find that the attacks based on the highest AggregTOPSIS containing the basic measures almost always lead to lower resilience, specifically to lower resilience when removing the top ten nodes, only leading to a slightly larger resilience in four situations, i.e. when deleting the top eleven, twelve, thirteen and seventeen nodes.

In summary, we can conclude that the new TOPSIS-based aggregation measure containing the basic measures DegCentr, EigenCentr, Effi, and FWEffi is a more suitable and effective one to identify the critical nodes of the transportation network.

Furthermore, the top ten nodes based on the new TOPSIS-based aggregation measure containing the four basic measures are nodes 103, 91, 1, 2, 41, 92, 4, 18, 26 and 107, which correspond to the stations Berlin Hbf, Hamburg Hbf, Frankfurt (Main) Hbf, Frankfurt (M) Flughafen Fernbf, Köln Hbf, Hamburg Dammtor, Mannheim Hbf, München Hbf, Fulda and Berlin Gesundbrunnen, based on which we can see that all of these top ten nodes are critical cities, so that it will lead to more substantial impacts once they are attacked by terrorists.

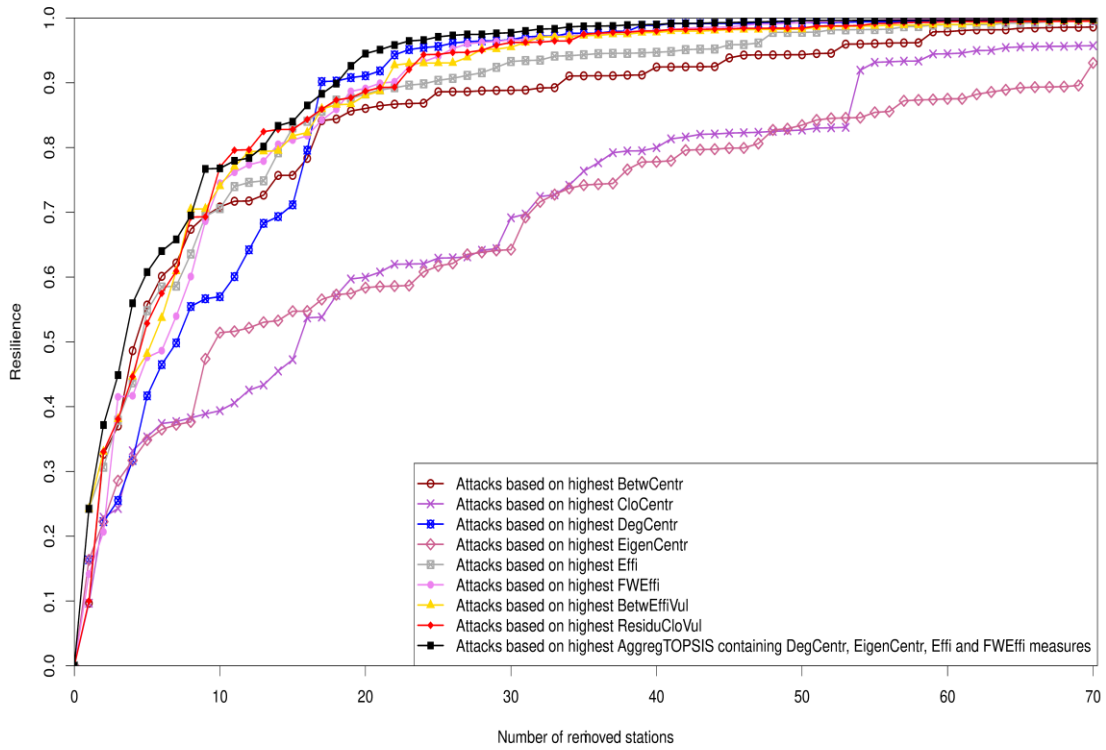



Figure 4.44: Comparisons of different measures

From Figure 4.44, we can find that the attacks based on each single measure (which only considers one or two factors and information) cannot always lead to lower resilience of the remaining network; especially the attacks based on highest CloCentr and the attacks based on highest EigenCentr always lead to higher resilience compared to other measures. However, when aggregating different measures, more information can be combined into the new aggregation measure, which can not only make full use of the advantages of every measure, but it can also compensate their disadvantages; as the results in Figure 4.44 show, there are only four cases where the attacks based on the new aggregation measure can result in higher resilience, but in the remaining situations, it can always lead to lower resilience, especially in the cases when a small number of top stations are attacked, which is practical and reasonable for terrorists, because it can still cause larger negative social influence, casualties and economic loss when they attack just a few critical stations.

## 4.4 Summary

In this chapter, when carrying out network resilience analysis, based on the resilience assessment approach presented by Nan and Sansavini (2017), we make some adaptations and propose a new quantitative resilience measure, which is based on a new proposed network performance metric.

Moreover, we make use of the new quantitative resilience measure in order to compare different graph measures and distinguish which one is more suitable and efficient to identify the principal stations in the network, thus further assist decision-makers to make appropriate and reasonable judgments.

Then they can take measures by deploying some specific security devices or allotting police in advance to protect these key spots which have more potential to be attacked by terrorists. Even though these kinds of attacks are almost inevitable, this will also decrease the economic loss and casualties to a large extent.

Furthermore, in this chapter, through resilience analysis, we find that among these eight graph measures, which are betweenness centrality measure (BetwCentr), closeness centrality measure (CloCentr), degree centrality measure (DegCentr), eigenvector centrality measure (EigenCentr), nodal efficiency measure (Effi), nodal flow-weighted efficiency measure (FWEffi), nodal betweenness-efficiency vulnerability measure (BetwEffiVul) and nodal residual closeness vulnerability measure (ResiduCloVul), not all of them make positive contributions to the TOPSIS-based aggregation measure.

Although BetwCentr, BetwEffiVul and ResiduCloVul are to a certain extent suitable and effective measures to identify the key nodes compared with CloCentr, DegCentr, EigenCentr, Effi, FWEffi and even sometimes compared with the TOPSIS-based aggregation measure containing these eight measures; however, the new TOPSIS-based aggregation measure without considering BetwCentr, BetwEffiVul and ResiduCloVul is a much more suitable and effective one to detect the key stations in transportation networks.

Finally, we find that the basic and necessary measures are only four, namely:

- Degree centrality measure (DegCentr): This measure can indicate if one given node in a network is a critical one based on the number of its directly connected neighbors (Freeman 1978, Boudin 2013). In this thesis, we identify the critical stations based on this measure by finding out how many train lines one given station has that can straightly reach the closest neighboring stations.

- Eigenvector centrality measure (EigenCentr): According to this measure, one given node of a network can be seen as critical if it has a higher number of critical neighbors (Maharani and Gozali 2014, Ruhnau 2000, Boudin 2013).

- Nodal efficiency measure (Effi): Based on this measure, if one given node in the network can efficiently and quickly reach the rest of the network, it can be regarded as the critical one (Latora and Marchiori 2003).

- Nodal flow-weighted efficiency measure (FWEffi): Based on the classical efficiency measure (Latora and Marchiori 2003), the flow-weighted efficiency measure is proposed by Nistor and Pickl et al. (2017) and specifically applied in transportation networks. It combines the new train flow information between the stations in a transportation network.

In this chapter, we present a new quantitative resilience measure, based on which we compare different measures, concluding that the new TOPSIS-based aggregation measure is suitable and effective to identify the critical stations in transportation networks.

Moreover, we also find that among the measures implemented in this thesis, not all of them are necessary and basic measures for the TOPSIS-based aggregation measure; meanwhile, we can conclude that there are only four key measures that are basic and necessary for the TOPSIS-based aggregation measure as aforementioned in this chapter.

However, the results in Figure 4.44 show that the attacks based on the new TOPSIS-based aggregation measure only containing the basic measures not always lead to lower resilience compared to other measures.

Therefore, in the next chapter, where we focus on outlook and perspectives, we examine a possible approach to compensate this disadvantage.

The implementation of the new resilience measure and application to RE(H)STRAIN-related aspects from section 4.2 is based on the following publication:

*Wang, Z., Nistor, M. S., & Pickl, S. W. (2020). Introducing a TOPSIS based quantitative resilience measure for railway systems. The international conference on railway technology. (submitted)*

# 5 Outlook and Perspectives

This dissertation contributes to the topic of *structure-based network analysis*, *network vulnerability analysis* and the *network resilience analysis* for decision support applied on public transport networks, specifically the German high-speed train network (ICE), under terrorist attacks.

To identify the critical spots in a network, we conduct the network structure analysis. Here, we mainly implement the existing graph measures including betweenness centrality measure (Freeman 1978, Newman 2008, Boudin 2013), closeness centrality measure (Freeman 1978, Boudin 2013, Tsiotas and Polyzos 2015), degree centrality measure (Freeman 1978, Boudin 2013), eigenvector centrality measure (Maharani and Gozali 2014, Ruhnau 2000, Boudin 2013), nodal efficiency measure (Nistor and Pickl et al. 2017, Latora and Marchiori 2003) and nodal flow-weighted efficiency measure (Nistor and Pickl et al. 2017) in the ICE network.

Inspired by the idea of global residual closeness vulnerability measure (Dangalchev 2006), based on betweenness centrality and nodal efficiency measures, we propose two new nodal vulnerability measures, which are nodal betweenness-efficiency vulnerability measure (Wang et al. 2018) and nodal residual closeness vulnerability measure. We apply these two new nodal vulnerability measures to the German high-speed train network, and the results in Chapter 3 show that the proposed new nodal vulnerability measures are promising to a certain extent.

However, because implementations of multiple measures will lead to different results (which can naturally cause the information overflow problem for decision-makers, who cannot be sure which measure is the most effective one to detect the suitable and meaningful vital nodes), for the sake of resolving the information overflow problem we therefore introduce and adapt the aggregation technique TOPSIS (Lai et al. 1994) from Multi-criteria Decision Making fields.

Furthermore, we develop a TOPSIS-based aggregation measure by proposing a new weighting estimation method in our research instead of the experts' experiences.

The TOPSIS-based aggregation measure can not only reduce the information overflow for decision-makers, but it can also combine a multitude of aspects considered by other different measures which only provide their unique perspectives. Thus, comparing to other measures which only consider their limited unique perspectives, this TOPSIS-based aggregation measure (that theoretically can take into account as many factors as possible) is a much more comprehensive approach to detect the critical nodes of a network.

And the results in Chapter 4 also show that the new TOPSIS-based aggregation measure for identifying the key nodes is promising and meaningful to a certain extent, compared to the other eight measures.

However, because in graph theory, so far there hasn´t been any unified criterion to compare different measures to tell which measure is the more suitable and useful one to detect the key nodes, therefore another issue has come up, namely that we still can't confirm whether the TOPSIS-based aggregation measure can identify the key nodes much more efficiently compared with the aforementioned other eight measures.

So, to further validate the effectiveness of the proposed TOPSIS-based aggregation measure, by taking into account the traveling time, train flow and also the number of people who can use the system as usual, even under some disruptive events like terrorist attacks, we develop a new network performance metric, which is used to carry out the quantitative network resilience analysis to compare different measures with each other.

In our research, when roughly estimating the number of people who can normally use the public transport network, we also take into account the network structure character, namely network degree centrality, according to which we propose the idea of an adjacency node-set level. And based on the adjacency node-set level, we also create a new calculating model to roughly estimate the number of people instead of the real statistic data.

The results show that on a large scale, we can say the TOPSIS-based aggregation measure is a promising and much more effective measure to identify the key nodes for the public transport network.

Furthermore, based on resilience analysis, degree centrality measure, eigenvector centrality measure, nodal efficiency measure, and nodal flow-weighted efficiency measure, they are distinguished as the basic and necessary measures (which can make positive contributions to the TOPSIS-based aggregation measure). In contrast, betweenness centrality measure, closeness centrality measure, nodal betweenness-efficiency vulnerability measure and nodal residual closeness vulnerability measure make negative contributions to the TOPSIS-based aggregation measure.

As Figure 4.46 shows, it is found that the attacks based on the new TOPSIS-based aggregation measure, which only aggregates the aforementioned basic measures, can in large frequencies lead to lower resilience in the remaining network; significantly, the resilience of the remaining network is always lower than those remaining networks caused by the other eight measures when removing the top ten nodes.

According to results of resilience analysis, we can conclude that the TOPSIS-based aggregation measure only aggregating the four identified basic measures is a much more useful measure to identify the critical nodes for the public transport network.

As Figure 4.46 shows, when removing the top eleven to thirteen nodes, the new TOPSIS-based aggregation measure only aggregating basic measures (including degree centrality measure, eigenvector centrality measure, nodal efficiency measure and nodal flow-weighted efficiency measure) leads to higher resilience than nodal residual closeness vulnerability measure, and it leads to higher resilience than the nodal betweenness-efficiency vulnerability measure when deleting the top seventeen nodes. Therefore, as a scientific outlook, the focus of future research is how to make the new TOPSIS-based aggregation measure always lead to lower resilience of the remaining network. Specifically, we mainly try to carry out research from two aspects:

First, we will further investigate more extant measures with different information and check whether they can be regarded as the basic measures or not.

If these new measures, for instance mobility centrality (Tsiotas and Polyzos, 2015), PageRank (Brin and Page, 1998) or Clustering coefficient (Wang et al., 2011) can be used as the basic measures. We aggregate them with current existing basic measures to make the new TOPSIS-based aggregation measure always lead to lower resilience when deleting any top number of nodes.

Second, we will aggregate different measures into a new one from a linear algebra point of view and compare it with the TOPSIS-based aggregation method to check which one is more effective to identify the key station in the public transportation network.

The general framework of the vector-based method for the future is introduced as follows:

## 5.1 A Possible Vector-based Approach

Linear algebra is used to study "the linear sets of equations and their transformation properties" (Mirsky 2012, Strang 1993, Weisstein 2020). Many research problems like "rotations in space, least-squares fitting, solution of coupled differential equations, determination of a circle passing through three given points", as well as "many other problems in mathematics, physics, and engineering" can be analyzed using linear algebra (Mirsky 2012, Strang 1993, Weisstein, 2020).

In particular, a linear algebra $\boldsymbol{L}$ over a field $\boldsymbol{F}$ has "the structure of a ring with all the usual axioms for an inner addition and an inner multiplication together with distributive laws, therefore giving it more structure than a ring" (Mirsky 2012, Strang 1993, Weisstein 2020). A linear algebra also admits "an outer operation of multiplication by scalars (that are elements of the underlying field $\boldsymbol{F}$)" (Weisstein 2020). For example, "the set of all linear transformations from a vector space $\boldsymbol{V}$ to itself over a field $\boldsymbol{F}$ forms a linear algebra over $\boldsymbol{F}$"; and "the set of all real square matrices over the field $\boldsymbol{R}$ of the real numbers" (Mirsky 2012, Strang 1993, Weisstein 2020).

In the field of linear algebra, the very useful tools are the matrix and determinant. One pivotal problem of linear algebra is to solve the matrix equation：

$$\boldsymbol{Ax} = \boldsymbol{b} \tag{5-1},$$

where $\boldsymbol{x}$ can be theoretically solved using a matrix inverse:

$$\boldsymbol{x} = \boldsymbol{A}^{-1}\boldsymbol{b} \tag{5-2}$$

In our research, we will aggregate different graph measures into a new one using linear algebra; here, $\boldsymbol{b}$ is the new aggregation measure; $\boldsymbol{x}$ denotes the weight vector of graph measures; the matrix $\boldsymbol{A}$ is formed by values derived from different graph measures ( $M_i$ , $i = 1,2,3,...,m$ , $m$ is the number of graph measures), where each column consists of the values computed by each graph measure, and the row number is $n$ (that is the number of nodes of the network). Since normally one complex network has a large number of nodes, the number of applied graph measures is still limited; therefore, basically, $m < n$ , for instance, in this thesis, $m = 8 < n = 121$ . So, in our future research what we focus on is how to find the suitable weight vector $\boldsymbol{x}$ in the weight vector space, so that the linear algebra-based aggregation measure $\boldsymbol{b}$ can lead to lower resilience of the remaining network to the utmost extent.

## 5.2 A New Algebraic Aggregation Measure

The new linear algebra-based aggregation measure can be expressed as:

$$\boldsymbol{b} = \boldsymbol{M_1}x_1 + \boldsymbol{M_2}x_2 + ,...,+\boldsymbol{M_m}x_m \tag{5-3}$$

Specifically, each element of the new linear algebra-based aggregation measure can be calculated by:

$$b_j = M_{j1}x_1 + M_{j2}x_2 + ... + M_{jm}x_m \tag{5-4}$$

It can be denoted using this matrix:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1m} \\ M_{21} & M_{22} & \cdots & M_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ M_{n1} & M_{n2} & \cdots & M_{nm} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} \tag{5-5}$$

where,

$$\boldsymbol{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}, \quad \boldsymbol{A} = \begin{bmatrix} \boldsymbol{M_1} & \boldsymbol{M}_2 & \cdots & \boldsymbol{M}_m \end{bmatrix} = \begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1m} \\ M_{21} & M_{22} & \cdots & M_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ M_{n1} & M_{n2} & \cdots & M_{nm} \end{bmatrix}, \quad \boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}$$

Here, $M_{mn}$ denotes the $n^{th}$ element of the values computed by $m^{th}$ graph measure. Based on (5-5), we can derive different linear algebra-based aggregation measures according to the different weight vector $\boldsymbol{x}$. Since in the vector space, the number of the vector is unlimited, thus, in theory, the number of new linear algebra-based aggregation measures is also unlimited. What we will research is to find the suitable weight vector $\boldsymbol{x}$ using certain algorithms in the vector space so that the derived linear algebra-based aggregation measure can lead to lower resilience of the remaining network to the utmost extent when conducting network resilience analysis.

For future research, we will compare the linear algebra-based aggregation measure with the TOPSIS-based aggregation measure through resilience analysis (introduced in Chapter 4), then conclude which kind of aggregation measure is more reasonable and effective to identify the critical stations in transportation network. In Formula (5-5), the matrix $\boldsymbol{A}$ is known, thus, once a group of weights $\boldsymbol{x}$ is determined, a new linear algebra-based aggregation measure is generated; afterward, the next step is comparing the resilience caused by the attacks based on these two kinds of aggregation measures. Therefore, the problem that we need to solve now is how to obtain a suitable weight vector $\boldsymbol{x}$. In order to achieve this goal to select a suitable weight vector, the Genetic Algorithms (Carr 2014, Mallawaarachchi 2017, Mitchell 1998) might be possible.

Inspired by "Charles Darwin's theory of natural evolution, one genetic algorithm is a search heuristic and a kind of optimization algorithm" (Mallawaarachchi 2017). Due to the fact that the genetic algorithms are designed to simulate a biological process, a lot of relevant terminology is thus borrowed from biology (Carr 2014). Actually, the procedure of natural selection is reflected by the genetic algorithm, "where the fittest individuals are selected to produce the offspring of the next generation" (Carr 2014, Mallawaarachchi 2017). The process of "natural selection starts with the selection of the fittest individuals from a population" (Mallawaarachchi 2017).

These fittest individuals produce "offspring, which inherit the characteristics from parents and that will be added to the next generation" (Mallawaarachchi 2017). If the parents are fit, so will be their children, maybe even more so than their parents; therefore, the offspring has a better chance to survive (Carr 2014, Mallawaarachchi 2017).

This process "keeps on repeating and a generation with the fittest individuals will be found at the end". In a genetic algorithm, there are five steps to follow (Carr 2014, Mallawaarachchi 2017, Mitchell 1998):

- Initial population of chromosomes: In this phase, we will randomly generate a set of individuals (i.e., weight vector $\boldsymbol{x}$ in our research).
- A fitness function for optimization: The fitness function is one of the most significant parts of a genetic algorithm; it will give each individual a fitness score, which determines how fit an individual is and whether the individual has a chance to be selected for reproduction (Carr 2014, Mallawaarachchi 2019). In our future research, we will take the new resilience measure as the fitness function.
- Selection of which chromosomes will reproduce. In this step, the fittest individuals will be selected and their genes will be passed on to the next generation.
- Crossover to produce the next generation of chromosomes: The phase of crossover is the most pivotal step of a genetic algorithm, during which a crossover point will be randomly chosen from within the genes of each pair of mated parents (Carr 2014, Mallawaarachchi 2019).

- Random mutation of chromosomes in the new generation: In a certain generated new offspring, a mutation with a low random probability might happen on some of their genes. The aim of mutation is to maintain diversity of the population and to prevent premature convergence (Carr 2014, Mallawaarachchi 2019).

When the selection, crossover and mutation are completed, the new population will be tested, based on the fitness function. And the genetic algorithm will be terminated once the population has converged; that is, the offspring, which is significantly different from the previous generation, won't be produced (Mallawaarachchi 2019).

According to the genetic algorithm, a set of suitable weight vectors $\boldsymbol{x}$ might be provided for the linear algebra-based aggregation measure. However, in this thesis, we won't further introduce the details.

# 6 Conclusions

In this thesis, we first introduce the fundamental issues concerning the research question on how to identify the critical stations in a transportation network considering terrorist attacks.

Before presenting the measures we will implement in the German ICE network, we first introduce some basic terms that are used in this thesis, for example, what is *graph* and *graph theory*, what is *network* and *network theory*. Moreover, in the beginning of this thesis, we review many contributions regarding centrality measures (including degree centrality, closeness centrality measure, betweenness centrality and eigenvector centrality), and their applications on the transportation networks. Furthermore, we also review the global efficiency measure, nodal efficiency measure, vulnerablility measures and the network quantitative resilience analysis.

In order to identify the critical stations in transportation networks (specifically, the German High-speed Train Network (ICE) in this thesis), we implement the existing graph theory measures like centrality measures (including degree centrality, closeness centrality measure, betweenness centrality and eigenvector centrality) and efficiency measures (including global efficiency measure and node efficiency measure) on the ICE network. Based on the graph global residual closeness, we propose a new nodal vulnerability measure, namely the nodal residual closeness vulnerability measure. Furthermore, based on the betweenness centrality measure and global efficiency measure, as well as the idea of nodal residual closeness vulnerability measure, we also propose another new nodal vulnerability measure, i.e. the betweenness-efficiency vulnerability measure. We also apply these two proposed new nodal vulnerability measures on the German ICE network and compare them with other aforementioned measures; the results show that the proposed new nodal vulnerability measures are suitable and effective.

However, different implemented graph measures will lead to different ranking orders of the critical stations identified by these measures; this will result in the information overflow for decision-makers, who cannot distinguish which ranking order of critical stations is reasonable, effective and suitable, then take some preventive measures to protect them based on the ranking order of these important stations.

Therefore, in order to reduce the information overflow for decision-makers, we introduce the aggregation method called Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) from the Multi-criteria Decision Making field, based on which we present the TOPSIS-based aggregation approach; here, we not only adapt this aggregation technique to our research, but more importantly, we also improve it by adding a new weighting approach (based on the global vulnerability analysis) to this thesis; the new weighting method is used instead of the traditional weight estimation methods like Analytic Hierarchy Process (AHP), Simple Multi-Attribute Rating Technique (SMART), Measuring Attractiveness by a Categorical-Based Evaluation Technique (MACBETH) , the Step-wise Weight Assessment Ratio Analysis (SWARA) method, and so forth.

In order to compare different methods and conclude which measure is more suitable and efficient to identify the critical stations in transportation network and validate the effectiveness of the proposed new TOPSIS-based aggregation measure, we develop a new quantitative resilience measure and conduct network resilience analysis in this thesis.

The new quantitative resilience measure combines traveling time, train flow and also the number of people who can use the system as usual, even under some disruptions. Here, when roughly estimating the number of people, we also consider the network characteristics like the degree of one given station.

In order to apply the idea of network degree properly, we also propose the concept of an adjacency node-set level, whose definition is introduced in detail in Chapter 4.

According to the results, we conclude that there are only four basic and necessary measures (which are degree centrality measure (DegCentr), eigenvector centrality measure (EigenCentr), nodal efficiency measure (Effi) and nodal flow-weighted efficiency measure (FWEffi)) for the TOPSIS-based aggregation measure through resilience analysis based on the new quantitative resilience measure; meanwhile, we also find that the TOPSIS-based aggregation measure only containing the four basic measures can effectively identify the critical stations.

In this thesis, we also present the outlook and perspectives for future research works. In the future, based on linear algebra, we will investigate a new algebraic aggregation measure and compare it with the aforementioned TOPSIS-based aggregation measure.

# - REFERENCES -

# References

Adams, T. M., Bekkem, K. R., & Toledo-Durán, E. J. (2012). Freight resilience measures. Journal of Transportation Engineering, 138(11), 1403-1409.

Adger, W. N. (2006). Vulnerability. Global environmental change, 16(3), 268-281.

Aggarwal CC. (2011). Social network data analytics. Springer, Boston, MA.

Alanko, S., Crevals, S., Isopoussu, A., Östergård, P., & Pettersson, V. (2011). Computing the domination number of grid graphs. The Electronic Journal of Combinatorics, 18(1), P141.

Albert, R., Albert, I., & Nakarado, G. L. (2004). Structural vulnerability of the North American power grid. Physical Review E, 69(2), 25103.

Altintas, G., & Royer, I. (2009). Renforcement de la résilience par un apprentissage post-crise: une étude longitudinale sur deux périodes de turbulence. M@ N@ Gement, 12(4), 266–293.

Amoaning-Yankson, S. (2013). A resiliency framework for planning in state transportation agencies (Doctoral dissertation, Georgia Institute of Technology).

Amokrane, N., Daclin, N., & Chapurlat, V. (2017, May). Deducing Complex Scenarios for Resilience Analysis: Application to the Franco-German High Speed Train Network. In ISCRAM.

Aslan, E., & Kirlangic, A. (2011). Computing The Scattering Number and The Toughness for Gear Graphs. Bulletin of International Mathematical Virtual Institute, 1(2011), 1-1.

Ayyub, B. M. (2014). Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making. Risk Analysis, 34(2), 340–355.

Bana e Costa, C. A., de Corte, J.-M., & Vansnick, J.-C. (2010). MACBETH (measuring attractiveness by a categorical based evaluation technique). Wiley Encyclopedia of Operations Research and Management Science.

Barefoot, C. A., Entringer, R., & Swart, H. (1987). Vulnerability in graphs: a comparative survey. J. Combin. Math. Combin. Comput, 1(38), 13–22.

Barron, F. H., & Barrett, B. E. (1996). The efficacy of SMARTER: Simple multi-attribute rating technique extended to ranking. Acta Psychologica, 93(1–3), 23–36.

Bauer, D., Broersma, H. J., van den Heuvel, J., Kahl, N., & Schmeichel, E. (2013). Toughness and vertex degrees. Journal of Graph Theory, 72(2), 209–219.

Bavelas, A. (1948). A mathematical model for group structures. Applied Anthropology, 7(3), 16–30.

Behzadian, M., Otaghsara, S. K., Yazdani, M., & Ignatius, J. (2012). A state-of the-art survey of TOPSIS applications. Expert Systems with Applications, 39(17), 13051–13069.

Biggs, N., Lloyd, E. K., & Wilson, R. J. (1986). Graph Theory, 1736-1936. Oxford University Press.

Boccaletti, S., Buldú, J., Criado, R., Flores, J., Latora, V., Pello, J., & Romance, M. (2007). Multiscale vulnerability of complex networks. Chaos: An Interdisciplinary Journal of Nonlinear Science, 17(4), 43110.

Boesch, F. T., Satyanarayana, A., & Suffel, C. L. (2009). A survey of some network reliability analysis and synthesis results. Networks: An International Journal, 54(2), 99–107.

Bollobás, B. (1998). Random graphs. In Modern Graph Theory (pp. 215–252). Springer.

Borcherding, K., Eppel, T., & Von Winterfeldt, D. (1991). Comparison of weighting judgments in multiattribute utility measurement. Management science, 37(12), 1603-1619.

Boudin, F. (2013). A comparison of centrality measures for graph-based keyphrase extraction. International Joint Conference on Natural Language Processing (IJCNLP), 834–838.

Brin, S., & Page, L. (1998). The anatomy of a large-scale hypertextual web search engine.

British Standards, B. S. (2014). BS 65000:2014 [electronic resource]: Guidance on organizational resilience. London: British Standards Institution.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., & Von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake spectra, 19(4), 733-752.

Buldyrev, S. V, Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. Nature, 464(7291), 1025–1028.

Bush, G. W. (2002). National strategy for homeland security. Washington, DC: The White House, 16.

Carr, J. (2014). An introduction to genetic algorithms. Senior Project, 1(40), 7.

Chen, D., Lü, L., Shang, M.-S., Zhang, Y.-C., & Zhou, T. (2012). Identifying influential nodes in complex networks. Physica a: Statistical Mechanics and Its Applications, 391(4), 1777–1787.

Chen, H., & Hu, Y. (2013). Finding Community Structure and Evaluating Hub Road Section in Urban Traffic Network. Procedia-Social and Behavioral Sciences, 96, 1494–1501.

Chen, S.-J., & Hwang, C.-L. (1992). Fuzzy multiple attribute decision making methods. In Fuzzy multiple attribute decision making (pp. 289–486). Springer.

Cheng, T. C. E., Li, Y.-K., Xu, C.-D., & Zhang, S.-G. (2014). Extreme tenacity of graphs with given order and size. Journal of the Operations Research Society of China, 2(3), 307–315.

Cheng, Y.-Y., Lee, R. K.-W., Lim, E.-P., & Zhu, F. (2013). DelayFlow centrality for identifying critical nodes in transportation networks. Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 1462–1463.

Cutter, S. L., Ahearn, J. A., Amadei, B., Crawford, P., Eide, E. A., Galloway, G. E., & others. (2013). Disaster resilience: A national imperative. Environment: Science and Policy for Sustainable Development, 55(2), 25–29.

Dangalchev, C. (2006). Residual closeness in networks. Physica A: Statistical Mechanics and Its Applications, 365(2), 556–564.

Dehmer, M., & Emmert-Streib, F. (2014). Quantitative Graph Theory: Mathematical Foundations and Applications. CRC press.

Derrible, S. (2012). Network centrality of metro systems. PloS One, 7(7), e40575.

Deutsche Bahn. (2018). ICE-netz 2018. Retrieved from https://www.bahn.de/p/view/service/fahrplaene/streckennetz.shtml

Dinh, T. N., Xuan, Y., Thai, M. T., Park, E. K., & Znati, T. (2010, March). On approximation of new optimization methods for assessing network vulnerability. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). IEEE.

Ducruet, C., & Lugo, I. (2013). Structure and Dynamics of Transportation Networks: Models. The SAGE Handbook of Transport Studies, 347.

Edwards, W., Miles, R. F., & Von Winterfeldt, D. (2007). Advances in decision analysis. Cambridge University Press.

Edwards, W., & von Winterfeldt, D. (1986). Decision analysis and behavioral research. Cambridge University Press, 604, 6–8.

Emmert-Streib, F., & Dehmer, M. (2011). Networks for systems biology: conceptual connection of data and function. IET Systems Biology, 5(3), 185–207.

Emmert-Streib, F. (2011). A brief introduction to complex networks and their analysis. Structural Analysis of Complex Networks, 1--26. Springer.

Ezell, B. C., Bennett, S. P., Von Winterfeldt, D., Sokolowski, J., & Collins, A. J. (2010). Probabilistic risk analysis and terrorism risk. Risk Analysis: An International Journal, 30(4), 575-589.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering & System Safety, 121, 90–103.

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. Social Networks, 1(3), 215–239.

Gaertler, M. (2005). Network analysis: Methodological foundations. U. Brandes, T. Erlebach (Eds.), 178–215.

Gao, J., Buldyrev, S. V, Havlin, S., & Stanley, H. E. (2011). Robustness of a network of networks. Physical Review Letters, 107(19), 195701.

Gilly, J.-P., Kechidi, M., & Talbot, D. (2014). Resilience of organisations and territories: The role of pivot firms. European Management Journal, 32(4), 596–602.

Gómez, D., Figueira, J. R., & Eusébio, A. (2013). Modeling centrality measures in social network analysis using bi-criteria network flow optimization problems. European Journal of Operational Research, 226(2), 354–365.

Guimera, R., Mossa, S., Turtschi, A., & Amaral, L. A. N. (2005). The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. Proceedings of the National Academy of Sciences, 102(22), 7794–7799.

Henry, D., & Ramirez-Marquez, J. E. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. Reliability Engineering & System Safety, 99, 114–122.

Holling, C. S. (1996). Engineering resilience versus ecological resilience. Engineering within Ecological Constraints, 31(1996), 32.

Holme, P., Kim, B. J., Yoon, C. N., & Han, S. K. (2002). Attack vulnerability of complex networks. Physical Review E, 65(5), 56109.

Holmgren, Å. J. (2006). Using graph models to analyze the vulnerability of electric power networks. Risk Analysis, 26(4), 955–969.

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47–61.

House, W. (2013). Presidential policy directive--critical infrastructure security and resilience. The White House, Washington, DC. Retrieved August, 31, 2015.

Hwang, C.-L., & Yoon, K. (1981). Methods for multiple attribute decision making. In Multiple attribute decision making (pp. 58–191). Springer.

Ip, W. H., & Wang, D. (2011). Resilience and friability of transportation networks: evaluation, analysis and optimization. IEEE Systems Journal, 5(2), 189–198.

Jenelius, E., Petersen, T., & Mattsson, L.-G. (2006). Importance and exposure in road network vulnerability analysis. Transportation Research Part A: Policy and Practice, 40(7), 537–560.

Ji, Y., & Geroliminis, N. (2012). On the spatial partitioning of urban transportation networks. Transportation Research Part B: Methodological, 46(10), 1639–1656.

Johansson, J., Hassel, H., & Zio, E. (2013). Reliability and vulnerability analyses of critical infrastructures: comparing two approaches in the context of power systems. Reliability Engineering & System Safety, 120, 27–38.

Kamath, C. (2010). Understanding wind ramp events through analysis of historical data. Transmission and Distribution Conference and Exposition, 2010 IEEE PES, 1–6.

Keeney, G. L., & Von Winterfeldt, D. (2010). Identifying and structuring the objectives of terrorists. Risk Analysis: An International Journal, 30(12), 1803-1816.

Keršuliene, V., Zavadskas, E. K., & Turskis, Z. (2010). Selection of rational dispute resolution method by applying new step‐wise weight assessment ratio analysis (SWARA). Journal of business economics and management, 11(2), 243-258.

Kirlangiç, A. (2002). A measure of graph vulnerability: scattering number. International Journal of Mathematics and Mathematical Sciences, 30(1), 1–8.

Lai, Y.-J., Liu, T.-Y., & Hwang, C.-L. (1994). Topsis for MODM. European Journal of Operational Research, 76(3), 486–500.

Landherr, A., Friedl, B., & Heidemann, J. (2010). A critical review of centrality measures in social networks. Business & Information Systems Engineering, 2(6), 371–385.

Latora, V., & Marchiori, M. (2003). Economic small-world behavior in weighted networks. The European Physical Journal B-Condensed Matter and Complex Systems, 32(2), 249–263.

Larcher, M., Casadei, F., Giannopoulos, G., Solomos, G., Planchet, J. L., & Rochefrette, A. (2011). Determination of the risk due to explosions in railway systems. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 225(4), 373-382.

Li, F., Ye, Q., & Li, X. (2011). Tenacity and rupture degree of permutation graphs of complete bipartite graphs. Bull. Malys. Math. Sci. Soc.(2).

Li, W., & Cai, X. (2007). Empirical analysis of a scale-free railway network in China. Physica A: Statistical Mechanics and Its Applications, 382(2), 693–703.

Li, W., & Cai, X. (2004). Statistical analysis of airport network of China. Physical Review E, 69(4), 46106.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., & others. (2014). Changing the resilience paradigm. Nature Climate Change, 4(6), 407–409.

LiPing, C., Ru, W., Hang, S., Xin-Ping, X., Jin-Song, Z., Wei, L., & Xu, C. (2003). Structural properties of US flight network. Chinese Physics Letters, 20(8), 1393.

Lotter A., Steyer F., Schleiner S., Mudimu O. A., & Lechleuthner A. (2016) Resilience in High-Speed Train Networks. Promising, New Approach. In: Global Risk Forum - GRF Davos (Hg.): "Integrative Risk Management - Towards Resilient Cities". Short Abstracts. IDRC DAVOS. Davos, 28.08. - 01.09.2016, p. 91.

Lü, L., Chen, D., Ren, X. L., Zhang, Q. M., Zhang, Y. C., & Zhou, T. (2016). Vital nodes identification in complex networks. Physics Reports, 650, 1-63.

Maharani, W., Gozali, A. A., & others. (2014). Degree centrality and eigenvector centrality in twitter. Telecommunication Systems Services and Applications (TSSA), 2014 8th International Conference On, 1–5.

Mallawaarachchi, V. (2017). Introduction to genetic algorithms-including example code. Towards Data Science, 8(07).

Mamut, A., & Vumar, E. (2008). Vertex vulnerability parameters of Kronecker products of complete graphs. Information Processing Letters, 106(6), 258–262.

Martin-Breen, P., & Anderies, J. M. (2011). Resilience: A literature review.

Mesgari, I., Kermani, M. A. M. A., Hanneman, R., & Aliahmadi, A. (2015). Identifying key nodes in social networks using multi-criteria decision-making tools. In Mathematical Technology of Networks (pp. 137–150). Springer.

Meyer-Nieberg, Silja and Dehmer, Matthias and Bracker, Holger and Schneider, B. (2014). Assessing the vulnerability of dynamical systems in public transportation. 251--256. Berlin: Proceedings of 9th future security - Security Research Conference.

Mirsky, L. (2012). An introduction to linear algebra. Courier Corporation.

Mishkovski, I., Biey, M., & Kocarev, L. (2011). Vulnerability of complex networks. Communications in Nonlinear Science and Numerical Simulation, 16(1), 341–349.

Mitchell, M. (1998). An introduction to genetic algorithms. MIT press.

Mohmand, Y. T., & Wang, A. (2014). Complex network analysis of Pakistan railways. Discrete Dynamics in Nature and Society, 2014.

Mohmand, Y. T., & Wang, A. (2013). Weighted complex network analysis of Pakistan highways. Discrete Dynamics in Nature and Society, 2013.

Montibeller, G., & Von Winterfeldt, D. (2015). Cognitive and motivational biases in decision and risk analysis. Risk analysis, 35(7), 1230-1251.

Motter, A. E., & Lai, Y.-C. (2002). Cascade-based attacks on complex networks. Physical Review E, 66(6), 65102.

Mouronte, M. L., & BENITO, R. (2012). Structural properties of urban bus and subway networks of Madrid. Networks & Heterogeneous Media, 7(3).

Muruganantham, A., & Gandhi, M. (2016). Discovering and ranking influential users in social media networks using Multi-Criteria Decision Making (MCDM) Methods. Indian Journal of Science and Technology, 9(32).

Nan, C., & Sansavini, G. (2017). A quantitative method for assessing resilience of interdependent infrastructures. Reliability Engineering & System Safety, 157, 35–53.

National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland. (2021). The Global Terrorism Database (GTD) [Data file]. Retrieved from: https://www.start.umd.edu/gtd

Newman, M. E. (2003). The structure and function of complex networks. SIAM review, 45(2), 167-256.

Newman, M. E. J. (2008). The mathematics of networks. The New Palgrave Encyclopedia of Economics, 2(2008), 1–12.

Nistor, M. S., Pickl, S., Raap, M., & Zsifkovits, M. (2017). Network efficiency and vulnerability analysis using the flow-weighted efficiency measure. International Transactions in Operational Research.

Otway, H., & von Winterfeldt, D. (1992). Expert judgment in risk analysis and management: process, context, and pitfalls. Risk analysis, 12(1), 83-93.

Ouyang, M., Zhao, L., Hong, L., & Pan, Z. (2014). Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability. Reliability Engineering & System Safety, 123, 38–46.

Pastor-Satorras, R., & Vespignani, A. (2002). Immunization of complex networks. Physical Review E, 65(3), 36104.

Powell, J., & Fletcher, D. (2011). The need for developing an effective and acceptable engineering response to terrorist attacks on railway systems. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 225(4), 359-371.

Puzis, R., Altshuler, Y., Elovici, Y., Bekhor, S., Shiftan, Y., & Pentland, A. (2013). Augmented betweenness centrality for environmentally aware traffic monitoring in transportation networks. Journal of Intelligent Transportation Systems, 17(1), 91–105.

Qi, X., Fuller, E., Wu, Q., Wu, Y., & Zhang, C. Q. (2012). Laplacian centrality: A new centrality measure for weighted networks. Information Sciences, 194, 240-253.

Qu, G., Rudraraju, J., Modukuri, R., Hariri, S., & Raghavendra, C. S. (2002). A Framework for Network Vulnerability Analysis. In Communications, Internet, and Information Technology (pp. 289-294).

RE(H)STRAIN. (2021). REsilience of the Franco-German High Speed TRAIn Network. Retrieved from https://rehstrain.comtessa.org/

Rezaei, J. (2015). Best-worst multi-criteria decision-making method. Omega, 53, 49-57.

Rinaldi, S. M. (2004). Modeling and simulating critical infrastructures and their interdependencies. System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference On, 8--pp.

Rodríguez-Núñez, E., & García-Palomares, J. C. (2014). Measuring the vulnerability of public transport networks. Journal of Transport Geography, 35, 50–63.

Rossetti, G. (2015). Social Network Dynamics (Doctoral dissertation, Università di Pisa).

Roszkowska, E. (2011). Multi-criteria decision making models by applying the TOPSIS method to crisp and interval data. Multiple Criteria Decision Making/University of Economics in Katowice, 6, 200-230.

Rueda, D. F., Calle, E., & Marzo, J. L. (2017). Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements. Journal of Network and Systems Management, 25(2), 269-289.

Ruhnau, B. (2000). Eigenvector-centrality -- a node-centrality? Social Networks, 22(4), 357–365.

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. European Journal of Operational Research, 242(1), 261-273.

Seager, T. P., Clark, S. S., Eisenberg, D. A., Thomas, J. E., Hinrichs, M. M., Kofron, R., ... & Alderson, D. L. (2017). Redesigning resilient infrastructure research. In Resilience and risk (pp. 81-119). Springer, Dordrecht.

Sen, P., Dasgupta, S., Chatterjee, A., Sreeram, P. A., Mukherjee, G., & Manna, S. S. (2003). Small-world properties of the Indian railway network. Physical Review E, 67(3), 36106.

Sienkiewicz, J., & Hołyst, J. A. (2005). Statistical analysis of 22 public transport networks in Poland. Physical Review E, 72(4), 46127.

Smith, J. E. (1988). Characterizing computer performance with a single number. Communications of the ACM, 31(10), 1202–1206.

Stillwell, W. G., Von Winterfeldt, D., & John, R. S. (1987). Comparing hierarchical and nonhierarchical weighting methods for eliciting multiattribute value models. Management Science, 33(4), 442-450.

Strang, G. (1993). Introduction to linear algebra (Vol. 3). Wellesley, MA: Wellesley-Cambridge Press.

Sullivan, J. L., Novak, D. C., Aultman-Hall, L., & Scott, D. M. (2010). Identifying critical road segments and measuring system-wide robustness in transportation networks with isolating links: A link-based capacity-reduction approach. Transportation Research Part A: Policy and Practice, 44(5), 323–336.

Teodorescu, H.-N. L., & Pickl, S. W. (2016b). Computing and optimizing the index of resilience of networks and information systems. Romanian Journal of Information Science and Technology (ROMJIST), 19(1--2), 116–126.

Todorovic, B., Trifunovic, D., Jonev, K., & Filipovic, M. (2017). Contribution to Enhancement of Critical Infrastructure Resilience in Serbia. In Resilience and Risk (pp. 531-551). Springer, Dordrecht.

Tsiotas, D., & Polyzos, S. (2015). Introducing a new centrality measure from the transportation network analysis in Greece. Annals of Operations Research, 227(1), 93–117.

Vardi, Y., & Zhang, C.-H. (2007). Measures of network vulnerability. IEEE Signal Processing Letters, 14(5), 313–316.

Vugrin, E. D., Warren, D. E., & Ehlen, M. A. (2011). A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Process Safety Progress, 30(3), 280–290.

Wang, J., Mo, H., Wang, F., & Jin, F. (2011). Exploring the network structure and nodal centrality of China's air transport network: A complex network approach. Journal of Transport Geography, 19(4), 712–721.

Wang, Z., Zsifkovits, M., & Pickl, S. W. (2018). Analyzing vulnerabilities of the German high-speed train network using quantitative graph theory. International Journal of Safety and Security Engineering, 8(1), 59–64.

Wasserman, S., & Faust, K. (1994). Social network analysis: Methods and applications (Vol. 8). Cambridge university press.

Weisstein, Eric W. (2020) Linear Algebra. From MathWorld--A Wolfram Web Resource. https://mathworld.wolfram.com/LinearAlgebra.html

West, D. B., & others. (2001). Introduction to graph theory (Vol. 2). Prentice hall Upper Saddle River.

White Jr, C. H. (2003). 9/11 Issues for Railroads. Logistics Spectrum, 9.

Winterfeldt, D. (1980). Structuring decision problems for decision analysis. Acta Psychologica, 45(1-3), 71-93.

Yoon, K. P., & Hwang, C.-L. (1995). Multiple attribute decision making: an introduction (Vol. 104). Sage publications.

Youn, B. D., Hu, C., & Wang, P. (2011). Resilience-driven system design of complex engineered systems. Journal of Mechanical Design, 133(10), 101011.

Yu, H., Liu, Z., & Li, Y.-J. (2013). Key nodes in complex networks identified by multi-attribute decision-making method. Acta Physica Sinica, 62(2).

Zemanová, L., Zhou, C., & Kurths, J. (2006). Structural and functional clusters of complex brain networks. Physica D: Nonlinear Phenomena, 224(1–2), 202–212.

Zhang, S., & Wang, Z. (2001). Scattering number in graphs. Networks, 37(2), 102–106.

Zhang, Z., Xu, B., Li, Y., & Liu, L. (1999). A note on the lower bounds of signed domination number of a graph. Discrete Mathematics, 195(1), 295–298.

Zhao, M., Zhou, T., Wang, B.-H., & Wang, W.-X. (2005). Enhanced synchronizability by structural perturbations. Physical Review E, 72(5), 57102.

Zobel, C. W. (2011). Representing perceived tradeoffs in defining disaster resilience. Decision Support Systems, 50(2), 394-403.

Zsifkovits M., & Pickl S. (2016a) Agent Based Modeling for Critical Infrastructure Protection - Modeling Attack Scenarios in the Public Transport, Poster presentation at The 11th Future Security Conference, Berlin, Germany.

Zsifkovits, M., & Pickl, S. (2016b). Strategic Risk Management in Counter-Terrorism for the Railbound Public Transport: Merging Qualitative and Quantitative Operations Research Techniques. In Proceedings of the International Conference on Security and Management (SAM) (p. 77). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

# - APPENDIX -

# Appendix: Tables

**Table A-1: The results based on betweenness centrality measure**

| ID | Betweenness | ID | Betweenness | ID | Betweenness | ID | Betweenness |
|---|---|---|---|---|---|---|---|
| 1 | 0.284033613 | 32 | 0.034173669 | 63 | 0.092156863 | 94 | 0.033053221 |
| 2 | 0.196778711 | 33 | 0.038795518 | 64 | 0.102941176 | 95 | 0.016666667 |
| 3 | 0 | 34 | 0.131092437 | 65 | 0 | 96 | 0 |
| 4 | 0.165266106 | 35 | 0.087955182 | 66 | 0.158823529 | 97 | 0.016666667 |
| 5 | 0.049159664 | 36 | 0 | 67 | 0.033613445 | 98 | 0.016666667 |
| 6 | 0.033053221 | 37 | 0.037114846 | 68 | 0.034313725 | 99 | 0 |
| 7 | 0 | 38 | 0.02394958 | 69 | 0.041736695 | 100 | 0.094677871 |
| 8 | 0 | 39 | 0 | 70 | 0 | 101 | 0 |
| 9 | 0.04929972 | 40 | 0.042857143 | 71 | 0.131512605 | 102 | 0.144257703 |
| 10 | 0 | 41 | 0.104761905 | 72 | 0.033053221 | 103 | 0.280392157 |
| 11 | 0.016526611 | 42 | 0.008683473 | 73 | 0.016666667 | 104 | 0.17464986 |
| 12 | 0 | 43 | 0.010644258 | 74 | 0 | 105 | 0.091316527 |
| 13 | 0 | 44 | 0.030812325 | 75 | 0 | 106 | 0 |
| 14 | 0.034313725 | 45 | 0.000840336 | 76 | 0.078571429 | 107 | 0.064985994 |
| 15 | 0.024229692 | 46 | 0.029551821 | 77 | 0.064985994 | 108 | 0.139915966 |
| 16 | 0.033473389 | 47 | 0.02394958 | 78 | 0.049159664 | 109 | 0.125490196 |
| 17 | 0 | 48 | 0.013865546 | 79 | 0.033053221 | 110 | 0.110784314 |
| 18 | 0.118627451 | 49 | 0 | 80 | 0.026190476 | 111 | 0.095798319 |
| 19 | 0.016666667 | 50 | 0.066666667 | 81 | 0.027310924 | 112 | 0.080532213 |
| 20 | 0 | 51 | 0.043557423 | 82 | 0.181652661 | 113 | 0.064985994 |
| 21 | 0.10952381 | 52 | 0.114845938 | 83 | 0.007282913 | 114 | 0.049159664 |
| 22 | 0.201960784 | 53 | 0.114145658 | 84 | 0.006162465 | 115 | 0.033053221 |
| 23 | 0.090616246 | 54 | 0.041736695 | 85 | 0.090616246 | 116 | 0.016666667 |
| 24 | 0.149019608 | 55 | 0.032492997 | 86 | 0.037885154 | 117 | 0 |
| 25 | 0 | 56 | 0.033053221 | 87 | 0.047478992 | 118 | 0.049159664 |
| 26 | 0.114565826 | 57 | 0.016666667 | 88 | 0 | 119 | 0.033053221 |
| 27 | 0.163585434 | 58 | 0 | 89 | 0.113165266 | 120 | 0.016666667 |
| 28 | 0.116526611 | 59 | 0.088935574 | 90 | 0.025770308 | 121 | 0 |
| 29 | 0.050280112 | 60 | 0.082913165 | 91 | 0.116946779 | | |
| 30 | 0.041736695 | 61 | 0.078291317 | 92 | 0.049439776 | | |
| 31 | 0.03487395 | 62 | 0.081372549 | 93 | 0 | | |

**Table A-2: The results based on closeness centrality measure**

| ID | Closeness | ID | Closeness | ID | Closeness | ID | Closeness |
|---|---|---|---|---|---|---|---|
| 1 | 0.222222222 | 32 | 0.129032258 | 63 | 0.13559322 | 94 | 0.142517815 |
| 2 | 0.203045685 | 33 | 0.13363029 | 64 | 0.148514851 | 95 | 0.125130344 |
| 3 | 0.187793427 | 34 | 0.143369176 | 65 | 0.160213618 | 96 | 0.111317254 |
| 4 | 0.204081633 | 35 | 0.14354067 | 66 | 0.171184023 | 97 | 0.12539185 |
| 5 | 0.171184023 | 36 | 0.135746606 | 67 | 0.146878825 | 98 | 0.081688223 |
| 6 | 0.147058824 | 37 | 0.146341463 | 68 | 0.153452685 | 99 | 0.075566751 |
| 7 | 0.128479657 | 38 | 0.14084507 | 69 | 0.165975104 | 100 | 0.146520147 |
| 8 | 0.128479657 | 39 | 0.123583934 | 70 | 0.131868132 | 101 | 0.111524164 |
| 9 | 0.174418605 | 40 | 0.152866242 | 71 | 0.153649168 | 102 | 0.144578313 |
| 10 | 0.149068323 | 41 | 0.1517067 | 72 | 0.133928571 | 103 | 0.149812734 |
| 11 | 0.149068323 | 42 | 0.129589633 | 73 | 0.11846002 | 104 | 0.148883375 |
| 12 | 0.130151844 | 43 | 0.144230769 | 74 | 0.106007067 | 105 | 0.141676505 |
| 13 | 0.172661871 | 44 | 0.169252468 | 75 | 0.133037694 | 106 | 0.130434783 |
| 14 | 0.180451128 | 45 | 0.144927536 | 76 | 0.165745856 | 107 | 0.133037694 |
| 15 | 0.155642023 | 46 | 0.147783251 | 77 | 0.106761566 | 108 | 0.133779264 |
| 16 | 0.140186916 | 47 | 0.140515222 | 78 | 0.097008892 | 109 | 0.12 |
| 17 | 0.119521912 | 48 | 0.125523013 | 79 | 0.088757396 | 110 | 0.108597285 |
| 18 | 0.11846002 | 49 | 0.132743363 | 80 | 0.156453716 | 111 | 0.099009901 |
| 19 | 0.10619469 | 50 | 0.160213618 | 81 | 0.144578313 | 112 | 0.090840273 |
| 20 | 0.096076861 | 51 | 0.148331273 | 82 | 0.184615385 | 113 | 0.083798883 |
| 21 | 0.126849894 | 52 | 0.156046814 | 83 | 0.145985401 | 114 | 0.077669903 |
| 22 | 0.141342756 | 53 | 0.151133501 | 84 | 0.130718954 | 115 | 0.072289157 |
| 23 | 0.193861066 | 54 | 0.128893663 | 85 | 0.142687277 | 116 | 0.067529544 |
| 24 | 0.172166428 | 55 | 0.127523911 | 86 | 0.13559322 | 117 | 0.063291139 |
| 25 | 0.192926045 | 56 | 0.124481328 | 87 | 0.156862745 | 118 | 0.118226601 |
| 26 | 0.179910045 | 57 | 0.111008326 | 88 | 0.135746606 | 119 | 0.10619469 |
| 27 | 0.167832168 | 58 | 0.1 | 89 | 0.159786951 | 120 | 0.096230954 |
| 28 | 0.161725067 | 59 | 0.132596685 | 90 | 0.161507402 | 121 | 0.087847731 |
| 29 | 0.150753769 | 60 | 0.12145749 | 91 | 0.165061898 | | |
| 30 | 0.136830103 | 61 | 0.116959064 | 92 | 0.142857143 | | |
| 31 | 0.128205128 | 62 | 0.124223602 | 93 | 0.125130344 | | |

**Table A-3: The results based on degree centrality measure**

| ID | Degree | ID | Degree | ID | Degree | ID | Degree |
|---|---|---|---|---|---|---|---|
| 1 | 0.066666667 | 32 | 0.016666667 | 63 | 0.016666667 | 94 | 0.016666667 |
| 2 | 0.075 | 33 | 0.016666667 | 64 | 0.025 | 95 | 0.016666667 |
| 3 | 0.016666667 | 34 | 0.041666667 | 65 | 0.016666667 | 96 | 0.008333333 |
| 4 | 0.075 | 35 | 0.041666667 | 66 | 0.041666667 | 97 | 0.016666667 |
| 5 | 0.016666667 | 36 | 0.016666667 | 67 | 0.016666667 | 98 | 0.016666667 |
| 6 | 0.033333333 | 37 | 0.033333333 | 68 | 0.016666667 | 99 | 0.008333333 |
| 7 | 0.016666667 | 38 | 0.033333333 | 69 | 0.016666667 | 100 | 0.016666667 |
| 8 | 0.016666667 | 39 | 0.008333333 | 70 | 0.008333333 | 101 | 0.008333333 |
| 9 | 0.033333333 | 40 | 0.041666667 | 71 | 0.033333333 | 102 | 0.025 |
| 10 | 0.016666667 | 41 | 0.066666667 | 72 | 0.016666667 | 103 | 0.041666667 |
| 11 | 0.016666667 | 42 | 0.016666667 | 73 | 0.016666667 | 104 | 0.025 |
| 12 | 0.016666667 | 43 | 0.016666667 | 74 | 0.008333333 | 105 | 0.016666667 |
| 13 | 0.016666667 | 44 | 0.033333333 | 75 | 0.016666667 | 106 | 0.008333333 |
| 14 | 0.033333333 | 45 | 0.016666667 | 76 | 0.016666667 | 107 | 0.025 |
| 15 | 0.016666667 | 46 | 0.025 | 77 | 0.016666667 | 108 | 0.025 |
| 16 | 0.041666667 | 47 | 0.025 | 78 | 0.016666667 | 109 | 0.016666667 |
| 17 | 0.016666667 | 48 | 0.025 | 79 | 0.016666667 | 110 | 0.016666667 |
| 18 | 0.05 | 49 | 0.033333333 | 80 | 0.016666667 | 111 | 0.016666667 |
| 19 | 0.016666667 | 50 | 0.041666667 | 81 | 0.016666667 | 112 | 0.016666667 |
| 20 | 0.008333333 | 51 | 0.016666667 | 82 | 0.058333333 | 113 | 0.016666667 |
| 21 | 0.016666667 | 52 | 0.025 | 83 | 0.016666667 | 114 | 0.016666667 |
| 22 | 0.05 | 53 | 0.025 | 84 | 0.016666667 | 115 | 0.016666667 |
| 23 | 0.025 | 54 | 0.016666667 | 85 | 0.033333333 | 116 | 0.016666667 |
| 24 | 0.041666667 | 55 | 0.016666667 | 86 | 0.016666667 | 117 | 0.008333333 |
| 25 | 0.016666667 | 56 | 0.016666667 | 87 | 0.033333333 | 118 | 0.016666667 |
| 26 | 0.05 | 57 | 0.016666667 | 88 | 0.008333333 | 119 | 0.016666667 |
| 27 | 0.033333333 | 58 | 0.008333333 | 89 | 0.025 | 120 | 0.016666667 |
| 28 | 0.025 | 59 | 0.016666667 | 90 | 0.025 | 121 | 0.008333333 |
| 29 | 0.016666667 | 60 | 0.016666667 | 91 | 0.041666667 | | |
| 30 | 0.016666667 | 61 | 0.016666667 | 92 | 0.025 | | |
| 31 | 0.016666667 | 62 | 0.016666667 | 93 | 0.008333333 | | |

**Table A-4: The results based on eigenvector centrality measure**

| ID | Eigenvector | ID | Eigenvector | ID | Eigenvector | ID | Eigenvector |
|---|---|---|---|---|---|---|---|
| 1 | 0.318157655 | 32 | 0.000880549 | 63 | 0.005456865 | 94 | 0.000831262 |
| 2 | 0.44534468 | 33 | 0.00281764 | 64 | 0.024629782 | 95 | 0.000183007 |
| 3 | 0.138525964 | 34 | 0.01251072 | 65 | 0.130379253 | 96 | 3.85E-05 |
| 4 | 0.340208367 | 35 | 0.022959051 | 66 | 0.085911453 | 97 | 0.000191916 |
| 5 | 0.09319374 | 36 | 0.015758375 | 67 | 0.020735938 | 98 | 6.79E-05 |
| 6 | 0.102709266 | 37 | 0.051935057 | 68 | 0.012639294 | 99 | 1.43E-05 |
| 7 | 0.027369765 | 38 | 0.054821745 | 69 | 0.039334259 | 100 | 0.00587981 |
| 8 | 0.027369765 | 39 | 0.011534974 | 70 | 0.066977548 | 101 | 4.04E-05 |
| 9 | 0.107775509 | 40 | 0.153290201 | 71 | 0.025688524 | 102 | 0.00177926 |
| 10 | 0.024879863 | 41 | 0.318321136 | 72 | 0.005667629 | 103 | 0.00166557 |
| 11 | 0.024879863 | 42 | 0.078956868 | 73 | 0.001247759 | 104 | 0.004843039 |
| 12 | 0.010469881 | 43 | 0.056933564 | 74 | 0.000262539 | 105 | 0.002256181 |
| 13 | 0.097305627 | 44 | 0.191628683 | 75 | 0.043788572 | 106 | 0.000350451 |
| 14 | 0.122251644 | 45 | 0.068258281 | 76 | 0.019095538 | 107 | 0.000471566 |
| 15 | 0.035730302 | 46 | 0.132779329 | 77 | 0.006331125 | 108 | 0.000471566 |
| 16 | 0.047562129 | 47 | 0.117451293 | 78 | 0.001396975 | 109 | 0.000104052 |
| 17 | 0.016044677 | 48 | 0.185394739 | 79 | 0.000308213 | 110 | 2.30E-05 |
| 18 | 0.028692674 | 49 | 0.240031329 | 80 | 0.00194871 | 111 | 5.07E-06 |
| 19 | 0.006316848 | 50 | 0.259668828 | 81 | 0.006238602 | 112 | 1.12E-06 |
| 20 | 0.00132912 | 51 | 0.083206129 | 82 | 0.010639024 | 113 | 2.47E-07 |
| 21 | 0.015437093 | 52 | 0.077128834 | 83 | 0.002623844 | 114 | 5.44E-08 |
| 22 | 0.04467449 | 53 | 0.023691731 | 84 | 0.001831201 | 115 | 1.20E-08 |
| 23 | 0.124849121 | 54 | 0.005220553 | 85 | 0.00607922 | 116 | 2.64E-09 |
| 24 | 0.100904217 | 55 | 0.001852431 | 86 | 0.003911486 | 117 | 5.56E-10 |
| 25 | 0.08817428 | 56 | 0.009856481 | 87 | 0.003583412 | 118 | 0.000104052 |
| 26 | 0.174302842 | 57 | 0.002169958 | 88 | 0.000753981 | 119 | 2.30E-05 |
| 27 | 0.114776651 | 58 | 0.000456578 | 89 | 0.003022941 | 120 | 5.05E-06 |
| 28 | 0.02770121 | 59 | 0.009869817 | 90 | 0.003785281 | 121 | 1.06E-06 |
| 29 | 0.025332039 | 60 | 0.002233336 | 91 | 0.003767696 | | |
| 30 | 0.005617775 | 61 | 0.000744457 | 92 | 0.00087173 | | |
| 31 | 0.001367304 | 62 | 0.001304812 | 93 | 0.00018342 | | |

**Table A-5: The results based on nodal efficiency measure**

| ID | Nodal Efficiency | ID | Nodal Efficiency | ID | Nodal Efficiency | ID | Nodal Efficiency |
|---|---|---|---|---|---|---|---|
| 1 | 0.550910552 | 32 | 0.412674384 | 63 | 0.312916896 | 94 | 0.262095193 |
| 2 | 0.548035509 | 33 | 0.439974163 | 64 | 0.340860688 | 95 | 0.231495986 |
| 3 | 0.436780381 | 34 | 0.476933148 | 65 | 0.298263797 | 96 | 0.208389606 |
| 4 | 0.4500774 | 35 | 0.531129609 | 66 | 0.350581726 | 97 | 0.25321087 |
| 5 | 0.385209401 | 36 | 0.526443122 | 67 | 0.344097099 | 98 | 0.357937124 |
| 6 | 0.342240772 | 37 | 0.532531152 | 68 | 0.334505875 | 99 | 0.27291817 |
| 7 | 0.307701164 | 38 | 0.61310813 | 69 | 0.345195934 | 100 | 0.32290037 |
| 8 | 0.270314433 | 39 | 0.557990423 | 70 | 0.317956059 | 101 | 0.229434079 |
| 9 | 0.344333421 | 40 | 0.580019524 | 71 | 0.331923556 | 102 | 0.498747746 |
| 10 | 0.297143103 | 41 | 0.829973494 | 72 | 0.267602788 | 103 | 1.007819958 |
| 11 | 0.264793425 | 42 | 0.435434518 | 73 | 0.326449425 | 104 | 0.66632525 |
| 12 | 0.222545919 | 43 | 0.362146644 | 74 | 0.321491912 | 105 | 0.310823527 |
| 13 | 0.407722334 | 44 | 0.521427572 | 75 | 0.59147338 | 106 | 0.850841497 |
| 14 | 0.288904099 | 45 | 0.498726806 | 76 | 0.277475412 | 107 | 0.768579411 |
| 15 | 0.256840396 | 46 | 0.42571089 | 77 | 0.301747847 | 108 | 0.365278835 |
| 16 | 0.28536991 | 47 | 0.414187613 | 78 | 0.313328921 | 109 | 0.341408694 |
| 17 | 0.448046219 | 48 | 0.441961277 | 79 | 0.36561432 | 110 | 0.317816841 |
| 18 | 0.585021067 | 49 | 0.508236251 | 80 | 0.322085769 | 111 | 0.305013377 |
| 19 | 0.539497879 | 50 | 0.827538527 | 81 | 0.299770488 | 112 | 0.312150223 |
| 20 | 0.23800596 | 51 | 0.506204901 | 82 | 0.340735711 | 113 | 0.329099472 |
| 21 | 0.270946784 | 52 | 0.491386291 | 83 | 0.353603312 | 114 | 0.308335308 |
| 22 | 0.329211001 | 53 | 0.488702033 | 84 | 0.411370288 | 115 | 0.27021973 |
| 23 | 0.452413137 | 54 | 0.352856094 | 85 | 0.436827523 | 116 | 0.278238131 |
| 24 | 0.311459895 | 55 | 0.299218341 | 86 | 0.422268248 | 117 | 0.26012499 |
| 25 | 0.379454447 | 56 | 0.235860158 | 87 | 0.289662748 | 118 | 0.267112696 |
| 26 | 0.374180036 | 57 | 0.211457664 | 88 | 0.251822708 | 119 | 0.248152582 |
| 27 | 0.359226494 | 58 | 0.18705816 | 89 | 0.32754573 | 120 | 0.254394978 |
| 28 | 0.333236794 | 59 | 0.323833203 | 90 | 0.402105778 | 121 | 0.24793685 |
| 29 | 0.353099139 | 60 | 0.297695071 | 91 | 0.811661689 | | |
| 30 | 0.3879089 | 61 | 0.278439999 | 92 | 0.809928402 | | |
| 31 | 0.398457448 | 62 | 0.279613747 | 93 | 0.386491181 | | |

**Table A-6: The results based on flow-weighted efficiency measure**

| ID | Flow-weighted Efficiency | ID | Flow-weighted Efficiency | ID | Flow-weighted Efficiency | ID | Flow-weighted Efficiency |
|---|---|---|---|---|---|---|---|
| 1 | 8.205000206 | 32 | 0.343294931 | 63 | 0 | 94 | 1.156188658 |
| 2 | 8.039463467 | 33 | 0.359733499 | 64 | 0 | 95 | 0.796831733 |
| 3 | 0.883422297 | 34 | 2.78623847 | 65 | 1.279354325 | 96 | 0.704385824 |
| 4 | 3.205859332 | 35 | 3.60125483 | 66 | 1.69262199 | 97 | 0.901388699 |
| 5 | 0.318865808 | 36 | 5.717509506 | 67 | 1.780470608 | 98 | 0 |
| 6 | 0.330665674 | 37 | 4.898113834 | 68 | 1.999672838 | 99 | 0 |
| 7 | 0.250088725 | 38 | 7.988746103 | 69 | 1.866925439 | 100 | 1.651692543 |
| 8 | 0.266090247 | 39 | 2.784404762 | 70 | 1.546630636 | 101 | 0.780289003 |
| 9 | 2.44311757 | 40 | 6.054302769 | 71 | 1.65985768 | 102 | 9.531676248 |
| 10 | 1.348511726 | 41 | 4.29486839 | 72 | 1.021917056 | 103 | 21.96744527 |
| 11 | 1.415467871 | 42 | 2.020750781 | 73 | 1.64520394 | 104 | 10.74468001 |
| 12 | 1.103738827 | 43 | 1.077411827 | 74 | 1.509419602 | 105 | 1.743948922 |
| 13 | 0.60977047 | 44 | 3.103645881 | 75 | 5.834645407 | 106 | 9.056525093 |
| 14 | 1.858967733 | 45 | 2.490685987 | 76 | 0.942897419 | 107 | 15.56829746 |
| 15 | 1.503851012 | 46 | 3.06642025 | 77 | 0 | 108 | 0.018853695 |
| 16 | 1.434075384 | 47 | 3.021786647 | 78 | 0 | 109 | 0 |
| 17 | 4.420575221 | 48 | 3.497835799 | 79 | 0 | 110 | 0.043243699 |
| 18 | 4.313112898 | 49 | 1.165667057 | 80 | 2.439643324 | 111 | 0.049880729 |
| 19 | 0.445518046 | 50 | 2.280393616 | 81 | 2.078405518 | 112 | 0.029753072 |
| 20 | 0.156248127 | 51 | 2.587130991 | 82 | 3.256669745 | 113 | 0 |
| 21 | 1.71569364 | 52 | 2.403324049 | 83 | 0.520734544 | 114 | 0.025025025 |
| 22 | 1.896376316 | 53 | 2.465378983 | 84 | 0.608971826 | 115 | 0.025025025 |
| 23 | 4.149721057 | 54 | 0.586547864 | 85 | 2.344921582 | 116 | 0 |
| 24 | 2.163949444 | 55 | 0.378134268 | 86 | 0.439934418 | 117 | 0 |
| 25 | 3.098846897 | 56 | 0.694486691 | 87 | 1.015498975 | 118 | 0 |
| 26 | 3.233535917 | 57 | 0.650542365 | 88 | 0 | 119 | 0 |
| 27 | 3.433849975 | 58 | 0.564227306 | 89 | 2.598892931 | 120 | 0 |
| 28 | 3.475020566 | 59 | 0.387161339 | 90 | 5.013649786 | 121 | 0 |
| 29 | 0.307944811 | 60 | 0.163953987 | 91 | 25.59644998 | | |
| 30 | 0.343418391 | 61 | 0 | 92 | 25.74422839 | | |
| 31 | 0.353773908 | 62 | 0 | 93 | 6.885654553 | | |

**Table A-7: The results based on nodal residual closeness vulnerability measure**

| ID | Nodal Resi-Clos | ID | Nodal Resi-Clos | ID | Nodal Resi-Clos | ID | Nodal Resi-Clos |
|---|---|---|---|---|---|---|---|
| 1 | 0.116802636 | 32 | 0.053094093 | 63 | 0.034841445 | 94 | 0.024125101 |
| 2 | 0.097166754 | 33 | 0.064226229 | 64 | 0.044570791 | 95 | 0.015041205 |
| 3 | 0.022007886 | 34 | 0.11897974 | 65 | 0.018327207 | 96 | 0.007201962 |
| 4 | 0.125085868 | 35 | 0.083402993 | 66 | 0.054007709 | 97 | 0.018222287 |
| 5 | 0.017057971 | 36 | 0.02764324 | 67 | 0.031096778 | 98 | 0.019099908 |
| 6 | 0.036776424 | 37 | 0.046371928 | 68 | 0.028350068 | 99 | 0.009606448 |
| 7 | 0.010115823 | 38 | 0.052811749 | 69 | 0.031001754 | 100 | 0.035941211 |
| 8 | 0.007401441 | 39 | 0.025939743 | 70 | 0.018030987 | 101 | 0.008756478 |
| 9 | 0.046341191 | 40 | 0.053010397 | 71 | 0.053535161 | 102 | 0.059461521 |
| 10 | 0.010902051 | 41 | 0.079164035 | 72 | 0.0257122 | 103 | 0.125085868 |
| 11 | 0.00878342 | 42 | 0.032506201 | 73 | 0.016449508 | 104 | 0.065506538 |
| 12 | 0.004016844 | 43 | 0.021871421 | 74 | 0.008716603 | 105 | 0.035795183 |
| 13 | 0.018463512 | 44 | 0.038808836 | 75 | 0.027020106 | 106 | 0.021418112 |
| 14 | 0.022196858 | 45 | 0.022953531 | 76 | 0.017039282 | 107 | 0.047061051 |
| 15 | 0.022572772 | 46 | 0.0312189 | 77 | 0.038345032 | 108 | 0.067872595 |
| 16 | 0.032566607 | 47 | 0.029871911 | 78 | 0.032387427 | 109 | 0.059374814 |
| 17 | 0.014717226 | 48 | 0.027002852 | 79 | 0.026508914 | 110 | 0.05187906 |
| 18 | 0.061201443 | 49 | 0.026544907 | 80 | 0.021605956 | 111 | 0.045716532 |
| 19 | 0.02403736 | 50 | 0.039133711 | 81 | 0.018539989 | 112 | 0.040351525 |
| 20 | 0.010293666 | 51 | 0.028268328 | 82 | 0.054681985 | 113 | 0.035851651 |
| 21 | 0.016796944 | 52 | 0.044595233 | 83 | 0.021842903 | 114 | 0.030097202 |
| 22 | 0.058882618 | 53 | 0.047002628 | 84 | 0.028204447 | 115 | 0.023339825 |
| 23 | 0.024005495 | 54 | 0.036514958 | 85 | 0.054308651 | 116 | 0.016367994 |
| 24 | 0.047192688 | 55 | 0.023665915 | 86 | 0.0238349 | 117 | 0.008479641 |
| 25 | 0.020554997 | 56 | 0.019153761 | 87 | 0.032366296 | 118 | 0.029682339 |
| 26 | 0.057707071 | 57 | 0.011653168 | 88 | 0.011888761 | 119 | 0.020957839 |
| 27 | 0.072234486 | 58 | 0.005360628 | 89 | 0.042755478 | 120 | 0.013115669 |
| 28 | 0.04039307 | 59 | 0.037317908 | 90 | 0.023795911 | 121 | 0.006963922 |
| 29 | 0.035714952 | 60 | 0.031120681 | 91 | 0.067484104 | | |
| 30 | 0.038881307 | 61 | 0.027074653 | 92 | 0.043990252 | | |
| 31 | 0.044662277 | 62 | 0.028010879 | 93 | 0.014920479 | | |

**Table A-8: The results based on nodal betweenness-efficiency vulnerability measure**

| ID | Nodal Betw-Effi | ID | Nodal Betw-Effi | ID | Nodal Betw-Effi | ID | Nodal Betw-Effi |
|---|---|---|---|---|---|---|---|
| 1 | 0.08595542 | 32 | 0.034677186 | 63 | 0.022838612 | 94 | 0.01440232 |
| 2 | 0.055255448 | 33 | 0.043213308 | 64 | 0.031585042 | 95 | 0.006461428 |
| 3 | 0.014874932 | 34 | 0.086379072 | 65 | 0.007390291 | 96 | 0.000578614 |
| 4 | 0.100842476 | 35 | 0.059023728 | 66 | 0.042705354 | 97 | 0.009188233 |
| 5 | 0.011224896 | 36 | 0.015292647 | 67 | 0.019623714 | 98 | 0.010543089 |
| 6 | 0.028245356 | 37 | 0.029239987 | 68 | 0.017305635 | 99 | 0.00175859 |
| 7 | 0.005803142 | 38 | 0.036277437 | 69 | 0.020004882 | 100 | 0.023823709 |
| 8 | 0.003587513 | 39 | 0.01416518 | 70 | 0.008332573 | 101 | 0.000751578 |
| 9 | 0.036438188 | 40 | 0.029199305 | 71 | 0.040287034 | 102 | 0.042393536 |
| 10 | 0.006463778 | 41 | 0.056847956 | 72 | 0.016114279 | 103 | 0.101247186 |
| 11 | 0.004788911 | 42 | 0.019818426 | 73 | 0.007904101 | 104 | 0.048974514 |
| 12 | 0.000821193 | 43 | 0.013264054 | 74 | 0.000855037 | 105 | 0.023388102 |
| 13 | 0.012283745 | 44 | 0.027748627 | 75 | 0.015064735 | 106 | 0.011239923 |
| 14 | 0.015699403 | 45 | 0.015415901 | 76 | 0.008307349 | 107 | 0.033867883 |
| 15 | 0.011608685 | 46 | 0.021602551 | 77 | 0.027998998 | 108 | 0.05149712 |
| 16 | 0.016246737 | 47 | 0.018775154 | 78 | 0.022638079 | 109 | 0.044343384 |
| 17 | 0.006315025 | 48 | 0.015652171 | 79 | 0.017328681 | 110 | 0.038086547 |
| 18 | 0.049221626 | 49 | 0.015075244 | 80 | 0.011454732 | 111 | 0.032951046 |
| 19 | 0.01494115 | 50 | 0.016701302 | 81 | 0.009133867 | 112 | 0.028543831 |
| 20 | 0.002364677 | 51 | 0.016103332 | 82 | 0.037265647 | 113 | 0.024821608 |
| 21 | 0.007751256 | 52 | 0.028368688 | 83 | 0.011046038 | 114 | 0.019888482 |
| 22 | 0.044675654 | 53 | 0.030208189 | 84 | 0.015866107 | 115 | 0.013996112 |
| 23 | 0.015727752 | 54 | 0.022794444 | 85 | 0.035991878 | 116 | 0.007809053 |
| 24 | 0.024933421 | 55 | 0.012468095 | 86 | 0.012466721 | 117 | 0.000627853 |
| 25 | 0.012666049 | 56 | 0.010484567 | 87 | 0.019832253 | 118 | 0.019179385 |
| 26 | 0.03214522 | 57 | 0.003713218 | 88 | 0.003258784 | 119 | 0.011639383 |
| 27 | 0.040447768 | 58 | 0.002102431 | 89 | 0.028143075 | 120 | 0.004806084 |
| 28 | 0.023686348 | 59 | 0.025073264 | 90 | 0.013439184 | 121 | 0.000754915 |
| 29 | 0.022505306 | 60 | 0.019499005 | 91 | 0.052164282 | | |
| 30 | 0.024368294 | 61 | 0.015843328 | 92 | 0.031783881 | | |
| 31 | 0.02844606 | 62 | 0.016683753 | 93 | 0.005994699 | | |

**Table A-9: Top thirty-one stations based on different measures**

| Rank | Centrality | | | | Nodal Efficiency | | Nodal Vulnerability | |
|---|---|---|---|---|---|---|---|---|
| | BetwCentr ($M_1$) | CloCentr ($M_2$) | DegCentr ($M_3$) | EigenCentr ($M_4$) | Effi ($M_5$) | FWEffi ($M_6$) | BetwEffiVul ($M_7$) | ResiduCloVul ($M_8$) |
| 1 | 1 | 1 | 2 | 2 | 103 | 92 | 103 | 4 |
| 2 | 103 | 4 | 4 | 4 | 106 | 91 | 4 | 103 |
| 3 | 22 | 2 | 1 | 41 | 41 | 103 | 34 | 34 |
| 4 | 2 | 23 | 41 | 1 | 50 | 107 | 1 | 1 |
| 5 | 82 | 25 | 82 | 50 | 91 | 104 | 35 | 2 |
| 6 | 104 | 3 | 18 | 49 | 92 | 102 | 41 | 35 |
| 7 | 4 | 82 | 22 | 44 | 107 | 106 | 2 | 41 |
| 8 | 27 | 14 | 26 | 48 | 104 | 1 | 91 | 27 |
| 9 | 66 | 26 | 16 | 26 | 38 | 2 | 108 | 108 |
| 10 | 24 | 9 | 24 | 40 | 75 | 38 | 18 | 91 |
| 11 | 102 | 13 | 34 | 3 | 18 | 93 | 104 | 104 |
| 12 | 108 | 24 | 35 | 46 | 40 | 40 | 22 | 33 |
| 13 | 71 | 5 | 40 | 65 | 39 | 75 | 109 | 18 |
| 14 | 34 | 66 | 50 | 23 | 1 | 36 | 33 | 102 |
| 15 | 109 | 44 | 66 | 14 | 2 | 90 | 66 | 109 |
| 16 | 18 | 27 | 91 | 47 | 19 | 37 | 102 | 22 |
| 17 | 91 | 69 | 103 | 27 | 37 | 17 | 27 | 26 |
| 18 | 28 | 76 | 6 | 9 | 35 | 18 | 71 | 82 |
| 19 | 52 | 91 | 9 | 6 | 36 | 41 | 110 | 85 |
| 20 | 26 | 28 | 14 | 24 | 44 | 23 | 82 | 66 |
| 21 | 53 | 90 | 27 | 13 | 49 | 35 | 9 | 71 |
| 22 | 89 | 50 | 37 | 5 | 51 | 48 | 38 | 32 |
| 23 | 110 | 65 | 38 | 25 | 102 | 28 | 85 | 40 |
| 24 | 21 | 89 | 44 | 66 | 45 | 27 | 32 | 38 |
| 25 | 41 | 87 | 49 | 51 | 52 | 82 | 107 | 110 |
| 26 | 64 | 80 | 71 | 42 | 53 | 26 | 111 | 24 |
| 27 | 111 | 52 | 85 | 52 | 34 | 4 | 26 | 107 |
| 28 | 100 | 15 | 87 | 45 | 23 | 44 | 92 | 53 |
| 29 | 63 | 71 | 23 | 70 | 4 | 25 | 64 | 37 |
| 30 | 105 | 68 | 28 | 43 | 17 | 46 | 53 | 9 |
| 31 | 23 | 40 | 46 | 38 | 48 | 47 | 37 | 111 |

**Table A-10: The values of $I_{M_i-S_{N_d}}$**

| | $I_{M_1-S_{N_d}}$ | $I_{M_2-S_{N_d}}$ | $I_{M_3-S_{N_d}}$ | $I_{M_4-S_{N_d}}$ | $I_{M_5-S_{N_d}}$ | $I_{M_6-S_{N_d}}$ | $I_{M_7-S_{N_d}}$ | $I_{M_8-S_{N_d}}$ |
|---|---|---|---|---|---|---|---|---|
| $S_1$ | 0.365664 | 0.365664 | 0.372984 | 0.372984 | 0.320151 | 0.365315 | 0.320151 | 0.355981 |
| $S_2$ | 0.296889 | 0.354686 | 0.33396 | 0.33396 | 0.320151 | 0.351683 | 0.287703 | 0.287703 |
| $S_3$ | 0.28072 | 0.350464 | 0.323854 | 0.309561 | 0.295542 | 0.28617 | 0.267821 | 0.267821 |
| $S_4$ | 0.269681 | 0.335602 | 0.299608 | 0.299608 | 0.278132 | 0.282984 | 0.242584 | 0.242584 |
| $S_5$ | 0.26026 | 0.33008 | 0.28797 | 0.272466 | 0.246632 | 0.280267 | 0.229048 | 0.23075 |
| $S_6$ | 0.257938 | 0.30649 | 0.259114 | 0.271838 | 0.245026 | 0.277891 | 0.209389 | 0.195283 |
| $S_7$ | 0.229833 | 0.303711 | 0.243409 | 0.269088 | 0.24184 | 0.277891 | 0.178612 | 0.178612 |
| $S_8$ | 0.185295 | 0.300553 | 0.214945 | 0.26861 | 0.239208 | 0.255378 | 0.152806 | 0.144269 |
| $S_9$ | 0.173912 | 0.297501 | 0.213021 | 0.251007 | 0.225771 | 0.2453 | 0.148612 | 0.140075 |
| $S_{10}$ | 0.169234 | 0.295024 | 0.212634 | 0.244552 | 0.220402 | 0.22938 | 0.124897 | 0.12163 |
| $S_{11}$ | 0.164886 | 0.291123 | 0.184614 | 0.244552 | 0.192287 | 0.22938 | 0.123082 | 0.120082 |
| $S_{12}$ | 0.160692 | 0.287616 | 0.158596 | 0.243512 | 0.188699 | 0.216025 | 0.111731 | 0.118898 |
| $S_{13}$ | 0.156736 | 0.283984 | 0.148431 | 0.243512 | 0.188699 | 0.216025 | 0.110626 | 0.098241 |
| $S_{14}$ | 0.130918 | 0.273453 | 0.14451 | 0.241275 | 0.167765 | 0.209558 | 0.108033 | 0.09761 |
| $S_{15}$ | 0.129813 | 0.261616 | 0.135389 | 0.230733 | 0.154102 | 0.207028 | 0.092239 | 0.096505 |
| $S_{16}$ | 0.115304 | 0.247542 | 0.107211 | 0.230733 | 0.153856 | 0.202341 | 0.091134 | 0.087505 |
| $S_{17}$ | 0.09573 | 0.244249 | 0.065068 | 0.225971 | 0.149309 | 0.1956 | 0.078181 | 0.080419 |
| $S_{18}$ | 0.095352 | 0.217873 | 0.063721 | 0.225246 | 0.138394 | 0.172136 | 0.074225 | 0.075906 |
| $S_{19}$ | 0.089573 | 0.209158 | 0.06208 | 0.223899 | 0.138394 | 0.152781 | 0.072975 | 0.073277 |
| $S_{20}$ | 0.088161 | 0.208717 | 0.061708 | 0.219347 | 0.122286 | 0.149759 | 0.068462 | 0.068179 |
| $S_{21}$ | 0.085161 | 0.2046 | 0.059001 | 0.219347 | 0.12183 | 0.141834 | 0.065861 | 0.064223 |
| $S_{22}$ | 0.084488 | 0.200665 | 0.055578 | 0.219347 | 0.118626 | 0.139085 | 0.057436 | 0.063373 |
| $S_{23}$ | 0.083238 | 0.200665 | 0.052417 | 0.219347 | 0.116993 | 0.133287 | 0.054807 | 0.053209 |
| $S_{24}$ | 0.083238 | 0.17109 | 0.049494 | 0.207518 | 0.116468 | 0.123701 | 0.053958 | 0.047491 |
| $S_{25}$ | 0.065043 | 0.166935 | 0.049038 | 0.203192 | 0.113684 | 0.111899 | 0.053603 | 0.046241 |
| $S_{26}$ | 0.064324 | 0.166935 | 0.044303 | 0.20296 | 0.111038 | 0.107878 | 0.052612 | 0.045005 |
| $S_{27}$ | 0.063333 | 0.166703 | 0.041674 | 0.198808 | 0.106203 | 0.079522 | 0.050104 | 0.044651 |
| $S_{28}$ | 0.063004 | 0.166703 | 0.040692 | 0.198808 | 0.103499 | 0.075328 | 0.048498 | 0.043099 |
| $S_{29}$ | 0.062476 | 0.165566 | 0.040692 | 0.198808 | 0.09203 | 0.074143 | 0.047779 | 0.042232 |
| $S_{30}$ | 0.062476 | 0.140075 | 0.040272 | 0.198808 | 0.090133 | 0.071503 | 0.045821 | 0.040264 |
| $S_{31}$ | 0.062476 | 0.136526 | 0.038973 | 0.184528 | 0.089754 | 0.070485 | 0.042266 | 0.039273 |

**Table A-11: The values of $D_{M_i - S_{N_d}}$**

| | $D_{M_1-S_{N_d}}$ | $D_{M_2-S_{N_d}}$ | $D_{M_3-S_{N_d}}$ | $D_{M_4-S_{N_d}}$ | $D_{M_5-S_{N_d}}$ | $D_{M_6-S_{N_d}}$ | $D_{M_7-S_{N_d}}$ | $D_{M_8-S_{N_d}}$ |
|---|---|---|---|---|---|---|---|---|
| $S_1$ | 0.024929 | 0.024929 | 0.017609 | 0.017609 | 0.070441 | 0.025278 | 0.070441 | 0.034612 |
| $S_2$ | 0.093703 | 0.035906 | 0.056633 | 0.056633 | 0.070441 | 0.03891 | 0.102889 | 0.102889 |
| $S_3$ | 0.109873 | 0.040128 | 0.066739 | 0.081032 | 0.095051 | 0.104423 | 0.122772 | 0.122772 |
| $S_4$ | 0.120912 | 0.054991 | 0.090985 | 0.090985 | 0.112461 | 0.107609 | 0.148009 | 0.148009 |
| $S_5$ | 0.130333 | 0.060513 | 0.102623 | 0.118127 | 0.143961 | 0.110326 | 0.161544 | 0.159843 |
| $S_6$ | 0.132655 | 0.084103 | 0.131478 | 0.118755 | 0.145567 | 0.112702 | 0.181204 | 0.19531 |
| $S_7$ | 0.16076 | 0.086882 | 0.147184 | 0.121505 | 0.148753 | 0.112702 | 0.211981 | 0.211981 |
| $S_8$ | 0.205298 | 0.09004 | 0.175648 | 0.121982 | 0.151385 | 0.135215 | 0.237787 | 0.246324 |
| $S_9$ | 0.21668 | 0.093091 | 0.177572 | 0.139586 | 0.164822 | 0.145293 | 0.241981 | 0.250518 |
| $S_{10}$ | 0.221359 | 0.095569 | 0.177958 | 0.146041 | 0.170191 | 0.161213 | 0.265695 | 0.268963 |
| $S_{11}$ | 0.225707 | 0.09947 | 0.205979 | 0.146041 | 0.198306 | 0.161213 | 0.267511 | 0.270511 |
| $S_{12}$ | 0.229901 | 0.102977 | 0.231997 | 0.147081 | 0.201894 | 0.174567 | 0.278862 | 0.271695 |
| $S_{13}$ | 0.233856 | 0.106608 | 0.242161 | 0.147081 | 0.201894 | 0.174567 | 0.279966 | 0.292352 |
| $S_{14}$ | 0.259675 | 0.11714 | 0.246083 | 0.149318 | 0.222828 | 0.181035 | 0.28256 | 0.292983 |
| $S_{15}$ | 0.260779 | 0.128977 | 0.255204 | 0.159859 | 0.236491 | 0.183565 | 0.298354 | 0.294087 |
| $S_{16}$ | 0.275288 | 0.14305 | 0.283381 | 0.159859 | 0.236737 | 0.188252 | 0.299459 | 0.303088 |
| $S_{17}$ | 0.294863 | 0.146344 | 0.325525 | 0.164622 | 0.241284 | 0.194992 | 0.312412 | 0.310173 |
| $S_{18}$ | 0.295241 | 0.172719 | 0.326872 | 0.165346 | 0.252199 | 0.218457 | 0.316368 | 0.314686 |
| $S_{19}$ | 0.30102 | 0.181435 | 0.328513 | 0.166694 | 0.252199 | 0.237812 | 0.317618 | 0.317315 |
| $S_{20}$ | 0.302432 | 0.181876 | 0.328885 | 0.171246 | 0.268307 | 0.240834 | 0.322131 | 0.322414 |
| $S_{21}$ | 0.305431 | 0.185993 | 0.331592 | 0.171246 | 0.268763 | 0.248759 | 0.324732 | 0.32637 |
| $S_{22}$ | 0.306105 | 0.189928 | 0.335014 | 0.171246 | 0.271967 | 0.251508 | 0.333157 | 0.327219 |
| $S_{23}$ | 0.307355 | 0.189928 | 0.338176 | 0.171246 | 0.273599 | 0.257305 | 0.335786 | 0.337384 |
| $S_{24}$ | 0.307355 | 0.219503 | 0.341099 | 0.183075 | 0.274125 | 0.266892 | 0.336635 | 0.343102 |
| $S_{25}$ | 0.32555 | 0.223658 | 0.341554 | 0.187401 | 0.276909 | 0.278694 | 0.336989 | 0.344352 |
| $S_{26}$ | 0.326268 | 0.223658 | 0.34629 | 0.187633 | 0.279555 | 0.282714 | 0.337981 | 0.345588 |
| $S_{27}$ | 0.32726 | 0.22389 | 0.348919 | 0.191785 | 0.284389 | 0.311071 | 0.340489 | 0.345942 |
| $S_{28}$ | 0.327589 | 0.22389 | 0.3499 | 0.191785 | 0.287094 | 0.315265 | 0.342095 | 0.347494 |
| $S_{29}$ | 0.328117 | 0.225027 | 0.3499 | 0.191785 | 0.298563 | 0.31645 | 0.342813 | 0.34836 |
| $S_{30}$ | 0.328117 | 0.250518 | 0.350321 | 0.191785 | 0.300459 | 0.31909 | 0.344772 | 0.350328 |
| $S_{31}$ | 0.328117 | 0.254067 | 0.35162 | 0.206065 | 0.300839 | 0.320107 | 0.348327 | 0.351319 |

**Table A-12: The values of separation distance from each node to every positive ideal solution**

| ID | $s_{ID}^{+}$ | ID | $s_{ID}^{+}$ | ID | $s_{ID}^{+}$ | ID | $s_{ID}^{+}$ |
|---|---|---|---|---|---|---|---|
| 1 | 0.108213504 | 32 | 0.267554286 | 63 | 0.27614541 | 94 | 0.299723602 |
| 2 | 0.145440905 | 33 | 0.256248189 | 64 | 0.255088865 | 95 | 0.315869987 |
| 3 | 0.299602325 | 34 | 0.179621607 | 65 | 0.307331245 | 96 | 0.334847378 |
| 4 | 0.151734935 | 35 | 0.201955864 | 66 | 0.213724862 | 97 | 0.310933705 |
| 5 | 0.298265457 | 36 | 0.288310462 | 67 | 0.286711204 | 98 | 0.308185062 |
| 6 | 0.270274011 | 37 | 0.249950344 | 68 | 0.289695607 | 99 | 0.331775639 |
| 7 | 0.31960366 | 38 | 0.238572929 | 69 | 0.283108299 | 100 | 0.271123898 |
| 8 | 0.324183965 | 39 | 0.299832966 | 70 | 0.316479022 | 101 | 0.332660096 |
| 9 | 0.252184624 | 40 | 0.236916333 | 71 | 0.231068351 | 102 | 0.21163983 |
| 10 | 0.317217622 | 41 | 0.176791292 | 72 | 0.296876963 | 103 | 0.108704544 |
| 11 | 0.317348558 | 42 | 0.288349397 | 73 | 0.308807102 | 104 | 0.193175191 |
| 12 | 0.329039188 | 43 | 0.301608718 | 74 | 0.328027737 | 105 | 0.272484997 |
| 13 | 0.30549264 | 44 | 0.25806816 | 75 | 0.287086593 | 106 | 0.29169346 |
| 14 | 0.284255097 | 45 | 0.295517717 | 76 | 0.296674269 | 107 | 0.226832899 |
| 15 | 0.299905997 | 46 | 0.274904935 | 77 | 0.277115114 | 108 | 0.227983905 |
| 16 | 0.265065795 | 47 | 0.279281483 | 78 | 0.287595223 | 109 | 0.245647853 |
| 17 | 0.304622864 | 48 | 0.282191483 | 79 | 0.295845351 | 110 | 0.256085461 |
| 18 | 0.190073169 | 49 | 0.282961485 | 80 | 0.299178122 | 111 | 0.265280873 |
| 19 | 0.295717591 | 50 | 0.247268247 | 81 | 0.303447006 | 112 | 0.273485818 |
| 20 | 0.331461419 | 51 | 0.282465921 | 82 | 0.210268857 | 113 | 0.28055756 |
| 21 | 0.288114321 | 52 | 0.246244841 | 83 | 0.305301927 | 114 | 0.290628182 |
| 22 | 0.192360489 | 53 | 0.244166406 | 84 | 0.297176084 | 115 | 0.302994001 |
| 23 | 0.260764594 | 54 | 0.282714947 | 85 | 0.237212553 | 116 | 0.314364786 |
| 24 | 0.223868586 | 55 | 0.300539936 | 86 | 0.294873802 | 117 | 0.333710573 |
| 25 | 0.29663808 | 56 | 0.302791838 | 87 | 0.276197726 | 118 | 0.291993805 |
| 26 | 0.210247032 | 57 | 0.319996366 | 88 | 0.328785229 | 119 | 0.305932002 |
| 27 | 0.204451371 | 58 | 0.335766442 | 89 | 0.252955 | 120 | 0.318774592 |
| 28 | 0.253884768 | 59 | 0.27207728 | 90 | 0.284711381 | 121 | 0.334544041 |
| 29 | 0.280430511 | 60 | 0.282615412 | 91 | 0.171986294 | | |
| 30 | 0.279357469 | 61 | 0.289282786 | 92 | 0.229550376 | | |
| 31 | 0.275313629 | 62 | 0.287413648 | 93 | 0.311391488 | | |

**Table A-13: The values of separation distance from each node to every negative ideal solution**

| ID | $S_{ID}^{-}$ | ID | $S_{ID}^{-}$ | ID | $S_{ID}^{-}$ | ID | $S_{ID}^{-}$ |
|---|---|---|---|---|---|---|---|
| 1 | 0.276028829 | 32 | 0.092209227 | 63 | 0.076780158 | 94 | 0.042621602 |
| 2 | 0.227086898 | 33 | 0.110875798 | 64 | 0.098536578 | 95 | 0.025732784 |
| 3 | 0.059801817 | 34 | 0.2204721 | 65 | 0.045011741 | 96 | 0.006408887 |
| 4 | 0.268161158 | 35 | 0.163534173 | 66 | 0.142468983 | 97 | 0.031069753 |
| 5 | 0.051925145 | 36 | 0.069169476 | 67 | 0.062081674 | 98 | 0.036760734 |
| 6 | 0.082853747 | 37 | 0.101901445 | 68 | 0.058932055 | 99 | 0.012792719 |
| 7 | 0.03007394 | 38 | 0.117929823 | 69 | 0.066725738 | 100 | 0.07933817 |
| 8 | 0.024402629 | 39 | 0.064334416 | 70 | 0.034206655 | 101 | 0.010541316 |
| 9 | 0.098850145 | 40 | 0.118327522 | 71 | 0.123274546 | 102 | 0.137531195 |
| 10 | 0.031460599 | 41 | 0.197217403 | 72 | 0.047606555 | 103 | 0.300651253 |
| 11 | 0.027556325 | 42 | 0.0650409 | 73 | 0.034012528 | 104 | 0.162131496 |
| 12 | 0.019395371 | 43 | 0.050185117 | 74 | 0.02148031 | 105 | 0.077270074 |
| 13 | 0.050132782 | 44 | 0.096807792 | 75 | 0.074204233 | 106 | 0.097987674 |
| 14 | 0.065335787 | 45 | 0.064802457 | 76 | 0.054596312 | 107 | 0.134209981 |
| 15 | 0.041714353 | 46 | 0.075186885 | 77 | 0.071839912 | 108 | 0.138503512 |
| 16 | 0.107981157 | 47 | 0.070855819 | 78 | 0.059216946 | 109 | 0.118695241 |
| 17 | 0.045692801 | 48 | 0.067961927 | 79 | 0.049587004 | 110 | 0.102994789 |
| 18 | 0.1588131 | 49 | 0.07809909 | 80 | 0.048074448 | 111 | 0.089619223 |
| 19 | 0.058185925 | 50 | 0.122268853 | 81 | 0.043930898 | 112 | 0.077755626 |
| 20 | 0.011372634 | 51 | 0.069224 | 82 | 0.160709169 | 113 | 0.067840934 |
| 21 | 0.066315585 | 52 | 0.105066662 | 83 | 0.046113149 | 114 | 0.055084689 |
| 22 | 0.176635329 | 53 | 0.107378918 | 84 | 0.056035816 | 115 | 0.040485542 |
| 23 | 0.090885206 | 54 | 0.066465757 | 85 | 0.113596046 | 116 | 0.028385944 |
| 24 | 0.148725359 | 55 | 0.044700136 | 86 | 0.055646997 | 117 | 0.010561391 |
| 25 | 0.058002619 | 56 | 0.039267966 | 87 | 0.073915544 | 118 | 0.05434171 |
| 26 | 0.149770933 | 57 | 0.022199779 | 88 | 0.01905407 | 119 | 0.037459302 |
| 27 | 0.151523661 | 58 | 0.004538251 | 89 | 0.097398492 | 120 | 0.023871974 |
| 28 | 0.096867014 | 59 | 0.078203829 | 90 | 0.060296692 | 121 | 0.008756918 |
| 29 | 0.070710441 | 60 | 0.06712183 | 91 | 0.197273316 | | |
| 30 | 0.072829656 | 61 | 0.060014413 | 92 | 0.159599216 | | |
| 31 | 0.079696162 | 62 | 0.062971211 | 93 | 0.044675869 | | |

**Table A-14: The results according to TOPSIS-based aggregation measure**

| ID | TOPSIS-based Measure | ID | TOPSIS-based Measure | ID | TOPSIS-based Measure | ID | TOPSIS-based Measure |
|---|---|---|---|---|---|---|---|
| 1 | 0.718371729 | 32 | 0.25630511 | 63 | 0.217553403 | 94 | 0.124498903 |
| 2 | 0.609583757 | 33 | 0.30201186 | 64 | 0.278646743 | 95 | 0.075329553 |
| 3 | 0.166391563 | 34 | 0.551051157 | 65 | 0.127749785 | 96 | 0.018780275 |
| 4 | 0.638636945 | 35 | 0.447438114 | 66 | 0.399975982 | 97 | 0.090846314 |
| 5 | 0.148276808 | 36 | 0.19349191 | 67 | 0.177990086 | 98 | 0.106569596 |
| 6 | 0.234628248 | 37 | 0.289614685 | 68 | 0.169040101 | 99 | 0.037126795 |
| 7 | 0.086004766 | 38 | 0.330796389 | 69 | 0.19073541 | 100 | 0.226381618 |
| 8 | 0.070004497 | 39 | 0.176661665 | 70 | 0.097542206 | 101 | 0.030714663 |
| 9 | 0.28159645 | 40 | 0.33308816 | 71 | 0.347896196 | 102 | 0.393879173 |
| 10 | 0.090228174 | 41 | 0.527307 | 72 | 0.138196903 | 103 | 0.734449727 |
| 11 | 0.079895434 | 42 | 0.184048348 | 73 | 0.099214061 | 104 | 0.456314227 |
| 12 | 0.055664315 | 43 | 0.142654908 | 74 | 0.061458698 | 105 | 0.220926244 |
| 13 | 0.140970749 | 44 | 0.272793329 | 75 | 0.205386429 | 106 | 0.251456037 |
| 14 | 0.186892135 | 45 | 0.179846874 | 76 | 0.155425233 | 107 | 0.371728646 |
| 15 | 0.122107342 | 46 | 0.214763329 | 77 | 0.205871551 | 108 | 0.377921603 |
| 16 | 0.289457282 | 47 | 0.20236581 | 78 | 0.170746449 | 109 | 0.325778758 |
| 17 | 0.130433221 | 48 | 0.194091861 | 79 | 0.143550548 | 110 | 0.286829446 |
| 18 | 0.455200202 | 49 | 0.216304675 | 80 | 0.138442311 | 111 | 0.252519581 |
| 19 | 0.164411831 | 50 | 0.330870305 | 81 | 0.126464285 | 112 | 0.221373723 |
| 20 | 0.033172416 | 51 | 0.196832482 | 82 | 0.433204011 | 113 | 0.194722237 |
| 21 | 0.187104937 | 52 | 0.299069802 | 83 | 0.131221317 | 114 | 0.15933653 |
| 22 | 0.478691954 | 53 | 0.30544829 | 84 | 0.158646456 | 115 | 0.117868859 |
| 23 | 0.258453741 | 54 | 0.190347738 | 85 | 0.323812034 | 116 | 0.08281804 |
| 24 | 0.39916204 | 55 | 0.129475515 | 86 | 0.158755193 | 117 | 0.030677464 |
| 25 | 0.163553194 | 56 | 0.11479854 | 87 | 0.211118944 | 118 | 0.156904815 |
| 26 | 0.416009609 | 57 | 0.064874428 | 88 | 0.054778371 | 119 | 0.109086344 |
| 27 | 0.425658115 | 58 | 0.013335847 | 89 | 0.278000631 | 120 | 0.06966938 |
| 28 | 0.276169698 | 59 | 0.223260197 | 90 | 0.17476893 | 121 | 0.025507993 |
| 29 | 0.201373382 | 60 | 0.19192074 | 91 | 0.534240169 | | |
| 30 | 0.2067925 | 61 | 0.171814756 | 92 | 0.410123045 | | |
| 31 | 0.224490039 | 62 | 0.179720127 | 93 | 0.125470275 | | |

**Table A-15(a): Node ID versus corresponding station name**

| ID | Station name | ID | Station name |
|---|---|---|---|
| 1 | Frankfurt(Main)Hbf | 32 | Lippstadt |
| 2 | Frankfurt(M) Flughafen Fernbf | 33 | Soest |
| 3 | Darmstadt Hbf | 34 | Hamm(Westf) |
| 4 | Mannheim Hbf | 35 | Dortmund Hbf |
| 5 | Neustadt(Weinstr)Hbf | 36 | Bochum Hbf |
| 6 | Kaiserslautern Hbf | 37 | Essen Hbf |
| 7 | Homburg(Saar)Hbf | 38 | Duisburg Hbf |
| 8 | Saarbrücken Hbf | 39 | Oberhausen Hbf |
| 9 | Karlsruhe Hbf | 40 | Düsseldorf Hbf |
| 10 | Baden-Baden | 41 | Köln Hbf |
| 11 | Offenburg | 42 | Bonn Hbf |
| 12 | Freiburg(Breisgau) Hbf | 43 | Koblenz Hbf |
| 13 | Heidelberg Hbf | 44 | Mainz Hbf |
| 14 | Stuttgart Hbf | 45 | Wiesbaden Hbf |
| 15 | Ulm Hbf | 46 | Limburg süd |
| 16 | Augsburg Hbf | 47 | Montabaur |
| 17 | München-Pasing | 48 | Siegburg/Bonn |
| 18 | München Hbf | 49 | Köln/Bonn Flughafen |
| 19 | München Ost | 50 | Köln Messe/Deutz Gl.11-12 |
| 20 | Rosenheim | 51 | Solingen Hbf |
| 21 | Ingolstadt Hbf | 52 | Wuppertal Hbf |
| 22 | Nürnberg Hbf | 53 | Hagen Hbf |
| 23 | Hanau Hbf | 54 | Münster(westf)Hbf |
| 24 | Würzburg Hbf | 55 | Osnabrück Hbf |
| 25 | Aschaffenburg Hbf | 56 | Regensburg Hbf |
| 26 | Fulda | 57 | Plattling |
| 27 | Kassel-Wilhelmshöhe | 58 | Passau Hbf |
| 28 | Göttingen | 59 | Erlangen |
| 29 | Warburg(Westf) | 60 | Bamberg |
| 30 | Altenbeken | 61 | Lichtenfels |
| 31 | Paderborn Hbf | 62 | Saalfeld |

**Table A-15(b): Node ID versus corresponding station name**

| ID | Station name | ID | Station name |
|---|---|---|---|
| 63 | Jena Paradies | 94 | Lübeck Hbf |
| 64 | Naumburg(Saale)Hbf | 95 | Oldenburg(Holst) |
| 65 | Frankfurt(Main)süd | 96 | Puttgarden |
| 66 | Erfurt Hbf | 97 | Neumünster |
| 67 | Gotha | 98 | Garmisch-Partenkirchen |
| 68 | Eisenach | 99 | Mittenwald |
| 69 | Bad Hersfeld | 100 | Bitterfeld |
| 70 | Aachen Hbf | 101 | Kiel Hbf |
| 71 | Leipzig Hbf | 102 | Berlin-Spandau |
| 72 | Riesa | 103 | Berlin Hbf |
| 73 | Dresden-Neustadt | 104 | Berlin Südkreuz |
| 74 | Dresden Hbf | 105 | Lutherstadt Wittenberg |
| 75 | Düsseldorf Flughafen | 106 | Berlin Ostbahnhof |
| 76 | Halle(Saale)Hbf | 107 | Berlin Gesundbrunnen |
| 77 | Tutzing | 108 | Eberswalde Hbf |
| 78 | Murnau | 109 | Angermünde |
| 79 | Oberau | 110 | Prenzlau |
| 80 | Braunschweig Hbf | 111 | Pasewalk |
| 81 | Hildesheim Hbf | 112 | Anklam |
| 82 | Hannover Hbf | 113 | Züssow |
| 83 | Minden(Westf) | 114 | Greifswald |
| 84 | Herford | 115 | Stralsund Hbf |
| 85 | Bielefeld Hbf | 116 | Bergen auf Rügen |
| 86 | Gütersloh Hbf | 117 | Ostseebad Binz |
| 87 | Bremen Hbf | 118 | Neustrelitz Hbf |
| 88 | Oldenburg(Oldb) | 119 | Waren(Müritz) |
| 89 | Wolfsburg Hbf | 120 | Rostock Hbf |
| 90 | Hamburg-Harburg | 121 | Warnemünde Werft |
| 91 | Hamburg Hbf | | |
| 92 | Hamburg Dammtor | | |
| 93 | Hamburg-Altona | | |

# - INDEX -

# Index

# ERKLÄRUNG

Hiermit versichere ich, dass ich die vorliegende Dissertation selbstständig angefertigt habe. Die aus fremden Quellen und Hilfsmitteln direkt oder indirekt übernommenen Gedanken und Zitate sind als solche kenntlich gemacht. Es wurden keine anderen als die in der Dissertation angegebenen Quellen und Hilfsmittel benutzt. Diese Dissertation wurde weder einer anderen Prüfungsbehörde vorgelegt noch veröffentlicht. Eine Veröffentlichung vor Abschluss des Promotionsverfahrens werde ich nicht vornehmen. Die Bestimmungen der Promotionsordnung sind mir bekannt. Die vorgelegte Dissertation ist von Professor Dr. Stefan Wolfgang Pickl betreut worden.

Neubiberg, den 26. Mai 2021

……..

(Unterschrift)