A Quantitative Approach for Assessment and Improvement of Network Resilience

Navid Ahmadian[a], Gino J. Lim[a,*], Jaeyoung Cho[b], Selim Bora[c]

[a]*Industrial Engineering, University of Houston*
[b]*Industrial Engineering, Lamar University*
[c]*Richard Fritz Holding GmbH, Hungary*

Abstract

This paper proposes a quantitative approach for measuring the resilience of the network components and the network itself. This study introduces a conceptual framework featuring the ability of the network system to adopt alternative plans when a component is disrupted. As a first step toward measuring network resilience, the component resilience is defined and quantified as a function of criticality, disruption frequency, disruption impact, and recovery capability. This quantification approach reflects the effect of component level disruption on the network. Hence, it is proposed that the network resilience is measured by the resilience of network component having the lowest resilience index. Efforts to enhance network resilience often require financial resources. Therefore, an optimization model is further introduced to maximize the network resilience under budget constraint through reinforcing the weakest components in the network. The proposed approach can help decision-makers assess the network resilience status and compare with it other networks, identify and improve components with low resilience, evaluate the cost of resilience improvement, and determine the extent of enhancement that can be achieved under a given budget limitation. Numerical experiments are conducted to illustrate our methodology using a supply chain network and a power network. Both examples show that considering the ability of the network to use alternative plans can enhance network resilience and result in lower demand loss when a disruption occurs.

Keywords: Resilience, Resilience Quantification, Network Resilience, Network Disruption, Resilience Improvement

1. Introduction

Natural disasters, political unrest, economic crises, pandemic diseases, human errors, and equipment failures can all pose a severe threat to the performance and endurance of physical networks. The term *physical network* in this paper refers to networks containing real-world components. Transportation networks, water networks, and power networks are a few examples of physical networks. Since we only consider physical networks in our study, "physical network" and "network" are used interchangeably in this paper. In 2017, Hurricane Harvey struck southern Texas and caused a massive power outage in the region. Several major refineries in Texas were shut down, causing a significant disruption to facilities that handle approximately 11.8% of total U.S refining capacity. Such examples underscore the frequency and high impact caused by disruptions, thus indicating the need for these occurrences to be mitigated as much as possible. The 2003 blackout in parts of the Northeastern and Midwestern United States [1] caused transportation and economic network disruptions. In 2011, an earthquake and tsunami hit Japan and led to more than 15,000 deaths and disturbances within global supply chain networks [2]. After Hurricane Sandy devastated New York and New Jersey in 2012, the subsequent power outage lasted for several months in some areas [3], and transportation networks were severely compromised [4]. All of these catastrophic events and their noticeable consequences on various networks highlight the importance of network resilience. In order to be able to improve

*Corresponding author
Email addresses: nahmadian@uh.edu (Navid Ahmadian), ginolim@uh.edu (Gino J. Lim), jcho@lamar.edu (Jaeyoung Cho), selim.bora@fritz-group.com (Selim Bora)

network resilience, the first step is to understand what resilience is and how it can be measured. In this context, several efforts and studies have attempted to define resilience.

The term "resilience" derives from the Latin word "resiliere", meaning to bounce back [5]. D. Henry *et al.* [6] believe that resilience is generally an entity's ability to recover from an external disruptive event. Some of the existing definitions for resilience include: 1) the ability to return to normal conditions after the occurrence of a disruptive event, 2) the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must, 3) the measure of a system's ability to absorb continuous and unpredictable change and still maintain its vital functions, and 4) the ability of the network system to withstand a major disruption within acceptable degradation parameters and to recover within a suitable time and reasonable costs and risk [7, 8]. Bruneau *et al.* [9] state that a resilient system shows low failure probabilities, fewer consequences from failures, and a shorter time to recovery.

Literature shows different approaches to measure resilience of various network systems. For instance, Pettit *et al.* [10] and Ponomarov *et al.* [11] have discussed resilience evaluation in the supply chain management domain. Sterbenzetal *et al.* [12], Vlacheas *et al.* [13], and Tortorella [14] have developed an approach for measuring resilience in telecommunication networks. Others have attempted to address the problem of resilience measurement domains, which include transportation systems [15, 16, 17], power systems [18, 19, 20], water networks and natural gas networks [21, 22, 23], urban communities [24, 25, 26] and financial systems [27, 28, 29]. Despite the differences in details and applications, the mentioned studies are based on common principles. Our work both integrates these principles and extends the current studies the proposed resilience measurement approach can be meaningfully applied to any physical network.

The literature related to general frameworks can be classified into two categories: qualitative and quantitative studies [30]. As for the qualitative efforts, Kahan *et al.* [31] identified eight principles for defining system resilience. The principles support three resilience objectives: resistance, absorption, and restoration. Vugrin *et al.* [32] included *absorptive capacity*, *adaptive capacity*, and *restorative capacity* to formulate the resilience of a system. According to their study, absorptive capacity is the ability of a network system to absorb the impact of system perturbations; adaptive capacity is the capability of the system to adapt itself using alternative plans to disrupted conditions; and restorative capacity is the potency of the system to restore itself to the original state.

As for general quantitative studies, Bruneau *et al.* [9] developed a measure $Q^B(t)$ to represent the quality of the infrastructure in a community, which varies over time. They introduced the loss of resilience, R^B, which is measured by the degradation in quality over time, as expressed in (1). In this equation, $Q^B(t)$ is the percentage of infrastructure quality at time t.

$$R^B = \int_{t_0}^{t_1} [100 - Q^B(t)]dt \tag{1}$$

Based on this study, Falasca *et al.* [33] suggested a quantitative approach to combine the system performance after a disruption using the resilience triangle [34] which involves three factors associated with supply chain network resilience: node criticality, complexity, and density. Mari *et al.* [35] proposed an optimization model and computed resilience through an expected disruption cost. Following the same approach, Cimellaro *et al.* [36] attempted to maximize the area under the curve of $Q^C(t)$ (Equation (2)).

$$R^C = \int_{t_0}^{t_1} Q^C(t)dt \tag{2}$$

Reed *et al.* [37] adopted the same measure for resilience. However, they considered a time interval of the construction and divided the area under the $Q^R(t)$ curve by that time interval (3). In this equation, R^R is resilience, $Q^R(t)$ is the quality function at time t, and t_0 and t_1 are two endpoints of the time interval.

$$R^R = \frac{\int_{t_0}^{t_1} Q^R(t)dt}{t_1 - t_0} \tag{3}$$

To make the measure comparable among different systems, Ouyang *et al*. [38] proposed to normalize the resilience quantity by dividing the area under the $Q^O(t)$ curve by the area under the targeted performance curve ($TP(t)$) over t_0 to t:

$$R^O = \frac{\int_{t_0}^{t_1} Q^O(t)dt}{\int_{t_0}^{t_1} TP(t)dt} \tag{4}$$

Li *et al*. [39] proposed a model considering the maximum allowable recovery time (T_a) determined by the users to construct a comparable measure, where the system may or may not recover within the time interval.

$$R^L = \frac{\int_{t_0}^{T_a+t_0} Q^L(t)dt}{T_a} \tag{5}$$

However, if the required time of recovery is more than T_a, the concept of a system bounce-back to the original state after a disruption will not be represented. This serves as a disadvantage, as this idea plays a critical role in the definition of resilience.

Najarian and Lim [40] proposed a performance-based metric that includes three aspects of a resilient system. Their metric includes absorption (R_1^N), adaptation (R_2^N), and rapid recovery (R_3^N) which are calculated using the following formulas:

$$R_1^N = \frac{\int_{t^o}^{t_d} F(t)dt}{\int_{t^o}^{t_d} TF(t)dt}, R_2^N = \frac{\int_{t_d}^{T} F(t)dt}{\int_{t_d}^{T} TF(t)dt}, \text{and } R_3^N = f(T) = \begin{cases} 1 \; T \leq T_0 \\ \frac{T_0}{T} \text{ otherwise} \end{cases} \tag{6}$$

In these equations, t_d is the time that the system functionality drops to its lowest. They defined the resilience as the convex combination of above three sub-metrics (Equation (7)). Furthermore, Najarian *et al*. [41] provided a method to assess the effect of resilience of a system on the resilience of another system.

$$R^N = \alpha_1 R_1^N + \alpha_2 R_2^N + \alpha_3 R_3^N, \text{ and } \alpha_1 + \alpha_2 + \alpha_3 = 1 \text{ and } \alpha_1, \alpha_2, \alpha_3 \geq 0 \tag{7}$$

In addition to the above studies, some approaches quantify network resilience by implementing the mentioned concepts associated with resilience [42, 43, 44, 23]. These studies encompass various distinguishable attributes of resilience for resilience quantification; however, in their resilience quantification, the potential of alternative plans for performing the operation of the disrupted component is not considered. In real-world situations, decision-makers look for potential alternative plans for quick demand satisfaction instead of simply waiting for the component to be recovered. For example, the Albuquerque fire at a chip provider company disrupted the routine performance of the supply chain network involving Nokia Corp and Ericsson in the year 2000. Nokia responded to this disruption by reaching out to other suppliers and thus, successfully achieved its sales plan. Unlike Nokia, Ericsson did not look for alternative suppliers, which resulted in about a $400 million loss of revenue [45].

This paper contributes to the literature by proposing a general-purpose quantitative measure for physical networks. In our proposed approach for resilience quantification, the resilience of the network is defined based on the resilience of its components: arcs and nodes. This approach can handle networks with different sizes, in which the nodes in the network can be as small as a generator in power networks or as large as a city in supply chain networks. There are two trade-offs in node size selection in a network. If the node is defined at a granular level (i.e., fine grid), the optimization model may produce more precise solutions. However, the resulting network size might be too large to solve. On the other hand, if the node is defined to encompass multiple components in the network (i.e., coarse grid), the resulting solution may not be as accurate as of the solution of the finer grid model. But, it becomes much easier to solve the corresponding optimization model.

The contributions of this paper are highlighted as follows:

- Building on the existing resilience factors in the literature (the probability of disruption, the importance of the disruption, and time to recover), a new concept "component criticality" is introduced to the resilience quantifi-

cation to reflect the network system's ability to utilize other network components to provide an alternative plan to compensate for the disruption of the component.

- Unlike domain-specific studies found in the literature, the proposed work is applicable to various physical network systems. This general-purpose quantitative framework for measuring resilience is based on a set of comprehensive resilience principles and factors. In order to make the measure less sensitive to the scale of factors such as network sizes and performance measurement units, the proposed network resilience and component resilience measures are normalized in scale.
- The proposed approach can help decision-makers assess the network resilience status, identify and improve the components with low resilience, evaluate the cost of resilience improvement, and determine how much improvement can be achieved under a given budget limitation. An optimization model is developed to identify, justify, and prioritize resilience improvement options.

The rest of the paper is organized as follows. Section 2 describes our methodology, network resilience definition, and the measurement approach. Section 3 illustrates the methodology through numerical examples. Finally, Section 4 concludes the paper with a future research direction.

2. Methodology

This section starts by describing a methodology for defining the resilience that combines the existing resilience factors found in the literature and a newly introduced resilience factor "*component criticality*." In Section 2.2, a new approach for quantifying the resilience of the network components is presented, and the procedure of network resilience improvement under budget limitation is discussed in Section 2.3.

2.1. Network Resilience Definition

There is almost no commonly accepted definition of resilience in the network management context. However, the literature agrees on several key aspects of resilience measurement including the probability of disruption, consequences of those disruptions, and the act of recovering from the disruptions to the normal state [8, 9, 30]. To quantify the resilience, this paper follows numerous quantitative studies in the literature, which calculate the resilience index by using the functionality loss of the network during the disruption time [9, 36, 37, 38, 39, 40]. However, the premise of this paper is that, if the network components (nodes and arcs) are resilient, the whole network is also resilient. Therefore, we focus our attention on the resilience of network components, and define the resilience index for each component. To quantify the resilience of each component, we measure the functionality loss that occurs to the whole network. In this paper, the resilience of a network component is defined by considering the following factors: 1) Readiness: the probability of disruption, 2) Response: consequences of those disruptions, 3) Recovery: recovery to the normal state, and 4) Criticality. In addition to the first three factors that are prevalent in the literature, this paper includes a component's criticality, which is defined based on the ability of the network system to perform in case of component failure. If there is no substitution for the component in the case of disruption, it is considered more critical. Our study considers different disruption causes. It is assumed that each disruption comes with a monetary consequence due to a decrease in the network system throughput, which is called "loss of functionality" in this paper. It comes also at the expense of bringing it to the normal state in the recovery process. This procedure is illustrated in the resilience triangle, as shown in Figure 1. The area of the resilience triangle is the total loss as a consequence of the disruption. Our goal is to minimize this loss. We attempt to quantify readiness, response, recovery, and criticality to calculate a component's resilience.

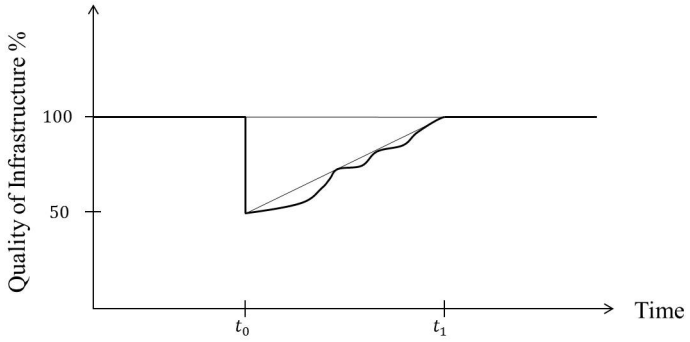


Figure 1: resilience triangle [34]

The following notation is introduced to define component resilience. A network $G = (\mathcal{N}, \mathcal{A})$ is considered by $\mathcal{N}$ as the set of nodes and $\mathcal{A}$ as the set of arcs; a refers to an arc and n refers to a node; and in the subscripts, i refers to the node $i \in \mathcal{N}$ and (i, j) refers to the arc $(i, j) \in \mathcal{A}$.

Figure 2 illustrates the notation by a simple supply chain network with four nodes and five arcs. In this example, the supply of Node 1 equals 10 (i.e., $s_1 = 10$), the flow of Arc (1,2) equals 4 (i.e., $f_{12} = 4$), and the demand at Node 4 is 8 (i.e., $d_4 = 8$).

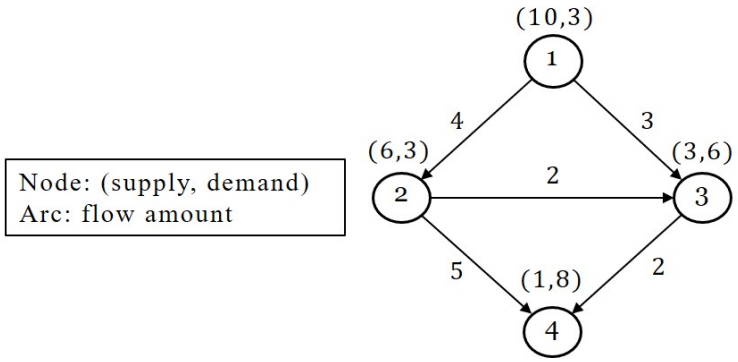


Figure 2: A simple supply chain network

2.2. Component Resilience Index (CRI)

To explain the procedure of measuring CRI, a set of definitions of parameters are introduced.

Definition: Impact of a Node Disruption (I_i^n)
The impact of a node disruption on the network, I_i^n, is the total loss when node i is disconnected from the network. The impact of a node disruption equals the summation of the node supply and its incoming flows. It can also be calculated as the summation of node demand and its outgoing flows.

$$I_i^n = \sum_j f_{ji} + s_i = \sum_k f_{ik} + d_i \ , \ \forall i \in \mathcal{N} \tag{8}$$

For example, the impact of Node 3 in Figure 2 equals 8, i.e., $I_3^n = \sum_j f_{j,3} + s_3 = 3 + 2 + 3 = 8$. It also can be calculated as $\sum_k f_{3,k} + d_3 = 2 + 6 = 8$.

Definition: Impact of an Arc Disruption (I_{ij}^a)
The impact of an arc disruption on the network is defined as the total loss in the case of disconnecting the arc from

the network. Impact of an arc disruption is defined as the flow of that arc.

$$I_{ij}^{a} = f_{ij} \ , \ \forall (i,j) \in \mathcal{A} \tag{9}$$

Definition: Repair Ratio Function ($Q(t)$)
A repaired ratio function of the i^{th} node or $(ij)^{th}$ arc is a function of time, which is defined as a cumulative function of the repair function. Also, a damage ratio function is defined as the ratio that has not been repaired after a disruption.

$$Q_{i}^{n}(t) = \int_{0}^{t} r_{i}^{n}(x)dx \ , \ \forall (i) \in \mathcal{N} \tag{10}$$

$$Q_{ij}^{a}(t) = \int_{0}^{t} r_{ij}^{a}(x)dx \ , \ \forall (i,j) \in \mathcal{A} \tag{11}$$

Equations (10) and (11) yield the area of the resilience triangle for node i and arc (i,j), respectively.

Definition: Node Criticality (C_i^n)
In this paper, the component criticality is measured as the network loss in a time period that the component is disrupted. The criticality of each component is calculated before a disruption happens by predicting the impact of the component disruption on the network and considering possible alternatives for performing the operation of the disrupted component. In this quantification approach, the disrupted flow is adjusted to the best alternative path where the demand loss is minimized. An optimization model is proposed to find the best alternative plan in order to minimize the total unmet demand during the time period that the component is disrupted. A node disruption affects all of the connected arcs as well as the supply that the node provides. However, the node's demand stays the same. If there is no proper substitution for the component's operation in the case of a disruption, the component is considered highly critical. The node criticality can be determined by solving the following optimization model. In these equations, φ shows the estimated damage level on the components, which can be obtained by existing methods in the literature [46]. To calculate the criticality of node i, the objective function is defined by Equation (12.1), which is the total unmet demand in the network per unit time:

$$C_{i}^{n} = minimize \sum_{k \in \mathcal{N}} l_{k} \tag{12.1}$$

The constraints are as follows. The flow in each arc is less than or equal to its capacity:

$$f_{jk} \leq \gamma_{jk}^{a} \tilde{\varphi}_{jki}^{a}, \forall (j,k) \in \mathcal{A}, \tag{12.2}$$

calculating the demand loss related to each node:

$$\sum_{k:(j,k)\in\mathcal{A}} f_{jk} + d_{j} - (\sum_{l:(l,j)\in\mathcal{A}} f_{lj} + s_{j}) = l_{j}, \forall j \neq i \in \mathcal{N}, \tag{12.3}$$

calculating the demand loss related to the disrupted node:

$$\sum_{h:(i,h)\in\mathcal{A}} f_{ih} + d_{i} - (\sum_{k:(k,i)\in\mathcal{A}} f_{ki} + s_{i}\varphi_{i}^{n}) = l_{i}. \tag{12.4}$$

Definition: Arc Criticality (C)
The criticality of an arc is defined in the same way as node criticality. If a disruption happens on an arc, the arc capacity reduces accordingly. To calculate the criticality of arc (i,j), the objective function is defined as:

$$C_{ij}^{a} = minimize \sum_{k \in \mathcal{N}} l_{k} \tag{13.1}$$

The constraints are as follows. The flow in each arc is less than or equal to its capacity:

$$f_{hk} \leq \gamma^a_{hk}, \forall (h,k) \neq (i,j) \in \mathcal{A}, \tag{13.2}$$

The flow in a disrupted arc is less than or equal to its undisrupted capacity:

$$f_{ij} \leq \gamma^a_{ij} \varphi^a_{ij}, \tag{13.3}$$

Calculating the demand loss related to each node:

$$\sum_{l:(k,l)\in\mathcal{A}} f_{kl} + d_k - \Big(\sum_{h:(h,k)\in\mathcal{A}} f_{hk} + s_k \Big) = l_k, \forall k \in \mathcal{N}. \tag{13.4}$$

After finding the criticality, impact, and repair ratio of each component, the component's CRI can be calculated. Figure 3 shows the resilience triangle related to a disruption with impact I on the network. The total loss is equal to the large, triangular area. However, the total loss decreases if an alternative plan is available while the disrupted component is being recovered. The alternative plan can be used from time t_S. Here, C is the loss in case of using the alternative plan, which is in the range of $[0, I]$. If there is no proper alternative plan, C is equal to I, indicating the full impact. By the same token, if there exists an alternative plan as good as the current plan, C becomes 0. So, the best solution is to use the current plan until time t_S, and then, start using the alternative plan until time t_E. It is assumed that before the disruption, the original plan works better than all of the alternative plans. Hence, there exists a time like t_E, where the partially restored original plan overcomes the alternative plan and should be selected as the optimal plan for the remaining period.

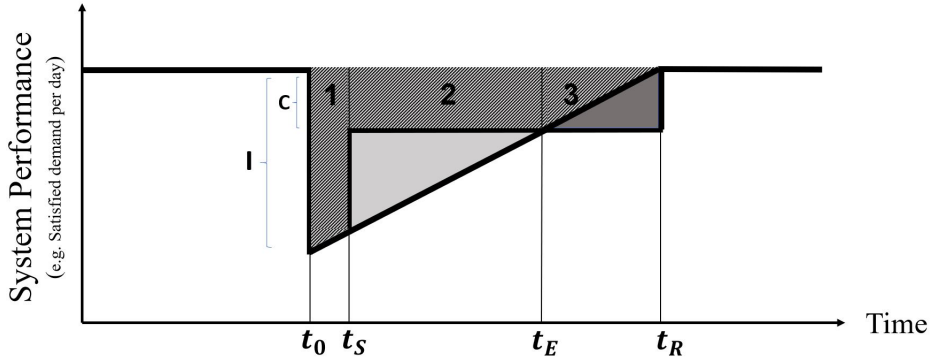


Figure 3: resilience triangle

The total loss is the summation of the following values: L_1, L_2, and L_3 (shown by the numbers one to three in resilience triangle in Figure 3). The demand loss represented in L_1 and L_3 is associated with the time intervals in which the original plan is selected as the optimal plan. In this study, we suggest considering the option of using alternative plans while the disrupted component is under recovery. The demand loss during t_S to t_E, represented as L_2, is associated with the time that the alternative plans are being used.

- L_1 : Loss associated with the time interval between the disruption and the implementation of the alternative plan

$$L_1 = \int_{t=t0_i^n}^{tS_i^n} I_i^n \varphi_i^n \mathcal{L}_i^n (1 - Q_i^n(t)) dt \tag{14}$$

for a node, and

$$L_1 = \int_{t=t_0{}_{ij}^{a}}^{t_{S_{ij}}^{a}} I_{ij}^{a} * \varphi_{ij}^{a} \mathcal{L}_{ij}^{a}(1 - Q_{ij}^{a}(t))dt \tag{15}$$

for an arc.

- L_2 : Loss related to the time interval between implementing the alternative plan and using the original plan

$$L_2 = C_i^n \mathcal{L}_i^n (t_{E_i}{}^n - t_{S_i}^n) \tag{16}$$

for a node, and

$$L_2 = C_{ij}^{a} \mathcal{L}_{ij}^{a} (t_{E_{ij}}{}^{a} - t_{S_{ij}}^{a}) \tag{17}$$

for an arc.

- L_3 : Loss related to the time interval between switching to the original plan and achieving full recovery

$$L_3 = \int_{t=t_{E_i}{}^n}^{t_{R_i}^n} I_i^n \varphi_i^n \mathcal{L}_i^n (1 - Q_i^n(t))dt \tag{18}$$

for a node, and

$$L_3 = \int_{t=t_{E_{ij}}{}^{a}}^{t_{R_{ij}}^{a}} I_{ij}^{a} \varphi_{ij}^{a} \mathcal{L}_{ij}^{a} (1 - Q_{ij}^{a}(t))dt \tag{19}$$

for an arc.

The total loss can be quantified by Equations (20) and (21) for nodes and arcs, respectively:

$$\int_{t=t_0{}_i^n}^{t_{S_i}^n} I_i^n \varphi_i^n \mathcal{L}_i^n (1 - Q_i^n(t))dt + C_i^n \varphi_i^n \mathcal{L}_i^n (t_{E_i}{}^n - t_{S_i}^n) + \int_{t=t_{E_i}{}^n}^{t_{R_i}^n} I_i^n \varphi_i^n \mathcal{L}_i^n (1 - Q_i^n(t))dt \tag{20}$$

$$\int_{t=t_0{}_{ij}^{a}}^{t_{S_{ij}}^{a}} I_{ij}^{a} \varphi_{ij}^{a} \mathcal{L}_{ij}^{a} (1 - Q_{ij}^{a}(t))dt + C_{ij}^{a} \varphi_{ij}^{a} \mathcal{L}_{ij}^{a} (t_{E_{ij}}{}^{a} - t_{S_{ij}}^{a}) + \int_{t=t_{E_{ij}}{}^{a}}^{t_{R_{ij}}^{a}} I_{ij}^{a} \varphi_{ij}^{a} \mathcal{L}_{ij}^{a} (1 - Q_{ij}^{a}(t))dt \tag{21}$$

To have a CRI that can be calculated independent of factors such as performance measurement unit or network size, the resilience of each component is normalized in scale. This makes the index comparable across various types of networks. To remove the time scale from the index, Ouyand *et al.* [38] suggest the inclusion of a time interval T in the index formulation. In our proposed approach, the CRI is calculated as the ratio of the demand loss during time interval T that begins from the disruption (Equation (22)).

$$\text{CRI} = 1 - \frac{\text{Total demand loss due to the component disruption}}{\text{Total demand in the network system during the time interval}} \tag{22}$$

To formulate the CRI for the network components, Equations (23) and (24) are proposed and show the resilience of node i and arc (i, j), respectively.

$$R_i^n(\mathcal{L}_i^n, \varphi_i^n, I_i^n, t_{R_i}^n, C_i^n) = 1 - \frac{\int_{t=t_0{}_i^n}^{t_{S_i}^n} I_i^n \varphi_i^n \mathcal{L}_i^n (1 - Q_i^n(t))dt + C_i^n \varphi_i^n \mathcal{L}_i^n (t_{E_i}{}^n - t_{S_i}^n) + \int_{t=t_{E_i}{}^n}^{t_{R_i}^n} I_i^n \varphi_i^n \mathcal{L}_i^n (1 - Q_i^n(t))dt}{T \sum_{i \in \mathcal{N}} d_i}, \forall i \in \mathcal{N} \tag{23}$$

$$R^a_{ij}(\mathcal{L}^a_{ij},\varphi^a_{ij},I^a_{ij},t_{R^a_{ij}},C^a_{ij}) = 1 - \frac{\int_{t=t_{0^a_{ij}}}^{t_{S^a_{ij}}} I^a_{ij}\varphi^a_{ij}\mathcal{L}^a_{ij}(1-Q^a_{ij}(t))dt + C^a_{ij}\varphi^a_{ij}\mathcal{L}^a_{ij}(t_{E^a_{ij}} - t_{S^a_{ij}}) + \int_{t=t_{E^a_{ij}}}^{t_{R^a_{ij}}} I^a_{ij}\varphi^a_{ij}\mathcal{L}^a_{ij}(1-Q^a_{ij}(t))dt}{T\sum_{i\in\mathcal{N}} d_i}, \forall (i,j) \in \mathcal{A} \quad (24)$$

Thus, the resilience indices are dimensionless, and take a value between 0 and 1.

2.3. Improving Network Resilience under Budget Limitation

The aim of the previous section was to develop an approach for measuring the resilience of a network and its components. Let us call the component corresponding to the lowest CRI value in the network the weakest component. In this paper, we represent the network resilience as the resilience of the weakest component(s). Hence, improving the resilience of the weakest component(s) increases the overall network resilience. This feature expands the index past simply being a means for assessing the network resilience; instead, this detail further transforms the index into a tool that upgrades the network and determines step-by-step network improvement decisions. The procedure for enhancing network resilience is illustrated in Figure 4, which showcases four components and their relative resilience indices. In the first step, Component 2 has the lowest resilience, or in other words, the weakest component. Thus, network resilience equals the resilience of Component 2. In the next step, the resilience of Component 2 is improved to match the same level as Component 4, then becomes the new resilience level of the network. This improvement is repeated until no further enhancement can be made due to budget limitation or other constraints.

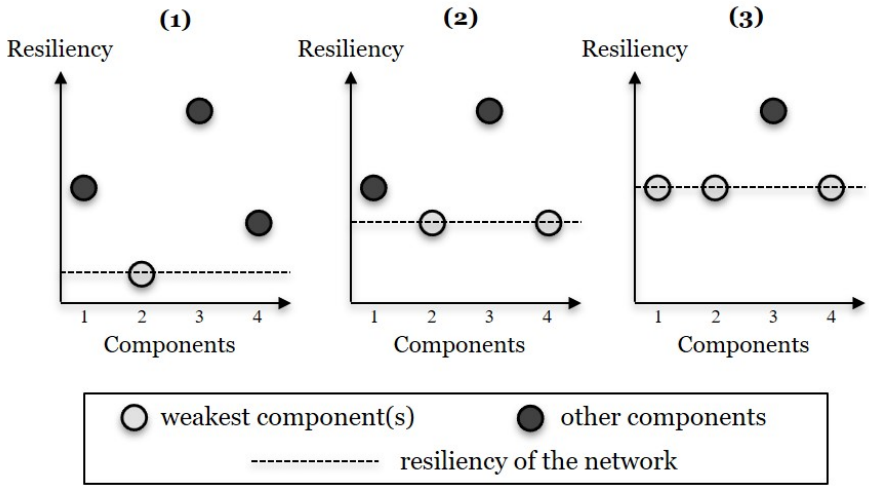


Figure 4: Improving Network resilience

The CRI of each component can be elevated through one or multiple of the following ways: 1) reducing the probability of having a disruption on the component ($\mathcal{L}$), 2) improving the component resilience in such a way that the estimated damage level (φ) will be decreased, 3) reducing impact of that component on the network (I) by changing the network structure, 4) enhancing the repair system (t^n_R) so that in case of having a disruption, the system can reach its original state faster, and/or 5) decreasing the criticality of that component (C) by improving the alternative approaches. To illustrate, let us consider an oil and gas company in which a node represents a refinery station. One way to enhance CRI is to reduce the probability of having a disruption (i.e., $\mathcal{L}^n$); however, this is not possible if the disruption is a natural disaster such as a flood or tornado. Safety and insurance factors in facing a flood should be enhanced to increase φ^n, and the construction of other refinery stations helps to reduce the impact (i.e., I^n) of the example refinery station. Another approach to enhance CRI is to develop a proper maintenance system that is capable of repairing the disrupted stations and bringing them back to their initial states in a short period of time (i.e., reducing t^n_R). The last option is to decrease the criticality (C^n) of this node by considering other stations as substitutions and transferring the work orders to the alternative stations.

Improving the resilience of a component by each of the mentioned approaches is associated with a cost function. We define five different cost functions for improving each node and each arc. Function $\mathcal{F}_i^{n_\varphi}(x)$ represents the value of variable φ_i after spending x amount of money on improving this resilience factor. Similarly, functions $\mathcal{F}_i^{n_\mathcal{L}}(x)$, $\mathcal{F}_i^{n_I}(x)$, $\mathcal{F}_i^{n_R}(x)$, and $\mathcal{F}_i^{n_C}(x)$ are defined for the rest of the approaches as explained earlier, and $\mathcal{F}_{ij}^{a_\mathcal{L}}(x)$, $\mathcal{F}_{ij}^{a_\varphi}(x)$, $\mathcal{F}_{ij}^{a_I}(x)$, $\mathcal{F}_{ij}^{a_R}(x)$, and $\mathcal{F}_{ij}^{a_C}(x)$ for the arcs. Based on the network, these functions can be different types of non-increasing functions (e.g., linear, exponential). The functions can be determined based on the available options for improving the resilience. The functions are based on available options for the system to enhance each resilience factor. These available options might include, but are not limited to, purchasing new equipment, building new structures, and creating new arcs in the network. For instance, $\mathcal{F}_8^{n_R}(\$1M) = 2$ means that there is a \$1M investment option to reduce the recovery time of Node 8 to two months. As a special case, if the resilience of a component cannot be improved by using an approach (e.g., reducing the possibility of having a disruption (i.e., $\mathcal{L}_i^n, \mathcal{L}_{ij}^a$)), the associated cost function is a constant function.

It is outlined here how network resilience can be improved under a limited budget. The aim is to maximize the resilience of the network by improving the resilience of the weakest components. An optimization problem is modeled and solved to find the maximum network resilience under a given budget, b. Since our aim is to improve the resilience of the weakest components, the objective function is defined to maximize the minimum component resilience, and thus, the problem becomes a max-min problem. The budget associated with the mentioned approaches to enhance $\mathcal{L}$, φ, I, R, and C are $x^\mathcal{L}$, x^φ, x^I, x^R, and x^C, respectively. The solution to the proposed model provides an optimal way to improve the components and the network resilience. In this model, Equation (25.1) is the objective function, Equations (25.2) through (25.3) are the constraints for the resilience of each node and each arc, and constraint (25.4) controls the budget.

$$R_b = \textit{maximize } r, \tag{25.1}$$

$$\text{s.t.} \quad r \le R_i^n(\mathcal{F}_i^{n_\mathcal{L}}(x_i^\mathcal{L}), \mathcal{F}_i^{n_\varphi}(x_i^\varphi), \mathcal{F}_i^{n_I}(x_i^I), \mathcal{F}_i^{n_R}(x_i^R), \mathcal{F}_i^{n_C}(x_i^C)), \forall i \in \mathcal{N}, \tag{25.2}$$

$$r \le R_{ij}^a(\mathcal{F}_{ij}^{a_\mathcal{L}}(x_{ij}^\mathcal{L}), \mathcal{F}_{ij}^{a_\varphi}(x_{ij}^\varphi), \mathcal{F}_{ij}^{a_I}(x_{ij}^I), \mathcal{F}_{ij}^{a_R}(x_{ij}^R), \mathcal{F}_{ij}^{a_C}(x_{ij}^C)), \forall (i,j) \in \mathcal{A}, \tag{25.3}$$

$$\sum_{i \in \mathcal{N}} x_i^\mathcal{L} + x_i^\varphi + x_i^I + x_i^R + x_i^C + \sum_{(i,j) \in \mathcal{A}} x_{ij}^\mathcal{L} + x_{ij}^\varphi + x_{ij}^I + x_{ij}^R + x_{ij}^C \le b. \tag{25.4}$$

Algorithm 1 summarizes the materials of Section 2 and shows the procedure of assessing and improving network resilience.

Algorithm 1 : Procedure of Network Resilience Assessment

Inputs:

The structure of the network (i.e., $G = (\mathcal{N}, \mathcal{A})$)
Supply (s_i) and demand (d_i) of each node
Flow (f_{ij}) and capacity (γ_{ij}) of each arc
Likelihood of having a disruption on a component, $\mathcal{L}_{ij}^{a}$ for arc (i, j), and $\mathcal{L}_{i}^{n}$ for node i
Estimated damage level on nodes and arcs, φ_i^n, φ_{ij}^a, and $\tilde{\varphi}_{ijn}^a$
Impact of a node (I_{ij}^a) or an arc I_i^n disruption on the network
Repair rate function, $r_{ij}^a(t)$, and $r_i^n(t)$
The time of starting the alternative approach, $t_{S_{ij}^a}$, and $t_{S_i^n}$
The cost function to improve the resilience of each component, $\mathcal{F}_i^{n_\varphi}(x)$,$\mathcal{F}_i^{n_\mathcal{L}}(x)$, $\mathcal{F}_i^{n_I}(x)$, $\mathcal{F}_i^{n_R}(x)$, $\mathcal{F}_i^{n_C}(x)$, $\mathcal{F}_{ij}^{a_\mathcal{L}}(x)$, $\mathcal{F}_{ij}^{a_\varphi}(x)$, $\mathcal{F}_{ij}^{a_I}(x)$, $\mathcal{F}_{ij}^{a_R}(x)$, $\mathcal{F}_{ij}^{a_C}(x)$
The budget associated to improve the network resilience

Step 1: Calculating the impact of each component
Find the impact of a disruption on each node and arc using Equations (8) and (9), I_i^n and I_{ij}^a

Step 2: Finding the criticality of each component
Solve optimization model (12) to find the criticality of each node, C_i^n
Solve optimization model (13) to find the criticality of each arc, C_{ij}^a

Step 3: Calculating the switching time from the alternative plan back to the initial plan
Use the repair rate function of each component to calculate switching times, $t_{E_{ij}^a}$ and $t_{E_i^n}$

Step 4: Calculating the resilience of each component
Use Equations (23) and (24) to determine the CRI of each node and arc, R_i^n and R_{ij}^a

Step 5: Determining the resilience of the network
Find the component with the lowest resilience among all nodes and arcs; the resilience of the network is equal to the resilience of that component.

Step 6: Developing the improvement plan
Solve the optimization model (25) to find the maximum network resilience that can be achieved under the budget and to determine how to improve the resilience of each component

Outputs:

The resilience index for each network component
The resilience strengths and weaknesses of each component
Network resilience index
Optimal approach to improve the resilience of each component
Optimal approach to improve the network resilience
Maximum potential network resilience under budget limitation

3. Numerical Examples

In this section, we provide two numerical examples to illustrate our methodology in different contexts: a supply chain network in Section 4.1 and a power system network in Section 4.2. The supply chain network case is an abstract example to show how the proposed method can be applied to supply chain networks and other similar networks. In this case, each node represents an area such as a county, city, or large warehouse, that has its own supply and demand. In the power network example, each node represents either a generator or a bus, and may have either generation or load, but not both. The resilience of a power network depends heavily on the functionality of the generators. We have assumed the equal time interval of T, in this case, 4 time units, to provide a fair comparison of the resilience of these two networks.

3.1. A Supply Chain Network

Figure 5 shows a randomly designed supply chain network. It is assumed that a disruption on a component disconnects it from the network (i.e., $\varphi_i^n = \varphi_{ij}^a = \tilde{\varphi}_{ijn}^a = 1$). The supplies and demands are shown above each node:

the first number represents the node supply, and the second number represents the node demand per time unit. An arc's flow per time unit at normal operation is displayed above each arc.

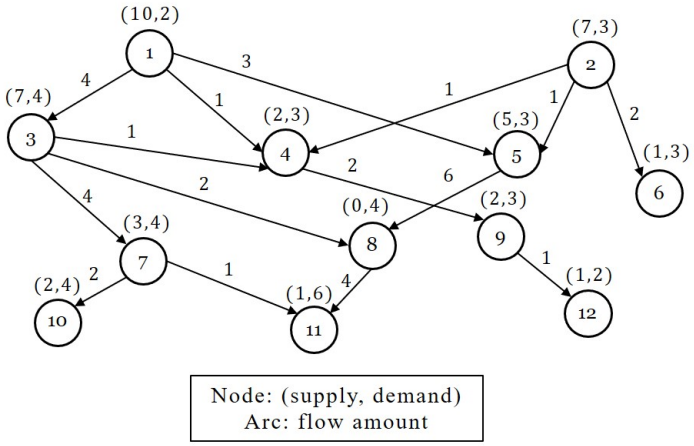


Figure 5: Supply Chain Network Example

To calculate the network resilience, the first step is to measure the CRI of each component. To do so, the impact of losing each component on the network (i.e., I_I^n and I_{ij}^a) is calculated and models (12) and (13) are solved to find the criticality of each node (i.e., C_i^n) and each arc (i.e., C_{ij}^a), respectively. Furthermore, Equations (23) and (24) are used to find the CRI of each node and arc. Table 1 shows the indices that are calculated and used for finding the resilience of the nodes, and Figure 6 presents their resilience values (last column of Table 1). In this figure, we observe that Node 1 and 11 have a low resilience level in comparison with the others. Node 11 has the lowest CRI among all of the components. The high probability of facing disruption and high criticality associated with this node are the main reasons for its low resilience. Furthermore, Node 1 is responsible for about 25% of the total network supply and provides the highest supply in the network. This great amount of supply from Node 1 results in the large impact index for this node ($I_{10}^n = 10$), meaning that a disruption on Node 1 causes a significant impact on the network. Also, Node 1 has no proper alternative to be used as a substitution of its operation, that makes this node highly critical. Contrarily, the most resilient node is Node 10, that has a short recovery time, low probability of facing disruption, and low criticality.

Table 1: resilience of each node in the supply chain network example

Node #	I_i^n	$\mathcal{L}_i^n$	C_i^n	$t_{S_i}^n$	$t_{E_i}^n$	$t_{R_i}^n$	L_1	L_2	L_3	L	R_i^n
1	10	0.2	10	0.2	0	4	0.39	0	3.61	4.00	97.56%
2	7	0.3	7	0.1	0	1	0.20	0	0.85	1.05	99.36%
3	11	0.1	8	0.4	0.55	2	0.40	0.12	0.58	1.09	99.33%
4	5	0.05	5	0.2	0	4	0.05	0	0.45	0.50	99.70%
5	9	0.2	6	0.4	0.67	2	0.65	0.32	0.80	1.77	98.92%
6	3	0.3	3	0.1	0	3	0.09	0	1.26	1.35	99.18%
7	7	0.15	6	0.2	0.29	2	0.20	0.08	0.77	1.05	99.36%
8	8	0.25	6	0.3	0.75	3	0.57	0.68	1.69	2.93	98.21%
9	4	0.2	4	0.5	0	4	0.38	0	1.23	1.60	99.02%
10	4	0.1	4	0.2	0	2	0.08	0	0.32	0.40	99.76%
11	6	0.5	6	0.1	0	3	0.30	0	4.21	4.50	97.26%
12	2	0.35	2	0.3	0	4	0.20	0	1.20	1.40	99.15%

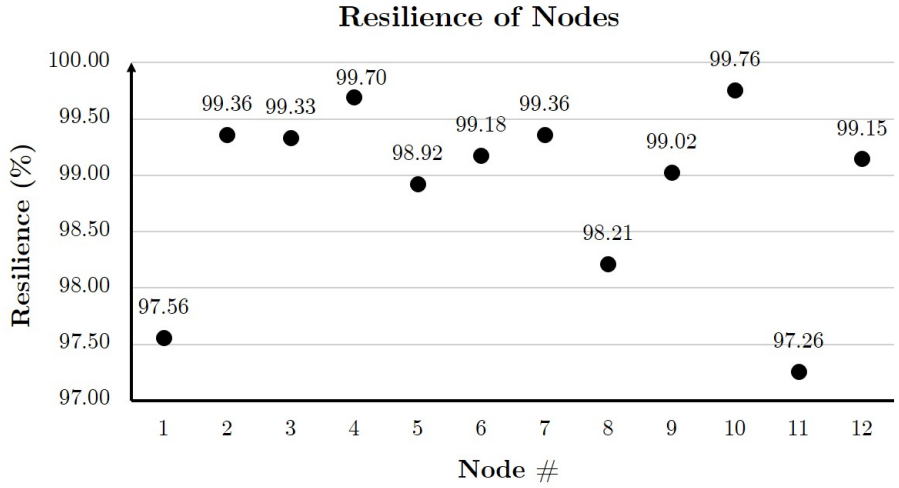


Figure 6: Resilience of each node in the supply chain network example

Following the same procedure, the related indices and resilience of all of the network arcs are calculated and shown in Table 2 (see Figure A.1 in Appendix). According to the results, Arc (8,11) has the lowest resilience among the arcs ($R^a_{8,11} = 98.98\%$). This arc provides the majority of incoming flow to Node 11, the node with the highest demand in the network. On the contrary, Arc (7,11) is the most resilient arc ($R^a_{7,11} = 99.99\%$). This large resilience value is justifiable by the fact that Arc (7,11) has the lowest flow and the demand for its flow can be alternatively satisfied by Arc (8,11).

In this study, the ability of the network to use alternative plans is considered. Neglecting and failing to consider this feature results in higher demand loss and consequently, lower CRI of the components. Disregarding the alternative plans increases the criticality of the components to the level of their impact. To demonstrate, consider Arcs (1,5) and (3,4) without having any alternative plans in consideration. In this case, the expected demand losses associated with their disruption would have increased from 0.34 and 0.10 to 1.35 and 1.00, respectively. Furthermore, the resilience indices of these two arcs would have dropped from 99.80% and 99.94% to 99.18% and 99.39%, respectively. This highlights that by having alternative plans, significant contribution to the enhancement of the component resilience can be achieved.

Table 2: Resilience of each arc in the supply chain network example

ID	Arc #	I^a_{ij}	$\mathcal{L}^a_{ij}$	C^a_{ij}	ts^a_{ij}	$t_{E^a_{ij}}$	$t_{R^a_{ij}}$	L_1	L_2	L_3	L	R^a_{ij}
1-3	1	4	0.4	1	0.2	2.25	3	0.31	0.82	0.15	1.28	99.22%
1-4	2	1	0.25	0	0.1	3	3	0.02	0	0	0.02	99.99%
1-5	3	3	0.3	0	0.4	3	3	0.34	0	0	0.34	99.80%
2-4	4	1	0.2	0	0.2	3	3	0.04	0	0	0.04	99.98%
2-5	5	1	0.15	0	0.4	2	2	0.05	0	0	0.05	99.97%
2-6	6	2	0.45	2	0.1	0	2	0.09	0	0.81	0.90	99.45%
3-4	7	1	0.5	0	0.2	4	4	0.10	0	0	0.10	99.94%
3-7	8	4	0.1	3	0.3	0.5	2	0.11	0.06	0.22	0.40	99.76%
3-8	9	2	0.05	0	0.5	3	3	0.05	0	0	0.05	99.97%
4-9	10	2	0.25	2	0.2	0	4	0.10	0	0.90	1.00	99.39%
5-8	11	6	0.3	3	0.1	1	2	0.18	0.81	0.45	1.44	99.12%
7-10	12	2	0.15	2	0.2	0	2	0.06	0	0.24	0.30	99.82%
7-11	13	1	0.2	0	0.1	3	3	0.02	0	0	0.02	99.99%
8-11	14	4	0.25	2	0.4	2	4	0.38	0.80	0.50	1.68	98.98%
9-12	15	1	0.3	1	0.3	0	4	0.09	0	0.51	0.60	99.63%

After calculating the CRI of the components, the network resilience can be enhanced by making an investment in improving the resilience of components with low CRI. Since the resilience of the weakest component in the network is 97.26%, the current network resilience is also 97.26% (i.e., $R^n_{11} = 97.26\%$). The next two weakest components are Node 1 and Node 8. As it is explained in Section 3.3, to improve the network resilience, the resilience of Node 11 can be enhanced to 97.56% (i.e., the resilience level of Node 1). To find the best approach to improving the resilience of Node 11, the optimization model (25) in Section 3.3 is solved. The same procedure should be followed to improve the weakest component(s) until no further enhancement can be made due to the budget limitation. Figure 7 shows the cost functions of Node 1, Node 8, and Node 11, all of which are used to determine the optimal enhancement approach. The cost functions associated with the probability of experiencing disruption and the impact of component disruption on the network (i.e., $\mathcal{F}_i^{n_\mathcal{L}}, \mathcal{F}_i^{n_I}$) are assumed to be constant functions, meaning that the probability and the impact of the disruption on these nodes cannot be changed by spending money.

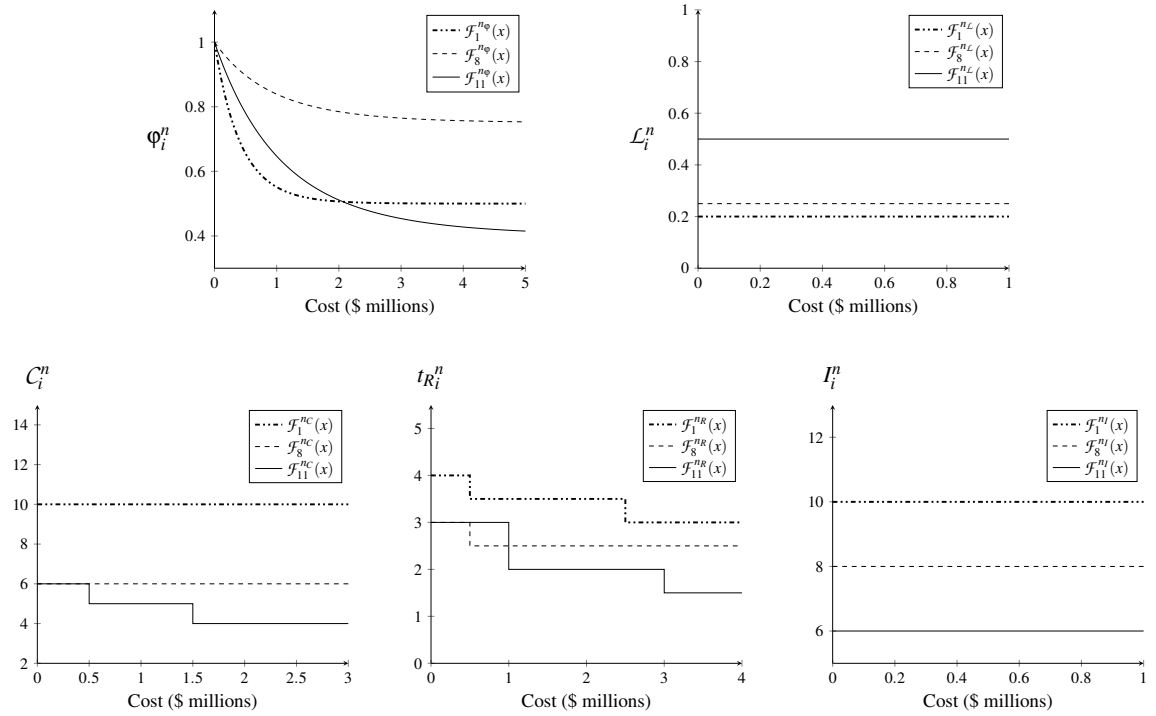
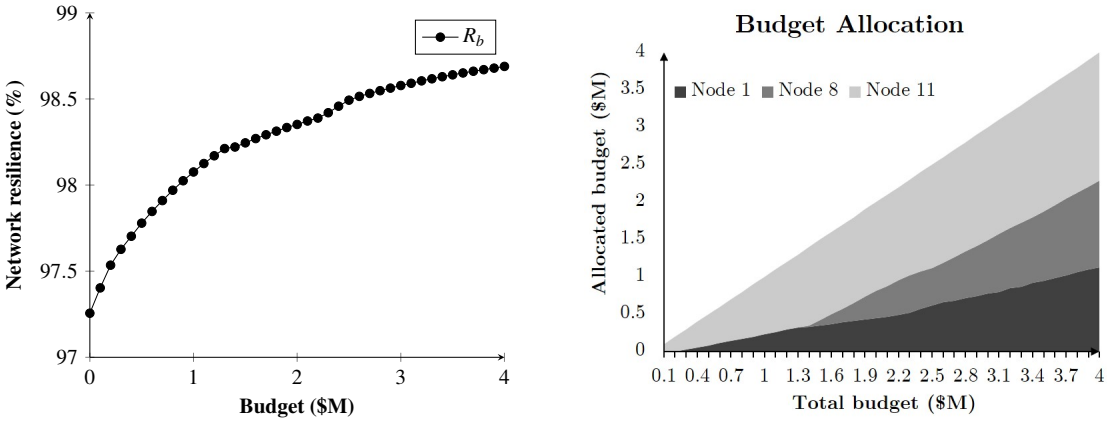


Figure 7: Cost functions of Node 1, Node 8, and Node 11, $\mathcal{F}_i^n(x)$ $i = 1, 8, 11$

The results of the optimization model indicate that, first, \$0.22 million should be spent on Node 11 to elevate its resilience from 97.26% to 97.56% (CRI of Node 1) through the reduction of φ^n_{11}. At this point, to enhance the network resilience, the resilience of both Nodes 1 and Node 11 should be improved. For the budget below \$1.3 million, the best decision is to reduce φ^n_1 and φ^n_{11}. However, by spending around \$1.3 million, the investors can decrease the total recovery time of Node 11 (i.e., R^n_{11}). Furthermore, spending \$1.4 million on Node 1 and 11 enhances their CRI to the level of Node 8 resilience. Figure 8 shows the improvement of network resilience under budget limitation. Figure 8a shows the maximum potential network resilience under certain budget values. The results of the optimization model under 40 different budget quantities (from 0.1 to 4.0 million) are presented in this figure. Additionally, Figure 8b illustrates the budget allocation to each node for each budget value.



(a) Improvement of network resilience

(b) Budget allocation to each node for resilience improvement

Figure 8: Improvement of the network resilience under budget limitation

3.2. Power Network Example

In this section, we use the single line diagram of the IEEE 14-Bus standard system [47](see Figure A.2 in Appendix) to illustrate our methodology for power networks. Figure 9 showcases a simplified power network in the form of a network graph. The first and second numbers located atop the nodes are power generation and load, respectively, and the number on each arc refers to its current flow. The capacity of each arc is assumed to be 200.

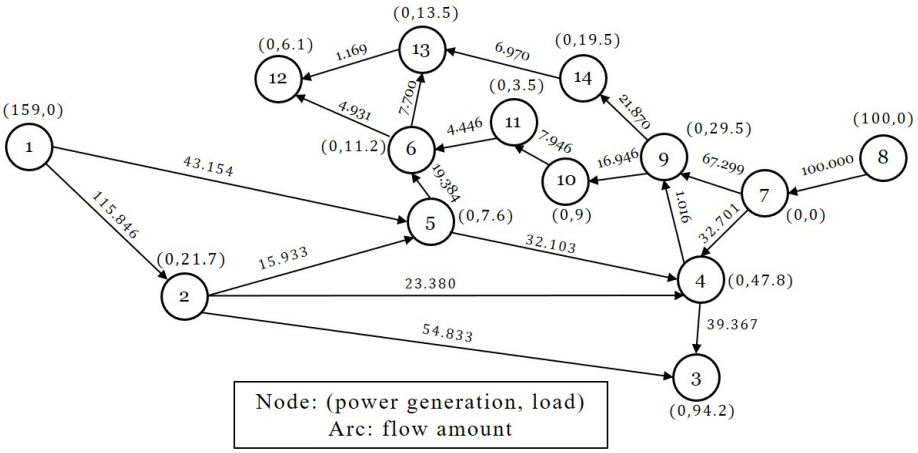


Figure 9: Power Network Example

It is assumed that the probability of having disruptions is the same for all components, and we focus on measuring the importance of the components' impact and criticality. The approach to solving this example is similar to the one explained in the supply chain instance. All of the necessary indices and the resilience values are calculated and shown in Table 3 and Figure A.3 in the Appendix. Nodes with positive generation quantity (i.e., Nodes 1 and 8) are the generators in the network and have high impact values (i.e., $I_1^n = 159$, $I_8^n = 100$). Node 7 is the only connection that joins Node 8 to the rest of the network, and if Node 7 is disrupted, there will be a noticeable overall loss. Hence, Nodes 1, 7, and 8 have the highest criticality and impact among the nodes and subsequently have the lowest CRI.

Table 3: resilience of each node in the power network example

Node #	I_i^n	$\mathcal{L}_i^n$	C_i^n	$t_{S_i}^n$	$t_{E_i}^n$	$t_{R_i}^n$	L_1	L_2	L_3	L	R_i^n
1	159.00	0.3	159.00	0.2	0	3	9.22	0	62.33	71.55	93.09%
2	115.85	0.3	21.70	0.2	2.44	3	6.72	14.57	1.83	23.12	97.77%
3	94.20	0.3	94.20	0.2	0	3	5.46	0	36.93	42.39	95.91%
4	88.18	0.3	47.80	0.2	1.37	3	5.11	16.83	11.66	33.61	96.76%
5	59.09	0.3	9.00	0.2	2.540	3	3.43	6.33	0.62	10.37	99.00%
6	23.83	0.3	11.20	0.2	1.59	3	1.38	4.67	2.37	8.42	99.19%
7	100.00	0.3	100.00	0.2	0	3	5.80	0	39.20	45.00	95.66%
8	100.00	0.3	100.00	0.2	0	3	5.80	0	39.20	45.00	95.66%
9	68.32	0.3	29.50	0.2	1.70	3	3.96	13.31	5.73	23.01	97.78%
10	16.95	0.3	9.00	0.2	1.41	3	0.98	3.26	2.15	6.39	99.38%
11	7.95	0.3	3.50	0.2	1.68	3	0.46	1.55	0.69	2.71	99.74%
12	6.10	0.3	6.10	0.2	0	3	0.35	0	2.39	2.75	99.73%
13	14.67	0.3	13.50	0.2	0.24	3	0.85	0.16	5.59	6.60	99.36%
14	21.87	0.3	14.90	0.2	0.96	3	1.27	3.38	4.57	9.22	99.11%

Table 4 and Figure A.4 in the Appendix present the calculations and resilience values corresponding to the arcs. Arcs (1,2), (1,5), and (7,8) are connected to the generators and have large criticality values ($C_{1,2}^a = 39$, $C_{1,5}^a = 39$, $C_{7,8}^a = 100$). While Arcs (1,2) and (1,5) have some alternatives that can partially cover their flows, Arc (7,8) is the only arc connected to Generator 8 and is the most critical arc in the network. Contrarily, Arc (4,9) has a low flow and has possible replacements, that agrees with its high resilience (99.99%).

Table 4: resilience of each arc in the power network example

ID	Arc #	I_{ij}^a	$\mathcal{L}_{ij}^a$	C_{ij}^a	$t_{S_{ij}}^a$	$t_{E_{ij}}^a$	$t_{R_{ij}}^a$	L_1	L_2	L_3	L	R_{ij}^a
1	1-2	115.85	0.3	39	0.2	1.99	3	6.72	20.94	5.91	33.57	96.76%
2	1-5	43.15	0.3	39	0.2	0.29	3	2.50	1.04	15.86	19.40	98.13%
3	2-3	54.83	0.3	0	0.2	3	3	3.18	0	0	3.18	99.69%
4	2-4	23.38	0.3	0	0.2	3	3	1.36	0	0	1.36	99.87%
5	2-5	15.93	0.3	0	0.2	3	3	0.92	0	0	0.92	99.91%
6	3-4	39.37	0.3	0	0.2	3	3	2.28	0	0	2.28	99.78%
7	4-5	32.10	0.3	0	0.2	3	3	1.86	0	0	1.86	99.82%
8	4-7	32.70	0.3	0	0.2	3	3	1.90	0	0	1.90	99.82%
9	4-9	1.02	0.3	0	0.2	3	3	0.06	0	0	0.06	99.99%
10	5-6	19.38	0.3	0	0.2	3	3	1.12	0	0	1.12	99.89%
11	6-11	4.45	0.3	0	0.2	3	3	0.26	0	0	0.26	99.97%
12	6-12	4.93	0.3	0	0.2	3	3	0.29	0	0	0.29	99.97%
13	6-13	7.70	0.3	0	0.2	3	3	0.45	0	0	0.45	99.96%
14	7-8	100.00	0.3	100	0.2	0	3	5.80	0	39.20	45.00	95.66%
15	7-9	67.30	0.3	0	0.2	3	3	3.90	0	0	3.90	99.62%
16	9-10	16.95	0.3	0	0.2	3	3	0.98	0	0	0.98	99.91%
17	9-14	21.87	0.3	0	0.2	3	3	1.27	0	0	1.27	99.88%
18	10-11	7.95	0.3	0	0.2	3	3	0.46	0	0	0.46	99.96%
19	12-13	1.17	0.3	0	0.2	3	3	0.07	0	0	0.07	99.99%
20	13-14	6.97	0.3	0	0.2	3	3	0.40	0	0	0.40	99.96%

According to Tables 3 and 4, on average, arcs are more resilient than nodes. Disruption on a node leads to disruption on the connected arcs as well as the node's output itself. However, experiencing a disruption on an arc only creates a problem in transferring the flow between two nodes. In the power network instance, the flow of all of the arcs except Arcs (1,2), (1,5), and (7,8) can be replaced by an alternative; hence, these arcs have criticality of 0. Contrarily, the nodes of the network have larger criticality indices and subsequently lower resilience.

The proposed network resilience measure is normalized in scale. Hence, it allows a fair comparison among different networks and applications. Comparing the supply chain network and the power system network examples, we observe that the latter has a lower resilience index than the former (93.09% compared to 97.26%). The total supply within the supply chain network has been distributed among all of the nodes, and no node carries a supply more than 25% of the supply of the network. This reduces the network vulnerability to disruptions on the nodes. Contrarily, there are only two generators in the power network system, and they are responsible for the total load in the network. This intensifies the network vulnerability to any disruption on these two nodes. Additionally, the flow of Arcs (7,8) and (1,2) form 44.7% and 38.6% of the total load in the network; thus, these two arcs have a lower CRI comparing to the other arcs in the supply chain network.

4. Conclusion

Physical networks are vulnerable to various natural and human-caused disasters. To mitigate the consequences of these disruptions, it is essential to enhance network resilience. In this study, a comprehensive method is proposed for quantifying network resilience; this method was developed based on the concept of the resilience triangle and its use to obtain total loss associated with network disruption. An additional resilience factor, "criticality," was introduced based on the ability of the system to perform in case of component failure. We defined a component to be critical if there is no alternative plan prepared given component disruption. To achieve the criticality of each component, an optimization model was developed to find the best alternative plan for the disrupted component. The resilience of each component is evaluated by considering the likelihood of component disruption, the impact of disruption on the network, the criticality of that component, and its recovery system. The proposed approach defines network resilience as the resilience of the lowest resilient component in the network. Based on this definition, it is essential to enhance the resilience of the components with the lowest resilience in order to improve the resilience of the network. An optimization model was developed to obtain the optimal approach in achieving the maximum network resilience under budget limitation. The proposed model can guide decision-makers in selecting an optimal option to enhance network resilience by improving the resilience of the weakest components. The proposed method is a general framework for various applications of physical networks to measure network resilience regardless of network type or size. We illustrated the method using two different sample networks: a randomly designed supply chain network and a power network example. Numerical results showed that the optimized investment strategy can help enhance the network resilience index by exploring alternative plans under the budget constraint.

A possible future extention to the proposed approach can include a methodology to capture network system dynamics to show how a disruption on a component affects the others. One can develop an optimization model (25) to consider the influence of resilience improvement of one component on the resilience of others. Furthermore, an approach is need to consider mutiple disruptions in the network and their cascading effects.

References

[1] J. Minkel, "The 2003 Northeast Blackout–Five Years Later," *Scientific American*, 2008.

[2] C. A.MacKenzie, J. R.Santos, and K. Barker, "Measuring changes in international production from a disruption: Case study of the Japanese earthquake and tsunami," *International Journal of Production Economics*, vol. 138, pp. 293–302, 2012.

[3] J. Manuel, "The Long Road to Recovery: Environmental Health Impacts of Hurricane Sandy," *Environmental Health Perspectives*, vol. 121, no. 5, p. a152, 2013.

[4] E. Lipton, "Cost of Storm-Debris Removal in City Is at Least Twice the U.S. Average," *The New York Times*, 2013.

[5] R. Li, Q. Dong, C. Jin, , and R. Kang, "A New Resilience Measure for Supply Chain Networks," *Sustainability*, vol. 9, no. 1, p. 144, 2017.

[6] D. Henry and J. E. Ramirez-Marquez, "Generic metrics and quantitative approaches for system resilience as a function of time," *Reliability Engineering & System Safety*, vol. 99, pp. 114–122, 2012.

[7] E. D. Vugrin, D. E. Warren, M. A. Ehlen, and R. C. Camphouse, "A framework for assessing the resilience of infrastructure and economic systems," in *Sustainable and resilient critical infrastructure systems*, pp. 77–116, Springer, 2010.

[8] E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd., 2006.

[9] 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, and D. Von Winterfeldt, "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthquake Spectra*, vol. 19, no. 4, pp. 733–752, 2003.

[10] T. J. Pettit, J. Fiksel, and K. L. Croxton, "Ensuring supply chain resilience: development of a conceptual framework," *Journal of Business Logistics*, vol. 31, no. 1, pp. 1–21, 2010.

[11] S. Y. Ponomarov and M. C. Holcomb, "Understanding the concept of supply chain resilience," *International Journal of Logistics Management, The*, vol. 20, no. 1, pp. 124–143, 2009.
[12] J. P. Sterbenz, E. K. Çetinkaya, M. A. Hameed, A. Jabbar, S. Qian, and J. P. Rohrer, "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation," *Telecommunication Systems*, vol. 52, no. 2, pp. 705–736, 2013.
[13] P. Vlacheas, V. Stavroulaki, P. Demestichas, S. Cadzow, D. Ikonomou, and S. Gorniak, "Towards end-to-end network resilience," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 3, pp. 159–178, 2013.
[14] M. Tortorella, "Service reliability theory and engineering, II: Models and examples," *Quality Technology & Quantitative Management*, vol. 2, no. 1, pp. 17–37, 2005.
[15] A. Reggiani, "Network resilience for transport security: Some methodological considerations," *Transport Policy*, vol. 28, pp. 63–68, 2013.
[16] B. Donovan and D. B. Work, "Empirically quantifying city-scale transportation system resilience to extreme events," *Transportation Research Part C: Emerging Technologies*, vol. 79, pp. 333–346, 2017.
[17] S. Enjalbert, F. Vanderhaegen, M. Pichon, K. A. Ouedraogo, and P. Millot, "Assessment of transportation system resilience," in *Human modelling in assisted transportation*, pp. 335–341, Springer, 2011.
[18] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on resilience of power systems under natural disasters—A review," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1604–1613, 2015.
[19] A. Khayatian, M. Barati, and G. J. Lim, "Market-based and resilient coordinated Microgrid planning under uncertainty," in *2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, pp. 1–5, IEEE, 2016.
[20] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the extreme: A study on the power system resilience," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1253–1266, 2017.
[21] G. Cimellaro, A. Tinebra, C. Renschler, and M. Fragiadakis, "New resilience index for urban water distribution networks," *Journal of Structural Engineering*, vol. 142, no. 8, p. C4015014, 2015.
[22] G. P. Cimellaro, O. Villa, and M. Bruneau, "Resilience-based design of natural gas distribution networks," *Journal of Infrastructure systems*, vol. 21, no. 1, p. 05014005, 2014.
[23] A. Golara and A. Esmaeily, "Quantification and enhancement of the resilience of infrastructure networks," *Journal of Pipeline Systems Engineering and Practice*, vol. 8, no. 1, p. 04016013, 2016.
[24] O. Kammouh, A. Zamani Noori, G. P. Cimellaro, and S. A. Mahin, "Resilience assessment of urban communities," *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, vol. 5, no. 1, p. 04019002, 2019.
[25] A. Kwasinski, J. Trainor, B. Wolshon, and F. M. Lavelle, "A conceptual framework for assessing resilience at the community scale," *Gaithersburg, MD: National Institute of Standards and Technology*, pp. 16–001, 2016.
[26] G. P. Cimellaro, C. Renschler, A. M. Reinhorn, and L. Arendt, "Peoples: a framework for evaluating resilience," *Journal of Structural Engineering*, vol. 142, no. 10, p. 04016063, 2016.
[27] K. Anand, P. Gai, S. Kapadia, S. Brennan, and M. Willison, "A network model of financial system resilience," *Journal of Economic Behavior & Organization*, vol. 85, pp. 219–235, 2013.
[28] H. Amini, R. Cont, and A. Minca, "Stress testing the resilience of financial networks," *International Journal of Theoretical and applied finance*, vol. 15, no. 01, p. 1250006, 2012.
[29] A. Khabazian and J. Peng, "Vulnerability analysis of the financial network," *Management Science*, 2019.
[30] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliability Engineering & System Safety*, vol. 145, pp. 47–61, 2016.
[31] J. H. Kahan, A. C. Allen, and J. K. George, "An operational framework for resilience," *Journal of Homeland Security and Emergency Management*, vol. 6, no. 1, 2009.
[32] E. D. Vugrin, D. E. Warren, and M. A. Ehlen, "A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane," *Process Safety Progress*, vol. 30, no. 3, pp. 280–290, 2011.
[33] M. Falasca, C. W. Zobel, and D. Cook, "A decision support framework to assess supply chain resilience," in *Proceedings of the 5th International ISCRAM Conference*, pp. 596–605, 2008.
[34] K. Tierney and M. Bruneau, "Conceptualizing and measuring resilience: A key to disaster loss reduction," *TR News*, no. 250, 2007.
[35] S. I. Mari, Y. H. Lee, and M. S. Memon, "Sustainable and resilient supply chain network design under disruption risks," *Sustainability*, vol. 6, no. 10, pp. 6666–6686, 2014.
[36] G. P. Cimellaro, A. M. Reinhorn, and M. Bruneau, "Seismic resilience of a hospital system," *Structure and Infrastructure Engineering*, vol. 6, no. 1-2, pp. 127–144, 2010.
[37] D. A. Reed, K. C. Kapur, and R. D. Christie, "Methodology for assessing the resilience of networked infrastructure," *IEEE Systems Journal*, vol. 3, no. 2, pp. 174–180, 2009.
[38] M. Ouyang, L. Dueñas-Osorio, and X. Min, "A three-stage resilience analysis framework for urban infrastructure systems," *Structural Safety*, vol. 36, pp. 23–31, 2012.
[39] R. Li, Q. Dong, C. Jin, and R. Kang, "A New Resilience Measure for Supply Chain Networks," *Sustainability*, vol. 9, no. 1, p. 144, 2017.
[40] M. Najarian and G. J. Lim, "Design and assessment methodology for system resilience metrics," *Risk Analysis*, 2019.
[41] M. Najarian, G. Lim, and M. Barati, "Levelized Resiliency Assessment of Interdependent Natural Gas and Electric Power Systems," *2018 IISE Annual Conference, Orlando, Florida, USA, 2018, p. 6.*, 2019.
[42] K. Barker, J. E. Ramirez-Marquez, and C. M. Rocco, "Resilience-based network component importance measures," *Reliability Engineering & System Safety*, vol. 117, pp. 89–97, 2013.
[43] P. Smith, D. Hutchison, J. P. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner, "Network resilience: a systematic approach," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 88–97, 2011.
[44] Y.-P. Fang, N. Pedroni, and E. Zio, "Resilience-based component importance measures for critical infrastructure network systems," *IEEE Transactions on Reliability*, vol. 65, no. 2, pp. 502–512, 2016.
[45] Y. Sheffi and J. B. Rice Jr, "A supply chain view of the resilient enterprise," *MIT Sloan Management Review*, vol. 47, no. 1, p. 41, 2005.

[46] X. Peng, D. B. Roueche, D. O. Prevatt, and K. R. Gurley, "An engineering-based approach to predict tornado-induced damage," in *Multi-hazard approaches to civil infrastructure engineering*, pp. 311–335, Springer, 2016.
[47] "Power Systems Test Case Archive." [Online], Available: http://www2.ee.washington.edu/research/pstca/.

Appendix A. Figures

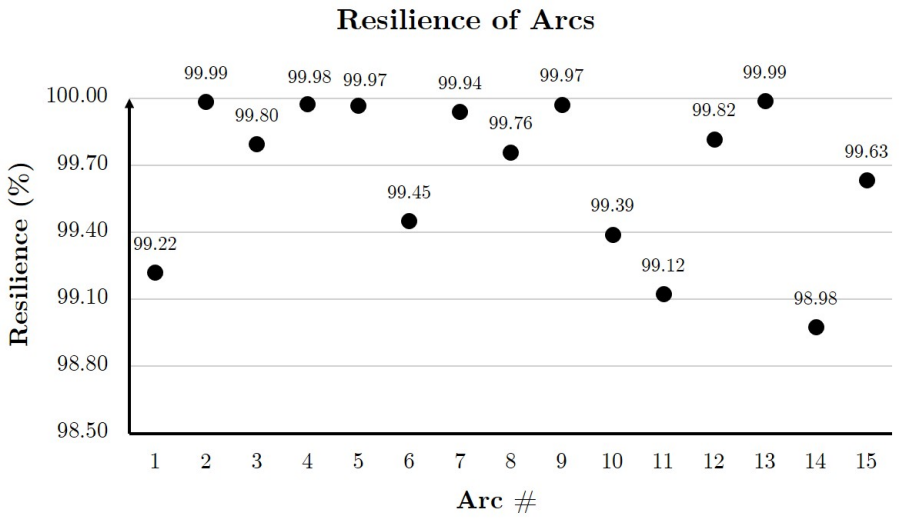


Figure A.1: Resilience of each arc in the supply chain network example

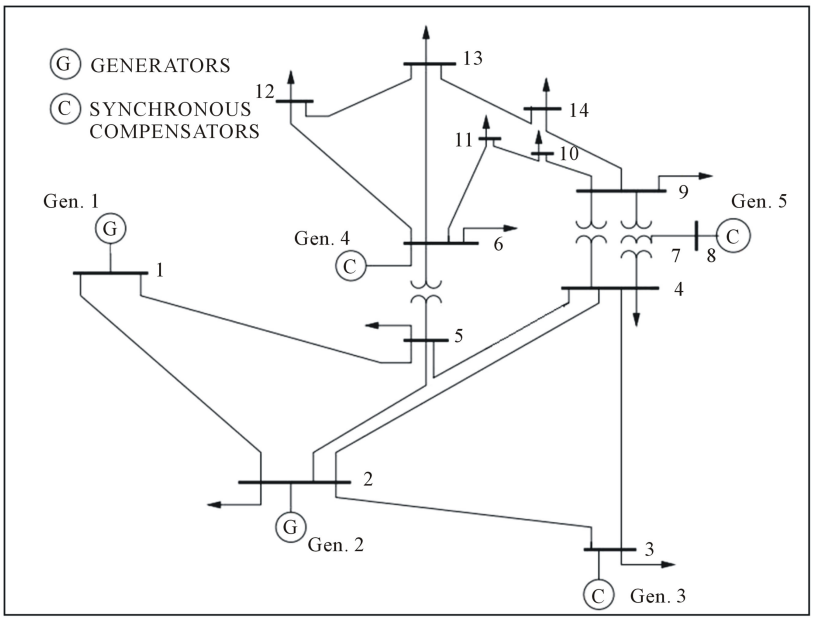


Figure A.2: IEEE 14 BUS test system [47]

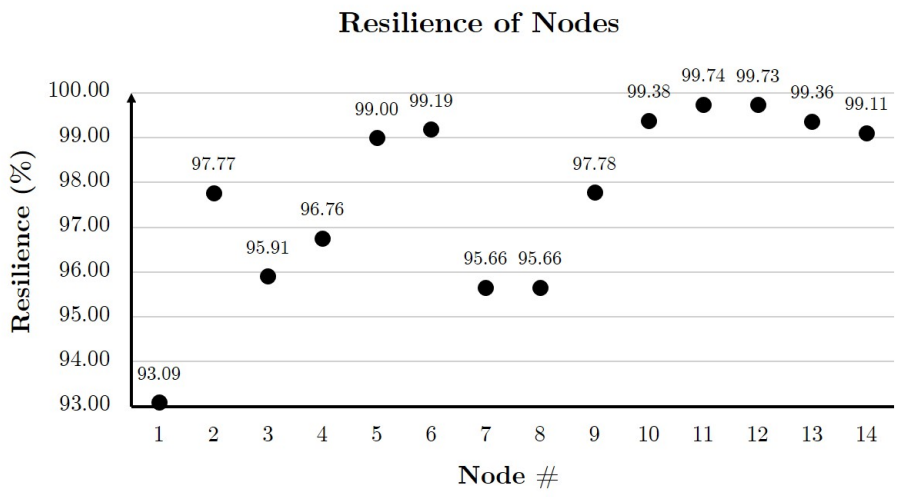


Figure A.3: Resilience of each node in the power network example

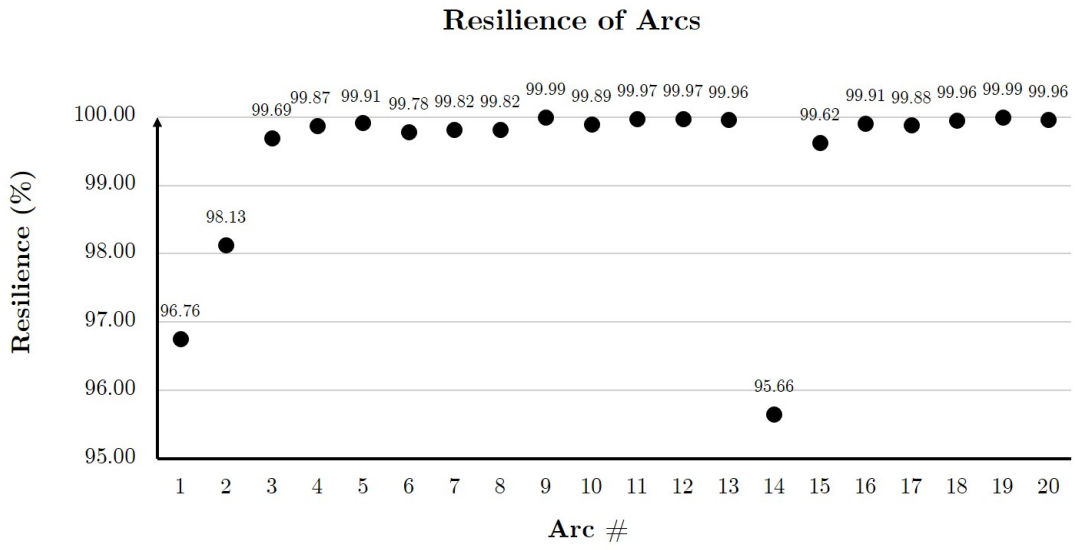


Figure A.4: Resilience of each arc in the power network example