Computer Networks 92 (2015) 189–207

Contents lists available at ScienceDirect

Computer Networks

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

Resilience support in software-defined networking: A survey

Anderson Santos da Silva[a,*], Paul Smith[b], Andreas Mauthe[c], Alberto Schaeffer-Filho[a]

[a] Institute of Informatics, Federal University of Rio Grande do Sul, Brazil
[b] Safety and Security Department, AIT Austrian Institute of Technology, Austria
[c] School of Computing and Communications, Lancaster University, United Kingdom

ARTICLE INFO

Article history:
Received 7 May 2015
Revised 30 July 2015
Accepted 14 September 2015
Available online 20 October 2015

Keywords:
Software-defined networking
Network resilience
OpenFlow
Network challenges

ABSTRACT

Software-defined networking (SDN) is an architecture for computer networking that provides a clear separation between network control functions and forwarding operations. The abstractions supported by this architecture are intended to simplify the implementation of several tasks that are critical to network operation, such as routing and network management. Computer networks have an increasingly important societal role, requiring them to be resilient to a range of challenges. Previously, research into network resilience has focused on the mitigation of several types of challenges, such as natural disasters and attacks. Capitalizing on its benefits, including increased programmability and a clearer separation of concerns, significant attention has recently focused on the development of resilience mechanisms that use software-defined networking approaches. In this article, we present a survey that provides a structured overview of the resilience support that currently exists in this important area. We categorize the most recent research on this topic with respect to a number of resilience disciplines. Additionally, we discuss the lessons learned from this investigation, highlight the main challenges faced by SDNs moving forward, and outline the research trends in terms of solutions to mitigate these challenges.

1. Introduction

Computer networks are important for businesses and to support the operation of societally critical infrastructures, such as future (smart) electrical grids and government services. The growth in number and variety of end-to-end services that networks must support has led to a great deal of heterogeneity in the way networks are implemented, resulting in (i) complex protocols to handle the communication between network devices [1], (ii) difficult deployment of network policies by network administrators [2] and (iii) limited routing scalability [3–5]. Additionally, challenges to normal network operation, such as malicious attacks and prohibitive communication delay, demonstrate that computer networks have long-standing resilience requirements [6].

Resilience is the ability of the network to maintain an acceptable level of service when confronted with operational challenges [7]. A challenge is an atypical event that hinders the expected normal network operation [6,8]. In order to deal with a wide range of challenges, network resilience encompasses six major disciplines: security, survivability (including fault tolerance), performability, traffic tolerance, disruption tolerance and dependability [7]. When a network challenge arises, mitigation mechanisms should be activated, ideally without human intervention, to rapidly protect a network and the services it supports. However, the broad range of potential challenges that could befall a network requires sophisticated network (resilience) management systems that can detect and mitigate their effects [8]. Existing

[*] Corresponding author. Tel.: +555180152104.
E-mail addresses: assilva@inf.ufrgs.br (A.S. da Silva), paul.smith@ait.ac.at (P. Smith), a.mauthe@lancaster.ac.uk (A. Mauthe), alberto@inf.ufrgs.br (A. Schaeffer-Filho).

http://dx.doi.org/10.1016/j.comnet.2015.09.012
1389-1286/© 2015 Elsevier B.V. All rights reserved.

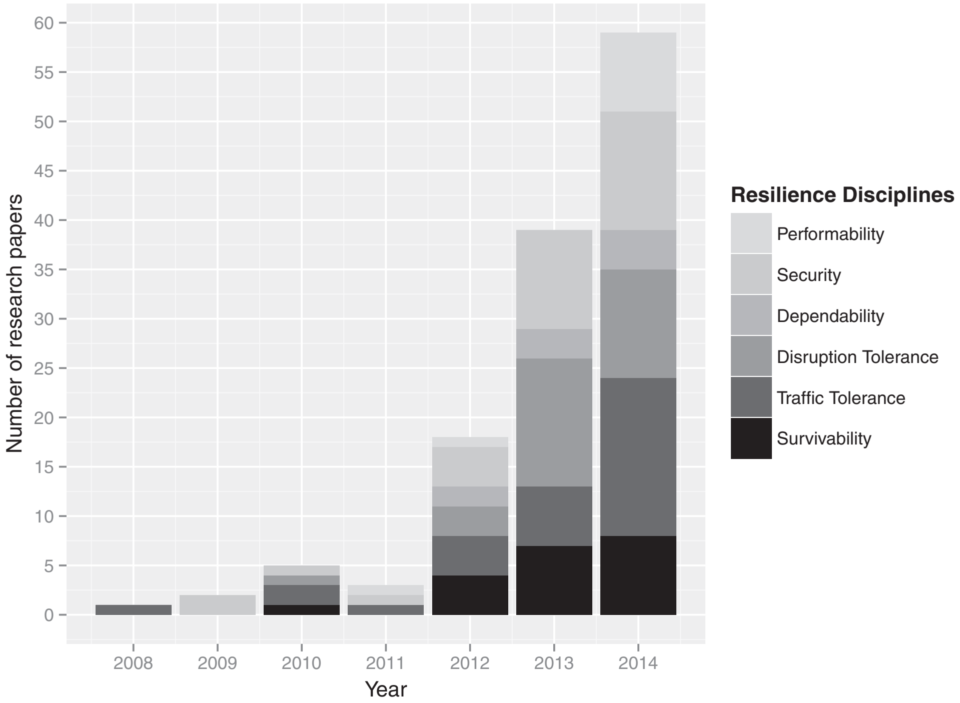

Fig. 1. Number of research papers included in this survey, according to their year of publication.

management systems have limitations, including a lack of flexibility with respect to challenge identification and mitigation, which has encouraged research that considers this problem in the context of new network architectures [9].

In both the research and industry communities, software-defined networking (SDN) [10] has recently gained significant attention. The main characteristic of the SDN architecture is that it decouples the implementation of network control logic from forwarding operations, thus enabling more flexible network control and management. In this context, a centralized *control plane* determines how forwarding devices, such as switches, will behave by configuring them using standardized protocols, such as OpenFlow [11]. The SDN architecture and the OpenFlow protocol, as its canonical implementation, offer (i) a comprehensive view of the network that is centralized in the *control plane*, (ii) high-levels of programmability of network applications, and (iii) fine-grained flow monitoring. These properties can be used to support the implementation of resilience mechanisms and help to minimize the complexity of managing them for network operators. Despite these benefits, new resilience challenges can arise because of the use of SDN, e.g., with respect to the fault tolerance of the control plane; research into addressing these issues is currently a major concern.

This paper presents a survey on the support for network resilience in software-defined networking. Research into this topic has recently intensified, as illustrated in Fig. 1, which summarizes the number of research papers addressing resilience aspects in SDN included in this survey, according to their year of publication. We organize the literature surveyed using the resilience taxonomy proposed by Sterbenz et al. [7], thus enabling a reliable categorization of the existing research efforts on SDN. Our survey discusses aspects such as existing solutions for resilience challenges, current open issues and research trends in this field. The aim of the survey is to present to the reader a comprehensive and structured view of network resilience in the SDN spectrum, and how resilience aspects are supported in these architectures.

We have observed that solutions related to fault management, infrastructure planning, routing and security applications, network measurement and anomaly detection are frequently used to address resilience challenges in the SDN context. However, we have identified several open issues in this research space, including the protection of the communication channel between network controller and forwarding devices; adequate support for sophisticated QoS solutions to enhance performability; and the need to detect novel malicious attacks targeting network devices.

The remainder of this paper is organized as follows. Section 2 presents necessary background material on SDN and network resilience. Section 3 discusses the proposed categorization of SDN efforts, with respect to different resilience disciplines. Section 4 shows a summary of the main research topics studied, topics already solved and others under investigation. Finally, Section 5 presents the concluding remarks.

2. Background

This section discusses the basic concepts and terminology used in this work. In particular, software-defined networking and network resilience are contextualized.