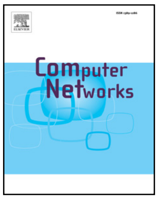
Computer Networks 100 (2016) 179–194

Contents lists available at ScienceDirect

Computer Networks

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



Bandwidth-aware allocation of resilient Virtual Software Defined Networks

Rafael L. Gomes[a,b,*], Luiz F. Bittencourt[b], Edmundo R.M. Madeira[b], Eduardo Cerqueira[a,c], Mario Gerla[a]

[a] Computer Science Department, University of California Los Angeles (UCLA), California, USA
[b] Institute of Computing, University of Campinas (UNICAMP), São Paulo, Brazil
[c] Faculty of Computer Engineering, Federal University of Pará (UFPA), Pará, Brazil

ARTICLE INFO

Article history:
Received 4 May 2015
Revised 1 February 2016
Accepted 26 February 2016
Available online 8 March 2016

Keywords:
Virtual networks allocation
Software Defined Network
Service Level Agreement
Resilience

ABSTRACT

Currently, it is hard to imagine our lives without the Internet, where services are accessed and shared by billions of users every day. However, even after many years, the Internet cannot guarantee Quality of Service (QoS) for the main services to current and future clients. To deal with this problem, clients establish Service Level Agreements (SLAs) with their Internet Service Providers (ISPs), including resilience parameters. The Internet is recognized to be resilient enough for many services, but it is still sensitive to failure events that affect the performance of these services. Software Defined Networks (SDNs) together with Virtual Network (VNs) approaches aim to enhance the management, planning and resource usage of networks. When both approaches are mixed together, we have Virtual Software Defined Network (VSDN). However, the allocation of VSDNs considering resilience issues is still an open issue. Within this context, this paper presents an algorithm for VSDN allocation, called *Bw-Risk-Ratio*, that considers resilience factors, as well as it deploys the VSDN according to QoS parameters defined in the SLA. Experiments using a real network topology show the effectiveness of the algorithm to deploy the VSDN resilient to failure events when compared to existing solutions.

1. Introduction

Nowadays, Internet services over communication networks play a vital role in our modern private, corporate, and institutional lives. As a consequence, users become frustrated when the Internet access fails and/or when application quality level drops. Currently, users share lots of content, which accounts for an expressive part of Internet traffic. In general, Internet traffic is composed of a variety of applications, which need high bandwidth and are sensitive to delay and packet losses.

Usually, to pursue Quality of Service (QoS) between companies/clients and Internet Service Providers (ISPs), a Service Level Agreement (SLA) is established to specify network parameters to be fulfilled by the ISPs [1], where resilience is a key requirement to avoid service disruption of networked applications. Network resilience has been defined as the capacity of the network to provide a minimum specified level of service in situations of faults in standard operation [2]. The concept of resilience involves not only incorporating reactive actions to manage post-event consequences, but also pre-event strategic planning. Moreover, reliability and traffic congestion concepts are important

[*] Corresponding author at: University of Campinas (UNICAMP), São Paulo, Brazil. Tel.: +55 19 982247245.

E-mail address: rafaellgom@ic.unicamp.br, rafaellgom@gmail.com (R.L. Gomes).

http://dx.doi.org/10.1016/j.comnet.2016.02.024

aspects of resilience to be considered during the service provisioning process [3].

Resilience and Bandwidth (Bw) are metrics closely related to the QoS, and they have direct impact in the user's impression/satisfaction about the service provided by the ISP. However, the current Internet design does not support both QoS and resilience guarantees, being necessary to improve the management and planning of ISPs to allow a better access to the Internet [3]. The implementation of these management and planning features involves ensuring SLA specifications, and thus impacts the user's experience during possible failure events in the ISP.

Network Virtualization (NV) and Software Defined Networks (SDNs) approaches emerge as prominent technologies to bring management and planning features for the future Internet. NV is a technology that enables the deployment of multiple network environments that share the same physical infrastructure [1], and SDN is a network architecture that allows us set up flows and subnetworks through controls that are separate from the data plane [4]. Both approaches can be mixed together through a Network Hypervisor (such as Flowvisor or OpenVirtex [5]), which allows slicing of the network in layers. Each layer is a customized Virtual Network (VN) that deploys a particular set of resources and protocols. We call this a *Virtual Software Defined Network* (VSDN). Through the VSDN approach, the ISP can isolate VNs in the SDN and separately deploy the functionalities requested by each client, for example packet routing, resource reservation, among others.

The flexibility and management control provided by VSDNs, however, does not come for granted. To deploy VSDNs, ISPs must develop allocation algorithms that decide which components (links and nodes) will take part on the VSDN to comply with client requests. In this context, this paper proposes the *Bw-Risk-Ratio* algorithm to deploy VSDNs with the best ratio between network reliability and bandwidth allocated to the VSDN. Thus, besides adapting the VSDN allocation according to the reliability, our proposal also aims to minimize the total bandwidth committed to solve the requests. To accomplish this, the proposed algorithm deploys a VSDN based on available Bw in the network and on the estimated risk of failure of the components allocated to VSDN. We also propose a risk model to define the failure risk of a component, which is used as input for our *Bw-Risk-Ratio* algorithm.

The objective of the proposed algorithm is to allocate a VSDN that is efficient (i.e., fulfills the SLA parameters using as few as possible resources from the ISP) under normal operating conditions, but is also planned to be resilient under failure events. The resilience is achieved with strategic planning for failure events, where the algorithm deploys alternative paths whose allocated Bw can be increased as necessary, called elastic Bw. This elastic Bw allocation is possible due to the dual characteristics of the proposed VSDN that combines the SDN and NV approaches [6].

The contribution of this paper is an allocation algorithm for VSDN, which focuses on searching relative disjoint paths to achieve resilience considering the events that can affect the network infrastructure, as well as the planning of resource allocation to ensure SLA. The contribution represents the utilization of distinct research topics that when mixed together can improve the service provision of ISPs.

This paper is organized as follows. Section 2 presents some basic concepts, including the description of the network reliability method and the presentation of some related work. Section 3 introduces the proposed algorithm. Section 4 describes the experimental results, and Section 5 concludes the paper and presents future work.

2. Background

This section provides key concepts for the understanding of this paper. Section 2.1 presents the concept of Virtual Software Defined Networks and an illustrative scenario, while Section 2.2 describes the network reliability calculation. Finally, Section 2.3 discusses the main related work of resilience strategies, encompassing disjoint path definition, failure recovery, survivability, and other.

2.1. Virtual Software Defined Networks

Virtualization is used to bring flexibility and isolation for computer networks. Traditionally, approaches to achieve virtualization of the network (for example, Xen [7], SR-IOV [8],, VIOLIN [9], and other) propose modification of existing network equipment and/or the usage of technologies that are not designed to perform the network virtualization, where the virtual components have autonomy and should be configured individually [4].

Another approach is the deployment of VNs over SDNs. The basic idea of SDN is to decouple control and forwarding planes to make the network more manageable. A *Controller* acts as the "brain", i.e., it is the entity responsible for network behavior, relaying information to the switches according to applications deployed on it. A network hypervisor can be deployed over an SDN infrastructure to provide an abstraction layer for the network components. Thus, it allows the creation of virtual networks that are completely decoupled and independent. The network hypervisor enables a virtual network to be independently managed by a controller and to be dynamically provisioned. These virtual networks created over the SDN infrastructures are called VSDNs, where the capability to customize both the network parameters and services provided by ISPs arises. Therefore, the solutions to deal with the virtualization over SDN infrastructures should interact directly with the network hypervisor and the flow tables inside the SDN switches.

Differently from the traditional approaches, in the VSDN context the virtualization is centralized in the network hypervisor and the intelligence of the network is based on the controller configuration, where one controller is responsible for one virtual network, which has a particular view of the network infrastructure composed of a subset of flows [4].

Fig. 1 illustrates each environment that exists in the context of VSDN in the ISPs and an *ISP Manager* represents the management entity of the ISP. *SDN Infrastructure* portrays the set of network components that compose the ISP. *Network Hypervisor* holds the configuration of VSDNs.