Journal of Network and Computer Applications 94 (2017) 33–49

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

Enabling network innovation in data center networks with software defined networking: A survey

Bin Dai[a,*], Guan Xu[a], Bengxiong Huang[a], Peng Qin[b], Yang Xu[c]

[a] School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, China
[b] China Academy of Electronics and Information Technology, Beijing, China
[c] School of Electrical and Computer Engineering, New York University, New York, USA

ARTICLE INFO

Keywords:
Software defined networking
Data centers
Automatic configuration
Network security
Resource allocation
Energy saving

ABSTRACT

With the rapid growth of cloud applications and users, Data Center Network (DCN) has become a critical component in the cloud ecosystem to sustain remarkable computation demand. It is facing great challenges in performance guarantee, security enforcement, and resource and energy management. Software Defined Networking (SDN), as an efficient way to collect network information and perform network management, has been adopted in DCN to enable automated network configuration and management. In this paper we aim at surveying the state-of-the-art techniques of using SDN in DCN and discuss the way SDN help DCN. We first present the introduction of SDN and DCN, then survey the SDN based DCN, and finally show some lessons and future trend.

1. Introduction

A data center is an industrial computing service infrastructure, with a facility to house computer systems and its associated components, such as storage devices, power supplies, communication devices, and security devices. It provides a cost-efficient way for companies and personal tenants to rent a slice of computation and communication resource to meet various requirements (Chen et al., 2013). A typical data center contains tens to hundreds of thousands of servers. For example, Google data center has been reported (Google architecture, 2008) to host more than 900,000 low-cost commodity servers in 2011, and a recent report (A. G., 2015) from IT consulting firm Anthesis Group infers that there are about 33 million physical servers deployed inside data centers around the world until 2015.

A fundamental challenge on Data Center Network (DCN) is to efficiently manage the huge number of network elements (Chen et al., 2013) to meet tenants' demands, and build DCN with low-cost commercial off-the-shelf hardware (Pries et al., 2012). According to literatures, there are many critical issues on DCN to achieve automatic configuration, security, resource allocation, energy saving and DCN virtualization (Dayarathna et al., 2016; Kachris and Tomkos, 2012). The DCN connection issues concern the bi-section bandwidth, which depends on the network structure. Innovated DCN structures, such as fatTree (Al-Fares et al., 2008) and VL2 (Albert et al., 2009), can achieve high bisection bandwidth by building rich connected topology with redundant switches and links (Chen et al., 2013). As the communication bandwidth demand of data center applications increases dramatically, the excessive power consumption is becoming another challenging issue in the design and deployment of a data center (Kachris and Tomkos, 2012). The traditional DCN architectures are not flexible enough to support DCN virtualization applications with QoS, deployability, manageability, and defense against security attacks (Bari et al., 2013).

To enable academic experiments on production networks without influencing the production traffic, Software Defined Networking (SDN) and OpenFlow are proposed as a novel network architecture (McKeown et al., 2008) with the network control decoupled from data forwarding. In the SDN architecture, the experiment rules are designed to handle experiment traffic and avoid influencing the production traffic on the same production network, as the rules on the flow tables of SDN switches can be instructed by the SDN controller. Besides OpenFlow, There are other SDN solutions including Cisco Open Network Environment (ONE) and Nicira Network Virtualization Platform (NVP). Cisco ONE is the DCN infrastructure solution that can solve challenges in both DCN computing and network management. For DCN network management, Cisco ONE can bring DCN greater agility and fast application delivery. For DCN infrastructures on Cisco Nexus Series devices, Cisco ONE provides foundation for Networking and advanced applications through Data Center Fabric. They focus on a scalable, resilient, high-performance physical and virtual network that

* Corresponding author.
E-mail address: nease.dai@gmail.com (B. Dai).

http://dx.doi.org/10.1016/j.jnca.2017.07.004
Received 4 April 2017; Received in revised form 2 June 2017; Accepted 4 July 2017
Available online 06 July 2017

provides workload mobility across multiple data centers. They propose a business-relevant SDN policy model across networks with Cisco Application Centric Infrastructure (Cisco ACI) to reduce Total Cost of Ownership (TCO), automate IT tasks and accelerate DCN application deployments. Nicira NVP can create an intelligent abstraction layer between virtualized hosts and an existing physical network. NVP is managed by a distributed controller system.

There is an increasing requirement of innovated networking technologies to meet the dynamic computing and storage demand. Firstly, the DCN applications commonly access databases and servers distributed in both public and private clouds, which requires flexible traffic management and enough bandwidth to guarantee the performance of transmission. Secondly, more and more users are accessing the databases and servers by their own devices as well as the working IT devices, which requires flexible networking technology to keep mobile devices online, and also requires security technology to detect malicious users. Thirdly, the parallel processing in DCN requires bandwidth for synchronization between distributed servers. The traditional network is constrained to provide dynamic and complex network rules, the large-scale parallel processing algorithms, and a standard and open interface for network devices.

To meet these DCN requirements, SDN has been used to implement network appliances such as load balancer, traffic engineering, in-network caching, malicious identification, access control policies enforcement, and dynamic resource allocation. As a free and open-source software platform, OpenStack has been exploited by both public and private cloud. And with the increasing scale of high-density and multi-tenancy cloud environment, the cloud operator and the tenants need to move, add or remove workload between servers or even between different clouds on the fly for new requirements, such as creating private networks, controlling the IP addressing, and additional network services. Therefore the networking services are redesigned with SDN to meet these new requirements. With the northbound APIs of the SDN controller, the cloud operator and tenants can program flow tables of hardware and software switches for flexible network services with lower cost and higher efficiency, implementing functions such as creating and configuring private networks, compliance & audit mandates, QoS, monitoring and troubleshooting, firewall, intrusion detection and Virtual Private Network (VPN). VMware provides an industry-leading Software Defined Data Center architecture to implement a unified platform for public, private and hybrid clouds, where cloud operators and tenants can rapidly develop, automatically deliver and manage all network applications. Their best-in-class virtualization product, VMWare vSphere, has been significantly improving IT efficiency and performance of worldwide enterprises networks. However the growing field of mobile cloud poses new challenges to infrastructure services of providing IT and networking resources in DCN. For these challenges, they extend the virtualization concept to all DCN resources and services with SDN. The DCN resources virtualization services deliver abstraction, pooling and automation of the compute, network, and storage infrastructure. And the provisioning and ongoing management of all these virtual resources are enabled by the policy-driven automation, with the advantages in reducing both capital expenditures and operating costs, accelerating application deployment and expansion, increasing the granularity of security and compliance for every application, and increasing the flexibility of customized cloud platform on various hardware, hypervisors, and clouds.

For DCN architecture, the SDN can deploy the network appliances flexibly to provide the application performance and security policies can be enforced by the security services on SDN controller applications. Since the first Data Center with SDN (DCSDN) (Tavakoli et al.,) has been attempted early in 2009, more and more novel studies have been proposed to integrate the DCN and SDN structures. Firstly, automatic configuration with SDN can automatically configure and re-configure the network to fulfil tenants' traffic (Liu et al., 2013a, 2013b). Secondly, middleboxes with SDN can be designed for network security (Lara et al., 2014). Thirdly, SDN based scheduling of flow and link workload is promising for future networks (Sharkh et al., 2013). Fourthly, the energy consumption of data centers is non-trivial, including switching/transmitting data traffic, storage/computation in DCN servers, cooling systems, and power distribution loss (Li et al., 2014). In this paper, we focus on the DCN issues that have been solved with SDN, and we divide these issues into automatic configuration, network security, network resource allocation, and energy saving. To the best of our knowledge, we are the first to survey DCSDN comprehensively. The remainder of this paper is organized as follows. Section 2 reviews the up-to-date surveys on SDN and DCN. Section 3 looks into the main improvement SDN has brought to DCN. Section 4 presents details of resource allocations. Section 5 lists promising aspect of DCSDN for future works. At last, we present the conclusion in Section 6.

2. Related work

There are excellent surveys investigating the state-of-the-art in SDN (Lara et al., 2014; Nunes et al., 2014; Hakiri et al., 2014; Scott-Hayward et al., 2013) and DCN (Chen et al., 2011; Bilal et al., 2014; Dayarathna et al., 2016; Ranjana and Raja, 2013; Jain and Paul, 2013; Azodolmolky et al., 2013; Zhang et al., 2013). For example, Hakiri et al. (2014) discussed the value of SDN in cloud based networks. They stated that SDN brings complementary network technology to DCN, and promotes the intelligence in network virtualization, automating resource provisioning and creating new services on top of the provisioned network resources. Also, they summarized SDN based interactive solutions in DCN that enable cloud services and applications to retrieve network topology and network failures for an optimized initialization and adjustment of network connectivity/tunneling. Wang et al. (2015) surveyed technologies for cloud DCN, including topology design and network technique of DCN, virtualized network elements, and routing for physical and virtual network elements. SDN is promising in providing intelligence in the control plane and traffic flexibility in the data plane for cloud DCN. As use cases for cloud computing, SDN can offer flexible routing scheme, reduce switching consumption, improve the performance of VLAN-based communications in various traffic management issues. Zhang et al. (2013) surveyed the transport layer challenges, such as latency and malicious attack in virtual data centers over multiple DCNs. They focus on the problems of TCP incast for many to one traffic pattern, the large latency of online queries and TCP performance deterioration for Visualized DCNs, and malicious user defense in multi-tenant DCNs.

As the cloud services become increasingly important, security becomes another important research issue. Yan et al. (2016) studied the DDoS attack problem in distributed DCNs, and surveyed some SDN based solutions. Rahman and Choo (2015) surveyed existing incident handling and digital forensic literature to fill the knowledge gaps in handling incidents in the cloud DCNs. Juliadotter and Choo (2015) presented a conceptual cloud attack taxonomy that follows the nature flow of an attack on a cloud service, divided into 5 dimensions, i.e. source, vector, target, impact and defense. With this taxonomy, they quantified the risk by rating values from 1 (low rise) to 9 (high risk), that can be used to estimate the likelihood and impact of a given attack. Subashini and Kavitha (2011) surveyed security issues in the stacks of different cloud service delivery models, i.e. SaaS, PaaS and IaaS, where the security issues can be classified into data storage security, data transmission security, application security and security related to the third party resources.

SDN promotes network virtualization in cloud DCNs, which has been studied in several surveys. Azodolmolky et al. (2013) compared SDN-based virtual networking implementations in cloud DCNs. Jain and Paul (2013) presented network virtualization methods in cloud DCNs, and pointed out the way the SDN architecture can facilitate network virtualization. The survey (Bari et al., 2013) studied various methods of network virtualization to support QoS, deployability,