applied sciences

MDPI

Article

Optimal Multiculture Network Design for Maximizing Resilience in the Face of Multiple Correlated Failures

Yasmany Prieto [1], Nicolás Boettcher [1,2], Silvia Elena Restrepo [3] and Jorge E. Pezoa [1,*]

1 Departamento de Ingeniería Eléctrica, Universidad de Concepción, Concepción 4070386, Chile; yprietoh@udec.cl (Y.P.); nboettcher@udec.cl (N.B.)
2 Escuela de Informática y Telecomunicaciones, Universidad Diego Portales, Santiago 8370190, Chile
3 Departamento de Medio Ambiente y Energía, Universidad Católica de la Santísima Concepción, Concepción 4090541, Chile; srestrepo@ucsc.cl
* Correspondence: jpezoa@udec.cl; Tel.: +56-41-220-3333

Received: 18 March 2019; Accepted: 24 May 2019; Published: 31 May 2019

Abstract: Current data networks are highly homogeneous because of management, economic, and interoperability reasons. This technological homogeneity introduces shared risks, where correlated failures may entirely disrupt the network operation and impair multiple nodes. In this paper, we tackle the problem of improving the resilience of homogeneous networks, which are affected by correlated node failures, through optimal multiculture network design. Correlated failures regarded here are modeled by Shared Risk Node Groups (SRNGs) events. We propose three sequential optimization problems for maximizing the network resilience by selecting as different node technologies, which do not share risks, and placing such nodes in a given topology. Results show that in the 75% of real-world network topologies analyzed here, our optimal multiculture design yields networks whose probability that a pair of nodes, chosen at random, are connected is 1, i.e., its ATTR metric is 1. To do so, our method efficiently trades off the network heterogeneity, the number of nodes per technology, and their clustered location in the network. In the remaining 25% of the topologies, whose average node degree was less than 2, such probability was at least 0.7867. This means that both multiculture design and topology connectivity are necessary to achieve network resilience.

Keywords: correlated failures; multiculture topology; network diversity; network vulnerability; network robustness; resilience; software risks

1. Introduction

Under normal circumstances, data networking systems are designed to provide connectivity to all its nodes while, simultaneously, managing limited resources such as bandwidth, buffers, and the number of simultaneous connections. In the presence of failures or attacks, the design problem becomes very challenging because it must jointly provide some level of connectivity to the operating nodes, using protection schemes, manage the available resources, and offer restoration schemes. Thus, the purpose of the resilient design is to ensure both that a large portion of a communication network remains connected after a failure occurs and recovers promptly. In the literature, this is referred to as the reliable path provisioning problem, and such issue evidences the fundamental trade-off between providing reliable paths and efficiently utilizing the network resources. Lastly, correlated failures affecting network nodes have raised the attention of researchers because they impact multiple nodes, thereby their consequence on both users and network operators is severe [1–5]. Correlated failures may be triggered from natural phenomena, such as earthquakes and hurricanes, or may be

induced intentionally by men, as in the case of weapons of massive destruction, electromagnetic pulses, or cyber attacks.

Data networking systems are highly homogeneous because the trend in networking has been that all the technologies, at each layer of the architecture, must converge to a single one. The main effect of such a tendency is that most of the nodes are purchased from a single vendor and, consequently, they turn out to be identical or very similar devices. Data networks designed in this fashion are termed as monoculture networks. From joint management, economic, and interoperability point of view, monocultures are appealing. However, operating monoculture networks may introduce severe problems to their survivability. For instance, the lack of diversity in monoculture networks introduces shared risks to attacks/failures such as exploits (0-day vulnerabilities). Thus, a single attack/failure may affect multiple nodes and entirely disrupt the network operation.

Nowadays, network operators have at hand new, flexible, compatible, and more importantly diverse technologies for managing networked systems. For instance, Software-defined Networking (SDN) allows network operators to manage and control networking devices from multiple vendors [6]. Besides, Network Function Virtualization (NFV) techniques implement Network Functions (NFs) exploiting software virtualization, and such functions are executed on commodity hardware from multiple vendors [7]. Practical examples of how these two technologies have enabled multivendor implementations are: The CloudNFV platform for cloud computing, [8], the SDN-based Packet Transport Network operated by China Mobile [9], the Optical SDN designed by China Telecom [9], and the NFV-based Service Orchestration implemented by Anuta Networks, [10]. Remarkably, the multivendor interoperability trend has been stated as a requirement in 5G implementations and applications such as Machine-to-Machine (M2M) and Internet of Things (IoT) [11].

Since the tide is turning now towards multivendor environments, we raise the following question: May we exploit the available node technology diversity to improve the resilience of an entire network, which faces multiple correlated node failures, by introducing in the design process multiculture networks? This seems to be a valid question because the diversity in biological systems is indeed a valuable commodity for survivability, and researchers have shown that provisioning an adequate number of different species may be one reason for preserving biodiversity [12].

In this paper, we tackle the problem of improving network resilience, in the presence of correlated failures, by carrying out an optimal multiculture network design. To do so, we divided this complicated problem into simpler, sequential optimization problems. First, we pose a constrained optimization problem for selecting as many different technologies as possible, which do not share common risks while are capable of communicating the network nodes. We termed this problem as "The optimal selection of the technology set." Second, we propose another constrained optimization problem for selecting the number of nodes to be used from each technology, in order to fulfill a network design requirement with a Capital Expenditure (CAPEX) restriction. We termed this problem as "The fair technology distribution problem." Lastly, we state yet another constrained optimization problem for placing the nodes within the network topology so that its resilience is maximized. We termed this last problem as "The reliable node placing problem." The correlated failures regarded in this paper are modeled using Shared Risk Node Groups (SRNGs). These failures represent here cyber attacks, which aim to take advantage of specific vulnerabilities shared in all the network nodes belonging to the same SRNG event. We comment that, in the eight real-world network topologies considered here, our multiculture design enhances network resilience as compared to a monoculture design. In fact, results show that the proposed multiculture network design, which regards individual and shared node risks, can cope with multiple node failures induced by correlated SRNG events. In doing so, it efficiently trades off the number of technologies to be used (i.e., the degree of heterogeneity in the network), the number of nodes to specify per technology, and their location in the network topology. We note that, when our algorithms select larger sets of technologies, an attacker should make more efforts to compromise the network integrity and the impact caused by a particular attack on the network infrastructure is reduced. Additionally, our results also show that the node placing