International Journal of Critical Infrastructure Protection 29 (2020) 100353

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Using a random road graph model to understand road networks robustness to link failures

Philippe Y.R. Sohouenou[a,b,c,*], Panayotis Christidis[c], Aris Christodoulou[c], Luis A.C. Neves[a], Davide Lo Presti[b]

[a] Resilience Engineering Research Group, Faculty of Engineering, The University of Nottingham, Nottingham, UK
[b] Nottingham Transportation Engineering Centre, Faculty of Engineering, The University of Nottingham, Nottingham, UK
[c] European Commission, Joint Research Centre (JRC), Directorate for Energy, Transport and Climate, Sevilla, Spain

ARTICLE INFO

Article history:
Received 5 November 2019
Revised 1 February 2020
Accepted 7 March 2020
Available online 29 April 2020

Keywords:
Random road network
Network robustness
Resilience assessment
Link criticality
Targeted attacks
Graph theory

ABSTRACT

Disruptions to the transport system have a greater impact on society and the economy now than ever before due to the increased interconnectivity and interdependency of the economic sectors. The ability of transport systems to maintain functionality despite various disturbances (i.e. robustness) is hence of tremendous importance and has been the focus of research seeking to support transport planning, design and management. These approaches and findings may nevertheless be only valid for the specific networks studied. The present study attempts to find universal insights into road networks robustness by exploring the correlation between different network attributes and network robustness to single, multiple, random and targeted link failures. For this purpose, the common properties of road graphs were identified through a literature review. On this basis, the GREREC model was developed to randomly generate a variety of abstract networks presenting the topological and operational characteristics of real-road networks, on which a robustness analysis was performed. This analysis quantifies the difference between the link criticality rankings when only single-link failures are considered as opposed to when multiple-link failures are considered and the difference between the impact of targeted and random attacks. The influence of the network attributes on the network robustness and on these two differences is shown and discussed. Finally, this analysis is also performed on a set of real road networks to validate the results obtained with the artificial networks.

1. Introduction

Transport systems are subject to recurrent disruptions caused by accidents, extreme weather conditions and infrastructure failures. Considering the increased interconnectivity and interdependency of the economic sectors, the unavailability of a small fraction of a transport network can lead to major consequences for society and the economy. For instance, the collapse of the I-35W Bridge in Minneapolis (USA) resulted in economic losses of US$71,000 to US$220,000 a day [1].

Consequently, the robustness of road networks (i.e. their ability to withstand a given level of stress without suffering degradation or loss of functionality) is of tremendous importance and has been the focus of research seeking to support transport planning, design and management. Numerous approaches were developed to measure and study transport systems robustness including [2–4]. Although these approaches and case studies provide interesting conclusions some of their findings may only be valid for the specific networks studied. Further investigations are thus required to evaluate the effectiveness of these approaches and the generality of their findings.

A major concern in robustness analyses is the identification of the most critical elements (set of road segments or intersections whose failure would result in the highest impacts on the entire system) in a network. The rationale for such studies is that the most critical elements should be given top priority for reinforcement to enhance the system pre-event robustness but also for post-event restoration. To identify the critical links, [5] proposed an approach based on single-link-failures (SLFs) where each link is removed from the network and the corresponding effect on the network performance estimated. The levels of impact are then ranked and the links demonstrating the most significant impacts considered to be the most critical. However, this approach

* Corresponding author.
E-mail address: philippe.sohouenou@nottingham.ac.uk (P.Y.R. Sohouenou).

https://doi.org/10.1016/j.ijcip.2020.100353

disregards multiple-link failures (MLFs). [3] showed that the most critical links when MLFs occur are not simply the combination of the most critical links with SLF. Their study was however limited to two different networks of up to 24 nodes. Hence, it remains unclear how the most critical links can be identified considering multiple-link failures, how different are the criticality rankings when only SLFs are considered as opposed to when MLFs are considered and how sensitive are these results to different network characteristics.

Another growing concern in robustness analyses of road networks is targeted attacks. Studies commonly distinguish between targeted and random failures. The latter model damage to a random set of links (e.g. pavement maintenance, pipe bursting or police incidents amongst others can lead to random road closures) whereas targeted attacks imply a driving force seeking to maximise damage to the network (e.g. the bombing of a critical bridge). As explained in [6], the simple conclusion that a network is more vulnerable to targeted attacks does not provide any novel insights since it is inherent to the definition of both kinds of attacks. A more interesting question is how much more vulnerable a network is to targeted attacks compared to random failures. In other words, the objective is rather to quantify the difference of impacts and subsequently determine if a particular network is well protected against targeted attacks or not.

The present paper aims at answering these questions by performing a robustness analysis on a variety of abstract road networks. These networks result from a model that randomly generates graphs presenting the topological and operational characteristics of real-road networks. This random network model is used because contrary to real maps its characteristics are controllable and allow for a sound sensitivity analysis of network robustness, which in turn can provide practical insights for network planners and operators. This novel approach allows the analysis of a large set of networks resulting in a clearer understanding of the generality of the results and conclusions, which are ultimately validated on a set of real network samples from *OpenStreetMap*

This study has four research objectives: (i) develop a random road network model, (ii) use this model to evaluate the correlation of topological and operational network characteristics with robustness to single, multiple, random and targeted link failures as well as (iii) the correlation between SLF and MLF based link criticality rankings and (iv) validate the results using real road network samples. The paper is organised as follows. Section 2 provides a background on robustness analyses, road network properties and random road graph models. The methodology is described in Section 3, including the random road graph model. The results are presented in Section 4 and discussed in Section 5. Finally, some conclusions and recommendations are provided in Section 6.

2. Background

2.1. Background on road network robustness analyses

2.1.1. Robustness definition and quantification

System robustness is generally defined as the ability to withstand a given level of stress or demand without suffering degradation or loss of function [7]. Robustness is often linked to the concept of resilience as the latter encompasses two parts: the ability to absorb perturbations (robustness) and recover quickly (rapidity). As a result, robustness measures (that don't address rapidity) are sometimes referred to as resilience measures in the literature e.g. [8,9]. These resilience indicators are hence considered as robustness measures in this paper although they are not referred to as is in the references.

There is no consensual indicator for road network robustness either. Some studies measured robustness as the ability to cope with loss in origin-destination pairs connectedness [2], while others focused on the increased travel time (TT). To compare the pre- and post-event situations, some considered the difference of total TT in the pre- and post-loss situations [9,10] while others considered their ratio [8].

2.1.2. Approaches to link criticality assessment

The approach of [5] - that uses single-link failures to identify critical links - has the disadvantage of requiring the computation of a number of traffic simulations equivalent to the number of links in the network studied, which is unrealistic in very large networks e.g. the road network of London has nearly 200,000 links [11]. This approach was however adopted and improved in studies [8,10] that also consider link-capacity reductions rather than complete link removals to model day-to-day disruptions. However, link-capacity reductions add to the - already high - computational cost of this approach since several scenarios need to be computed per link.

Besides, this approach disregards the combined effect of multiple-links failures, which may be problematic as the most critical links when MLFs occur are not always simply the combination of the most critical links with SLF [3]. As MLFs also add to the computational cost of link-criticality studies, there is a need to understand if and when SLFs provide a reasonable approximation of the criticality rankings resulting from MLFs.

2.1.3. Random and targeted attacks modelling

The research community in complex network theory has studied robustness as the changes of some metric of the network functionality against the fraction of removed nodes (or links) to understand how many nodes (links) have to be removed to fragment a network into isolated components [6,12,13]. These studies distinguish between random and targeted attacks, the latter resulting in more rapid and severe robustness losses.

One of the rare applications of this "dismantling process" approach to road networks was proposed by [14]. The authors measured the robustness of self-organised street networks (e.g. Rome) as the fraction of removed nodes leading to a 50% reduction in the size of the largest connected component of the original network. This indicator is however arbitrary (i.e. the 50% limit is not justified) and does not fully capture road network functionality (i.e. the evolution of drivers travel time).

Furthermore, most of these studies conclude that transport networks are less robust to targeted attacks than random ones but do not attempt to quantify the extended impact of targeted attacks [6].

2.2. Background on road network properties

The abstract representation of a transport system as a network of nodes (or vertices) and links (or edges), whether it involves roads, railways or airspace, defines a network topology. In the case of road networks, the most intuitive and popular approach is to model both intersections and dead-ends as nodes and the street segments between them as links. This section surveys the literature to characterise road networks and their graph representations.

2.2.1. Road networks approximate planarity and patterns

An important characteristic of road networks noted in the literature is their approximate planarity [15,16]. Road networks essentially lie in a plane such that when two roads intersect, a link between them is necessarily created. Few exceptions to this rule exist such as elevated highway bridges spanning other roads. [17] investigated the planarity of 50 urban street networks

worldwide. The results show that many road networks can be described as approximately planar. However, the planar simplification can misrepresent intersection densities, street lengths and routing in certain cites that contain a non-negligible number of grade separations (e.g. Moscow).

Several publications [18,19] analysed and classified the patterns of urban road networks. [20] summarised these studies and classified all road networks as grid (four-legged intersections with right angles and parallel lines), warped parallel (straight lines mostly parallel to each other with curved or rectilinear formations and three-legged intersections), mixed (no dominant pattern), loops & lollipops (tree-like structure with cul-de-sacs, branches and three-legged intersections) and sparse (discontinuous and decentralised with a high proportion of cul-de-sacs). As an indication, in [20] all of these patterns could be identified in community areas in Florida's Orange County (USA).

2.2.2. Road network intersections

Network topologies are typically characterised by the distribution of the degree (i.e. number of adjacent links) of their nodes. The studies of [11,21] and [22] evaluating the topology of network samples from 20 cities, London (UK) and Xiamen Island (China) respectively allow characterising the degree distribution in road networks. Undirected graphs representing road networks generally have very few six-or-more road intersections, few five-road intersections, a large number of four-road intersections and a very large number of three-road intersections except in cities presenting a dominant square-grid structure (e.g. San Francisco) where four-street intersections are more frequent than three-street intersections.

These empirical studies show that the number of connections of road intersections is limited as in road networks two distant nodes are less likely to be directly connected due to the distance-dependence of the links travel costs [12]. Hence, although intersections connecting more than six roads exist (e.g. the roundabout at Place Charles de Gaulle in Paris connects 12 streets) they are very rare and can be treated as exceptions.

2.2.3. Road network links

Another important characteristic of road networks noted in [16] is the heterogeneity resulting from road hierarchy (i.e. roads are typically categorised into minor and major local streets, regional roads and highways) that differentiate between functional properties and operational performance of roads, which provide both property access and travel mobility. Local streets mainly serve the land access function while arterial roads (e.g. highways) provide a high level of mobility for through movement.

Road hierarchy results in heterogeneous link travel costs. It is, however, difficult to go beyond this statement and define a general distribution for the link travel costs in road networks because these costs depend on dynamic factors such as the link travel time (which depends on a variety of parameters including the link length, speed limit and traffic conditions). Furthermore, even the distributions of static parameters like the links length present several configurations. [23] found that self-organised cities e.g. Cairo (Egypt) exhibited single-peaked distributions while planned cities e.g. Los Angeles (USA) exhibited multimodal distributions due to their grid pattern. However, [23] did not report any specific distribution. [11] fitted a power-law (with a cut off for the longest streets) to the London street network. The study of [24] that considered 10 European cities showed slightly different results as a power law emerged in the distribution tails but the fitting worsened with decreasing link lengths. They observed that the percentage of streets failing inside the power law region ranged from 4% (Barcelona) to 29% (Lancaster) and suggested that cities may be composed of streets following two distributions.

2.2.4. Summary of road networks properties

Finally, the review of the different studies of real-world road networks topologies and patterns allowed identifying the main properties of road graphs:

- road networks are not universally planar but many road graphs can be approximated as planar;
- road networks include patterns ranging from the regular grid and wrapped parallel structures to the more irregular loops, lollipops and sparse structures;
- road graphs have a negligible proportion of intersections with six or more connections;
- road graphs comprise a large majority of three or four road intersections;
- the functional properties and performance of road links are heterogeneous.

2.3. Background on random road network models

Random road network models were developed for different purposes. [25] used a grid model to evaluate the impact of mobility (e.g. connected vehicles on a freeway) on the performance of routing protocols for ad hoc networks. This model is very regular and doesn't hold many features of real road networks like the heterogeneity in nodal degrees. More sophisticated models for random road network have been proposed by the research community in complex network theory. [26] proposed a planar variant of the classical Erdös–Rényi random graph model (in complex network theory a "random network" refers to a network where each node pair is connected with a fixed probability). [11] built on this basis to propose the Growing Random Planar Graph (GRPG) that seeks to mimic the effect of urban sprawls. Unfortunately, both models tend to generate more high degree nodes (superior to six) than observed in real networks. [27] also notes that the GRPG model results in an unrealistic abundance of acute-angled intersections.

Other works focused on developing models for road networks at a larger scale (e.g. national scale) that hence account for the diversity in road hierarchy. [28] studied the topological and geometric structure of the national road networks of three countries (i.e. Denmark, England and the USA). The study revealed that all journeys from a postal code to another, regardless of their length, have an identical structure. Drivers seeking to optimise their travel time would typically start their journey in a local street close to their point of origin, and progressively move to larger and faster roads (which are higher in the road hierarchy) until they reach the fastest single road between their origin and destination. On this road, they cover as much distance as possible, and then progressively descend to smaller roads until their destination. This finding led [28] to introduce a square-grid fractal model for road placement that reproduces both the observed hierarchical and scale-invariant structure of journeys. Noting that the basic fractal model was too regular to resemble real-road networks, [27] proposed the quadtree model, which employs the fractal model but uses a random tree to distribute the smaller square grids in the network. The drawback of both models is that the degree of the intersections in the networks generated is limited to four.

To overcome the shortcomings of the grid model, [15] developed the Grid model with Random Edges (GRE). The main idea of this model is to randomly introduce the effects of obstacles and shortcuts in the basic grid model. Obstacles (e.g. buildings, parks and rivers) normally make a road network sparser as they prevent certain roads from being built while shortcuts (i.e. diagonal links in the grid) make a road network denser. Using an optimisation algorithm and six parameters (the area length and width, the average lengths of vertical and horizontal lines in the network, a probability controlling the presence of horizontal and vertical lines

to simulate obstacles, and a probability controlling the presence of shortcuts), they fit the model to real road network samples from 66 main cities in Europe and the USA. The topological characteristics (i.e. average nodal degree, average shortest path length and density of nodes and links) of the abstract models and real networks were reasonably correlated especially in the case of the US cities (for which the fitting process was easier since they generally don't have shortcuts).

3. Methods

This section describes the research method adopted. Firstly, the abstract road network model is introduced. The network attributes and the robustness metrics used are then presented, followed by the experimental procedure. Finally, the road network samples used for validation are presented.

3.1. Grid network with Random Edges and Regional Edge Costs (GREREC) model

The model used to generate random road networks is an improvement of the GRE model (Section 2.3) since this model synthesizes most of the topological characteristics of road networks. Four modifications were introduced to the GRE model to better fit the purpose of the present study:

- the removal of the links at the rim of the network is allowed;
- the unconditional removal of vertical and horizontal links is allowed;
- the generation of all types of diagonals (i.e. shortcuts) is possible;
- the geometric lengths of the edges are not considered instead the links are directly assigned a random travel cost depending on the link position in the network.

The first three modifications allow the generation of a larger spectrum of network topologies. To ensure that the graphs generated by the original GRE model are connected (i.e. a path exist between every pair of nodes), the model always keeps the edges at the rim of the area and only allows the removal of a vertical edge if its adjacent bottom left horizontal edge exists. The elimination of these two constraints allows the generation of sparser and more irregular topologies. In addition, keeping the edges at the rim of the area means that for any pair of nodes in the network there is a path connecting them through the network periphery, which may not always be the case in real networks. This assumption may be especially problematic for robustness analyses, which aim at evaluating the consequences of link failures in the network. One implication of these two modifications is however that the graphs generated can be disconnected. An analysis of the connectedness of GREREC model is provided in Appendix A.1.

Besides, the GRE model only generates shortcuts departing form specific nodes to ensure planarity (two diagonals cannot intersect without creating a node). In the present model, the construction of both diagonals was made possible by allowing the construction of one diagonal providing that the other one doesn't exist (see rule 3) and 4) in the procedure below).

The fourth modification increases the flexibility of the model and allows the introduction of road hierarchy effects in the network. To this end, travel-cost values are randomly assigned to the links depending on their origin node. The area around a node hence describes a "region" where roads are likely to present the same characteristics (length, speed limits, etc.). This modification implies that contrary to the original GRE model, the present model doesn't generate geometric grid networks with straight lines. The networks generated have a "grid" topology but their spatial representation may include curved roads to respect the geometric distances between the nodes.

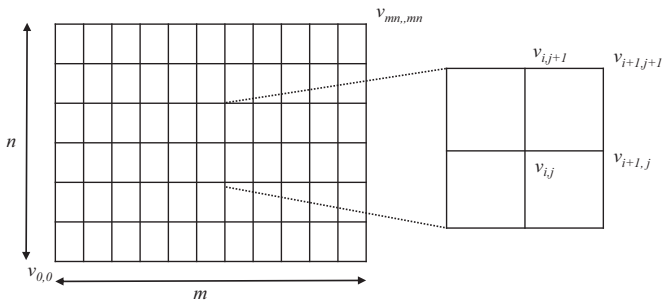


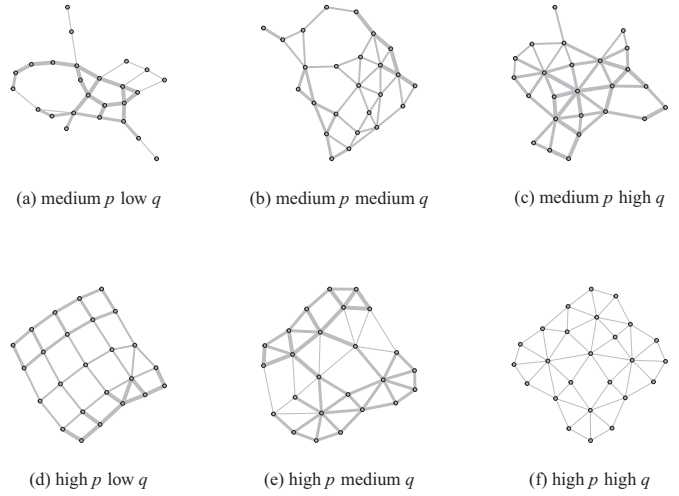
Fig. 1. Grid network used in the procedure to build the GREREC model

This new model is called the Grid network with Random Edges and Regional Edge Costs (GREREC). The procedure used to generate a graph with the GREREC model is described below:

1. Generate a graph with a rectangular grid topology. The dimensions m and n of the rectangle (i.e. the number of nodes per row and columns respectively) are the only parameters necessary to define the grid. The graph generated has $N = mn$ nodes and the vertex on the i-th column and j-th row is denoted as $v_{i,j}$.
2. Check and remove the existing edges by the order "left to right, bottom to top" with probability $(1 - p)$.
3. For each vertex $v_{i,j}$ where both i and j are odd numbers, generate the four diagonal edges departing from $v_{i,j}$ with probability q.
4. For each vertex $v_{i,j}$ where i is an even number (regardless of j), generate the four diagonal edges departing from $v_{i,j}$ with probability q providing that the diagonal is not intersecting an existing one.
5. Randomly assign a travel cost to the edges by the order "left to right, bottom to top" with the following rule: all the links departing from the same node have the same cost of travel.

The grid network model used in the procedure is shown in Fig. 1. The sequences of travel costs assigned to the links in rule 5 were generated as normally distributed random numbers in the discrete interval $[1, \max(n, m)]$ to ensure that the costs diversity was proportional to the network size. In other words, a larger network is more likely to be composed of a more diverse range of road types. Considering the huge variety of link cost distributions observed in real road networks (Section 2.2), the standard normal distribution was arbitrarily adopted to generate random sequences of link costs that at least were unlikely to result in uniform distributions since none of the distributions observed in real road networks was uniform.

The GREREC model hence uses four parameters: m and n (the dimensions of the rectangular grid), p (the probability of keeping horizontal and vertical edges in the grid) and q (the probability of generating shortcuts in the grid) to generate random road graphs. The standard deviation of the link costs in the network can also be used to measure the link cost heterogeneity in the network. Fig. 2 shows examples of graphs generated by the GREREC model. The topologies generated range from relatively sparse and decentralized structures (Fig. 2.a) to very compact structures (Fig. 2.f) but also include the very ordered grid-like structure (Fig. 2.d) and more irregular structures (Fig. 2.b).



(a) medium p low q (b) medium p medium q (c) medium p high q

(d) high p low q (e) high p medium q (f) high p high q

Fig. 2. Examples of graphs generated by the GREREC model depending on p (probability of keeping horizontal and vertical edges) and q (probability of generating shortcuts) - the edge thickness indicates a higher cost of travel ($m = n = 5$)

3.2. Network topological and operational characteristics

3.2.1. Network topological characteristics

To characterise the topology of the graphs generated, five topological measures with potential relevance to network robustness were selected: the network alpha, beta and gamma indices, as well as the average and standard deviation (heterogeneity) of the degree distribution in the network.

The alpha, beta and gamma indices are measures of the connectivity (or density) of planar graphs presented in [29]. The alpha index (α) is the ratio of the number of cycles (i.e. path wherein a node is reachable from itself without using the same link more than once) to the maximum possible number of cycles ($2N - 5$):

$$\alpha = \frac{L - N + \mu}{2N - 5} \tag{1}$$

where L, N and μ are the numbers of links, nodes and sub-graphs in the graph respectively. The case when $\mu = 1$ (the graph is connected) is referred to in [12] as the meshedness coefficient, which varies from zero (tree structures) to one (complete planar graph, which is a triangulation).

The beta index (β) is the ratio between the number of links and the number nodes.

$$\beta = \frac{L}{N} \tag{2}$$

Minimally connected networks (where the links form a cycle) have a beta value close to one while denser networks have a higher β. A network only composed of four-legged intersections with a few outliers (e.g. the grid pattern) would present a value of β close to two. The average degree and β are equivalent in undirected graphs (i.e. $\beta = 2 < Degree >$) since in these graphs the total number of links equals two times the sum of the node degrees [30].

The gamma index (γ) is the ratio of the number of links to the maximum possible number of links in a planar graph $3(N - 2)$:

$$\gamma = \frac{L}{3(N-2)} \tag{3}$$

All of these indices (i.e. α, β, γ) increase with the network connectivity.

3.2.2. Operational characteristics

The main function of road networks is to provide mobility i.e. connect origin-destination (OD) pairs in a timely manner. In the graphs representing road networks, some of the nodes don't serve as origin-destination points. To take this specificity into account, we assumed that the bottom-left ($v_{0,\,0}$) and top-right ($v_{mn,\,mn}$) nodes of the original grid (Fig. 1) were OD points and randomly selected additional OD points in the network with the probability r. When $r = 0$ only these two nodes were considered as OD points, while when $r = 1$ all the nodes in the network served as OD points.

Therefore, besides their topological characteristics, the GREREC networks have two operational characteristics: r_{OD} the ratio between the number of OD points and the number of nodes and h_{lc} the heterogeneity of the link travel costs (standard deviation of the links cost distribution).

3.3. Robustness, link criticality and attack extended impact indicators

3.3.1. Robustness indicator

As explained in Section 2.1.1, there is no consensual indicator for road network robustness. Since the main function of road networks is to connect origin-destination pairs in a timely manner, previous research measured robustness as the increase in total travel time across the network. However, similar total TT values can result from different situations, thus the related indicators may be unable to discriminate between the impacts caused by these situations [31]. Hence, the robustness indicator (RO) adopted in this study focuses on the impact of the disruption on the TT in the OD pairs:

$$RO = \sum_{w} k_w \left(1 + \frac{TT_d^w - TT_0^w}{TT_0^w}\right)^{-1} \tag{4}$$

where w and k_w are an OD pair and the associated weighting factor, respectively. k_w is the ratio between the travel demand on w and the total travel demand. TT_0^w and $TT_d^{(w)}$ are the undisrupted and disrupted travel times respectively. RO has the advantages of being scaled between 0 and 1 and being able to differentiate between the impacts on network performance when few or many OD pairs are disconnected by using a weighted average of the relative change of the TT on the OD pairs [31]. $RO = 100\%$ indicates that despite the disruptive event the TT remains equal to the initial travel time (TT_0^w) on all OD pairs. Then, the robustness indicator decreases as TT_d^w increases, the decrease being more important when highly demanded routes are impacted.

In the present study, a shortest path analysis was used to evaluate the robustness of the networks based on their structure rather than more computationally expensive traffic simulations that also account for capacity constraints. Hence, the OD pairs were considered to be of equal importance (i.e. $k_w = 1/N_{OD}$, N_{OD} being the number of OD pairs) and TT^w is the travel cost on the least-path cost for w.

3.3.2. Criticality indicator

To identify the most critical links with regards to multiple-link-failures, a criticality index was computed for each link depending on the effect of its degradation on the network performance in all of the scenarios considered. In this study, the scenario types considered were single, two (2LF) and three link failures (3LF).

The criticality index (Cr_a) of link a is:

$$Cr_a = \sum_{t} \frac{1}{L_t} \langle 1 - RO_s \rangle_t^a \tag{5}$$

where RO_s is the network robustness to the hazard s as defined in Eq. 4. The notations t and L_t indicate a scenario type (e.g. 2LF) and the number of links damaged by the hazards of this scenario type respectively. In other words, it was assumed that a scenario in which L_t links fail is L_t times less probable than a SLF scenario. Another possible interpretation of this division by L_t is that the

failed links were assumed to equally contribute to the loss of performance. $\langle 1 - RO_s \rangle_t^a$ means that the expression is averaged over the scenarios of the same type t in which a is damaged. The averages per scenario type ensure that the contributions of the different scenario types to the link criticality are in the same range. Indeed, there are more scenarios of multiple-link failures than SLFs i.e. if L is the number of links in the network, there is one, $(L-1)$ and $(L-1)(L-2)$ scenarios of SLF, 2LFs and 3LFs per link, respectively, hence a simple sum would inherently give more importance to multiple-link failures. The links that are not critical to the network performance would have a Cr_a value close to zero as $RO_s \approx 1$ in the hazards where these links fail, while Cr_a increases with the link criticality.

3.3.3. Comparison of the link criticality rankings derived from different scenarios

To compare the rankings derived from the criticality index (Cr_a) when only single-link failures are considered as opposed to when multiple-link failures are considered, Spearman's rank-order correlation coefficient was used. Spearman's and Kendall's coefficients are the most popular indicators to evaluate the correlation of non-parametric measures and have equivalent performances [32]. The choice of Spearman's coefficient has been motivated by the fact that [32] found better results when the data contain ties, which is the case in the present study. This coefficient provides a measure in [-1, 1], where -1 and 1 indicate a very strong negative and positive correlation respectively while zero indicates no correlation.

3.3.4. Measurement of the extended impact of targeted attacks

In this section, an indicator is developed to quantify the difference in impact between random and targeted attacks. The "dismantling process" approach found in complex network theory studies [6,13] is used to develop a single measure of road networks robustness to a mode of attack (e.g. targeted attacks) that doesn't present the arbitrariness of the indicator used in [14] and accounts for the increased TT. This measure is called "cumulative" robustness (CRO_z) and is given by the expression:

$$CRO_z = \frac{1}{L}\int_0^L RO_z(x)dx \tag{6}$$

where z is the attack mode considered and L the total number of links in the network. $RO_z(x)$ is the road network robustness (Eq. 4) when x links failed. As $RO_z(x)$ is scaled between 0 and 1, the division by L also scales CRO_z between 0 and 1. The value obtained can hence be used to compare the robustness of networks of different sizes.

The computation of the network cumulative robustness to targeted attacks requires a sequence of failed links resulting in rapid and severe robustness losses. Criticality-based attacks were excluded because of their computational costs, as these require the analysis of $L!$ SLF scenarios in a network containing L links. Instead, the betweenness centrality (i.e. the number of shortest paths that go through an edge) first introduced by [33] were used to identify important links in the networks. The betweenness centrality of link a is given by:

$$BETW(a) = \sum_{x \neq y} \frac{\sigma_{xy}(a)}{\sigma_{xy}} \tag{7}$$

where σ_{xy} and $\sigma_{xy}(a)$ are the number of shortest paths between the nodes x and y and the number of shortest path between x and y that contain a respectively [34]. The link betweenness can be used as an indicator of the link importance [4] as an edge with a high betweenness score connects many pairs of nodes through the shortest path between them.

In the interactive (or dynamic) betweenness attack, the links with the highest betweenness scores are iteratively removed while the betweenness of the links are recomputed after each removal. Dynamic betweenness attacks hence target potentially highly critical links in each step, making the attack more harmful to the network than attacks based on initial estimations of link importance in the original network. Interactive betweenness attacks were selected to model targeted attacks in this study since they have been reported as the most detrimental attack among different attacks [6,35].

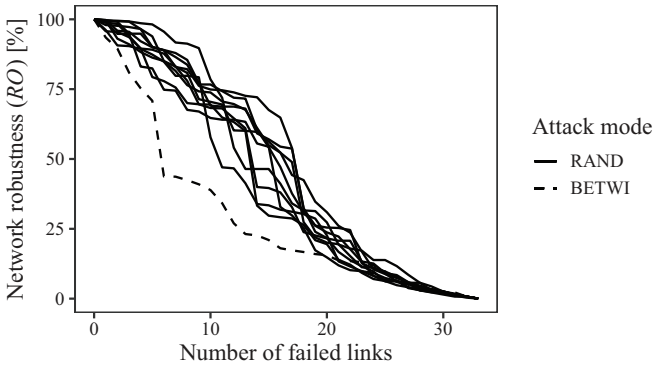


Fig. 3. Comparison of the impact of a targeted attack (BETWI) and 10 random attacks (RAND) on a 33-link GREREC network.

To evaluate the extended impact of targeted attacks in a specific network, the cumulative robustness of the network to an interactive betweenness attack (CRO_{BETWI}) and a representative random attack (CRO_{RAND}) were compared. The latter was obtained by averaging the impact of 1000 random attacks. The extended impact of targeted attacks (TA_{EI}) is defined as the difference between both values:

$$TA_{EI} = CRO_{RAND} - CRO_{BETWI} \tag{8}$$

The concepts described in this section are illustrated in Fig. 3 where CRO_{BETWI} corresponds to the area under the dashed curve and CRO_{RAND} is the mean area under the solid curves.

3.4. Experimental procedure and simulations

To identify the characteristics that influence network robustness to single, multiple, random and targeted link failures in the GREREC model, quasi Monte-Carlo (QMC) simulations were employed to obtain 300 samples that are as different from each other as possible. Contrary to standard Monte-Carlo methods based on pseudo-random numbers, QMC methods use sequences of quasi-random numbers providing values that are better equidistributed in a given volume than pseudo-random numbers [36]. These methods were originally designed for integration but were used here to ensure that the results covered a large parameter space with limited samples and thus save computation time. Sobol's algorithm was adopted as one of the most popular and effective algorithms for generating quasi-random sequences [37].

The parameters values (n, m, p, q, r) were chosen in [2,15] × [2, 15] × [0, 1] × [0, 1] × [0,1] each parameter being uniformly sampled from its interval (n and m were discretely sampled). The values of n and m were limited to 15 for computational cost reasons. As an indication for $n = m = 15$, the basic grid network has 420 links leading to 12,225,940 scenarios of three-link failures to analyse.

For each set of parameter values, the simulations were performed as:

1. Use the parameter values to generate an undirected graph using the GREREC model (Section 3.1)
2. Check whether the graph is connected; if the graph is not connected go to the next iteration.

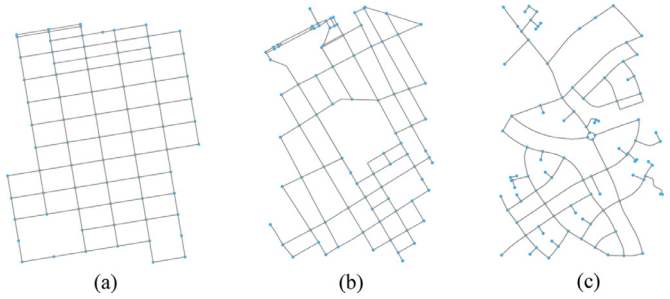


Fig. 4. Examples of road network samples extracted from *OpenStreetMap* and analysed: (a) Pacific Heights, San Francisco, (b) Levallois-Perret, Greater Paris and (c) West Kensington, London

3. Select a random set of OD pairs in the network with probability r.
4. Perform an analysis of the network robustness to single, multiple, random and targeted link failures as well as an analysis of the link criticality rankings correlation.

3.5. Validation using real road maps

To validate the results of the analysis of the GREREC networks, the same analysis was performed on 30 real network samples. These samples were extracted from the road networks of six urban areas around the world: Johannesburg, London, New York, Paris, San Francisco and Seville. Five samples were arbitrarily extracted in each of these areas using bounding boxes defined by latitude and longitude bands of 0.01 width to obtain graphs of the same order of magnitude as the GREREC networks analysed. To acquire the samples, the Python package *OSMnx* [38] was used to download drivable street network data within the chosen boundaries from *OpenStreetMap* and automatically processed into length-weighted nonplanar graphs. In *OpenStreetMap* intersections of two divided roads, small roundabouts and sometimes intersections where opposite streets are not perfectly aligned create clusters of nodes that correspond to single intersections in the real world. Hence, these network samples slightly underestimate the number of high degree intersections. For the sake of reproducibility, it was however decided to keep the existing models unaltered. Fig. 4 shows examples of the graphs analysed.

4. Results

The simulations were performed in **R** 3.4.4 and used the libraries *randtoolbox* and *igraph* for quasi-random number sequence generation and network analysis respectively. The **R** script was run in seven days on the University of Nottingham's high-performance computer, using in parallel twelve compute nodes with 2×20 core processors (Intel Skylake 6138 2.0GHz) and 192GB memory each. The simulations resulted in 161 connected GREREC networks analysed in the following subsections.

4.1. Evaluation of the GREREC networks topology and patterns

The topological indices presented in Section 3.2 were computed to evaluate the topology of the networks generated. Furthermore, the networks were categorised into structural pattern groups based on the division of the values of p and q into three equally spaced intervals (Table 1). As only one connected network was generated with a value of p inferior to 0.33 (low values of p are highly likely to result in disconnected networks), this network was excluded from the structural pattern analysis since it can't support a statistical analysis. The distributions of the nodal degree in each of these structural pattern groups are summarised in Fig. 5.

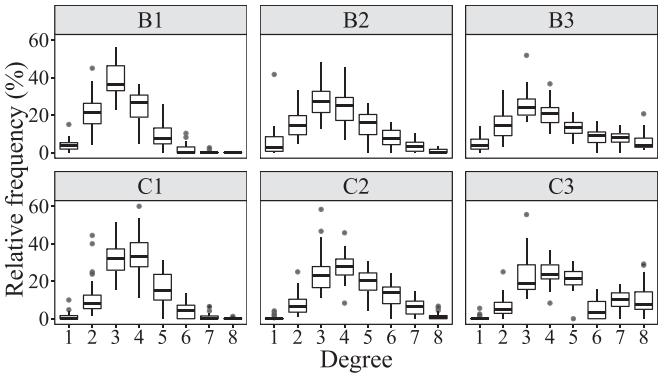


Fig. 5. Nodal degree frequencies in the GREREC network structural pattern groups (box = 25th and 75th percentiles).

Alpha, beta, gamma and the average degree provided the same information as the correlation between these different values ranged from 0.98 to 1. Hence, regardless of the index considered, the two extremes structures are the sparse structures of B1 and the very compact structures of C3 (i.e. lowest and highest connectivity values respectively in Table 1).

The low degree heterogeneity of B1 and C1 (0.98 and 1.02 respectively) suggest that both structures are rather homogeneous compared to the other ones. Indeed, B1 and C1 present a dominant frequency (median superior to 35%) of 3-legged and 3 and 4-legged intersections respectively, whereas the frequency peaks are less pronounced in the other groups (Fig. 5). B1 represents sparse structures with a high proportion of 3-legged intersections that provides some "regularity" to the structure. This group is close to the warped parallel structure in [20]. B2 and B3 represent more organic structures with a mixture of vertical and horizontal links and shortcuts. C1 is the very ordered grid-like structure with a majority of vertical and horizontal links. Finally, C2 and C3 are more compact structures where an increasing proportion of shortcuts are introduced in this grid-like structure.

4.2. Correlation between the network characteristics and robustness metrics in the GREREC networks

To model single and multiple link failures, three types of scenarios were considered: single, two and three-link failures. The robustness indicators of the networks generated in each scenario were computed using Eq. 4. The mean robustness of each network to each type of failures was used as a general measure of the network robustness to this type of failures. The robustness values were also used to compute the link criticality indicators using Eq. 5. SLF, 2LF and 3LF based criticality rankings were compared to the rankings derived from the combination of all of these scenarios (ALL) using Spearman's correlation coefficient. These correlation values evaluate the extent to which SLF (or 2LF, etc.) based criticality measures represent the overall link criticality. The indicators related to the impact of targeted attacks (CRO_{BETWI}, CRO_{RAND} and TA_{EI}) were computed using Eqs. 6 to 8.

All of these robustness metrics were evaluated against three types of network characteristics: the network size (i.e. no. of nodes in the network), topology (i.e. alpha, beta, gamma and the degree distribution) and operational characteristics (i.e. proportion of nodes serving as OD pairs and heterogeneity of the link costs). Spearman's coefficient was used to assess whether a monotonic relationship existed between these variables (Table 2). An analysis of the distributions of the network attributes in the sample analysed is provided in Appendix A.2.

Table 1
Topological characteristics of the GREREC networks generated depending on p (probability of keeping horizontal and vertical edges) and q (probability of generating shortcuts).

Network group	p	q	α	β	γ	$\langle Degree \rangle$	h^{**}_{Degree}
B1	[0.33, 0.66]	[0, 0.33)	0.291(0.11)	1.51(0.26)	0.538(0.066)	3.02(0.53)	0.969(0.32)
B2	[0.33, 0.66]	[0.33, 0.66]	0.446(0.14)	1.82(0.31)	0.637(0.090)	3.64(0.62)	1.413(0.15)
B3	[0.33, 0.66]	(0.66, 1]	0.543(0.11)	2.01(0.24)	0.699(0.068)	4.02(0.48)	1.753(0.20)
C1	(0.66, 1]	[0, 0.33)	0.476(0.09)	1.88(0.21)	0.655(0.058)	3.77(0.41)	1.021(0.19)
C2	(0.66, 1]	[0.33, 0.66]	0.612(0.11)	2.14(0.26)	0.745(0.070)	4.26(0.51)	1.336(0.15)
C3	(0.66, 1]	(0.66, 1]	0.713(0.11)	2.32(0.29)	0.812(0.067)	4.64(0.58)	1.619(0.30)

mean(standard deviation); ** Degree heterogeneity

Table 2
Correlation (R_S) between the network characteristics and robustness metrics in the set of GREREC networks analysed. ^{ns}, *, ** and *** denote the significance at $p > 0.05$, $p < 0.05$, $p < 0.005$ & $p < 0.001$ respectively.

	Network characteristics				
	Network size (N)	Network connectivity (α, β, γ)	Degree heterogeneity	Link costs heterogeneity	Proportion of nodes being OD points
Mean robustness to SLF	0.92***	[0.72, 0.83]***	0.38***	-0.33***	-0.10^{ns}
Mean robustness to 2LF	0.93***	[0.72, 0.83]***	0.38***	-0.33***	-0.10^{ns}
Mean robustness to 3LF	0.93***	[0.72, 0.83]***	0.39***	-0.33***	-0.10^{ns}
SLF vs ALL(1)	0.16*	[-0.04, 0.00]^{ns}	-0.19*	-0.16*	0.86***
2LF vs ALL	0.41***	[0.19, 0.24]*	-0.05^{ns}	-0.16*	0.66***
3LF vs ALL	0.73***	[0.63, 0.71]***	0.45***	-0.26***	-0.35***
Robustness to a BETWI(2)	-0.28***	[0.29, 0.43]***	0.16*	0.06^{ns}	0.20*
Robustness to a RAND(3)	0.20*	[0.78, 0.87]***	0.58***	-0.10^{ns}	0.17*
Targeted attack extended impact	0.59***	[0.68, 0.74]***	0.63***	-0.15^{ns}	-0.00^{ns}

(1) Correlation of the link criticality rankings derived from single (SLF), two (2LF) and three (3LF) link failures, and the combination of all three (ALL); (2) Interactive betweenness attack; (3) Representative random attack

Concerning the network connectivity, the highest correlation value in absolute was systematically obtained with beta (or its equivalent the average degree). β is hence the preferred connectivity indicator for the plots of this paper except for the robustness to random and targeted attacks that had the strongest correlation with γ.

4.2.1. Mean robustness to single, two and three link failures

The proportion of nodes serving as OD points was not correlated with the network mean robustness to SLFs, 2LFs and 3LFs ($|R_S| < 0.20$ and p-value > 0.05). The degree and link cost heterogeneities both showed weak correlations with the network mean robustness to SLFs, 2LFs and 3LFs (Table 2). The network characteristics that exhibited the strongest correlation with the mean network robustness were the network size and connectivity (Table 2) suggesting a potential relationship between these values showed in Fig. 6.

Two domains appear in the plots of Fig. 6.a. On the left side, the smallest networks exhibit a large variability in their mean robustness to SLFs, 2LFs and 3LFs while on the right side, the mean robustness of the largest networks seems independent of N. A visual assessment suggested that the change point for SLB, 2LB and 3LB could be $N = 30$, $N = 35$, $N = 40$ respectively. Furthermore, an assessment of the results across the different scenarios showed that the average mean robustness of the small networks (less than 30 nodes) went from 96% (sd = 0.04) in SLFs to 87% (sd = 0.14) in 3LFs. In contrast, the average mean robustness of the large networks ($N > 30$) only decreased from 99% (sd = 0.01) in SLFs to 98% (sd = 0.02) in 3LFs.

Two domains are also present in the data of Fig. 6.b that could be well represented by a piecewise linear model ($R^2 \approx 0.89$). Hence, the mean network robustness linearly increased with β, the slope being sharper before the breakpoint ($\beta \approx 1.55$). Besides, the gaps between the mean robustness of the networks to SLFs, 2LFs and 3LFs gradually decreased with β. The average mean robustness of the weakly connected networks ($\beta \leq 1.55$) went from 93% (sd = 0.04) in SLFs to 77% (sd = 0.16) in 3LFs while in the highly connected networks it only decreased from 99% (sd = 0.01) to 98% (sd = 0.02).

Table 3
Correlation (R_S) between the link criticality rankings derived from different scenarios: single (SLF), two (2LF) and three (3LF) link failures and the combination of all three (ALL)

	SLF vs ALL	2LF vs ALL	3LF vs ALL
Min	0.460	0.698	0.878
Median	0.985	0.999	0.999
Mean	0.934	0.983	0.995
Max	1.000	1.000	1.000

4.2.2. Correlation between the link-criticality rankings

The distributions of the link ranking correlation values are summarised in Table 3. These results indicate that SLF-based criticality rankings were generally very strongly correlated with the rankings based on all scenarios (the mean correlation value being 0.934) however low correlation values were also observed (e.g. 0.460). 2LF and 3LF based rankings showed even stronger mean correlations with the rankings based on ALL (0.983 and 0.995 respectively).

Table 2 shows that SLF vs ALL was not correlated with the network attributes ($|R_S| < 0.20$) except for the proportion of nodes serving as OD points ($R_S = 0.86$). The correlations between 2LF vs ALL and the network attributes were weak at best ($|R_S| < 0.40$) except for the proportion of nodes serving as OD points ($R_S = 0.66$). In the case of 3LF-based criticality rankings, the correlation with the ratio of OD points to nodes became weak and negative ($R_S = -0.35$) while other network attributes started to play a role (i.e. the correlation of 3LF vs ALL with N and β were 0.73 and 0.71 respectively).

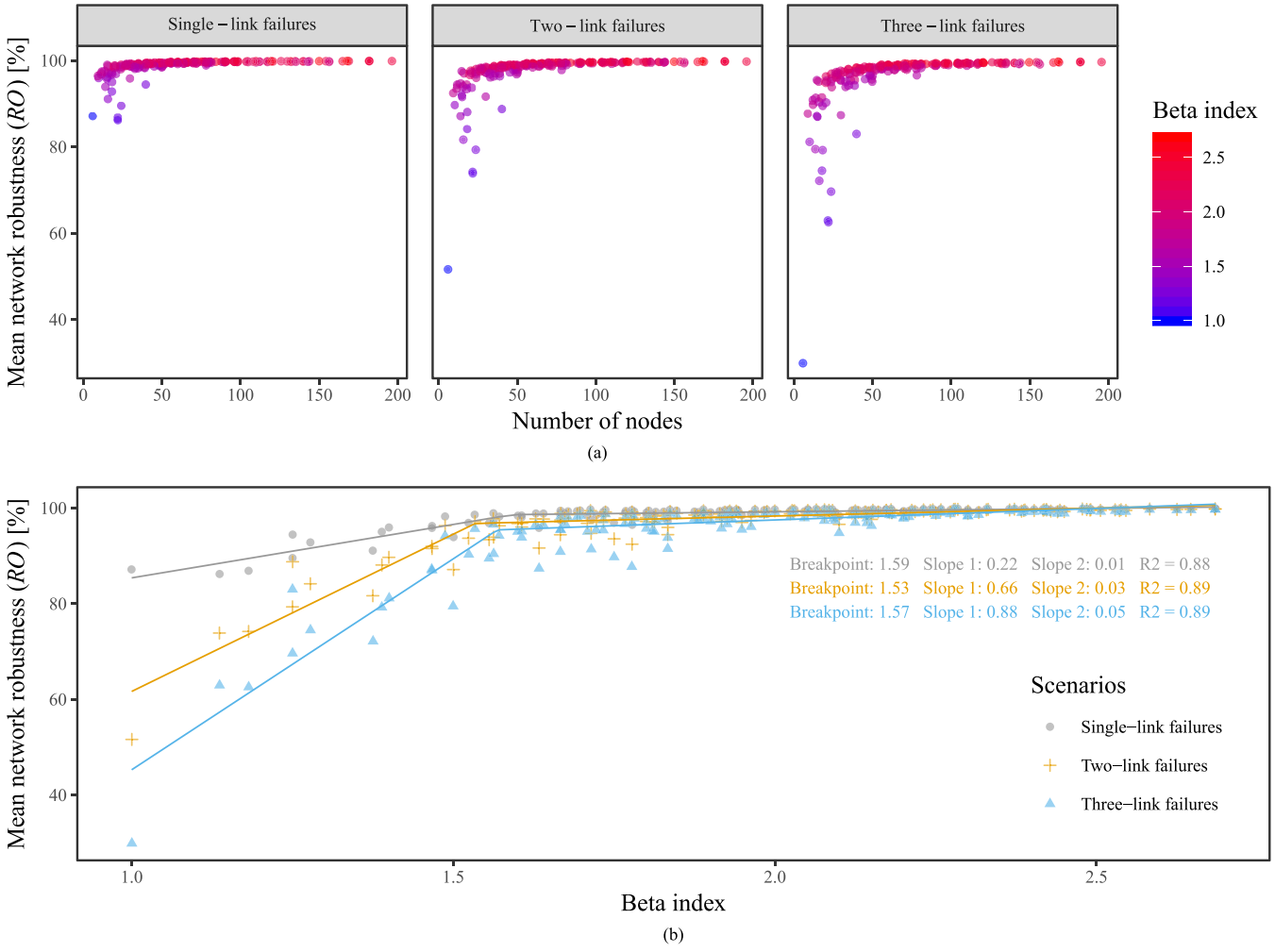


Fig. 6. Mean robustness of the GREREC networks to single, two and three-link failures depending on their (a) size and connectivity and (b) connectivity.

The influence of the network size on the rankings correlation is shown in Fig. 7.a, where it can be seen that there were no significant relationship between the number of nodes in the network and both SLF vs ALL and 2LF vs ALL. In contrast, the minimum value of 3LF vs ALL increased with N. The influence of the proportion of nodes being OD points on the rankings correlation is shown in Fig. 7.b, where it can be observed that the accuracy of SLF-based rankings increased with r_{OD} i.e. when $r_{OD} \leq 0.5$ the mean value of SLF vs ALL is 0.87 (sd = 0.12) but reaches 0.99 (sd = 0.01) when $r_{OD} > 0.5$.

4.2.3. Extended impact of targeted attacks

None of the network attributes demonstrated a strong correlation with the network robustness to a dynamic betweenness attack ($|R_S| < 0.43$). In contrast, the network robustness to random attacks demonstrated a strong correlation with the network connectivity ($0.78 \leq R_S \leq 0.87$), a moderate correlation with the degree heterogeneity ($R_S = 0.58$) and no correlation or an uncertain weak correlation with the other attributes (p-value > 0.001). The results are similar for the targeted attack extended impact except that the network size demonstrated a moderate correlation with TA_{EI} ($R_S = 0.59$).

Fig. 8 shows the influence of the network connectivity, size and structural pattern group membership on both CRO_{RAND} and TA_{EI}. In Fig. 8.a the largest networks seemed to follow a linear model relatively supported by a regression performed on the networks with more than 10 nodes ($R^2 = 0.76$). In contrast, the linear model appeared less relevant for TA_{EI} ($R^2 = 0.45$).

4.3. Comparison with the real road networks

4.3.1. Topology of the road network samples

As the topology of a network can be characterised by its degree distribution, the average and standard deviation of the degree distributions in the GREREC and real networks (Fig. 9) were used for comparing their topology. The real network topologies ranged from tree-like structures (Fig. 4.c) to more compact and ordered grid-like structures (Fig. 4.a) with average degrees of 2.33 and 3.32 respectively. In Fig. 9, it can be seen that the topology of the real networks was close to the topology of some of the GREREC networks but that the latter also contained a large range of networks with higher average degree and degree heterogeneity values. Furthermore, the comparison with Table 1 and Fig. 5 suggests that B1, B2, C1 and C2 were the GREREC structural pattern groups that are the closest to the real networks, while B3 and C3 present higher proportions of high degree nodes (superior to six) than real networks. Hence, the GREREC model better represents real road networks when the probability of generating shortcuts is low ($q < 0.66$).

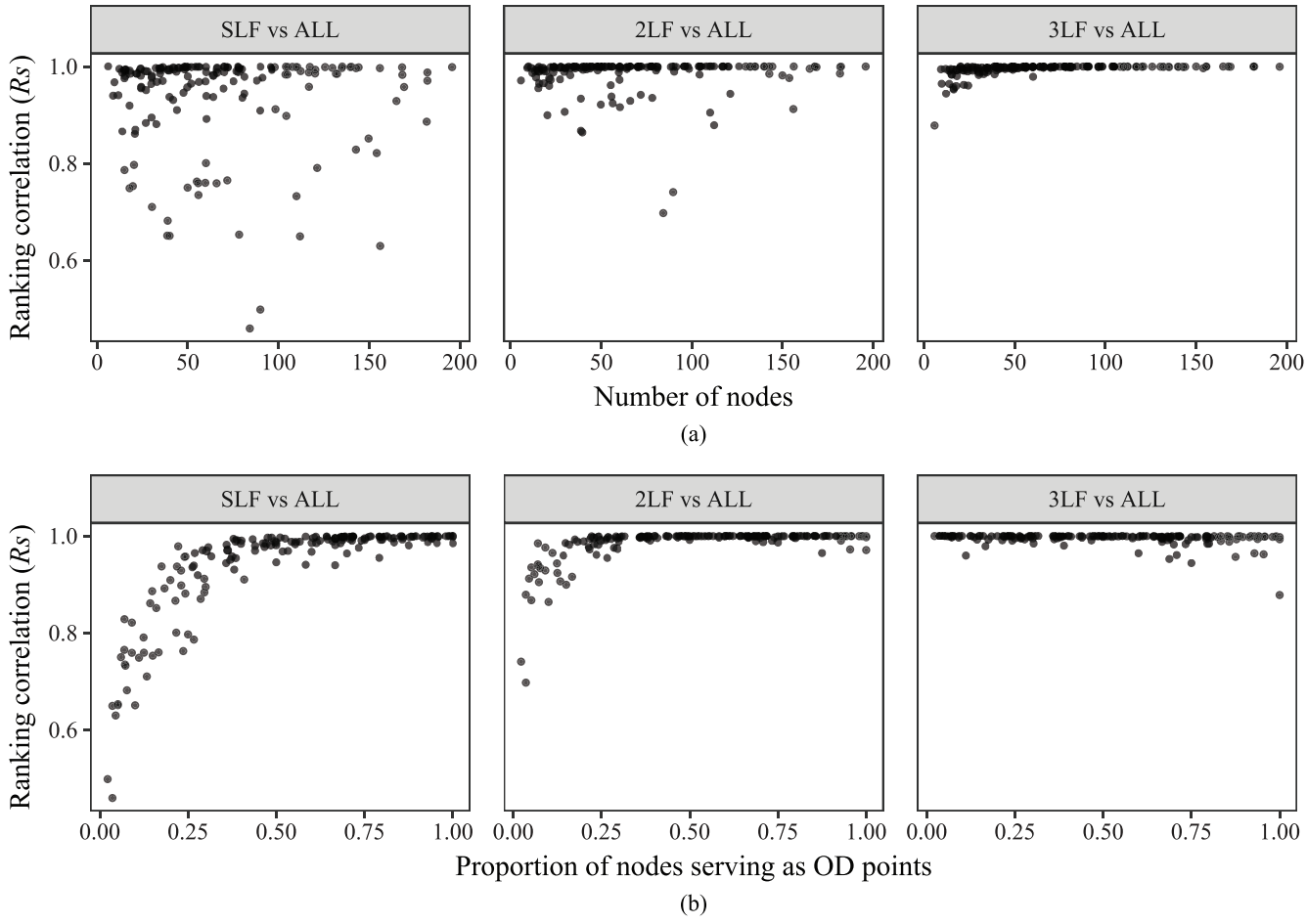


Fig. 7. Correlation of the link criticality rankings derived from single (SLF), two (2LF) and three (3LF) link failures and the combination of all three (ALL) depending on (a) the network size and (b) the proportion of nodes serving as OD points in the GREREC networks

Table 4
Correlation (R_S) between the network characteristics and robustness metrics in the road network samples analysed. ^{ns}, *, ** and *** denote the significance at $p > 0.05$, $p < 0.05$, $p < 0.005$ & $p < 0.001$ respectively.

	Network characteristics				
	Network size (N)	Network connectivity (α, β, γ)	Degree heterogeneity	Link costs heterogeneity	Proportion of nodes being OD points
Mean robustness to SLF	0.66^{***}	$[0.74, 0.83]^{***}$	-0.20^{ns}	-0.55^{**}	-0.17^{ns}
Mean robustness to 2LF	0.67^{***}	$[0.73, 0.82]^{***}$	-0.20^{ns}	-0.57^{**}	-0.17^{ns}
Mean robustness to 3LF	0.68^{***}	$[0.72, 0.81]^{***}$	0.17^{ns}	-0.59^{***}	-0.16^{ns}
SLF vs ALL[(1)]	0.28^{ns}	$[0.20, 0.21]^{ns}$	-0.08^{ns}	-0.29^{ns}	0.59^{***}
2LF vs ALL	0.41^{*}	$[0.22, 0.24]^{ns}$	-0.10^{ns}	-0.39^{*}	0.40^{*}
3LF vs ALL	0.35^{ns}	$[0.01, 0.02]^{ns}$	-0.00^{ns}	-0.30^{ns}	-0.25^{ns}
Robustness to a BETWI[(2)]	-0.43^{*}	$[0.53, 0.67]^{**}$	-0.11^{ns}	0.43^{*}	0.01^{ns}
Robustness to a RAND[(3)]	0.27^{ns}	$[0.70, 0.83]^{***}$	-0.18^{ns}	0.31^{*}	0.11^{ns}
Targeted attack extended impact	0.30^{ns}	$[0.48, 0.52]^{**}$	-0.22^{ns}	-0.18^{ns}	0.24^{ns}

[(1)] Correlation of the link criticality rankings derived from single (SLF), two (2LF) and three (3LF) link failures, and the combination of all three (ALL); [(2)] Interactive betweenness attack; [(3)] Representative random attack

4.3.2. Correlation of the network robustness metrics with the network characteristics in the real networks

The correlation between the networks attributes and robustness metrics was also evaluated in the real network models (Table 4). These correlations were generally consistent with the correlation observed with the GREREC networks (Table 2) as they often had the same signs, ranges and p-values.

Although the correlations of the network mean robustness in SLFs, 2LFs and 3LFs with the network size were lower in the real networks (0.67 in average) than in the GREREC networks (0.93 in average), the network size and connectivity remained the only parameters strongly correlated to the mean network robustness. Furthermore, the smallest real networks also exhibited a large variability in their mean robustness to SLFs, 2LFs and 3LFs while the robustness of the largest networks seemed independent of N. The average mean robustness of the small real networks ($N \leq 30$) went from 91% (sd = 0.04) in SLFs to 73% (sd = 0.10) in 3LFs, while the average mean robustness of the large networks ($N > 30$) only decreased from 98% (sd = 0.01) in SLFs to 95% (sd = 0.04) in 3LFs.

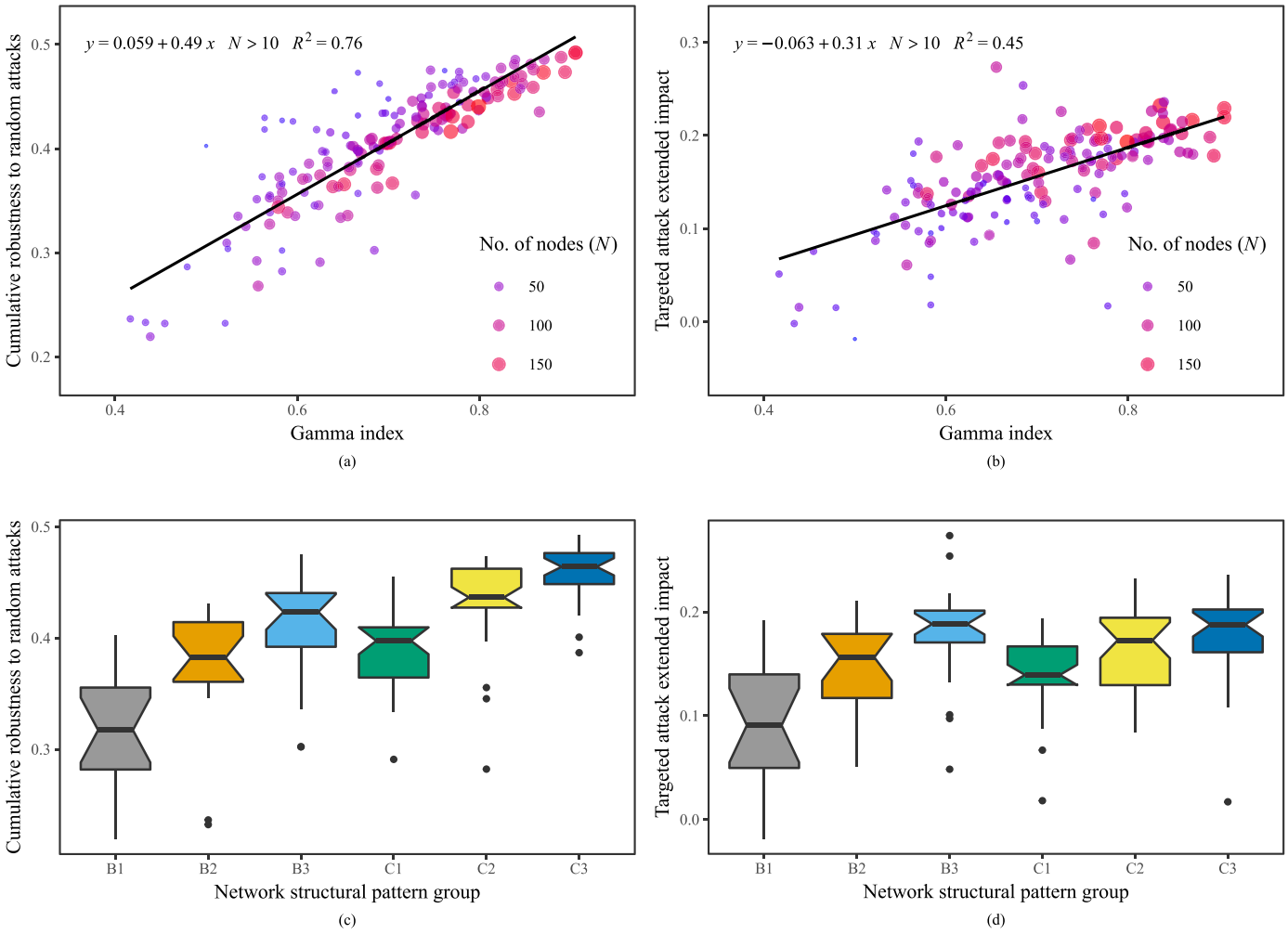


Fig. 8. Relation between the robustness to random dismantling processes (i.e. cumulative robustness to random attacks) and the extended impact of targeted attacks and three networks attributes: (a and b) the network connectivity and size and (c and d) the structural pattern group membership. box = 25th and 75th percentiles, notch = $\pm 1.58 IQR/\sqrt{n}$.

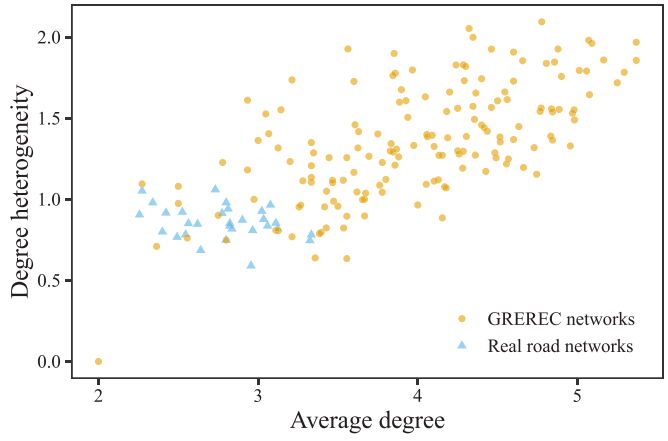


Fig. 9. Comparison of the topology of the GREREC and real networks analysed. The degree heterogeneity is the standard deviation of the degree distribution in the network.

However, in the real networks, the correlation of the mean robustness to single and multiple link failures with the degree heterogeneity was uncertain (p-value $>$ 0.05) while the correlation with the link cost heterogeneity appeared stronger (-0.57 in average). Besides, the piecewise linear model connecting the network mean robustness and connectivity (Fig. 6.b) remained relevant for the real networks but less accurate ($R^2 \approx 0.59$ in Fig. 10.a).

In the real networks, the correlation of the robustness to the interactive betweenness attack with the network parameters remained weak or moderate at best (Table 4). The GREREC and real network correlation results were also similar for the robustness to random dismantling processes except that the latter was now uncorrelated with the degree heterogeneity. In contrast, the correlation of the extended impact of targeted attacks with the network size, connectivity and degree heterogeneity went from being strong in the GREREC networks to being not significant, moderate and not significant, respectively.

The linear model connecting network connectivity and robustness to random dismantling processes remained relevant ($R^2 = 0.87$ in Fig. 10.b) for the real networks but with a steeper slope of 1.1 compared to 0.49 for the GREREC networks.

Table 4 shows that SLF vs ALL, 2LF vs ALL and 3LF vs ALL were at best weakly correlated with the network attributes ($|R_S| < 0.40$ and p-value > 0.005) apart from the proportion of nodes serving as OD points that was strongly correlated with SLF vs ALL ($R_S = 0.59$). This is also consistent with the GREREC results except that 3LF vs ALL was also strongly correlated with the network size and connectivity in the GREREC networks.

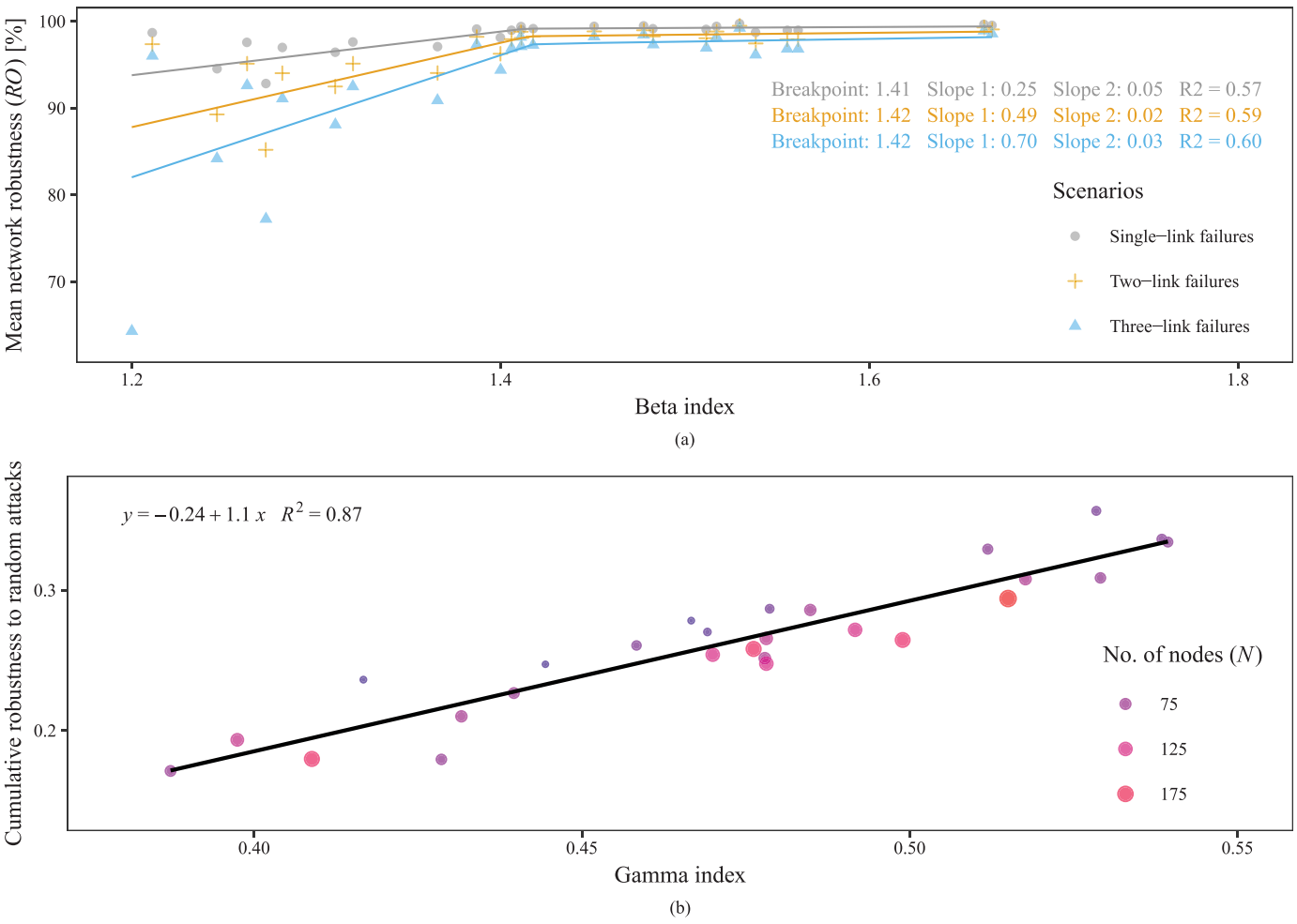


Fig. 10. Influence of the network connectivity (beta and gamma) on the (a) mean robustness to single, two and three-link failures and (b) robustness to random dismantling processes (i.e cumulative robustness to random attacks) in the road network samples

Table 5
Correlation (R_S) between the link criticality rankings derived from single (SLF), two (2LF) and three (3LF) link failures and the combination of all three (ALL) in the road network samples

	SLF vs ALL	2LF vs ALL	3LF vs ALL
Min	0.803	0.998	0.974
Median	0.993	0.999	0.995
Mean	0.973	0.998	0.995
Max	1.000	1.000	1.000

The results of the link criticality rankings comparisons in the real networks are summarised in Table 5. As with the GREREC networks (Table 3), SLF-based criticality rankings were generally very strongly correlated with the rankings based on all scenarios (the mean correlation being 0.973) while 2LF and 3LF based rankings showed even stronger mean correlations with the rankings based on ALL (0.999 and 0.995 respectively).

5. Discussion

The comparison of the topology of the GREREC and real road networks suggests that the former contain a wider set of properties. For example, the structural patterns groups B3 and C3 have higher proportions of six to eight degree nodes than real networks. Although these networks may be rare in the real-world due to costs and land-use constraints, their inclusion in this analysis remains useful to assess the benefits in terms of robustness of designing and building networks with a higher proportion of intersections connecting more than six streets.

The robustness analysis performed on both sets of networks allowed determining the influence of certain network attributes on network robustness. Firstly, the variations of the correlation between the robustness metrics and the network attributes (Table 2 and 5) depending on the aspect of robustness considered (mean robustness, link criticality and targeted attacks extended impact) reflect the fact that network robustness is a complex and multidimensional problem in which different network characteristics play more or less important roles depending on the aspect of robustness considered. Hence, none of the network attributes on its own is sufficient to explain the road network robustness.

5.1. Influence of the link cost and degree heterogeneities on network robustness

Among the indicators considered, the link cost heterogeneity (i.e. the standard deviation of the link cost distribution) was the only indicator that showed no significant correlation with the robustness metrics of the GREREC networks. It is, however, difficult to conclude that the road network robustness is generally independent of the link cost heterogeneity as this could be specific to the indicator tested or to the process used to generate the link costs in the GREREC model. Indeed, the link cost heterogeneity of the real

networks had a stronger (but still moderate) correlation with the mean robustness to single, two and three link failures. Hence, the present results show that the link cost heterogeneity has a weak to moderate influence on the network robustness and more importantly that the links travel costs are much less important than the other parameters considered (i.e. the network topology and proportion of nodes serving as OD points) in terms of robustness.

In the GREREC networks, the degree heterogeneity (i.e. the standard deviation of the degree distribution) was positively moderately correlated with network average robustness (i.e. mean robustness to SLFs, 2LFs and 3LFs and robustness to random dismantling processes). This correlation could not be verified in the real network samples. Considering the strong correlation between the network connectivity and robustness in both sets of networks, this difference may be explained by the fact the degree heterogeneity and connectivity were correlated in the GREREC networks ($R_S = 0.64,\ p\text{-value} < 10^{15}$) but uncorrelated in the real graphs ($R_S = -0.21,\ p\text{-value} = 0.256$). This highlights one of the weaknesses of the GREREC model where higher degree heterogeneity is often paired with higher connectivity while it may not always be the case in the real-world.

The present results may explain why previous research found that the degree heterogeneity positively impacted road network robustness. Considering the tail of degree distribution as an indicator of the degree heterogeneity, [14] noticed that the latter was positively correlated with the network robustness in random dismantling processes. The suitability of this indicator to reflect the degree heterogeneity is however problematic for two reasons. Firstly, the accuracy of this index depends on whether degree distribution tails (for degrees superior to three) can be approximated by exponential decays. This is not the case for example in cities presenting a dominant square-grid structure (e.g. San Francisco) where four-street intersections are more frequent than three-street intersections. Secondly, tails also contain information about the network connectivity as lower-decay rates also imply that more high-degree nodes are present in the network and therefore that the network connectivity and robustness are higher.

5.2. Influence of the network size and connectivity on the network robustness to single, multiple, random and targeted link failures

The analysis showed that a linear model connected the network density and robustness in both the GREREC (Fig. 8.a) and real (Fig. 10.b) networks. These observations are consistent with the conclusions of [14] who also found a linear relationship between those metrics although they considered a different robustness indicator. The steeper slope observed in the real networks can be explained by the smaller range of γ in this set of networks [0.38, 0.58] compared to [0.41, 0.91] in the GREREC networks since the data in Fig. 8.a suggests that the slope of the linear model would also be steeper in this range. Hence, the network robustness to a random dismantling process linearly increases with the density (i.e. proportion of possible links or cycles that are actually present in the network).

In both the GREREC and the real networks, the weak to moderate correlation observed between the network robustness to a dynamic betweenness attack (CRO_{BETWI}) and the connectivity indicators (α, β and γ) contrasts with the strong correlation found between the network connectivity and its mean robustness to SLFs, 2LFs, 3LFs and random dismantling processes. This may be because CRO_{BETWI} - like any other measure of the impact of a targeted attack - essentially looks at the impact in the worst-case scenario. As two networks can perform similarly in a targeted attack but differently in a wider range of disturbances, such measures may not be sufficient on their own to compare the robustness (ability to maintain functionality despite various disturbances) of different networks. It is, therefore, more meaningful to study and quantify the impact of targeted attacks in comparison with other attacks in the same network.

The positive correlations observed between the network connectivity, CRO_{RAND} and the extended impact of targeted attacks suggest that although highly-connected networks are likely to be more robust to random failures than sparse networks, the extended impact of a targeted attack would also be larger in the former. Highly connected networks hence offer more opportunities for malicious attacks to be more detrimental than random attacks. In practice, this means that in sparse networks most of the links should equally be protected as the impacts of random and targeted attacks are close, whereas high-betweenness links should be given a higher priority for protection in complex networks.

However, network dismantling processes and the related robustness indicators lack applicability as real-life perturbations (car accidents, floods or sabotage actions) rarely follow this mechanism. Hence, the present study also considered single and multiple link failures, which allowed determining the influence of the network size (number of intersections) on the network robustness. Like the network connectivity, the network size was strongly correlated to the mean robustness to SLFs, 2LFs and 3LFs in both the GREREC and the real networks. These strong correlations can be explained by the fact that both parameters increase the number of alternatives routes available to substitute the disrupted ones. Furthermore, the correlation of the network size with the robustness to SLFs, 2LFs and 3LFs but lack of correlation with the robustness to random dismantling processes suggests that most of the MLFs scenarios had a local impact.

The present results also showed that the relationship between the network connectivity and mean robustness tends to follow a piecewise linear model in the case of SLFs, 2LFs and 3LFs (Figs 5.b and 10.a), in which the effect of the network density on the mean robustness decreases to almost zero after the breakpoint. The value of this breakpoint slightly increased from $\beta = 1.41$ in the real networks to $\beta = 1.55$ in the GREREC graphs and should, therefore, be around those values.

Finally, if the conclusion that single and multiple link failures are more harmful in small and sparse networks was expected, the present research still provided quantitative estimates showing that the impact of SLFs and 3LFs are comparable in large networks (more than 30 nodes) while their impacts differ of 9% (18% in the real networks) in robustness on average in the small networks. Similarly, in the sparse networks ($\beta < 1.55$) the mean impact of SLFs and 3LFs differed of 16% (7% in the real networks) in robustness but only of 1% in the compact networks.

Similar behaviours could be expected for scenarios involving a greater number of failed links (four-link failures, etc.) although the size and connectivity thresholds may slowly increase with the number of failed links considered. Therefore, when designing or upgrading a road network, the addition of redundant routes in the network (by building additional roads and intermediate intersections) is an efficient way to improve the network mean robustness up to a certain size ($N \approx 40$) and connectivity ($\beta \approx 1.5$) threshold after which the robustness enhancement is limited.

5.3. Influence of the ratio of OD points to nodes on the link criticality rankings

The comparison of the link criticality rankings derived from single, two and three link failures and the combination of all three showed that these rankings depend on the scenarios and network considered in both the GREREC and the real networks. The low correlation values obtained in some cases (e.g. the minimum value was 0.460 in the GREREC networks) indicate that SLFs and ALL can provide substantially different lists of links which are most critical

to the network performance in case of disruption. The minimum value (0.803) obtained in the real networks was certainly higher than in the GREREC model because the set of real networks (30) was smaller than the sample of GREREC networks (161). These results hence confirm and give more depth to the conclusions of [3]: the most critical links when multiple-link failures occur are not simply the combination of the most critical links with single-link failures.

The present study showed that SLF vs ALL was significantly positively correlated with the proportion of nodes being OD points in both the GREREC and real networks. Furthermore, SLF-based rankings were well correlated with the rankings based on all scenarios in networks with a high proportion of nodes serving as OD points ($r_{OD} > 0.5$). In such networks, OD pairs are more likely to be originally connected by direct routes for which the alternatives routes are much more costly or don't exist. In these networks, SLFs are hence very critical while the contribution of MLF scenarios to the link criticality is limited. In contrast, SLF-based rankings are likely to misrepresent the overall link criticality in networks with a low ratio of OD points to nodes where SLFs are less relevant due to the availability of several "equivalent routes".

Although the correlation between 3LF and ALL based rankings remained generally high (above 0.878 in the GREREC networks), the variability of the correlation between both rankings further decreased with the network size. This may be explained by the fact that most of 3LF scenarios are likely to be very critical in small networks resulting in more difficulty in distinguishing between the impacts of these scenarios on the network performance and thus in ranking the links.

One practical implication of these findings is that the classical method assessing link criticality based exclusively on SLFs is likely to misrepresent the overall link criticality in road networks where the population (demand) is not homogeneously distributed among all the intersections. The application of this method outside of this case could lead to inefficient prevention and restoration measures in the advent of events disrupting several road segments (e.g. flooding) or several events affecting different parts of the network at the same time (e.g. a car accident could cause the unavailability of a road while a bridge is closed for repair work in another part of the network).

On the other hand, the brute-force approach - testing all possible scenarios of MLFs - is limited due to its computational cost and only appropriate for small to medium (sub)networks. Considering this, two-link failures seemed to provide a possible solution balancing accuracy and computational cost (the mean values of 2LF vs ALL being 0.981 and 0.998 for the GREREC and real networks respectively compared to 0.933 and 0.973 for SLF vs ALL) at least to represent the overall link criticality in failures of up to three links. Future research could seek to determine more precisely when it is necessary to consider 2LF, 3LF, 4LF, etc. and accordingly develop less computationally expensive methods for link criticality ranking.

6. Conclusions

The present study is an attempt to find universal insights into road networks robustness to single, multiple, random and targeted link failures. For this purpose, a review of studies examining real-road networks topologies and patterns was conducted to identify the common properties of road graphs including approximate planarity, negligible proportion of intersections with six or more connections and heterogeneity in roads functionality and performance. On this basis, the GREREC model was developed to randomly generate a variety of abstract networks presenting the topological and operational characteristics observed in real-road networks, on which a robustness analysis was performed. This analysis was also reproduced on a set of real network samples for validation.

The results showed that the GREREC model can generate networks with topologies similar to real maps (ranging from tree-like structures to more compact and ordered grid-like structures) but also more diverse topologies presenting, for example, higher proportions of intersections connecting six to eight streets than real maps. Hence, the analysis performed on both sets of networks allowed to assess the robustness of real networks but also networks that could be designed and built for greater resilience. As the scenarios considered model a large range of disruptive events leading to the closure of sets of roads (e.g. serious car accidents, bridge failures and repair works), the results provide a framework to understand the potential influence of different network attributes on different aspects of road network robustness to such events.

The network size and connectivity strongly influenced the network mean robustness to multiple-link failures and allowed to distinguish small (sparse) networks where the impact of MLFs heavily depend on the attack size from large (compact) networks where the increased attack size has a negligible effect. The results also showed that the addition of redundant routes in road networks (through additional roads and intermediate intersections) is an efficient way to enhance the network robustness to multiple-link failures up to a certain size and connectivity threshold.

As the construction of new roads requires significant investments, the proposed link criticality indicator can be used as a tool to identify and prioritise the road segments for which alternatives connections should be built. This indicator should, however, be used carefully as the present research shows that link criticality rankings are sensitive to the type of disruption scenarios considered (i.e. single or multiple link failures) and that the network attribute controlling the correlation between SLF-based rankings and the rankings based on all scenarios is the ratio of OD points to nodes. The classical method assessing link criticality based exclusively on single-link failures is hence likely to misrepresent the overall link criticality in road networks where the population (demand) is not homogeneously distributed among all the intersections, which could lead to inefficient prevention and restoration measures in the advent of events disrupting several road segments or several events affecting different parts of the network at the same time.

The comparison of the impact of targeted and random attacks showed that highly-connected networks are more robust but also offers more opportunities for malicious attacks to be more harmful than random failures. The identification and protection of the most critical road segments are hence more crucial in compact road networks than in sparse networks where most links are equally important to the network performance.

Ultimately, the present study provides findings that should be of interest to researchers, industry professionals and policy-makers aiming to perform robustness and resilience analyses of road networks. The GREREC model and the results presented here could be used as a relevant null model to benchmark the robustness of road networks.

Although limited by computational capacity, the approach adopted - that consists in analysing a large set of randomly generated transport networks - is scalable and probably applicable to other transport networks (using suitable random network models). Future works could hence extend this approach to other road network performance metrics or other transport modes.

Disclaimer

The views expressed are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

Acknowledgments

The research presented in this paper was carried out as part of the H2020-MSCAETN-2016. This project has received funding from the European Union's H2020 Programme for research, technological development and demonstration under grant agreement number 721493.

We are grateful for access to the University of Nottingham's Augusta High-Performance Computer(HPC) service.

Appendix

A1. Connectedness of the GREREC model

As the GREREC model can generate disconnected networks, the probability of the networks being connected depending on the parameters *n, m, p* and *q* was estimated through a Monte Carlo method (500 simulations per set of values). The results are shown in Fig. A.1.

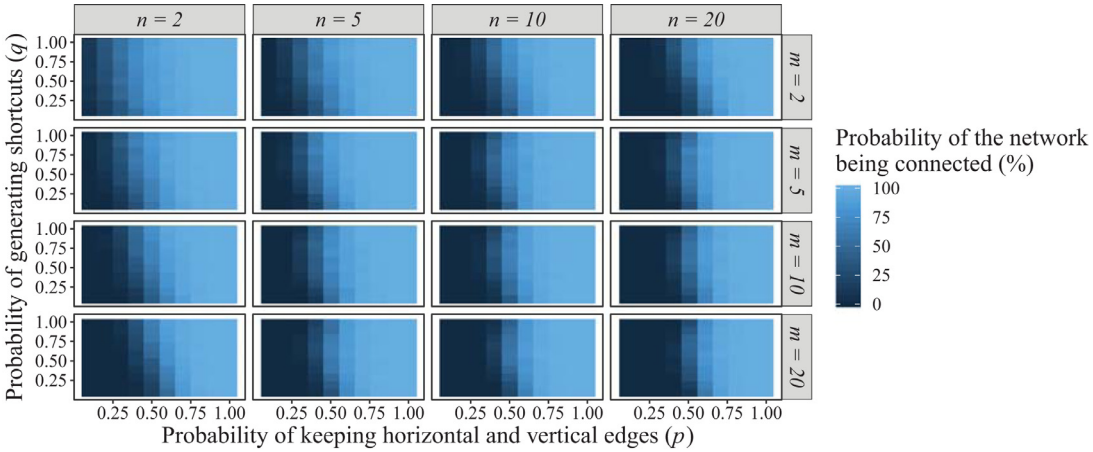


Fig. A.1. Connectedness of the GREREC model depending on the dimensions *m* and *n* of the graph (i.e. number of nodes per row and columns in the rectangle respectively) and the parameters *p* and *q*

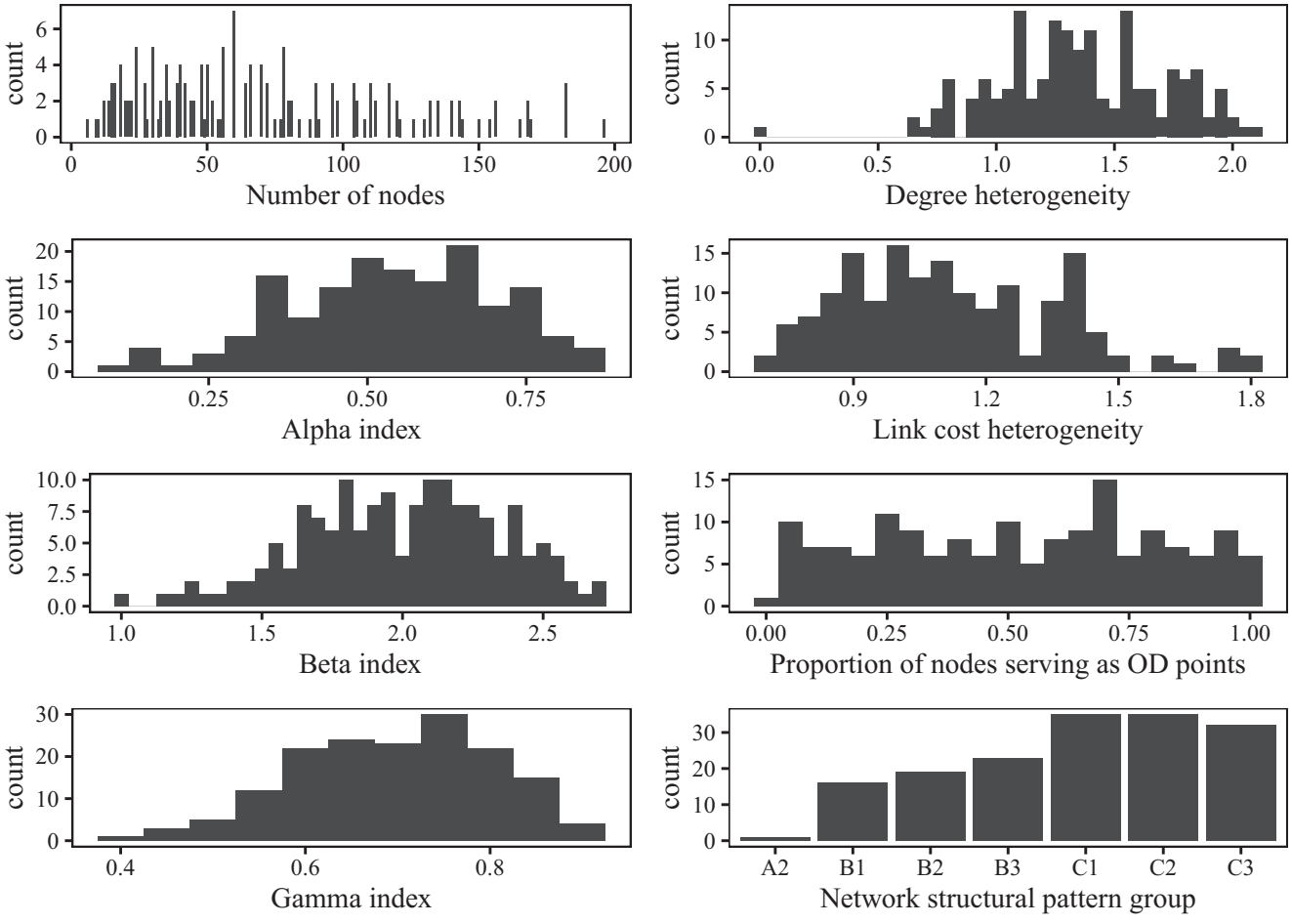


Fig. A.2. Histograms of the network attributes in the set of GREREC networks analysed.

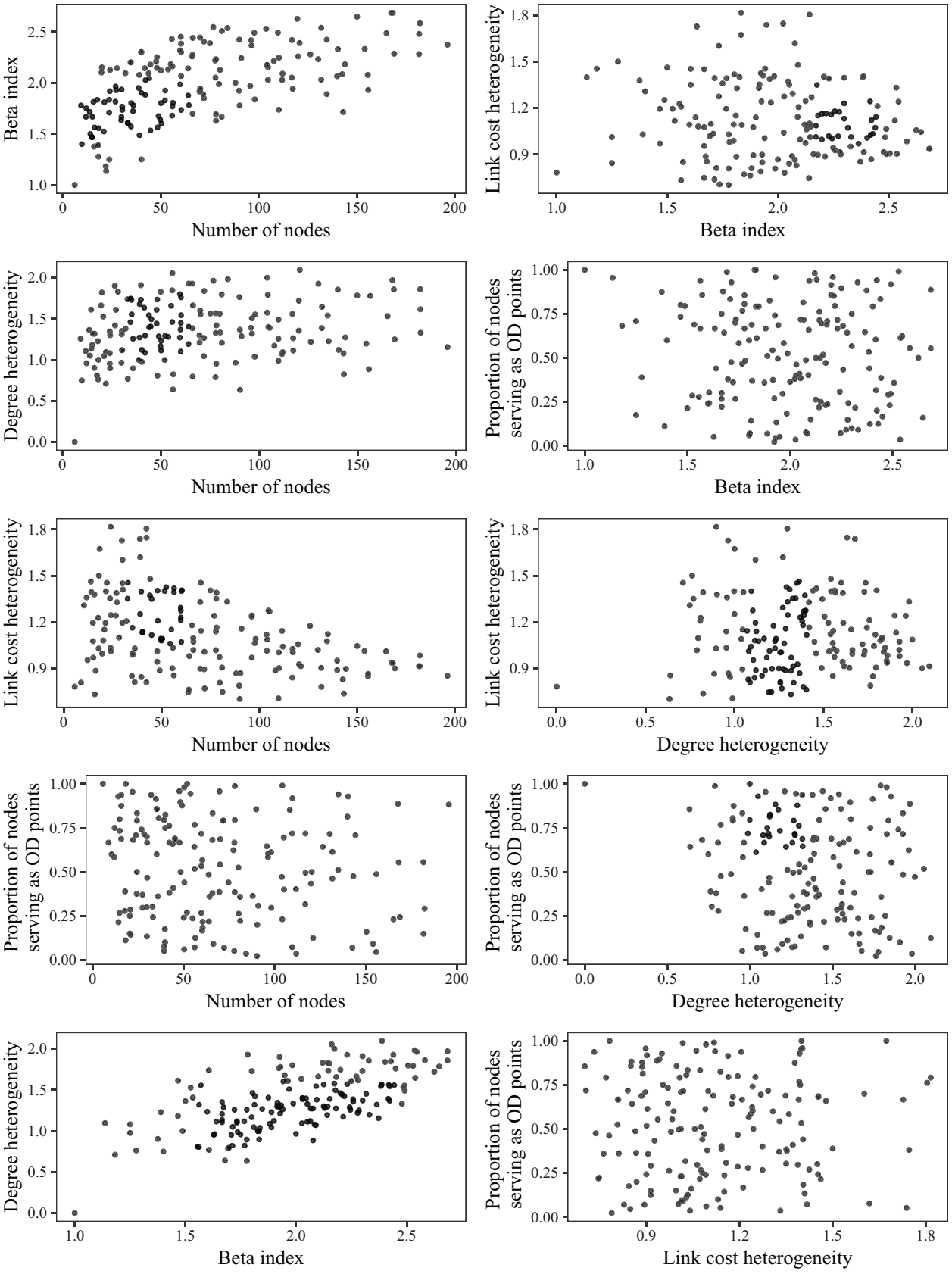


Fig. A.3. Relationship between the network attributes in the set of GREREC networks analysed.

As shown in Fig. A.1, the values of p and q for which the graphs were connected with a certain probability increased with their size (controlled by m and n). Furthermore, p plays a more important role than q, as the probability of the graph being connected exceeds 48% for $p \geq 0.6$ regardless of q. This is because the shortcuts alone are not sufficient to connect the network nodes since they only depart from certain nodes (see rule 3) and 4) in the procedure in Section 3.1), whereas horizontal and vertical edges depart from every node.

A2. The attribute space of the set of GREREC networks analysed

A Quasi-Monte Carlo method was used to obtain a sample of networks that homogeneously covered the parameter space of the GREREC model, which however didn't necessarily imply that the volume of the network attributes would be also homogeneously covered. This appendix evaluates the distribution of the attribute values in the set of networks analysed to verify if the possible attribute values were well represented in this sample. Fig. A.2 shows the histograms of the network attributes considered in this study. It can be observed that the distributions were generally well-spread in their domains. The largest networks were less represented because they correspond to high values of m and n (the dimensions of the rectangular grid). The lowest values of α, β and γ were underrepresented because they correspond to unconnected graphs. As an indication the minimum number of links required to connect a planar graph of N nodes is $N-1$ [21].

The relationships between the network attributes are shown in Fig. A.3, where it can be seen that these attributes were generally uncorrelated.

References

[1] F. Xie, D. Levinson, Evaluating the effects of the I-35W bridge collapse on road-users in the twin cities metropolitan region, Transportation Planning and Technology 34 (7) (2011) 691–703, doi:10.1080/03081060.2011.602850.

[2] X. Zhang, E. Miller-Hooks, K. Denny, Assessing the role of network topology in transportation network resilience, Journal of Transport Geography 46 (2015) 35–45, doi:10.1016/j.jtrangeo.2015.05.006.

[3] D.Z.W. Wang, H. Liu, W.Y. Szeto, A.H.F. Chow, Identification of critical combination of vulnerable links in transportation networks – a global optimisation approach, Transportmetrica A: Transport Science 12 (4) (2016) 346–365, doi:10.1080/23249935.2015.1137373.

[4] O. Cats, M. Yap, N. van Oort, Exposing the role of exposure: Public transport network risk analysis, Transportation Research Part A: Policy and Practice 88 (2016) 1–14, doi:10.1016/j.tra.2016.03.015.

[5] M.A. Taylor, S.V. Sekhar, G.M. D'Este, Application of accessibility based methods for vulnerability analysis of strategic road networks, Networks and Spatial Economics 6 (3-4) (2006) 267–291, doi:10.1007/s11067-006-9284-9.

[6] M. Zanin, X. Sun, S. Wandelt, Studying the Topology of Transportation Systems through Complex Networks: Handle with Care, Journal of Advanced Transportation 2018 (2018), doi:10.1155/2018/3156137.

[7] M. Bruneau, S.E. Chang, R.T. Eguchi, G.C. Lee, T.D. O'Rourke, A.M. Reinhorn, M. Shinozuka, K. Tierney, W.A. Wallace, D. Von Winterfeldt, A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities, Earthquake Spectra 19 (4) (2003) 733–752, doi:10.1193/1.1623497.

[8] M. Omer, A. Mostashari, R. Nilchiani, Assessing resilience in a regional road-based transportation network, International Journal of Industrial and Systems Engineering 13 (4) (2013) 389–408, doi:10.1504/IJISE.2013.052605.

[9] A.A. Ganin, M. Kitsak, D. Marchese, J.M. Keisler, T. Seager, I. Linkov, Resilience and efficiency in transportation networks, Science Advances 3 (12) (2017) e1701079, doi:10.1126/sciadv.1701079.

[10] J.L. Sullivan, D.C. Novak, L. Aultman-Hall, D.M. Scott, 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) (2010) 323–336, doi:10.1016/j.tra.2010.02.003.

[11] A.P. Masucci, D. Smith, A. Crooks, M. Batty, Random planar graphs and the London street network, European Physical Journal B 71 (2) (2009) 259–271, doi:10.1140/epjb/e2009-00290-4.

[12] J. Buhl, J. Gautrais, R.V. Solé, P. Kuntz, S. Valverde, J.L. Deneubourg, G. Theraulaz, Efficiency and robustness in ant networks of galleries, European Physical Journal B 42 (1) (2004) 123–129, doi:10.1140/epjb/e2004-00364-9.

[13] A. Réka, J. Hawoong, A.-L. Barabási, Error and attack tolerance of complex networks, Nature 406 (July) (2000) 378–382.

[14] J. Buhl, J. Gautrais, N. Reeves, R.V. Solé, S. Valverde, P. Kuntz, G. Theraulaz, Topological patterns in street networks of self-organized urban settlements, European Physical Journal B 49 (4) (2006) 513–522, doi:10.1140/epjb/e2006-00085-1.

[15] W. Peng, G. Dong, K. Yang, J. Su, A random road network model and its effects on topological characteristics of mobile delay-tolerant networks, IEEE Transactions on Mobile Computing 13 (12) (2014) 2706–2718, doi:10.1109/TMC.2013.66.

[16] F. Xie, D. Levinson, Measuring the structure of road networks, Geographical Analysis 39 (3) (2007) 336–356, doi:10.1111/j.1538-4632.2007.00707.x.

[17] G. Boeing, Planarity and street network representation in urban form analysis, Environment and Planning B: Urban Analytics and City Science (2018), doi:10.1177/2399808318802941.

[18] M. Southworth, E. Ben-Joseph, Streets and the Shaping of Towns and Cities, Island press(first edition McGraw-Hill), Washington, DC (USA), 2003.

[19] S.M. Rifaat, R. Tay, A. De Barros, Effect of street pattern on the severity of crashes involving vulnerable road users, Accident Analysis and Prevention 43 (1) (2011) 276–283, doi:10.1016/j.aap.2010.08.024.

[20] X. Wang, S. You, L. Wang, Classifying road network patterns using multinomial logit model, Journal of Transport Geography 58 (2017) 104–112, doi:10.1016/j.jtrangeo.2016.11.013.

[21] A. Cardillo, S. Scellato, V. Latora, S. Porta, Structural properties of planar graphs of urban street patterns, Physical Review E - Statistical, Nonlinear, and Soft Matter Physics 73 (6) (2006) 1–8, doi:10.1103/PhysRevE.73.066107.

[22] S. Wang, L. Zheng, D. Yu, The improved degree of urban road traffic network: A case study of Xiamen, China, Physica A: Statistical Mechanics and its Applications 469 (2017) 256–264, doi:10.1016/j.physa.2016.11.090.

[23] P. Crucitti, V. Latora, S. Porta, Centrality in networks of urban streets, Chaos 16 (1) (2006), doi:10.1063/1.2150162.

[24] E. Strano, M. Viana, L.d.F. Costa, A. Cardillo, S. Porta, V. Latora, Urban street networks, a comparative analysis of ten European cities, Environment and Planning B: Planning and Design 40 (6) (2013) 1071–1086, doi:10.1068/b38216.

[25] F. Bai, N. Sadagopan, A. Helmy, IMPORTANT: a Framework to Systematically Analyze the Impact of Mobility on Performance of RouTing Protocols for Adhoc NeTworks, in: IEEE INFOCOM, 2, 2003, pp. 825–835. https://doi.org/10.1109/INFCOM.2003.1208920.

[26] S. Gerke, D. Schlatter, A. Steger, A. Taraz, The Random Planar Graph Process, Random Structures and Algorithms (2007) 236–261, doi:10.1002/rsa.

[27] D. Eisenstat, Random road networks: the quadtree model, in: P. Flajolet, D. Panario (Eds.), Proceedings of the Eighth Workshop on Analytic Algorithmics and Combinatorics (ANALCO), San Francisco, CA, USA, 2011, doi:10.1137/1.9781611973013.9.

[28] V. Kalapala, V. Sanwalani, A. Clauset, C. Moore, Scale invariance in road networks, Physical Review E - Statistical, Nonlinear, and Soft Matter Physics 73 (2) (2006) 1–6, doi:10.1103/PhysRevE.73.026130.

[29] K.J. Kansky, Structure of transportation networks : relationships between network geometry and regional characteristics, University of Chicago, Dept. of Geography, Chicago, UsA, 1963.

[30] A.-L. Barabási, M. Pósfai, Network Science, Cambridge University Press, Cambridge, 2016.

[31] P.Y.R. Sohouenou, L.A.C. Neves, D. Lo Presti, Resilience indicators for road networks: the role of robustness and rapidity, in: 2019 International Conference on Smart Cities (ICSC), Seoul, South Korea, 2019.

[32] M.T. Puth, M. Neuhäuser, G.D. Ruxton, Effective use of Spearman's and Kendall's correlation coefficients for association between two measured traits, Animal Behaviour 102 (2015) 77–84, doi:10.1016/j.anbehav.2015.01.010.

[33] L.C. Freeman, Centrality in social networks, Social Networks 1 (3) (1979) 215–239, doi:10.1016/0378-8733(78)90021-7.

[34] P. De Meo, E. Ferrara, G. Fiumara, A. Ricciardello, A novel measure of edge centrality in social networks, Knowledge-Based Systems 30 (2012) 136–150, doi:10.1016/j.knosys.2012.01.007.

[35] P. Holme, B.J. Kim, C.N. Yoon, S.K. Han, Attack vulnerability of complex networks, Physical Review E - Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics 65 (5) (2002) 14, doi:10.1103/PhysRevE.65.056109.

[36] I.L. Dalal, D. Stefan, J. Harwayne-Gidansky, Low discrepancy sequences for monte carlo simulations on reconfigurable platforms, Proceedings of the International Conference on Application-Specific Systems, Architectures and Processors (2008) 108–113, doi:10.1109/ASAP.2008.4580163.

[37] P. Bratley, B.L. Fox, ALGORITHM 659: implementing Sobol's quasirandom sequence generator, ACM Transactions on Mathematical Software 14 (1) (1988) 88–100, doi:10.1145/42288.214372.

[38] G. Boeing, OSMnx: New methods for acquiring, constructing, analyzing, and visualizing complex street networks, Computers, Environment and Urban Systems 65 (2017) 126–139, doi:10.1016/j.compenvurbsys.2017.05.004.