This article appeared in a journal published by Elsevier. The attached copy is furnished to the author for internal non-commercial research and education use, including for instruction at the authors institution and sharing with colleagues.

Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.

In most cases authors are permitted to post their version of the article (e.g. in Word or Tex form) to their personal website or institutional repository. Authors requiring further information regarding Elsevier’s archiving and manuscript policies are encouraged to visit:

http://www.elsevier.com/authorsrights
Resilience-based network component importance measures

Kash Barker, Jose Emmanuel Ramirez-Marquez, Claudio M. Rocco

Abstract

Disruptive events, whether malevolent attacks, natural disasters, manmade accidents, or common failures, can have significant widespread impacts when they lead to the failure of network components and ultimately the larger network itself. An important consideration in the behavior of a network following disruptive events is its resilience, or the ability of the network to "bounce back" to a desired performance state. Building on the extensive reliability engineering literature on measuring component importance, or the extent to which individual network components contribute to network reliability, this paper provides two resilience-based component importance measures. The two measures quantify the (i) potential adverse impact on system resilience from a disruption affecting link i, and (ii) potential positive impact on system resilience when link i cannot be disrupted, respectively. The resilience-based component importance measures, and an algorithm to perform stochastic ordering of network components due to the uncertain nature of network disruptions, are illustrated with a 20 node, 30 link network example.

1. Introduction and motivation

The ubiquitous nature of many infrastructure networks has led to their criticality in performing the functions of everyday life. Their criticality is due to their interconnectedness with other infrastructure networks, as well as industries and workforces that rely upon them. Among these critical infrastructure networks are electric power, telecommunications, and transportation, among others [11,29]. Disruptive events, whether malevolent attacks, natural disasters, manmade accidents, or common failures can have significant widespread impacts when they lead to the failure of network components. For example, the recent blackout that left over 600 million people without access to energy underscores the need for adequate protective measures against disruptive events and also for rapid and appropriate response when in the presence of such events.

While original work in planning for infrastructure network disruptions focused on prevention and protection, recent efforts have focused on "preparedness, timely response, and rapid recovery" [11] from such disruptive events. This emphasis on the inevitable occurrence of a disruptive event highlights the need for resilience in infrastructure networks, where resilience is often defined as an ability of a system to "bounce back" after a disruption. Domain-specific discussion of resilience range from ecological systems [16,6], to economic systems [30,31,24], to organizational systems [17,18]. Specifically for infrastructure systems, the Infrastructure Security Partnership (2011) noted that a resilient infrastructure sector would "prepare for, prevent, protect against, respond or mitigate any anticipated or unexpected significant threat or event" and "rapidly recover and reconstitute critical assets, operations, and services with minimum damage and disruption." In general, however, no common definition or quantitative approach has been adopted [13].

The analysis of systems, regardless of domain, often includes determining which system components are most influential on the performance of the system. Some examples include the interconnectedness of a node in a computer network may be of interest to a hacker whose objective is to maximize the damage of an attack [15], the interconnectedness of certain transportation assets may factor in investment priorities [20], and the influence of certain workforce-driven industry sectors on a regional economy in the event of an epidemic [4]. This is a well-studied topic in reliability, where component importance measures have been introduced to measure the influence of particular components on the overall reliability of the system. For all of the above domains, the study of influential components allows for focus to be given to those components that require more attention, perhaps through planning and investment to ensure a satisfactory performance of the system.
The contributions of this paper are twofold: (i) to introduce two network component importance measures to identify the components that are most influential when considering the resilience of the entire network and given that resilience is stochastic in nature, and (ii) provide a discrimination algorithm to identify component importance.

The remainder of the paper is as follows: Section 2 provides a notional and quantitative discussion of resilience. Section 3 focuses on stochastic descriptors of component vulnerability and recoverability and how they fit into the larger quantification of network resilience, as well as two resilience-based component importance measures for describing how individual components contribute to network resilience. Section 4 illustrates how these component importance measures, with concluding remarks provided in Section 5.

2. Methodological background

This section provides the definition of, as well as aspects of modeling, system (network) resilience originally discussed by Refs. [34,13]. Also, background on component importance measures is provided.

Along the bottom of Fig. 1 is the state transition among three distinct states in which a system can operate

- \( S_0 \): Original, or as-planned (or baseline) state.
- \( S_d \): Disrupted state, resulting from an event \( e \) disrupting the system.
- \( S_r \): Recovered state, that results from a recovery effort.

These states are related by the disruptive event \( e \) as follows: the system operates in \( S_0 \) until disruptive event \( e' \) occurs at \( t_0 \) and up to time \( t_d \) when the system reaches its maximum disrupted state \( S_d \). Recovery from the disruption commences at time \( t_r \) and state \( S_r \) is attained at time \( t_r \) and is maintained thereafter.

System resilience can be defined as the time dependent ratio of recovery over loss, or \( R(t) = \frac{\text{Recovery}(t)}{\text{Loss}(t)} \). Note the notation for resilience, \( R \) [34], as \( R \) is historically reserved for quantifying reliability. To quantify \( R(t) \), system performance is overlaid with the system state transition in Fig. 1. System service function \( \phi(t) \) describes the behavior or performance of the system at time \( t \) (e.g., \( \phi(t) \) could describe traffic flow for a highway network, throughput for a manufacturing facility). Resilience in the system at time \( t \) is exhibited if there is an external disruptive event, \( e' \) from a set \( D \) of possible disruptive events, that affects the original system state, \( S_0 \), where performance is measured as \( \phi(t_0) \). Disrupted at time \( t_d \), a period of degradation of length \( (t_d - t_0) \) transitions the system to \( S_d \) with corresponding performance \( \phi(t_d) \). After a period of time of length \( (t_r - t_d) \), the system restoration commences until the system reaches a stable recovered state, \( S_r \), at time \( t_r \) with corresponding performance \( \phi(t_r) \). Note that state \( S_r \) need not be the same as \( S_r \) as the new state may reach an alternative (\( \phi(t_r) \) may be lower, or perhaps higher) equilibrium level (e.g., the state of infrastructure following the 2010 earthquake in Haiti may be improved over pre-disruption levels). Based on this description, system resilience is provided in Eq. (1) [13]. Eq. (1), read resilience of the system at time \( t \) given event \( e \), describes the point in time, \( t_r \), when resilience is quantified and provides the ratio of recovery over loss at such point in time. Also, the values of \( t_d \) and \( t_r \) can change depending on the point in time when the recovery starts, the point in time when resilience needs to be quantified and the point time when recovery activities are finalized, respectively.

\[
R(t;e) = \frac{\phi(t;e) - \phi(t_0)}{\phi(t_0) - \phi(t_d)} \quad t \in (t_d, t_r)
\]

Fig. 1 also highlights four distinct dimensions of resilience: reliability, vulnerability, survivability, and recoverability. In the absence of an external disruptive event, the operation of the system during time period \( (t_0 - t_0) \) is governed by its reliability. Broadly, system availability can be described as the ratio of system uptime to system downtime. Thus, availability describes the proportion of time that a system can be used. According to the description in Fig. 1, resilience describes at any point in time, after recovery actions have started, the proportion of service restored due to the loss associated to event \( e' \). These two metrics share in that an approach to increase their values is to reduce system downtime/system restoration time.

Fig. 1 considers vulnerability as the study of the adverse effect on system performance caused by event \( e' [9,36,23,38] \), similar in concept to “robustness” in “resilience triangle” literature in civil infrastructure [5,39]. A mitigation approach to the vulnerability of a network is survivability, or the minimization of the original impact of disruptive events [33]. Finally, Ref. [32] explored an approach to quantify the effectiveness of a contingency system the reliability of a supply chain.

Finally, recoverability refers to “the speed at which an entity or system recovers from a severe shock to achieve a desired state” [30], similar in concept to “rapidity” in “resilience triangle” discussions [5,39].

This paper focuses on two dimensions of resilience over time, vulnerability and recoverability, for the development of a resilience-based component importance measure (CIM). CIMs identify system components that are more critical than others in terms of the reliability of the entire system [22,19]. Several reliability-based CIMs have been proposed [12,18,21,37,25], and they are generally calculated as some ratio of a measure of component contribution to system reliability and a measure of system reliability itself. The nature of system resilience in Eq. (1) lends itself to calculating the component contribution to system resilience when component \( i \) is isolated, discussed subsequently in Section 3.

3. Resilience-based component importance measure

Primary drivers in network resilience are vulnerability and recoverability. Means to measure these two dimensions are discussed in this section, as well their role in measuring network resilience.

3.1. Defining the network

Let \( G = (\mathcal{N}, \mathcal{A}) \) represent a network where \( \mathcal{N} \) is the set of nodes, and \( \mathcal{A} = \{a \mid 1 \leq i \leq m \} \) is the set of arcs. The state variable of link \( i \) at
time $t$ is defined by $x_i(t)$. The state variable could evaluate, for example, the full traffic flow capacity across a bridge or the transfer of output from one member of a supply chain to another. The network state vector at time $t$, $\mathbf{x}(t) = (x_1(t), x_2(t), ..., x_{n}(t))$, denotes the state of all the arcs at time $t$. The service function, $\varphi(\mathbf{x}(t))$, which can be analyzed for any possible realization of $\mathbf{x}(t)$, maps the performance of the collection of links into a measure of network performance at time $t$. Assume that disruptive event $e'$ leads to a degradation in the performance of the network.

### 3.2. Describing vulnerability in network components

Noted previously, vulnerability relates to the initial impact experienced by the network after a disruptive event. This corresponds to the reduced functionality in network components (e.g., reduced flow in network links after a disruption). Previous treatments of network resilience have assumed that the function of the links was binary [34], though a more general presentation is provided here. Let $x_i(t_0)$ represent the as-planned state on the $i$th link prior to the onset of disruptive event $e'$. Assume that the effect of $e'$ is a proportional reduction in the as-planned state of the $i$th link by $V_i^e = V_i^e$.

For the ease of flow, the effect of $e'$ on the state variable associated to link $i$ is provided in Eq. (2). Note that a complete reduction in the functionality of the link occurs when $V_i = 1$. Preparedness activities (e.g., protection, system hardening, and false target) that reduce the initial impact on the system would reduce vulnerability. That is, investments in risk management can reduce vulnerability. That is, investments in risk management can be relaxed with a known trajectory (e.g., linear, convex, and concave) relationship describing $x_i(t)$ for $t \in [t_0, t_f]$. It has also been assumed that $P(t_i < U_i(V_i^e) \leq t_i) = P(t_i < U_i(V_i^e) \leq t_i)$ for every $(V_i^e) > 0$. This assumption describes that recovery time is the same for any positive value of vulnerability.

Given a recoverability description for each component from Eq. (3), a metric describing the time until the system bounces back to its original state is $T_{\text{loss}(e)}(t_i)$, known as the time to full network service resilience.

This metric records the total time spent from the point when recovery activities start, at time $t_i$, up to the time, $t_f$, when system service is completely restored to the initial service function value $\varphi(\mathbf{x}(t_0))$. That is, the random value $t_f$ is given by such value ensuring that $H_{\mathbb{P}}(t_f|e) = 1$ and $H_{\mathbb{P}}(t_f - \delta|e) < 1 \forall \delta > 0$ given disruptive event $e'$.

Since $T_{\text{loss}(e)}(t_i)$ is stochastic, one can define the probability that network service resilience is reached before mission time $t_i$ as $P_{\text{loss}(e)}(t_i) = P(T_{\text{loss}(e)}(t_i) \leq t_i)$.

### 3.3. Describing recoverability in network components

As recoverability refers to the speed at which the network recovers, recoverability can manifest itself following a network disruption through the time required to recover the functionality of a network component. Recovery time for the ith link given its vulnerability, $U_i(V_i^e) = U_i(V_i^e)$, is uncertain and thus, $U_i(V_i^e)$ is a stochastic term. The probability that link $i$ recovers prior to time $t_i$ is found in Eq. (4).

$$P(t_i < U_i(V_i^e) \leq t_i) = \int_{t_i}^{t_f} f(u_i(V_i^e))du_i$$

(4)

For this paper, it is assumed that $x_i(t_0) = x_i(t_0)$ until the recovery time is met, suggesting a step function to repair. This assumption could be relaxed with a known trajectory (e.g., linear, convex, and concave) relationship describing $x_i(t)$ for $t \in [t_0, t_f]$. It has been assumed that $P(t_i < U_i(V_i^e) \leq t_i) = P(t_i < U_i(V_i^e) \leq t_i)$ for every $(V_i^e) > 0$. This assumption describes that recovery time is the same for any positive value of vulnerability.

**Figure 2.** Illustrative network example, adapted from Hillier and Lieberman [14].

**Figure 3.** Trajectory of resilience over time for (a) deterministic arc recovery activity time of 10 time units and (b) stochastic arc recovery activity time following UNI(8,12).
this network, disruptive event, and recovery activity set when a deterministic time duration is assumed.

To illustrate $T_{X(t)}(x^i)$, consider a uniform distribution for arc recovery time, $U_i^j \sim \text{UNI}(8,12)$, $i=1,\ldots, 5$. The trajectory of resilience under the stochastic recovery time assumption is provided in Fig. 3(b), where interval representations replace point estimates following a 1000-iteration discrete event simulation. Note that full network resilience is achieved after the first three recovery activities (the recovery of arcs 1, 2, and 3, leading to the full capability of the network), while full network restoration does not occur until all five disrupted arcs are recovered after all five recovery activities (as restoration implies that all arcs are fully functional). Fig. 3(b) highlights the difference in the average time to full network resilience and full network restoration.

Approximate probability distribution and cumulative distribution function representations of $T_{X(t)}(x^i)$ are provided in Fig. 4 for particular recovery order 1–2–3–4–5. Note that $T_{X(t)}(x^i)$ is approximately bounded by the interval (24, 36).

3.4. Component importance from resilience

Mentioned in Section 1, the primary contribution of this paper is the introduction of two resilience-based component importance measures. The majority of CIs have been developed to quantify importance of components to system reliability. In the reliability case [22,19], CIs illustrate the effect on system reliability as a function of changes in the component state. Other work has extended traditional reliability-based component importance measures to various metrics of availability [7,3]. When considering vulnerability, CIs illustrate the adverse effect on the system service function as a function of disruptions to the original state of the components.

Sections 3.2 and 3.3 described how individual components are initially impacted (via component vulnerability) and then recover (via component recoverability) following disruptive event $e^i$. And Eq. (1) incorporates these dimensions for all components to quantify network resilience. When considering component importance in a resilience setting, the interest is in understanding the effect that both disruption magnitude and recovery speed at the component level have on the time to full network service resilience, $T_{X(t)}(x^i)$. Eq. (5) mathematically illustrates the first resilience-based CI:

$$CI_{\phi_{\phi}(t)}(x^i) = \frac{\phi(x(t_0)) - \phi(x(t_0), x(t_1)|V_j)}{\max_{x}(\phi(x(t_0), x(t_1)|V_j))} T_{X(t)}(x^i) \cdot$$

The numerator in the ratio of Eq. (5) describes the system service loss due to the disruption effect on link $i$, while the denominator describes the maximum loss among all the links. This ratio is the multiplied by the time required to restore the system service to its original state. As $V_j$ and $U_i^j$ are stochastic terms, $CI_{\phi_{\phi}(t)}(x^i)$ has a distribution for $t \in [t_1, t_2]$. $CI_{\phi_{\phi}}(x^i)$ is a measure of the weighted contribution of link $i$ to the time until full network service is restored, with the weighting factor interpreted as the proportion of the maximum possible change in performance described by link $i$. This CI can be regarded as comparable to risk reduction worth (RRW) [26], an index that quantifies the potential damage to a system caused by a particular component.

In reliability engineering, there is also interest in measuring the reliability achievement worth (RAW) of a component, or the maximum proportion increase in system reliability generated by that component. The second resilience-based CI addresses this perspective as the “resilience worth” of link $i$, $W_{\phi_{\phi}}(t_i|e^i)$, or an index that quantifies how the time total network service resilience is improved for scenario $e^i$ if link $i$ is inoperative. The mathematical representation of $W_{\phi_{\phi}}(t_i|e^i)$ is provided in Eq. (6):

$$W_{\phi_{\phi}}(t_i|e^i) = \frac{T_{\phi_{\phi}}(x^0)}{T_{\phi_{\phi}}(x^i)} = 0,$$

3.5. Component ordering according to importance

Ordering links in terms of magnitude with respect to the resilience-based CIs provides an account of greatest to least link impact at $t$, on (i) potential adverse impact on system resilience from a disruption to link $i$ (with $CI_{\phi_{\phi}}(t_i|e^i)$), and (ii) potential positive impact on system resilience when link $i$ cannot be disrupted (with $W_{\phi_{\phi}}(t_i|e^i)$). An algorithm for generating an order of component importance is described for $CI_{\phi_{\phi}}(x^i)$ below, though the same algorithm would apply for the $W_{\phi_{\phi}}(t_i|e^i)$ measure:

1. For each link $i$, and based on probability distributions defined in Eqs. (3) and (4), generate a realization of $V_j$ and $U_i^j$ for each link $i$, and calculate $CI_{\phi_{\phi}}(t_i|e^i)$ for $t_i \in [t_1, t_2]$.
2. Repeat Step 1 for a chosen number, $\eta$, of iterations, producing a distribution of $CI_{\phi_{\phi}}(t_i|e^i)$ at each time period $t_i \in [t_1, t_2]$.
3. Given the distributions of $CI_{\phi_{\phi}}(t_i|e^i)$ for each link $i$, perform a stochastic ranking of links according to ascending $CI_{\phi_{\phi}}(t_i|e^i)$.

Note that when event $e^i$ affects more than one link, recoverability strategies (i.e., recovery orders) must be defined a priori [28].

3.5.1. Stochastic ranking

To generate the stochastic order of links at Step 3, an approach based on the Copeland Score method has been developed. The Copeland Score (CS) is a simple non-parametric ranking technique that does not require any information about decision maker preference and operates on a multi-indicator matrix, formed by $m$ objects characterized by $\Omega$ attributes. The CS implemented here corresponds to a modification proposed by Al-Sharrah [2]. The CS is computed based on pair-wise comparisons between objects.
The resilience-based component importance measure approach is illustrated for a 20-node, 30-link network as depicted in Fig. 5 (adapted from Ref. [10]). Under baseline behavior, the network can handle a maximum flow of 44 units. The disruptive event, \( e^i \), causes component vulnerability in link \( i \), as a uniform distribution in [0,1]. Recovery time is simplified to assume that regardless of component vulnerability, time to recover is uniformly distributed in \([1,2]\) arbitrary time units.

**Case 1.** To illustrate the evaluation process considering vulnerability and resilience, Fig. 6 illustrates the flow reduction of the network as a function of link vulnerability. To develop this figure, a disruption \( V_j \sim \text{UNI}(0,1) \) is generated for each link \( i \) and the total loss is computed as the difference between baseline and disrupted maximum flow. Fig. 6 indicates that links 25 through 28 produce the largest vulnerability, or initial losses in functionality, with link 25, which connects nodes M and R, as the highest contributor. However, note that for component vulnerability \( \geq 0.4 \), the set of important links would include link 23.

Fig. 7 illustrates the cdf of \( C_{\text{fl}}(t_i|x^i) \) for each link, using the procedure described in Section 3.5 (for \( n=2000 \) samples). This figure illustrates the probability that \( C_{\text{fl}}(t_i|x^i) \) will be less than or equal to a target value \( x \). Considering a target value \( x=0.10 \), as per Fig. 7, the \( C_{\text{fl}}(t_i|x^i) \) value associated with link 4 will not have a value above 10 units; in terms of resilience, this link impacts system resilience the least. In contrast, link 25 will be below the same target value 15% of the time. Moreover, the curve for link 25 is always “dominated” by the remaining curves. Therefore, a disruption in link 25 has the most adverse effect on the resilience of the network. Finally, consider links 23 and 27. For a target value \( x<0.20 \), the curve for link 27 is below the curve of link 23 (i.e., link 27 is more important than link 23). However this behavior changes for \( x>0.20 \) and link 23 becomes more important. This behavior underscores that excluding link 25, there is no clear second most important link. For this reason, CS is used to distinguish the importance of links. Fig. 8 shows the CS of all the links, ordered in descending order with link 25 as the most important, followed by links 28, 26, 27, and so on.

**Case 2.** To illustrate \( W_{\text{fl}}(t_i|x^i) \), consider event \( e^i \) as impacting links 9, 23, 24 and 25 with \( V_j=1 \) and \( V_j=0 \) for every other link.

4. **Illustrative example**

The resilience-based component importance measure approach is illustrated for a 20-node, 30-link network as depicted in Fig. 5 (adapted from Ref. [10]). Under baseline behavior, the network can handle a maximum flow of 44 units. The disruptive event, \( e^i \), causes component vulnerability in link \( i \), as a uniform distribution in [0,1]. Recovery time is simplified to assume that regardless of component vulnerability, time to recover is uniformly distributed in [1,2] arbitrary time units.

**Case 1.** To illustrate the evaluation process considering vulnerability and resilience, Fig. 6 illustrates the flow reduction of the network as a function of link vulnerability. To develop this figure, a disruption \( V_j \sim \text{UNI}(0,1) \) is generated for each link \( i \) and the total loss is computed as the difference between baseline and disrupted maximum flow. Fig. 6 indicates that links 25 through 28 produce the largest vulnerability, or initial losses in functionality, with link 25, which connects nodes M and R, as the highest contributor. However, note that for component vulnerability \( \geq 0.4 \), the set of important links would include link 23.

Fig. 7 illustrates the cdf of \( C_{\text{fl}}(t_i|x^i) \) for each link, using the procedure described in Section 3.5 (for \( n=2000 \) samples). This figure illustrates the probability that \( C_{\text{fl}}(t_i|x^i) \) will be less than or equal to a target value \( x \). Considering a target value \( x=0.10 \), as per Fig. 7, the \( C_{\text{fl}}(t_i|x^i) \) value associated with link 4 will not have a value above 10 units; in terms of resilience, this link impacts system resilience the least. In contrast, link 25 will be below the same target value 15% of the time. Moreover, the curve for link 25 is always “dominated” by the remaining curves. Therefore, a disruption in link 25 has the most adverse effect on the resilience of the network. Finally, consider links 23 and 27. For a target value \( x<0.20 \), the curve for link 27 is below the curve of link 23 (i.e., link 27 is more important than link 23). However this behavior changes for \( x>0.20 \) and link 23 becomes more important. This behavior underscores that excluding link 25, there is no clear second most important link. For this reason, CS is used to distinguish the importance of links. Fig. 8 shows the CS of all the links, ordered in descending order with link 25 as the most important, followed by links 28, 26, 27, and so on.

**Case 2.** To illustrate \( W_{\text{fl}}(t_i|x^i) \), consider event \( e^i \) as impacting links 9, 23, 24 and 25 with \( V_j=1 \) and \( V_j=0 \) for every other link.

![Fig. 5. Illustrative network example 2, adapted from Ref. [10].](image-url)
Also, consider that recovery time for each of these links is assumed as uniformly distributed between [10, 17]. There are $4! = 24$ different recoverability combinations that can be implemented if the recovery of the four links is done in series (i.e., combinations $\{S_1, \ldots, S_{24}\}$). The nine histograms in Fig. 9 illustrate the time to full network service resilience (TTSR) corresponding to a sample of nine out of the total 24 sequences ($S_1, S_2, S_3, S_{11}, S_{12}, S_{21}, S_{22}$, and $S_{23}$). As evidenced by Fig. 9, the time to full service resilience associated to the event considered (i.e., failure of links 9, 23, 24, and 25), is at most 40 units roughly 50% of the time independent of the restoration sequence implemented. Note that Fig. 9 depicts the denominator in Eq. (6). Fig. 10 illustrates the effect of $T_{\text{res}(S_i)}(t|\epsilon)$ on links 9, 23, 24, and 25 one at a time and for the first sequence respectively; clearly time to total network service resilience has been reduced (note the maximum on the time axis in Fig. 10 relative to Fig. 9). For these cases, the time to full network service resilience is at most 30 units for roughly 50% of the time independent of the sequence implemented.

To identify the most important link, Fig. 11 illustrates the case when the worst-case (least resilient) restoration sequence is implemented. After applying the Copeland score approach, link 25 exhibits the highest stochastic order and has the most adverse effect on the resilience of the network in the worst case.
Fig. 9. Histograms of the time to total network service resilience for an event impacting links 9, 23, 24, and 25.

Fig. 10. Histograms for time to total network service resilience as a function of link invulnerability, for links 9, 23, 24, and 25.
5. Concluding remarks

The purpose of this paper has been to highlight that considerations related to network resilience, as opposed to only network protection and disruption prevention, should become more prevalent in risk-based analysis and planning efforts. The ability of a network to “bounce back” from seemingly inevitable disruptive events is a vital consideration. This work defines resilience as a function of four interacting paradigms: reliability, vulnerability, survivability, and recoverability. Modeling emphasis is devoted to vulnerability, or the impact experienced in a network following a disruptive event, and recoverability, or the ability of a network to recover functionality in a timely manner. As such the paper contributes two approaches to measure the importance of network components from the perspective of component contribution to network resilience as a function of stochastic vulnerability and recoverability terms.

The first resilience-based component importance measure, $CI_{rφ,i}(t_r|e^i)$ in Eq. (5), quantifies the potential adverse impact on system resilience at time $t_r$ when disruption $e^i$ affects link $i$. Analogous to the risk reduction worth CIM common in the reliability engineering literature, it measures the proportional contribution of link $i$ to the time required to achieve full network service resilience. Due to the stochastic nature of the elements comprising $CI_{rφ,i}(t_r|e^i)$, ordering the components according to this measure requires a stochastic ranking technique (e.g., the Copeland Score method). The comparison of the cdfs for the illustrative example in Fig. 7 demonstrate some non-obvious conclusions about the contributions of certain links to the resilience of the network in Fig. 5. The second resilience-based component importance measure, $WN_{rφ,i}(t_r|e^i)$ in Eq. (6), quantifies the potential positive impact on network resilience when vulnerability-strengthening measures are put into place such that link $i$ cannot be disrupted.

As with all importance measures, the two proposed in this paper can serve as guides to prioritize resilience improvement activities. As illustrated by the results such activities can be in the form of vulnerability reduction policies (i.e., protecting or hardening components) or in the form of accelerating the speed of recovery activities. Future research should be focused on the optimal allocation of resources among these different activities, including the cost assessment of losses due to performance deterioration.

References


