Reliability Engineering and System Safety 94 (2009) 1685–1693

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Resiliency as a component importance measure in network reliability

John C. Whitson, Jose Emmanuel Ramirez-Marquez *

School of Systems & Enterprises, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030, USA

ARTICLE INFO

Article history:
Received 21 January 2009
Received in revised form
16 April 2009
Accepted 7 May 2009
Available online 14 May 2009

Keywords:
Reliability
Two-terminal
Network
Resiliency
Component importance

ABSTRACT

This paper seeks to define the concept of *resiliency* as a component importance measure related to network reliability. Resiliency can be defined as a composite of: (1) the ability of a network to provide service despite external failures and (2) the time to restore service when in the presence of such failures. Although, Resiliency has been extensively studied in different research areas, this paper will study the specific aspects of quantifiable network resiliency when the network is experiencing potential catastrophic failures from external events and/or influences, and when it is not known a priori which specific components within the network will fail. A formal definition for Category I resiliency is proposed and a step-by-step approach based on Monte-Carlo simulation to calculate it is defined. To illustrate the approach, two-terminal networks with varying degrees of redundancy, have been considered. The results obtained for test networks show that this new quantifiable concept of resiliency provides insight into the performance and topology of the network. Future use for this work could include methods for safeguarding critical network components and optimizing the use of redundancy as a technique to improve network resiliency.

1. Introduction

In the physical sciences, resiliency or elasticity refers to the ability of a substance or material to resume its natural shape after being distended by the application of forces. The elastic property of a material quantifies the degree of deformation that may occur before the material is unable to return to its original shape, or catastrophically, break [1]. Mathematically, this relationship is described in a stress–strain curve for a solid. Broadly, then, the physical resiliency concept has two components: (1) the material degree of deformation when a force is applied and, if deformation occurs, (2) the time to return to its original state.

The insight offered by this physical science description can be very useful to the systems engineer. Instead of a physical material, one can apply the resiliency concept to a system or a network by taking into account three key considerations: (1) the application of forces, (2) the degree of deformation, and (3) the capability to return to original shape. By taking into account these three key considerations, network resiliency should be related to the ability of a network to (1) provide a network function when under "the application of external forces" and if unable to do so, (2) restore the network function. Unfortunately from the perspective of this manuscript, and based on the extensive literature review undertaken for this research, resiliency, or the resilience of a network, is yet not clearly defined nor quantified in the context of network performance.

Although significant research has been performed on resiliency, when applied to specific network functions there is a problem regarding the concise definition of the concept. Currently, the concept of a resilient network can be mistaken or misunderstood for a network that is reliable or, survivable or, robust or, recoverable. For example, Westmark [2] in his extensive review for information system survivability reviews two definitions of survivability that are strongly similar to what resiliency defines, these are: (1) "the ability of a network to maintain or restore an acceptable level of performance during network failure conditions by applying various restoration techniques and the mitigation or prevention of service outages from potential network failures by applying preventative techniques" and (2) "that a system can be made robust to partially successful attack through general architecture features, through adaptability (flexible response to unanticipated changes) and flexibility (ability to adapt to a range of adverse events without having to anticipate the particular response in advance)." Moreover, and even most importantly, according to Wesmark [2] while most of the authors agree that "survivability" is highly important less than 1% of the articles he reviewed provide a computational approach.

The vagueness regarding the concept of resiliency illustrates that there is a need to clarify the concept and then, introduce computational techniques that quantify or support it. To address

Abbreviations: CIM, component importance measure; MANET, mobile ad-hoc network; RAW, reliability achievement worth; CCF, common cause failures

* Corresponding author. Tel.: +1 201 216 8003.
E-mail addresses: jmarquez@stevens.edu, Jose.Ramirez-Marquez@stevens.edu (J.E. Ramirez-Marquez).

0951-8320/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2009.05.001

Nomenclature

$G=(N, A)$	stochastic capacitated network where N represents the set of nodes and A the set of arcs
d	network flow requirement between source node s and sink node t
x_i	current state (capacity) of arc i
$\mathbf{b}_i$	$\mathbf{b}_i=(b_{i1}=0, b_{i2}, \ldots, b_{i\omega_i}=M_i)$ potential states for arc i
$\mathbf{p}_i$	$\mathbf{p}_i=(p_{i1}, p_{i2}, \ldots, p_{i\omega})$ Probability associated with each of the values taken by x_i (i.e. $p_{ij}=P(x_i=b_{ij})$)
$\mathbf{x}$	system state vector $\mathbf{x}=(x_1, x_2, \ldots, x_m)$ denotes the state of all the arcs of the network
$\varphi(\mathbf{x})$	network structure function representing capacity between s and t under system state vector $\mathbf{x}$
$R(\mathbf{x})$	network reliability $R(\mathbf{x})=P(\varphi(\mathbf{x})\geq d)$
$\Re_{(\alpha,\beta)}$	category I resiliency
α	number of component failures due to external causes
β	specific failure case containing α
$\Re_{\alpha}$	expected value of Category 1 resiliency for α
$M(m,n)$	uniform random number generator

the first issue, and based on the key considerations in the physical concept, network resiliency can be sorted into two main categories:

I. The sensitivity of network service to abnormal/external influences.
II. The sensitivity of network service restoration when in the presence of abnormal/external influences.

Rose [3] proposed a similar categorization for economic resilience. In his discussion, Category I (or static resiliency) is related to "*…the ability of an entity or system to maintain function (e.g., continue producing) when shocked…*" From a network perspective, the interest in Category I resiliency is then, on understanding the effect that external influences—herein understood as external causes of component failure—have on network service. Under this category, resiliency is tightly related to the network time to failure.

Similarly, Rose [3] describes Category II (or dynamic resiliency) as related to "*…the speed at which an entity or system recovers from a severe shock to achieve a desired state…*" From a network perspective, this category relates to the concept of time to restore services due to external causes of component failure. And, thus, resiliency is related to the network time to repair acceptable performance.

Thus, from the perspective of this manuscript resiliency is a composite of these two categories. That is, quantifying network resiliency is a two-step process that should first, describe the network's ability to tolerate external causes of component failure and second, based on this understanding, focus on quantifying the ability of the network to restore performance.

The main contribution of this paper is to provide an approach to quantify Category I resiliency in the context of networks. The specific networks under consideration are two-terminal networks that contain multiple nodes and links. Two-terminal networks allow to analyze systems that provide some kind of service between a specified set of nodes [4], usually called source and sink, where the source node can be thought of as the origin, and the sink node as the destination. For these networks, performance is quantified based on their ability to process such a service.

Specifically, the paper considers both binary and multi-state two-terminal networks as described in reliability research [4–6]. From a reliability perspective, two-terminal network analysis is based on quantifying the probability that the source and sink nodes can communicate (i.e. a binary case where the network and its components either work or fail [4]) or the probability that a required flow—generally defined as a network source–sink demand—can be satisfied from the source node to the sink node (i.e. a multi-state case that is a mixture of source–sink connectivity and capacity where the network and its components can have multiple "performance" states [6,7]).

At this point it is important to describe the main difference between the concepts of network reliability and Category I resiliency. Reliability quantifies the probability that the network performs its intended function, for a specific mission time, under normal and known operating conditions [8]. As defined in this paper, Category I resiliency quantifies the probability that the network performs its intended function, for a specific mission time, when in the presence of external causes of component failure–potential catastrophic failures due to attacks, disasters, etc. Thus, the main difference between these two concepts is the failure source. In reliability, network failure sources are internal and due to the wear, the tear or the intrinsic life of the network components. In Category I resiliency, the failure sources are external and internal; external, because components may cease to function due to man-made or natural events (events not considered under the normal and known operating conditions) and internal, because even under the external events the components adhere to their intrinsic life characteristics.

To quantitatively address the definition of Category I resiliency, this paper uses concepts from the area of reliability component importance measures (CIM). The concept of reliability importance is related to the sensitivity of the network function to changing conditions. In reliability, CIM quantify the sensitivity of network reliability to component failure [8,9] and have been widely used for identifying system weaknesses and to prioritize reliability improvement activities [10–15]—a task of high importance in large complex networks where component criticality is not immediately obvious to the designer. For example, systems engineering practice stresses the importance of examining component reliability early on in the engineering process for identifying critical components and for performance optimization via redundancy allocation and/or replication. Detailed reviews of CIM can be found in Ramirez-Marquez and Coit [10,11], Song and Der Kiureghian [16], Zio and Podofillini [12,13], and Rausand and Hoyland [9].

However, most CIM are based on single perturbation points (i.e. failure of one component) to describe the impact on network reliability and do not completely encompass Category I resiliency. Although, common cause failures (CCF) can be described as events that lead to simultaneous failure of multiple components due to a common cause, they are usually considered and estimated as part of the system reliability analysis [17,18]. That is, CCF when necessary should be included as a potential cause of failure within the operating environment. Thus, CCF are generally not implemented as CIM but as part of the reliability modeling. In Butler [19] the concept of cut set importance identifies component criticality based on the total number of distinct minimal cut sets of specific cardinality containing a specific system component. However, although obtained from a group analysis (i.e. cut set) this CIM provides insight about single component impact (i.e. the importance of the component based on its appearance on cut sets). Finally, it is important to note that recently Podofillini and