Assessing Supply Chain Robustness to Links Failure

Belarmino Adenso-Díaz[a]♣, Julio Mar-Ortiz[b] and Sebastián Lozano[c]

[a] Escuela Politécnica de Ingeniería, Universidad de Oviedo, Spain, adenso@uniovi.es

[b] Faculty of Engineering, Universidad Autónoma de Tamaulipas, Mexico, jmar@docentes.uat.edu.mx

[c] Department of Industrial Management, Universidad de Sevilla, Spain, slozano@us.es

THIS PAPER WAS PUBLISHED IN 2018 IN

INTERNATIONAL JOURNAL OF PRODUCTION RESEARCH

doi: https://doi.org/10.1080/00207543.2017.1419582

Abstract

Supply chain networks need to respond efficiently to operation disruptions, as one of their aims is to guarantee the on time delivery of products. Hence, robustness has become one of the important issues to consider when designing supply networks. There are alternative ways to measure what robustness means in this context. In this paper we propose a new metric based on the effect on service level of the collapse of active transportation links. Numerical experiments are carried out to understand how different design factors affect robustness. Robustness under a targeted attack is compared with robustness to random failures. Results show that flow complexity (i.e. the number of potential transportation links between supply network nodes) is the most influential factor affecting supply network and its robustness, as well as the service level that can be maintained after disruptions. Thus, diversification both in supply sources and transportation routes seems to be key to robustness.

Keywords: Supply networks; Supply chain resilience; Supply chain design; Service level; Robustness.

1. INTRODUCTION AND MOTIVATION

As globalisation is becoming more and more important, logistics is playing a more relevant role as the means that allows the efficient movement of goods around the globe. Hence, the design of the supply chain (SC) networks represents a key feature in logistics strategy. This decision includes the definition of nodes (plants, regional warehouses, etc.), transportation modes, haulage companies, facilities locations, product flows, etc. Inefficient designs lead to, for example, more expensive operations due to redundancies, and poorer service levels due to late and/or unreliable deliveries, etc.

Among the reasons for a poor service level, risk considerations are becoming more evident as a result of many recent events. The tsunami of Japan in 2011 and the earthquake of 2007 (Chozick, 2007), the "superstorm" of 1993 on the USA's east coast, Tropical Storm Sandy in 2012, countless strikes and many other accidents and events, have been reported as causing significant economic disruptions as shipments were interrupted. Different design recommendations have been published in order to increase the robustness of logistics networks. For instance, Kamalahmadi and Parast (2016b) observed that it is more effective to source from a few reliable suppliers, while Behzadi et al. (2017) analyse the effectiveness of allocation flexibility for mitigating market demand disruption in the special case of the agribusiness industry.

The design of resilient supply networks (Ponomarov and Holcomb, 2009) is crucial, meaning the ability to reduce the probability of occurrence, the consequences and the time to recover after a disruption (Falasca et al., 2008); these latter authors propose a simulation-based methodology for this purpose. Many authors have defined programming models to optimize the resilience level of SCs (Khalili et al., 2017, for instance), by trying to restore the lost capacities when the disruptions occur, but many others have used similar models. Instead, Mohapatra et al. (2015) propose a methodology to calculate the global resilience of the supply network based on successive calculations of Chaotic Supply Reliability and

Recoverability for each node. Researchers agree that one of the issues is how to measure this network characteristic.

The resilience of supply networks has also been studied using complex network analysis tools. Typically, scale free/power law networks are considered and both random disruptions and targeted attacks are implemented (e.g. Nair and Vidal 2010, Hearnshaw and Wilson 2013, Mari et al. 2015, Wang et al. 2015). Some of these studies' findings are that denser/more complex networks are not always more resilient and that redundancy may not always lead to greater resilience (Kim et al., 2015).

The idea behind our proposed approach is to assess the robustness of a given SC network when some of its active transportation links fail, as regards the percentage of demand that the company will be able to satisfy, i.e. the service level that it can maintain. To that end, we first formulate a standard cost minimization model aimed at satisfying all the required demand. This leads to the base network whose robustness is to be analysed by how it responds to the collapse of links. From the base network, we formulate a lexicographic, bi-objective model that minimizes unserved demand and costs, so as to identify the best re-routing alternative when some links in the base network collapse. In that way, as links successively fail, a pair of values [service level; cost] can be computed by measuring the percentage of demand still served, and the minimum cost of delivering the product. As progressively more links fail, the percentage of products delivered will be non-increasing and the area under that curve can be used as the robustness index of the network.

This robustness index depends on the order in which the links are assumed to fail. This can be seen in Figure 1, which shows how the service level is affected for two different sequences of collapsing links. Note that the Final Service Level, which corresponds to removing all the initial active links in the base network, is the same irrespective of the order in which the links are assumed to fail. Moreover, that Final Service Level is not necessarily zero; this depends on the availability of alternative routes for delivering the product, beyond the base network.

========= FIG 1 ==========

Apart from the proposed approach to measuring the robustness of a supply network, this paper also carries out an experimental study of those factors that can affect that robustness. We differentiate between failure due to natural (random) causes (accidents or weather, for instance), and cases where link failures are targeted to generate the maximum disturbance (strikes or terrorist attacks, for instance). These experiments are presented and discussed in Section 4. Before that, In Section 3, the optimization models used to compute the base network and to re-compute product flows after link failures are formulated.

2. RELEVANT LITERATURE

The changing environment in which businesses (and their SCs) are involved makes the study of how to manage risk and how to confront the effects of such uncertainty of special importance. Recalling some worldwide prominent news, we can find all sorts of events that have made huge impacts on the global economy. Consider, for example, devastating earthquakes, such as the one that occurred in Taiwan in September 1999, which seriously affected the infrastructures of Hsinchu Industrial Park where 10% of the world's computer chips are manufactured, therefore disrupting supply to the big global computer companies (Bhamra et al., 2011). Many other examples of natural (fires, floods, epidemics, volcanic eruptions, storms,…) or man-made (nuclear accidents, terror attacks, sabotage, strikes) disasters are periodically reported as damaging the SCs of many companies, and in some cases affecting their long-term competitiveness.

For the above reasons, the research on Supply Chain Risk Management (SCRM) has gained importance both from the practitioner and academic points of view (Hohenstein et al., 2013). However identifying and classifying potential events that can affect the logistics of a company is not enough. The main goal of

SCRM is to design and maintain resilient SCs (Grötsch et al., 2013), i.e., to be prepared for the potential events disrupting the flows, respond quickly to minimize those effects and restore the system functioning to a normal state.

The concept of Supply Chain Resilience (SCRES) dates back to the first decade of this century (Hohenstein et al., 2013) as a consequence of some major issues such as the 9/11 terror attacks in New York and other natural disasters of those years. Initially the concept of resilience was taken from ecology and the physical property of a material returning to its original state after deformation (Spiegler et al., 2012), and for that reason the focus of SCRES was on the ability to react in order to return to normal operation. Different strategies were proposed in the literature for making the SC more resilient, mainly through the use of flexible, redundant and collaborative networks (Hohenstein et al., 2013).

The so-called "resilience triangle" (Tukamuhabwa et al., 2015) can be used to represent the effects of what resilience means in the SC (Figure 2). Here, two of the concepts around resilience are visualized: the time to recovery after a disruption, and the consequence of such disruption (segment NR). A possible static measure of SC resilience is to calculate the area of such a triangle, since small values would imply no huge consequences or a quick recovery. However, Tukamuhabwa et al. (2015) consider this tool more in a dynamic context, using it for comparing, under different events in time, how the area of such a triangle evolves, as proof of an improvement in the resilience of the network.

==== FIGURE 2 ====

The concept of resilience is not the only one used by SC researchers as some other related concepts are being used as well, in many cases interchangeably (Miller-Hooks et al., 2012). Faturechi and Miller-Hooks (2015) summarize them in the context of transportation networks considering *vulnerability* as the susceptibility of the system to incidents, causing operational degradation; the complement (i.e., measuring strength instead of loss; see Reggiani et al., 2015) would be *robustness* (ability of a system to

continue in operation) and *reliability* (probability that the network remains operative at least at a minimum service level, i.e., reliable implies robust); also, *survivability* measures the percentage of demand that could be met after disruption. Finally, *resilience* would be the ability to resist and absorb disturbance (built on all the previous concepts) and then to adapt to be able to return to normal functionality. Therefore, according to this taxonomy, a robust system has the ability to resist a disturbance, while a resilient one is able to absorb disturbance, adapt itself and return to the original state.

In the approach proposed in this paper, since we measure exclusively the effects explained by the segment NR in Figure 2 (i.e., how deeply the SC is affected by the disturbance) and the time to recovery is not a factor in our study, we are really measuring the survivability of the network according to the categorization by Faturechi and Miller-Hooks (2015). However, as already commented, the above terminology is not unanimously used. Peng et al. (2011), for instance, consider robustness as the ability to perform well in the future with respect to uncertain scenarios, while reliability means to perform well when parts of the system fail.

In spite of growing interest in SC resilience, just a few papers (see review by Kamalahmadi and Parast, 2016a, or Ivanov et al., 2017) have dealt with how to measure it. Given the difficulty of the measurement, some authors propose approaches based on personal judgment (Yilmaz-Börekci et al., 2015), or subjective procedures relying on survey assessment of different vulnerability factors affecting a specific SC (Pettit et al., 2013).

Regarding methodology, Reggiani et al. (2015) state that most contributions to the study of transport resilience measurement are based on simulation. Munoz and Dunbar (2015) use a commercial simulation software, ExtendSim, to analyse disruptions in a three-tier SC. Jain and Leong (2005) propose the use of simulation to assess SC performance under stress, by considering different scenarios, with the simulation model determining the capacities and inventories needed at different nodes to meet the requirements. In fact, according to Lou and Zhang (2011) the ultimate goal of measuring transportation resilience would

be to know where to assign resources in order to improve the response after an attack. In any case, according to Spiegler et al. (2012) the resilience should always be measured as the result for the end customer, regardless of where in the supply network the disruptive event has occurred. In our case, we measure the effects of disruptions using the service level attained after the event.

Zhang et al. (2015) hypothesize that the resilience of a network to a disaster depends heavily on its topology. They selected 17 standard topologies grouped into four clusters: highly connected (common in large urban streets such as grid, diamond networks,…); centrally connected (common in air networks, such as hub and spoke, rings,…); circuit-like connected (common in the underground and urban road, such as central ring, double U,…); and random connected (common in roadway systems, such as random, scale-free, or small-world). By considering three measures of resilience (throughput, connectivity between origin-destination pairs, and the average reciprocal distance between all O-D pairs), they developed an experiment framework concluding that the three resilience measures decrease with the network diameter and increase with average degree. Moreover, they found that the first and third topology clusters seemed to be the most resilient, while the fourth and second were less resilient. Kim et al. (2015) also base their analysis on network structure characteristics, considering four different topologies usually found in real logistics networks (block-diagonal, scale-free, centralized and diagonal). They define a measurement of the resilience by performing a Monte Carlo procedure considering the times that disrupting a randomly chosen node does not imply a total collapse of the network.

However, to base all the vulnerability analysis in the topological characteristics of the network, as a number of authors have done, does not seem reasonable for some authors (Nagurney and Qiang, 2012) as there are some other dynamic factors (such as flows or behaviour of the users) which are part of the complexity of the problem and must be considered as well. In fact, in their discussion, Mattsson and Jenelius (2015) identify a second group of works in the field (which they call a system-based vulnerability analysis of transport networks) that consider many more aspects (demand, travel time, costs,

etc.) beyond the pure topology of the network, as being able to provide a more complete description of the consequences of different disruptive events.

Miller-Hooks et al. (2012), in the model they present to measure and maximize the resilience of a transportation network, consider as the objective function the percentage of demand that can be satisfied post-disaster. Morohosi (2010) measures the robustness of a network by analysing pairs of nodes still connected and the distribution of the shortest path lengths, after the removal of some edges. Monte Carlo was again the methodology used for that. When dealing with transportation systems, Lou and Zhang (2011) noted the difficulty in providing a straightforward definition of performing at an acceptable level, and for that reason they propose as measures the network connectivity, travel time, capacity or client satisfaction. Some other authors have also proposed ways to measure robustness. For instance, Soni et al. (2014) use a six-step procedure involving surveys, Structural Equation Modelling (SEM) and matrix calculus. Our procedure, however, represents an intuitive and quite straightforward method to evaluate the asymptotic behaviour of any logistic network.

In the analysis of the behaviour of a network when some disruptions occur, Norrenbrock et al. (2016) consider three main strategies when selecting the node to remove as a result of the disruption. In the most simplistic, *random failure*, the node (or arc) that breaks down or fails is picked uniformly at random. Alternatively, there can be *targeted attacks* when the selected node is chosen based on some relevant measure: degree-based picking (the most used according to Tan et al., 2016) where nodes with more connections are more likely to be attacked; or betweenness-based picking where the nodes crossed by the highest number of shortest paths between any two nodes are more likely to be attacked. This situation corresponds to deliberate actions against the performance of the SC (such as strikes or terrorist actions). It is well reported (e.g. Norrenbrock et al., 2016) that scale-free networks are quite robust under random failure but not so under targeted attack. Duan and Lu (2014) use the same two strategies for analysing the robustness of different cities' networks.

Our approach considers, as Miller-Hooks et al. (2012) do, the service level post-disaster as the objective measure of the resilience of a specific logistics network, acknowledging the efficient delivery of goods as the main function of the SC. In order to assess its robustness under stress, the idea is similar to the procedure carried out by some of the authors mentioned above: by removing some edges, the performance of the networks is measured and, based on that information, an index will be computed. Note that although Peng et al. (2011) only consider scenarios in which only one link is disrupted considering it to be very unlikely that more than one facility is down at the same time, related links are indeed likely to fail (for instance, an earthquake will shut down many facilities in a region, or a strike will impede the service of many different transportation companies). Therefore disruptions propagation is a topic of practical interest (Scheibe and Blackhurst, 2017).

Again, the way in which links are removed will affect the network performance. As mentioned above, there are two main strategies to remove edges when doing complex networks analysis: randomly and under targeted attack. Although the under targeted attack degree-based picking is usually considered (attack first the nodes with a higher degree, see Tan et al., 2016), in our case however we have found it more appropriate for a SC network to select links based on the assigned flow. It seems reasonable to assume that links moving more goods could be more harmful for the whole network when collapsing, and therefore they could be targeted first when looking for intentional, major damage.

3. MODELLING THE NETWORK RESPONSE TO LINK FAILURE

The scenario considered in this paper is a standard supply network with four levels: suppliers, plants, wholesalers and retailers. This is a common topology used in many previous researches (Sabri and Beamon, 2000). There are just a few standard assumptions. Thus, the demand occurs at the retailers. There are no fixed costs at any of the facilities (this assumption could be relaxed at the expense of requiring binary variables in the optimization model). The flows along the different transportation links

are decision variables and they are subject to maximum flow capacity constraints (Figure 3). In order to control how close to a complete graph the logistics network is, some sets of non-existent links (compared to the complete subgraph between two consecutive echelons) are defined.

===== FIG 3 =====

The notation used is the following:

Data

s	index for suppliers
p	index for plants
w	index for wholesalers
r	index for retailers
$P^X(s)$	{p: arc (s,p) is non-existent in the logistic network}
$W^X(p)$	{p: arc (p,w) is non-existent in the logistic network}
$R^X(w)$	{p: arc (w,r) is non-existent in the logistic network}
D_r	demand at retailer r
U_{sp}	maximum flow capacity of link between supplier s and plant p
U_{pw}	maximum flow capacity of link between plant p and wholesaler w
U_{wr}	maximum flow capacity of link between wholesaler w and retailer r
c_{sp}	unit transportation cost between supplier s and plant p
c_{pw}	unit transportation cost between plant p and wholesaler w
c_{wr}	unit transportation cost between wholesaler w and retailer r

Variables

x_{sp}	product flow between supplier s and plant p

x_{pw} product flow between plant p and wholesaler w

x_{wr} product flow between wholesaler w and retailer r

It is assumed that the optimal supply network design is computed using the following cost minimization model:

$$\text{Min} \quad \sum_s \sum_p c_{sp} x_{sp} + \sum_p \sum_w c_{pw} x_{pw} + \sum_w \sum_r c_{wr} x_{wr} \tag{1}$$

s.t.

$$\sum_w x_{wr} = D_r \qquad \forall r \tag{2}$$

$$\sum_s x_{sp} = \sum_w x_{pw} \qquad \forall p \tag{3}$$

$$\sum_p x_{pw} = \sum_r x_{wr} \qquad \forall w \tag{4}$$

$$0 \le x_{sp} \le U_{sp} \quad \forall s \forall p \notin P^X(s) \qquad x_{sp} = 0 \quad \forall s \forall p \in P^X(s) \tag{5}$$

$$0 \le x_{pw} \le U_{pw} \quad \forall p \forall w \notin W^X(p) \qquad x_{pw} = 0 \quad \forall p \forall w \in W^X(p) \tag{6}$$

$$0 \le x_{wr} \le U_{wr} \quad \forall w \forall r \notin R^X(p) \qquad x_{wr} = 0 \quad \forall w \forall r \in R^X(p) \tag{7}$$

This is a simple minimum cost flow linear programming (LP) model in which the demand at each retailer has to be satisfied without exceeding the maximum flow constraints at the transportation links and without using the non-existent links. The optimal supply network that results will be the "base network" against which we will compare the network operation when we study how to respond to transportation links' failures. Thus, links not used in the base network may be activated later, if necessary, after some base links have failed, since they are fully operative although they were not initially selected for the base network.

The base network corresponds, therefore, to the optimal product flows $x^*_{sp}, x^*_{pw}, x^*_{wr}$ which lead to the following sets of active links:

$P^*(s) = \{p : x^*_{sp} > 0\}$ Subset of plants supplied by supplier s in the base network

$W^*(p) = \{w : x^*_{pw} > 0\}$ Subset of wholesalers supplied from plant p in the base network

$R^*(w) = \{r : x^*_{wr} > 0\}$ Subset of retailer r supplied from wholesaler w in the base network

Therefore, the subset of arcs that are active in the base network correspond to $\{(s,p) : p \in P^*(s)\}$, $\{(p,w) : w \in W^*(p)\}$ and $\{(w,r) : r \in R^*(w)\}$.

In order to measure the robustness of the base network we must be able to re-compute the optimal product flows, given that certain links have failed. Specifically, let

$P^-(s)=\{p \in P^*(s)$: arc (s,p) has failed$\}$

$W^-(p)=\{w \in W^*(s)$: arc (p,w) has failed$\}$

$R^-(w)=\{r \in R^*(s)$: arc (w,r) has failed$\}$

When considering link failures, the above model (1)-(7) is no longer adequate as it may have no feasible solutions, and we have to foresee the possibility that the demand may not be completely satisfied. Then, in addition to minimizing costs, we should also maximize the service level measured by the percentage of demand satisfied. This makes our model become a bi-objective optimization problem that may be solved lexicographically.

$$\text{Lex Min} \quad \left\{ \sum_r d_r, \sum_s \sum_p c_{sp} x_{sp} + \sum_p \sum_v c_{pw} x_{pw} + \sum_w \sum_r c_{wr} x_{wr} \right\} \tag{8}$$

s.t.

(3)-(7)

$$\sum_{w} x_{wr} = D_r - d_r \qquad \forall r \tag{9}$$

$$x_{sp} = 0 \qquad \forall s \forall p \in P^{-}(s) \tag{10}$$

$$x_{pw} = 0 \qquad \forall p \forall w \in W^{-}(p) \tag{11}$$

$$x_{wr} = 0 \qquad \forall w \forall r \in R^{-}(p) \tag{12}$$

This lexicographic optimization model is still a min-cost flow network problem but only in that the first objective function aims at maximizing the amount of demand satisfied and, once that is achieved and if there are alternative optima, the cost is minimized.

Therefore, to summarize, the supply networks considered could not be fully connected (depending on the cardinality of the non-existent link sets). The links that in principle can be used are designated as *potential links* because they are ready to be used. Of those, some are used in the base network solution, after optimizing the operation costs. Those links are called *base links*. When the base links fail then some potential links not used in the base network may need to be used in order to minimize the service level impact (and cost) of the failures.

As indicated in the introduction, and shown in Figure 1, the idea is to measure the robustness of the base network by seeing how it can accommodate link failures without reducing the service level, or reducing it as little as possible. Since that depends on how the link failures are supposed to occur, a certain assumption in this regard has to be made. Thus, link failures may be expected to occur at random or they may be assumed to occur according to some intentional attack strategy. The latter may be guided by different link centrality measures that may require local (e.g. flow level) or global information (e.g. betweenness centrality) and the ordering of the links to fail can be predetermined (static link ordering) or

it can be updated dynamically (dynamic link ordering). Although the latter may be more effective in terms of damaging the network performance, it is more complex and requires more computation.

Once we have computed for a given sequence of link failures in the resulting service levels, we obtain a function showing the evolution of the demand fulfilment for that specific sequence of link shutdowns (see Figure 1). If the network is robust, that function should be flat since final customers will hardly be affected and the service will stay close to 100%; however, for vulnerable SCs, as links fail the service level is significantly affected and the function will decrease rapidly. For that reason, we define our index of robustness R as the ratio between the area below the service level function corresponding to a specific links failure strategy, and the area below the constant 100% service level function.

4. EXPERIMENTAL FRAMEWORK AND RESULTS

In this section the results of an experimental design aimed at testing which factors have an effect on the robustness of the base network are presented. For the link failures, both a random and a static link ordering have been considered. The targeted attack considered ranks the links according to product flow, so it is assumed that the link with the largest product flow is the first to fail, followed by the link with the second largest product flow, and so on.

Three experimental factors have been considered. The first two factors refer to the network complexity, which, according to Craighead et al. (2007), can affect the severity of disruptions in a supply network. Thus, factor F1 is node complexity (i.e. the number of nodes in the different levels of the supply network), while factor F2 is flow complexity (i.e. the number of potential links in the supply network). For each of these two factors two levels have been considered, as shown in Table 1. The third factor considered comes from the effects of excess capacity on resilience, as reported by Mohapatra et al. (2015). Again, two levels have been considered for factor F3 link capacity (low and high).

==== TABLE 1 ====

Note that from a managerial point of view, F1 captures the centralization (respectively, decentralization) logistics strategy, i.e. having a smaller number of facilities but of higher capacity (versus a high number of smaller plants). In a similar way, F2 corresponds to the strategy of subcontracting a small number of transportation companies (with high capacity in order to be able to fulfil all the demand) versus working with a high number of smaller companies.

For each of the 2^3 factor level combinations, 50 random instances were generated which makes a total of 400 problem instances. Unit transportation costs for each link were randomly generated between one and ten. For each instance, the demand of each retailer was randomly generated between 30 and 130 units.

Figure 4 shows an example of the evolution of service level under both types of link failure ordering (random and static targeted attack based on product flow), for a specific instance corresponding to the case of low node and flow complexity and high link capacity. As can be seen, the service level when the link failures are targeted decreases sooner and faster than under random link failure. The curve corresponding to random failures is the average of 100 random runs.

==== FIG 4 ====

Looking at all the 400 instances and their robustness for the two types of link failure considered (see Figure 5), we observe that, as expected, it always happens that a targeted attack is more (or at least as) damaging as random failures. The vertical axis represents the robustness index R, measured as the area under the curve of the service level evolution (see Figure 1). The maximum theoretical value of the robustness index is 100% although that level, which would correspond to a situation in which the network can accommodate successive link failures with no service level reduction at all, is difficult to be achieved in practice. For most factor combinations, the difference in robustness between the random failure and the targeted attack is more or less constant and quite significant (around 40%).

However, for some factor level combinations (specifically in the case of small flow complexity, F2=1) both results are similar, with a resulting small amount of demand not satisfied (Final Service Level close to 100%) and with a greater dispersion when the node complexity is also small (F1=1; see Figure 6). In fact, a t-test confirms that in the case of F2=1, the difference between the robustness under a targeted attack is statistically similar to the robustness under random failures (p-value=0.41). This means that when the number of potential links is smaller (i.e., there is a higher number of non-existent arcs in the complete graph), then those used in the base solution are likely to carry a significant amount of flow so that removing any of them randomly has a similar effect to removing first those with the largest flows.

==== FIGS 5 and 6 =====

Also, from Figure 5 we can observe that moving from F3=1 to F3=2 (i.e. adding capacity to links) increases robustness, *ceteris paribus*, except in the mentioned case of F2=1 in which the results are the same.

Regarding the service level Final_SL maintained after all the links in the base network have failed (and therefore only links not initially used in the base network can be considered for delivering the product), it is clearly affected only by flow complexity (F2): in the case of high flow complexity (F2=2), the service level at the end is notably smaller than the service level in low flow-complexity scenarios (see Figure 7). In order to understand this result, it must be noted that F2=2 means that many potential links (actually the complete subgraph between every two consecutive echelons) all with a low capacity can be used for designing the network, and therefore the base network being assessed will use many of those links; therefore, when the base links start failing (and given networks of comparable size) there are fewer alternative potential links to reroute the flow and hence the service level is clearly affected.

==== FIG 7 =====

To appraise how the three response variables (namely the Robust Index for Targeted attack, R_target, the Robust Index for Random failures, R_random, and the Final Service Level after all base network links failed, Final_SL) are related, a correlation between them is computed, with all of them being significant. Thus, R_random exhibits a high positive correlation with R_target (0.991) and with Final_SL (0.989). Similarly, the correlation between R_target and Final_SL is also high and positive (0.998).

Given this dependence relationship, the statistical analysis of results relies on a MANOVA analysis (Huberty and Morris, 1989). MANOVA allows the simultaneous testing of both: 1) the equality of means from different responses; and 2) if the response variables are altered by the manipulation of the independent variables (factors). Thus, it provides further evidence of the relative contribution of the response variables to the resultant effects of the treatment variables. In addition: (*i*) the power of the test increases, as it is able to detect differences too small to be detected through individual analysis of variance (ANOVA); (*ii*) it can detect multivariate response patterns; and (*iii*) it minimizes the probability of making one or more Type I errors (i.e. concluding that a difference exists when it does not) for the entire set of comparisons. MANOVA requires the checking of nine assumptions, which in our case were successful.

With the aim of examining individually each of the three response variables, an ANOVA was performed to evaluate the effects of the three factors and their two-way interactions on each response variable. Before using ANOVA, the three main assumptions (normality, homogeneity of variance, and independence of residuals) were checked without finding any basis for questioning their validity.

The ANOVA in Table 2 shows the effects of the studied factors on R_target. These ANOVA results (R^2 = 99.93%) show that all factors and their corresponding two-way interactions are statistically significant. It should be noted that the flow complexity (F2) is the main contributor to the resulting robust index in the case of target attack. It explains about 97.63% of the variance in the R_target index, while node complexity (F1) only explains 0.32% of the observed variability.

==== TABLE 2 ====

The ANOVA in Table 3 shows the effects of the studied factors on R_random. These ANOVA results (R^2 = 99.64%) again show that all factors and their corresponding two-way interactions are statistically significant. Also in this case flow complexity (F2) is the main contributor to the resulting robust index. It explains about 92.49% of the variance in the R_random index, while node complexity (F1) only explains 0.99% of the observed variability.

==== TABLE 3 ====

The ANOVA in Table 4 shows the effects of the studied factors on Final_SL (R^2 = 99.79%). In this case, the three factors and the interaction between F2 and F3 are statistically significant. As before, flow complexity (F2) is the main contributor to Final_SL. It explains about 97.66% of the variance in Final_SL, while node complexity (F1) only explains 0.57% of the observed variability.

==== TABLE 4 ====

In order to explain this situation, where flow complexity (F2) is the main contributor for the three response variables, it should be observed that, as mentioned above, when we consider an instance with a complete graph (i.e. F2=2) there can be more links in the base network, as a consequence of the strategy of subcontracting a high number of small transportation companies. In fact, there is a negative correlation between the number of links in the base network and the R_target index (-0.628), with the R_random index (-0.591) and with Final_SL (-0.625). This means that as the number of links used in the base network increases, the value in these response variables decreases, which could be interpreted as follows: choosing the SC strategy of using few big transportation companies makes the SC network more likely to be resilient (robust) under both targeted attacks and random failures, and to maintain higher service levels. This can be explained by the fact that when the base design uses only a few of the potential links, it gives the distribution network more opportunities to reconfigure by utilizing the unused potential links.

We also examined the variability, error, and partial correlation matrices to assess the performance of the MANOVA. To appraise how the response variables are related, a partial correlation between them is computed. We use the Wilk test to judge whether there is significant evidence for model effects. In Table 5, the *p* values for the F1–F3 factors show that different levels of each factor affect the responses differently; also, there is significant evidence for interactions between factors at α level 0.05. The second column in Table 5 shows the relative contribution of each factor to each response variable. The Eigen analysis was used to assess how the response means differ among the levels of the different factors. Considering the flow complexity (F2), the highest absolute value within these eigenvectors is for the response R_target, the second highest is for R_random, and, finally, the value for Final_SL is small. This implies that the R_target means have the largest differences between these factor levels, the R_random means have the next largest differences, and the Final_SL means have the smallest differences. From the results of the Eigen analysis, it is evident that the R_target means have larger differences among all factor levels as well as in some two-way interactions.

==== TABLE 5 ====

From the previous analysis, we conclude that (a) all factors and their corresponding two-way interactions are statistically significant for the three response variables; (b) flow complexity is mainly responsible for the variance in the three response variables; and (c) link capacity is the second factor most responsible for the observed variability in the three response variables.

5. CONCLUSIONS

In this paper a novel measure of the robustness of a supply network under the successive collapse of its transportation links is proposed. It is based on the area under the curve that shows the evolution of the

service level as the links collapse sequentially. Extensive numerical experiments have been carried out considering both random failures and targeted attacks.

The results show that the robustness of the network under random failures is always greater than (or at least equal to) the robustness under targeted attacks, for all the scenarios considered. Flow complexity (i.e. the number of potential links) is the main factor that affects the robustness index in both cases, as well as affecting the Final Service Level, with more flow complexity leading to less robustness and lower Final_SL, as less flow complexity means a smaller number of higher-capacity links are used in the base network being assessed (and therefore, more alternatives are available to mitigate the links' collapse). In other words, the existence of more alternative potential links to mitigate the links' collapse increases robustness. The capacity of the transportation links does not seem to have much influence on robustness and less so the node complexity.

Additional experiments must be carried out to confirm these results, mainly considering certain relationships among failing links (e.g. shutdown of all the links in a region due to an earthquake, unionized strikes, etc.), instead of links that are absolutely independent. Also, other link failure orderings (see for instance Nie et al., 2015) could be used to assess the robustness of the network.

Finally, what we are measuring here is the ability of the system to continue servicing the customers in a cost-effective way when disturbances appear. This is a mixture of robustness and survivability. Analyzing and building resilience is also important and might involve additional assumptions on how to be able to return to normal functionality. Such a study is clearly a topic for further research.

Acknowledgements. This research was carried out with the financial support of the Spanish Ministry of Science and the European Regional Development Fund (ERDF), grant DPI2017-85343-P. The authors are also grateful to the reviewers for their helpful comments and suggestions.

REFERENCES

Behzadi, G., O'Sullivan, M.J., Olsen, T.L. and Zhang, A. (2017) Allocation flexibility for agribusiness supply chains under market demand disruption, International Journal of Production Research, in press.

Bhamra, R., Dani, S. and Burnard, K. (2011) Resilience: the concept, a literature review and future directions, International Journal of Production Research, 49, 18, pp. 5375-5393.

Chozick, A. (2007) A key strategy of Japan's car makers backfires. Wall Street Journal, July 20, 2007 http://www.wsj.com/articles/SB118486495637071861 (last accessed February 2017).

Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J. and Handfield, R.M. (2007) The severity of supply chain disruptions: design characteristics and mitigation capabilities. Decision Sciences, 38, 1, pp. 131-156.

Duan Y. and Lu, F. (2014) Robustness of city road networks at different granularities, Physica A, 411, pp. 21-34.

Falasca, M., Zobel, C.W. and Cook, D. (2008) A Decision Support Framework to Assess Supply Chain Resilience. Proceedings of the 5th International ISCRAM Conference, Washington, DC, USA, May 2008, pp. 596-605.

Faturechi, R. and Miller-Hooks, E. (2015) Measuring the performance of transportation infrastructure systems in disasters: A comprehensive review, ASCE Journal of Infrastructure Systems, 21, 1, pp. 0401402501-0401402515.

Grötsch, V.M., Blome, C. and Schleper, M.C. (2013) Antecedents of proactive supply chain risk management – a contingency theory perspective, International Journal of Production Research, 51, 10, pp. 2842-2867.

Hearnshaw, E.J.S. and Wilson, M.M.J. (2013) A complex network approach to supply chain network theory, International Journal of Operations & Production Management, 33, 4, pp. 442-469.

Hohenstein, N.O., Feisel, E. and Hartmann, E. (2013) Research on the phenomenon of supply chain resilience, International Journal of Physical Distribution & Logistics Management, 45, 1/2, pp. 90-117.

Huberty, C. J. and Morris, J. D. (1989) Multivariate analysis versus multiple univariate analyses. Psychological Bulletin, 105, 2, pp. 302-308.

Ivanov, D., Dolgui, A., Sokolov, B and Ivanova, M. (2017) Literature review on disruption recovery in the supply chain, International Journal of Production Research, 57, 20, pp. 6158-6174.

Jain, S. and Leong, S. (2005) Stress testing a supply chain using simulation, Proceedings of the 2005 Winter Simulation Conference, Orlando, FL, December 2005, pp. 1650-1657.

Khalili, S.M., Jolai, F. and Torabi S.A. (2017) Integrated production–distribution planning in two-echelon systems: a resilience view, International Journal of Production Research, 55, 4, pp. 1040-1064.

Kamalahmadi, M. and Parast, M.M. (2016a) A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research, International Journal of Production Economics, 171, pp. 16-133.

Kamalahmadi, M. and Parast, M.M. (2016b) Developing a resilient supply chain through supplier flexibility and reliability assessment, International Journal of Production Research, 54, 1, pp. 302-321.

Kim, Y., Chen, Y.S. and Linderman, K. (2015) Supply network disruption and resilience: A network structural perspective, Journal of Operations Management, 33-34, pp. 43-59.

Lou, Y. and Zhang, L. (2011) Defending Transportation Networks against Random and Targeted Attacks, Transportation Research Record: Journal of the Transportation Research Board, 2234, pp. 31-40.

Mari, S.I., Lee, Y.H. and Memon, M.S. (2015) Complex network theory-based approach for designing resilient supply chain networks, International Journal of Logistics Systems and Management, 21, 3, pp. 365-384.

Mattsson, L.-G. and Jenelius, E. (2015) Vulnerability and resilience of transport systems – A discussion of recent research, Transportation Research A, 81, pp. 16-34.

Miller-Hooks, E., Zhang, X. and Faturechi, R. (2012) Measuring and maximizing resilience of freight transportation networks, Computers & Operations Research, 39, pp. 1633-1643.

Mohapatra, P., Nanda, S. and Adhikari, T. (2015) Resilience Measurement of a Global Supply Chain Network, IEEE 9th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, January 2015 (doi: 10.1109/ISCO.2015.7282383).

Morohosi, H. (2010) Measuring the network robustness by Monte Carlo estimation of shortest path length distribution, Mathematics and Computers in Simulation, 81, pp. 551-559.

Munoz, A. and Dunbar, M. (2015) On the quantification of operational supply chain resilience, International Journal of Production Research, 53, 22, pp. 6736-6751.

Nagurney, A. and Qiang, Q. (2012) Fragile networks: identifying vulnerabilities and synergies in an uncertain age, International Transactions in Operational Research, 19, pp. 123-160.

Nair, A. and Vidal, J.M. (2010) Supply network topology and robustness against disruptions – an investigation using multi-agent model, International Journal of Production Research, 49, 5, pp. 1391-1404.

Nie, T., Guo, Z., Zhao, K. and Lu, Z.M. (2015) New attack strategies for complex networks, Physica A, 424, pp. 248-253.

Norrenbrock, C., Melchert, O. and Hartmann, A.K. (2016) Fragmentation properties of two-dimensional proximity graphs considering random failures and targeted attacks, Physical Review E, 062125, pp. 1-11.

Peng, P, Snyder, L.V., Lim, A. and Liu, Z. (2011) Reliable logistics networks design with facility disruptions, Transportation Research B, 45, pp. 1190-1211.

Pettit, T.J., Croxton, K.L. and Fiksel, J. (2013) Ensuring supply chain resilience: Development and implementation of an assessment tool, Journal of Business Logistics, 34, 1, pp. 46-76.

Ponomarov, S.Y. and Holcomb, M.C. (2009) Understanding the concept of supply chain resilience, The International Journal of Logistics Management, 20, 1, pp. 124-143.

Reggiani, A., Nijkamp, P. and Lanzi, D. (2015) "Transport resilience and vulnerability: The role of connectivity", Transportation Research A, 81, pp. 4-15.

Sabri, E.H. and Beamon, B.M. (2000) A multi-objective approach to simultaneous strategic and operational planning in supply chain design, Omega, 28, 5, pp. 581-598.

Scheibe, K.P. and Blackhurst, J. (2017) Supply chain disruption propagation: a systemic risk and normal accident theory perspective, International Journal of Production Research, in press.

Soni, U., Jain, V. and Kumar, S. (2014) Measuring supply chain resilience using a deterministic modelling approach, Computers and Industrial Engineering, 74, pp. 11-23.

Spiegler, V.L., Naim, M.M. and Wikner, J. (2012) A control engineering approach to the assessment of supply chain resilience, International Journal of Production Research, 50, 21, pp. 6162-6187.

Tan, S.-Y., Wu, J., Lü, L., Li, M.-J. and Lu, X. (2016) Efficient network disintegration under incomplete information: the comic effect of link prediction, Scientific Reports, 6, article no. 22916. (doi: 10.1038/srep22916).

Tukamuhabwa, B.R., Stevenson, M., Busby, J. and Zorzini, M. (2015) Supply chain resilience: definition, review and theoretical foundations for further study, International Journal of Production Research, 53, 18, pp. 5592-5623.

Wang, W., Street, W.N. and de Matta, R.E. (2015) Topological Resilience Analysis of Supply Networks under Random Disruptions and Targeted Attacks, Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Paris, France, August 2015, pp. 250-257.

Yilmaz-Börekci, D., Iseri Say, A. and Rofcanin, Y. (2015) Measuring Supplier Resilience in Supply Networks, Journal of Change Management, 15, 1, pp. 64-82.

Zhang, X., Miller-Hooks, E. and Denny, K. (2015) Assessing the role of network topology in transportation network resilience, Journal of Transport Geography, 46, pp. 35-45.

List of figures and table captions

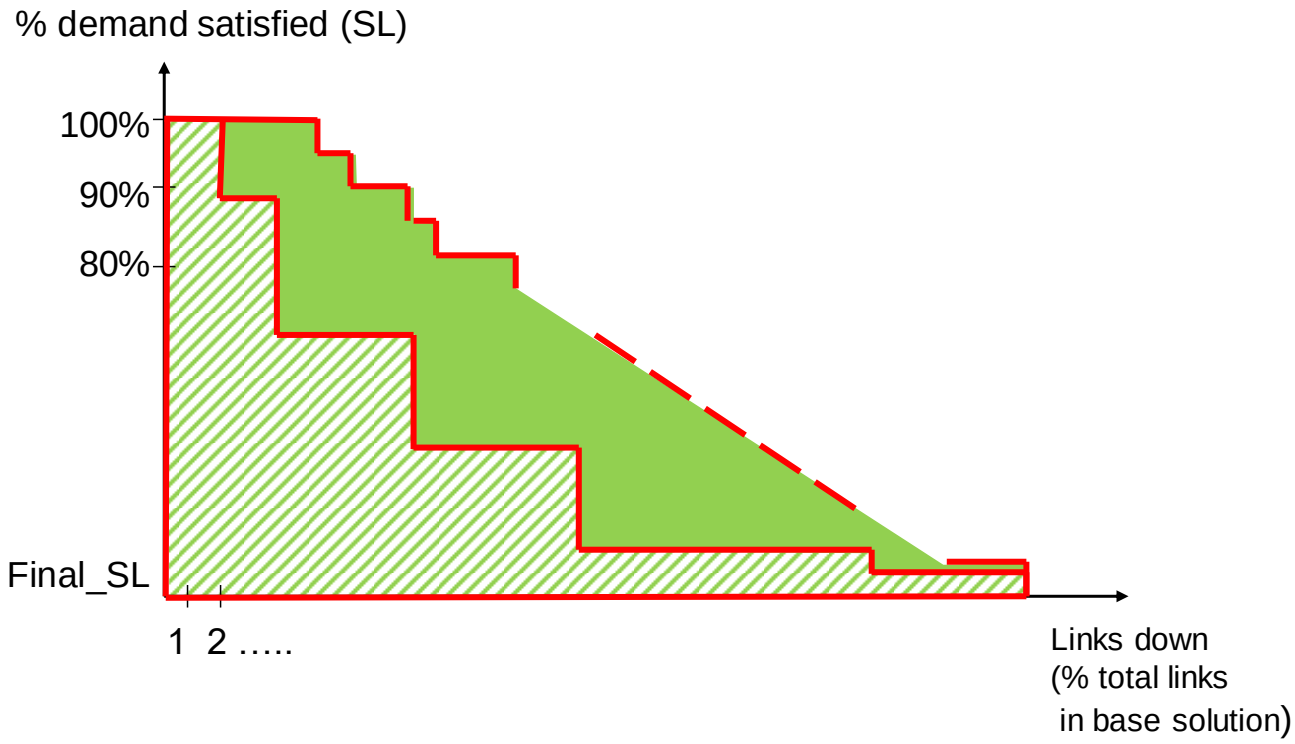

Figure 1. Evolution of service level (SL) for two different strategies for ordering the links that successively fail.

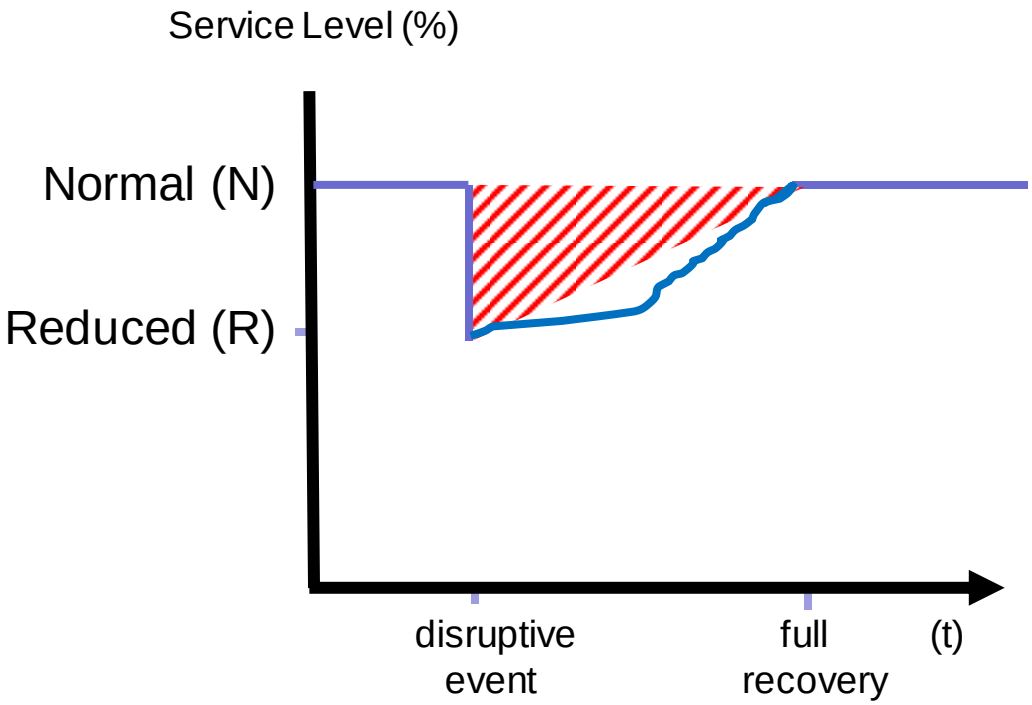

Figure 2. Resilience triangle concept.

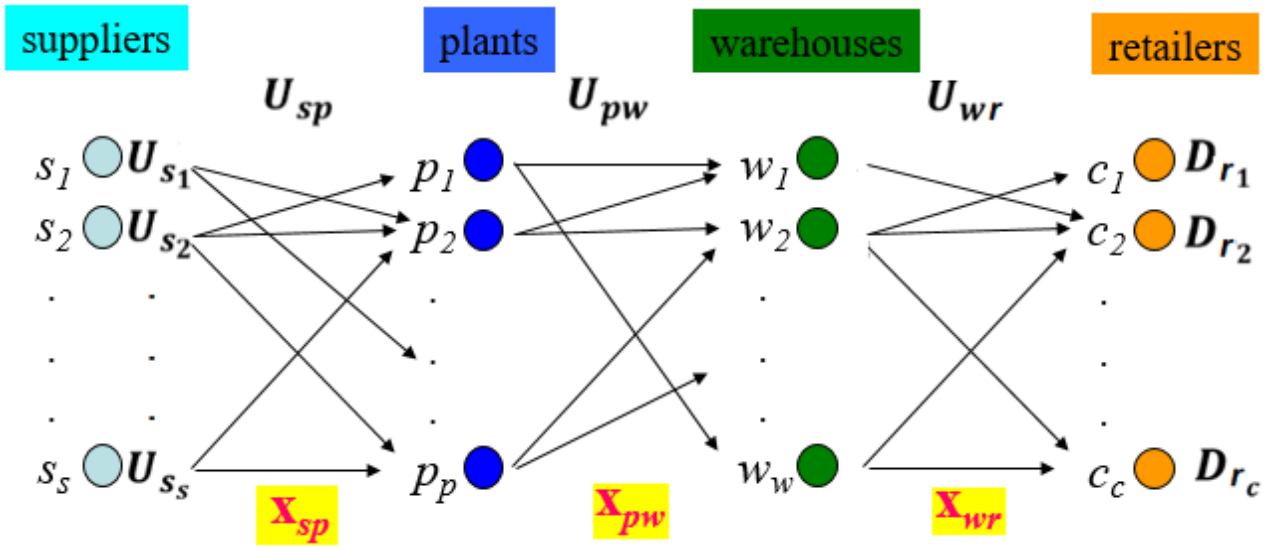

Figure 3. Standard four echelon supply network considered.

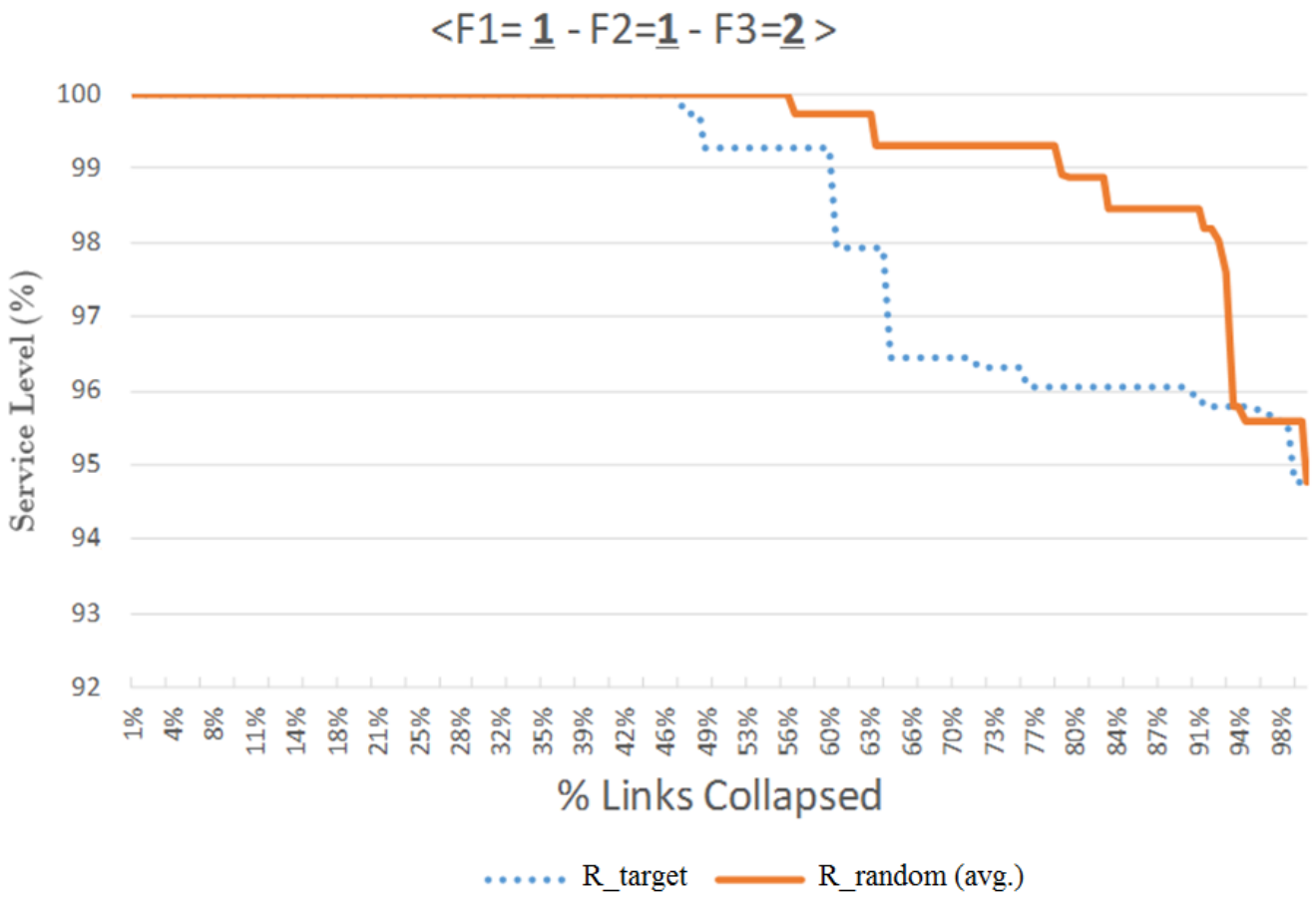

Figure 4. Evolution of service level under targeted attack and random failures, for an instance with low node and flow complexities (F1=F2=1) and high link capacity (F3=2). As observed, service level decreases quicker under targeted attack.

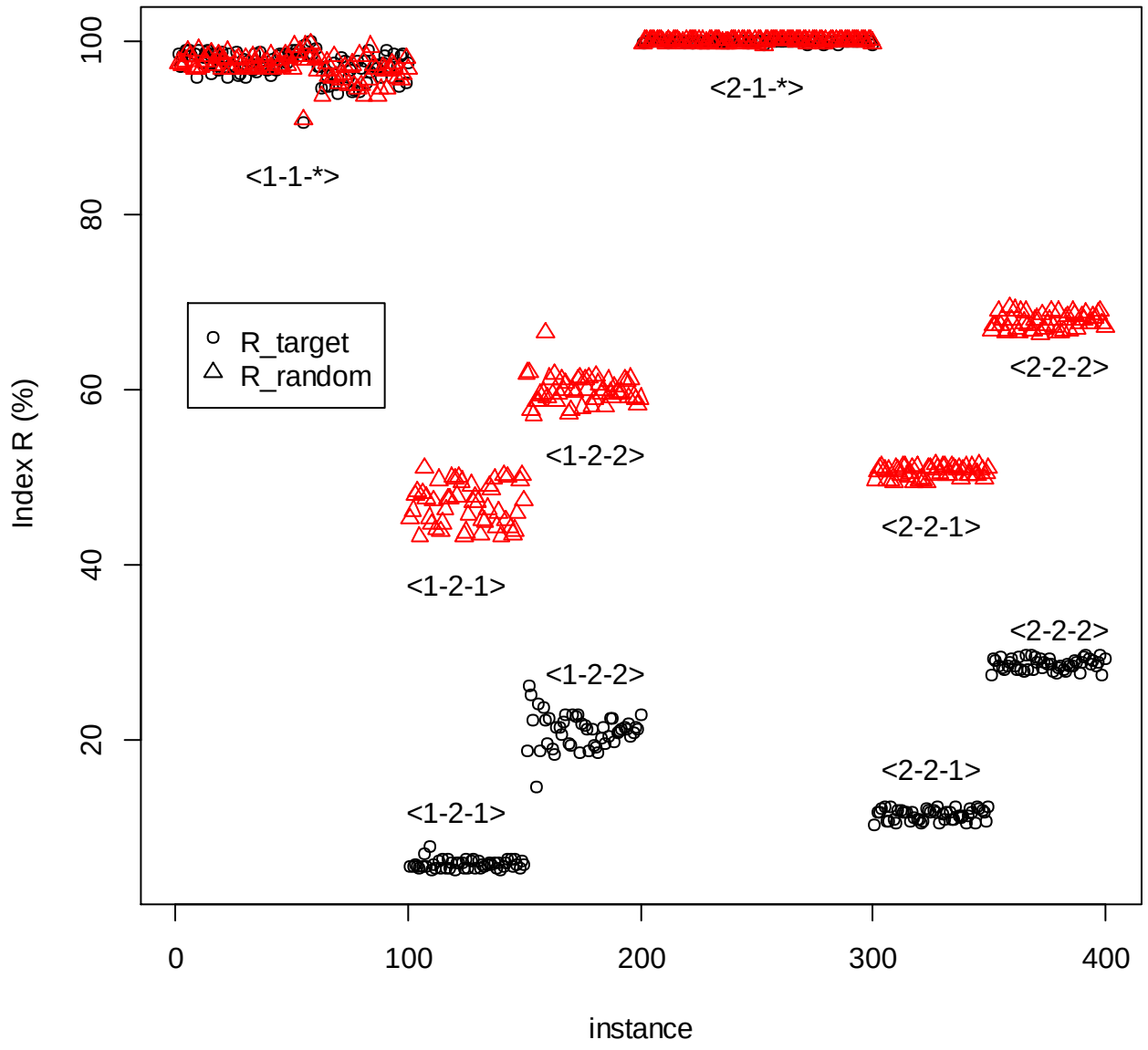

Fig. 5. Robustness under random failure and under targeted attack for each of the 400 instances used in the experiment. Levels (1-low; 2-high) of the different factors are shown as ⟨F1-F2-F3⟩.

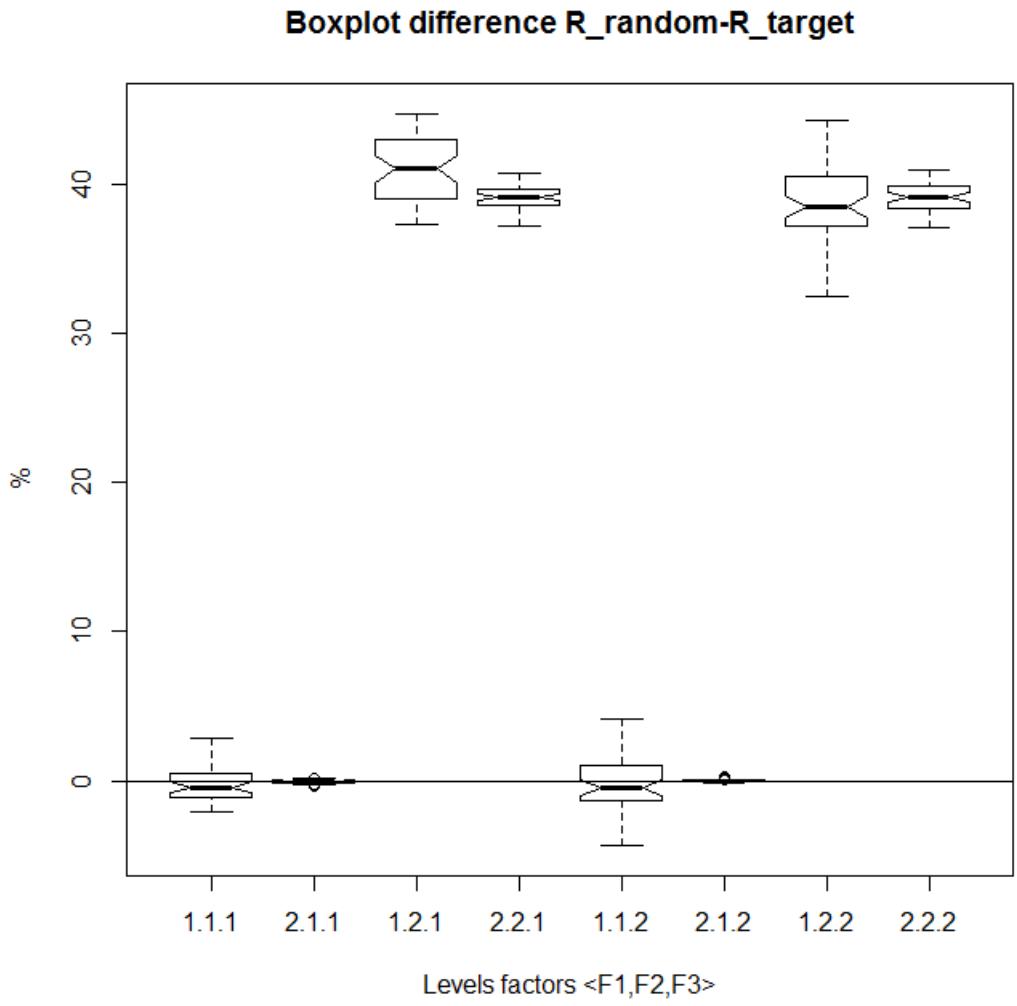

Figure 6. Boxplot of the difference between the robustness under random failure and under targeted attack. Positive values imply targeted attack is more harmful than random failure. Levels of the different factors are shown as F1.F2.F3.

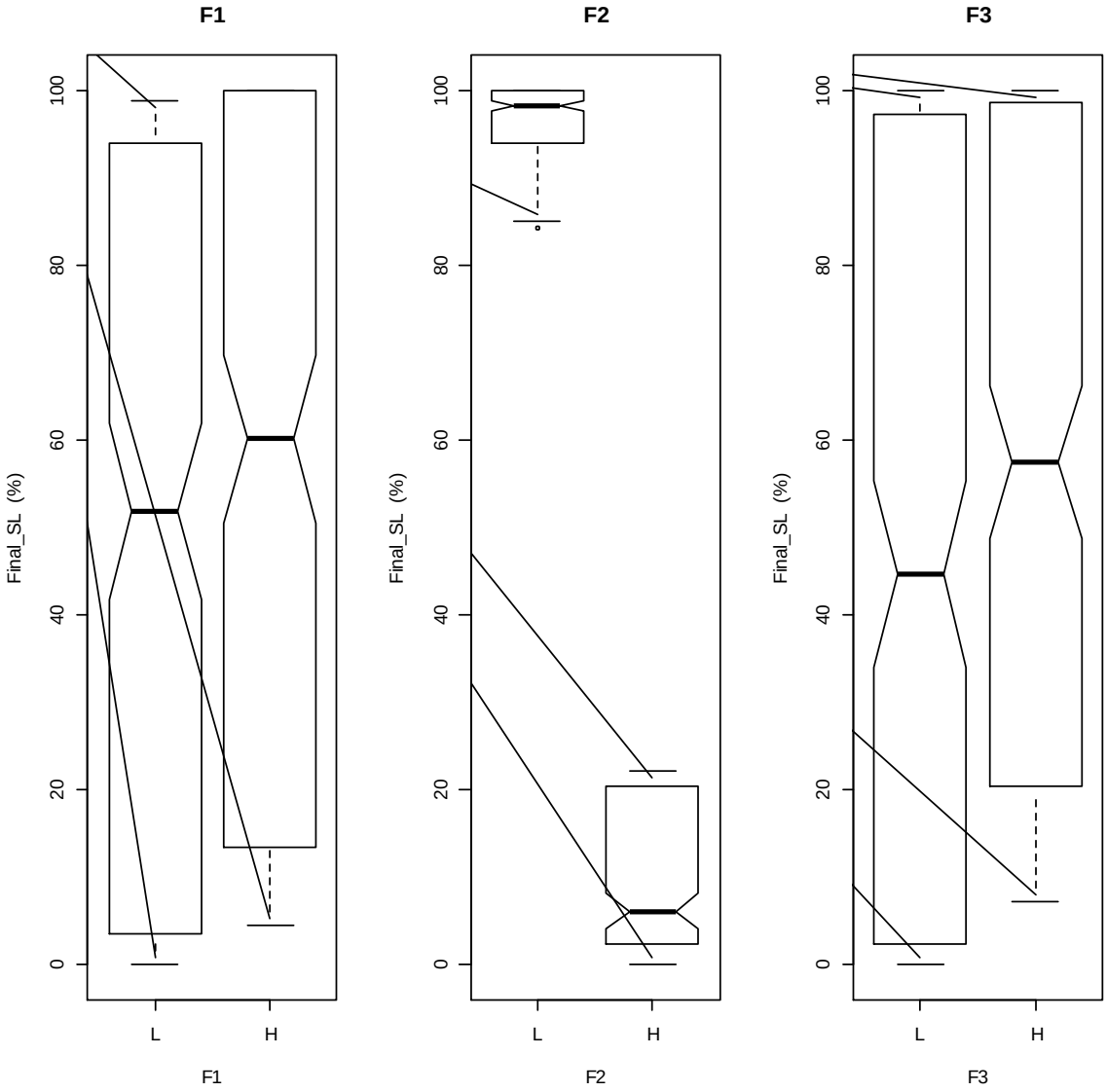

Figure 7. Boxplot of the final service level (SL).

Table 1. Factors levels considered.

Factor	Factor level 1 (low)	Factor level 2 (high)
Node Complexity (F1)	# nodes in each echelon = 10/3/10/50	# nodes in each echelon = 20/6/20/100
Flow Complexity (F2)	no. of potential links is 70% of all possible links between consecutive-echelons (i.e. 30% of all consecutive-echelons links are non-existent)	no. of potential links is 100% of all possible links between consecutive-echelons (i.e. none of the consecutive-echelons links is non-existent)
Link Capacity (F3)	average demand per node at origin echelon*Rand(1.0,1.2)	average demand per node at origin echelon*Rand(1.2,1.4)

Table 2. ANOVA for R_target.

Source	*df*	Sum of Squares	Mean Square	*p* value	Contribution (%)	Cumulative Contribution (%)
Flow Complexity (F2)	1	668927.00	668927.00	0.0000	97.63	97.63
F2*F3	1	6928.00	6928.00	0.0000	1.01	98.64
Link Capacity (F3)	1	6250.00	6250.00	0.0000	0.91	99.55
Node Complexity (F1)	1	2185.00	2185.00	0.0000	0.32	99.87
F1*F2	1	385.00	385.00	0.0000	0.06	99.93
F1*F3	1	50.00	50.00	0.0000	0.01	99.93
Error	393	461.00	1.00		0.07	100.00
Total	399	685185.00				

$S = 1.0830$, $R^2 = 0.9993$ (adjusted $R^2 = 0.9993$)

Table 3. ANOVA for R_random.

Source	*df*	Sum of Squares	Mean Square	*p* value	Contribution (%)	Cumulative Contribution (%)
Flow Complexity (F2)	1	177636.00	177636.00	0.0000	92.49	92.49
F2*F3	1	6061.00	6061.00	0.0000	3.16	95.64
Link Capacity (F3)	1	5411.00	5411.00	0.0000	2.82	98.46
Node Complexity (F1)	1	1899.00	1899.00	0.0000	0.99	99.45
F1*F2	1	213.00	213.00	0.0000	0.11	99.56
F1*F3	1	166.00	166.00	0.0000	0.09	99.64
Error	393	683.00	2.00		0.36	100.00
Total	399	192069.00				

$S = 1.3183$, $R^2 = 0.9964$ (adjusted $R^2 = 0.9964$)

Table 4. ANOVA for Final_SL.

Source	*df*	Sum of Squares	Mean Square	*p* value	Contribution (%)	Cumulative Contribution (%)
Flow Complexity (F2)	1	744341.00	744341.00	0.000	97.66	97.66
Link Capacity (F3)	1	7427.00	7427.00	0.000	0.97	98.64
F2*F3	1	4487.00	4487.00	0.000	0.59	99.22
Node Complexity (F1)	1	4333.00	4333.00	0.000	0.57	99.79
F1*F2	1	0.00	0.00	0.847	0.00	99.79
F1*F3	1	0.00	0.00	0.738	0.00	99.79
Error	393	1574.00	4.00		0.21	100.00
Total	399	762162.00				

$S = 2.0015$, $R^2 = 0.9979$ (adjusted $R^2 = 0.9979$)

Table 5. MANOVA results.

Source	Wilks' test (*p* value)	Variance Contribution (%)			Eigenvectors		
		R_target	R_random	Final_SL	R_target	R_random	Final_SL
F1	0.000	0.32	0.99	0.57	**-0.0290**	-0.0168	-0.0084
F2	0.000	97.63	92.49	97.66	**-0.0390**	-0.0073	-0.0058
F3	0.000	0.91	2.82	0.97	**-0.0325**	-0.0183	-0.0046
F1*F2	0.000	0.06	0.11	0.00	**-0.0421**	-0.0161	0.0093
F1*F3	0.000	0.01	0.09	0.00	-0.0238	**-0.0315**	0.0075
F2*F3	0.000	1.01	3.16	0.59	**-0.0351**	-0.0194	-0.0008
Error		0.07	0.36	0.21			