DOI: 10.3969/j. issn. 1673-5188. 2016. 01. 008
http://www.cnki.net/kcms/detail/34.1294.TN.20160118.1527.002.html, published online January 18, 2016

From CIA to PDR: A Top-Down Survey of SDN Security for Cloud DCN

Zhi Liu[1, 2], **Xiang Wang**[1, 2], **and Jun Li**[1, 3]
(1. Research Institute of Information Technology, Tsinghua University, Beijing 100084, China;
2. Department of Automation, Tsinghua University, Beijing 100084, China;
3. Tsinghua National Laboratory for Information Science and Technology, Beijing 100084, China)

Abstract

By extracting the control plane from the data plane, SDN enables unprecedented flexibility for future network architectures and quickly changes the landscape of the networking industry. Although the maturity of commonly accepted SDN security practices is the key to the proliferation of cloud DCN, SDN security research is still in its infancy. This paper gives a top-down survey of the approaches in this area, discussing security challenges and opportunities of software-defined datacenter networking for cloud computing. It leverages the well-known confidentiality-integrity-availability (CIA) matrix and protection-detection-reaction (PDR) model to give an overview of current security threats and security measures. It also discusses promising research directions in this field.

Keywords

SDN security; cloud DCN; CIA; PDR

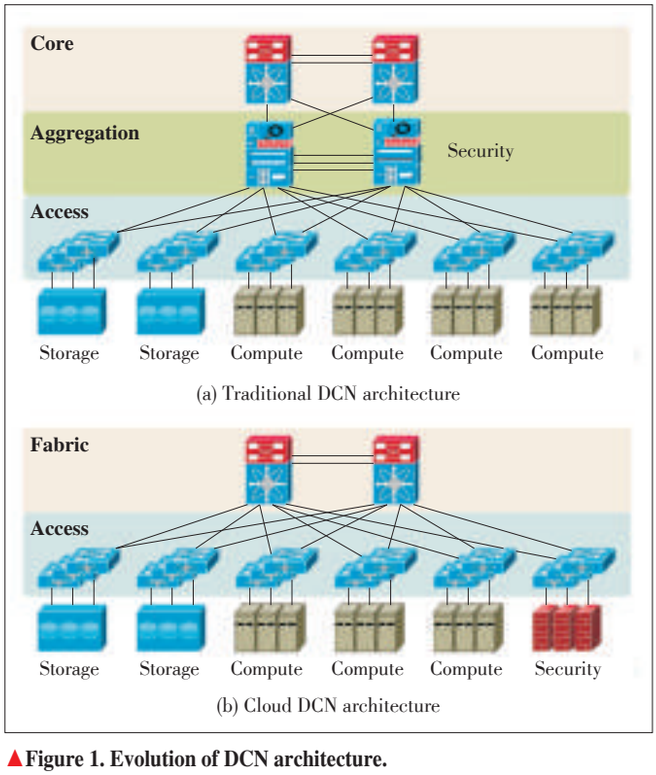
1 Introduction

Information technology has come a long way — from mainframes to personal computing and on to mobile computing. Now we are embracing cloud computing that was previously called utility computing or grid computing. In this fascinating transition, datacenters are similar to the mainframes of the old days, and mobile devices are like the old terminals, only much smarter and not tethered.

Traditional datacenters usually host proprietary services backed by a number of static and tightly coupled applications. Traditional datacenter networks (DCNs) mainly deal with large volumes of north-south traffic and usually have three layers (**Fig. 1a**). The access layer provides the connectivity for servers and storage facilities, normally through top-of-rack (ToR) switches. The aggregation layer mediates the access layer to the core layer, which in turn interfaces to the Internet. As the cloud evolves towards virtualization and multi-tenancy, this architecture often lacks elasticity and suffers from vendor lock-in [1].

Modern cloud datacenters support a variety of heterogeneous services for multiple tenants simultaneously. These datacenters are commonly built with a two-tier DCN (**Fig. 1b**). Tenants can deploy their own services on the shared infrastructure and pay-as-they-go. Several software-defined datacenter (SDDC) solutions have been proposed so that capacity can be expanded using infrastructure multiplexing and all tenant systems can be managed in an efficient, automatic manner.

Making datacenter services public instead of proprietary significantly increases infrastructure utilization and drastically affects the DCN design. Virtual machines (VMs) are frequently brought up, shut down, and even migrated across datacenters. Moreover, VMs of the same tenant may interconnect across multiple physical servers, and VMs of different tenants may share the same physical server. These complex scenarios make it very difficult to guarantee service-level agreements (SLAs)



▲**Figure 1. Evolution of DCN architecture.**

for each and every tenant.

In the cloud era, novel technologies are required to cope with emerging DCN security challenges [2]. Such technologies include topology-independent service assignment and policy enforcement, flow-based (rather than packet-based) processing, and awareness of virtualization and multi-tenancy. From many industrial surveys, we see that security concerns are still an obstacle to the proliferation of cloud computing [3].

Software-defined networking (SDN) is central to addressing complex network management and security issues. It decouples the control plane from the data plane by extracting the mostly autonomous embedded controllers from traditional network elements. The virtually centralized SDN control plane leverages its global knowledge of network topology and status, and acts as a network operating system. This enables a network development and operation (DevOps) team to program network services via open and standard application programming interfaces (APIs) such as OpenFlow. This also instigates the rise of white boxes, as opposed to closed proprietary products of a few dominant vendors.

Because SDN is not yet mature, cloud DCN security is in its infancy. Cloud DCN security is a hot research topic and there is no consensus on it yet. Standardization and industrial application of cloud DCN security is still at a very early stage. This paper focuses on the challenges and opportunities related to cloud DCN. We provide a top-down survey of recent approaches to SDN security and employ the confidentiality-integrity-availability (CIA) matrix [4] and protection-detection-response (PDR) model [5] for analyzing security threats and measures. Section 2 reviews related work. Section 3 discusses DCN building blocks and corresponding security demands. Section 4 and section 5 summarize security threats and security measures, respectively. Section 6 concludes the paper.

2 Previous Work

Although SDN and network function virtualization (NFV) are very recent trends in networking, several comprehensive surveys of related security research and technologies have already been published [6]–[9]. Some are even updated from time to time to reflect the fast progress in this area. Existing surveys have different perspectives on SDN security. Some distinguish between research on protecting the network and research on providing security as a service, i.e., secure SDN (security of SDN) and SDN security (security by SDN) [6], [7]. Others analyze and summarize SDN security technologies in different target environments [8] or according to types of middlebox functions [9].

In [7], the authors review SDN characteristics and present a survey of security analysis and potential threats in SDN. They then describe a holistic approach to designing the security architecture required by SDN. Their summary of the problems and solutions for each of the main threats to SDN is helpful for an overall understanding of SDN security advances. The authors conclude that, evidenced by the commercially available applications, work on leveraging SDN to increase network security is more mature than the solutions addressing the security issues inherited or introduced by SDN.

In [8], the authors give an overview of existing research on SDN security, focusing on an analysis of security threats and potential damage. Such threats include spoofing, tampering, repudiation, information disclosure, denial-of-service (DoS), and elevation of privilege. The authors also discuss SDN security measures, such as firewall, intrusion detection system (IDS) (or intrusion prevention system, IPS), policy management, monitoring, auditing, privacy protection, and others controls to threats in specific networking scenarios. A comprehensive list of references categorized into different SDN security functionalities is provided.

This paper takes a more fundamental and focused point of view from the perspective of practical conditions. We first partition the cloud DCN into intra-DCN, access-DCN, and inter-DCN, and differentiate the unique properties of them. Then, we analyze the changing attributes of the traditional PDR model from the perspective of CIA matrix.

3 The Three Networks

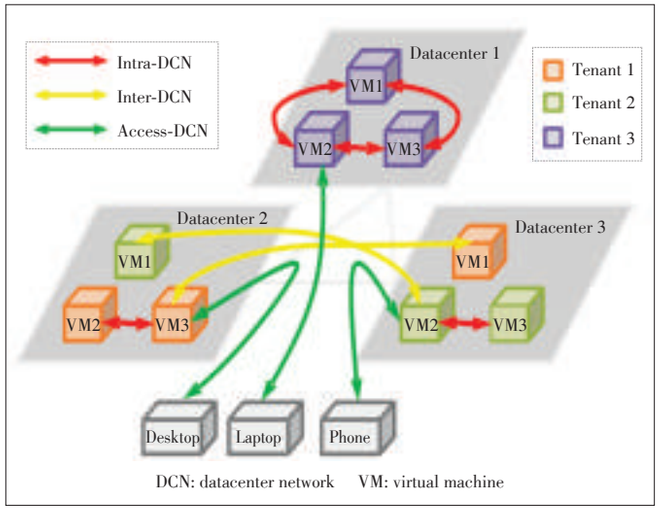
In a traditional DCN, there are various middleboxes that provide rich network services in addition to basic connectivity offered by forwarding devices, such as switches and routers. Firewalls, IDS/IPS, and other security middleboxes are normally deployed at the aggregation layer to inspect and steer network traffic. In this outdated model, policy enforcement is closely coupled with actual reachability; therefore, the middleboxes have to sit on the physical packet path, causing administration difficulties and performance bottlenecks [2].

Leveraging SDN, cloud DCN relies on a flat architecture to achieve better elasticity and is designed for cost efficiency and performance enhancement. In this new model, especially in public cloud DCN with pervasive multi-tenancy and high resource utilization, north-south traffic gives way to east-west traffic [10]. The hierarchical partition of the DCN is no longer valid, and DCN building blocks can be categorized according to functional characteristics, such as intra-DCN, inter-DCN, and access-DCN [10] (**Fig. 2**).

3.1 Intra-Datacenter Network

Intra-DCN is the network of resources inside the datacenter. The intra-DCN connects all IT elements together to create clouds for tenants. With virtualization and multi-tenancy, the clear network boundaries between traditional security zones of networks usually disappear; thus, network security policies are now enforced on dynamically distributed network security functions [11].

The correctness and efficiency of security policy deployment



▲Figure 2. Three networks of cloud DCN.

depends on the controller's real-time awareness of network topology, service status, and traffic pattern. Several approaches to providing a wide variety of security functionalities for intra-DCN and adapting to network changes have been proposed. VXLAN [12] and a few other encapsulation protocols are deployed for network virtualization to isolate traffic of different tenants or subnets. Service function chaining (SFC) [13] has been proposed to orchestrate multiple middleboxes of the same or different functions. Micro-segmentation provides middlebox functions within L2 networks and delivers fine-grained network security. In OpenStack, the most promising open-source cloud platform, neutron network service program also incubates firewall-as-a-service (FWaaS), VPN-as-a-service (VPNaaS), IDS-as-a-service (IDSaaS), and load-balancing-as-a-service (LBaaS) projects for security service provision within cloud datacenters.

In existing works on intra-DCN security, the focus is on providing security capacity and functions with agility and elasticity.

3.2 Access-Datacenter Network

Access-DCN is the network of clients outside datacenters that provide direct and pervasive connectivity for users so that they can access applications running in the cloud.

Distributed denial-of-service (DDoS) is one of the most hotly discussed topics related to access interfaces of cloud datacenters. There has been some recent advancement on the application delivery controller (ADC) and web application firewall (WAF). Other work has also been done on mobile access and more application-specific areas. Existing network security devices, such as unified threat management (UTM) and next-generation firewall (NGFW), can also provide high performance at this location, including hardware accelerations.

Because the access points of all tenants are connected to the Internet, which shares the same IP address space, tenants can take full advantage of the security hardware resources to complete common security inspections. In summary, solutions of access-DCN security mainly focus on optimizing security inspections.

3.3 Inter-Datacenter Network

Inter-DCN is the network of clouds for federation networking between public and private cloud datacenters or optimizing network resources between multiple datacenter sites.

Google's B4 [14] is the most influential achievement in inter-datacenter networking. Microsoft's software-driven WAN [15] is also constructed for peak load shifting. There has not been a lot of security R&D on this front, mostly because mature virtual private network (VPN) technologies already satisfy the basic security requirements of cloud providers.

The rest of this paper is mainly focused on intra-DCN, which is the focal point of network security and advancement.

4 The Three Threats

Network security threats are becoming more sophisticated and powerful. Advanced persistent threat (APT) uses blended hacking schemes to penetrate a network and compromise the target systems. Recent DDoS attacks have reached 400 Gbps aggregated network traffic volume, and the number of attacks over 100 Gbps has greatly increased [16]. Network security threats all basically boil down to interception, modification, interruption, and fabrication. The fundamental security matrix is still CIA, although authenticity, non-repudiation, and other security mechanisms are equally important.

4.1 Threat to Confidentiality

In cloud datacenters, confidentiality may be ensured by access control list (ACL) and cryptographic solutions. However, the fundamental challenge lies in tenant isolation. For intra-DCN, this means tenant traffic isolation: one tenant should not be able to send or receive network packets to or from another tenant unless explicitly permitted by the security policy. Tenant isolation is a key feature supported by the SDN virtual networking PaaS.

PortLand [1] is an example of the design and implementation of a non-blocking network fabric for virtualized datacenters. Multi-tenancy and tenant isolation are achieved by changing the processing logic of access switches with the rewriting of hierarchical pseudo MAC addresses. NetLord [17] proposes an encapsulation scheme for overlay network virtualization. It can be deployed on existing networking devices without any modification and enables different tenants to share the same L2/L3 address spaces. NetLord also has very good scalability.

NVP [18] describes the overall design of network virtualization platform, including both data plane and control plane. It leverages Open vSwitch and packet encapsulation to implement the overlay network virtualization, and designs a datalog-

based declaration language to define and implement network policy. LiveCloud [19] further addresses the integration of hardware networking devices in clouds. It uses both hardware and software switches to compose the access layer for various resources.

Reviewing these existing approaches, it can be observed that traffic is almost always isolated at the network edge, where the bulk of computing resources can be used for complex processing logic. At the same time, this requires dynamic policy coordination and deployment for on-demand stateful inspection, such as NFV-ed firewall, to ensure that policies are globally correct and locally conflict-free.

4.2 Threat to Integrity

In terms of integrity in the broader perspective, deep inspection prevents intrusion and/or extrusion and is the most critical demand [20], including NFV-ed IDS/IPS and data leakage prevention (DLP).

Player [2] introduces a policy-aware switching layer for deployment of middleboxes. This approach removes middleboxes from traffic paths and steers traffic to traverse these devices in a user-defined sequence. It essentially decouples network policies from physical topology, which introduces much more flexibility into middlebox deployment. SIMPLE [21] addresses the same problem but also solves the problems of traffic routing loops and the negative effects of packet modification. It also takes into consideration routing and load balancing given switch constraints. A reliable solution for dynamic middlebox actions, FlowTags [22] designs a tagging scheme that exposes the internal mapping of flows before and after middlebox processing. The introduced tags can be recognized and leveraged by SDN switches to compose service chains.

On the control plane level, Stratos [23] proposes a framework for middlebox orchestration according to workload variation. Tackling the closed middlebox implementation in Stratos, OpenNF [24] abstracts the middlebox API and designs a series of APIs for middlebox configuration and notification. These APIs can be used to coordinate the state control of both middleboxes and forwarding devices. SDSA [25] introduces a dedicated security controller for security-related functionalities, such as security device management, security policy deployment, and security event monitoring. The security controller also cooperates with the network controller to obtain a global view and enforce security policies such as ACL. Considering topology changes caused by VM migration and dynamic resource relocation, real-time security capacity redistribution and policy instance update are vitally important.

4.3 Threat to Availability

In terms of availability, most security efforts are directed towards DoS/DDoS mitigation. To counter attacks and prevent service unavailability, security middleboxes and policies are often deployed dynamically on these middleboxes. DFence [26] dynamically instantiates DDoS mitigation middleboxes, intercepts suspicious network traffic, and filters attacking traffic. A dynamic throttling method was also proposed in [27] to prevent DoS attack. With this method, flows originating from the same client are limited when the request rate from the client exceeds a dynamically determined threshold. Pushback [28] has a cooperative mechanism to mitigate DDoS attacks. The rate of upstream devices is limited when a DDoS attack occurs so that the attacking traffic is blocked near its entry point.

Availability security threats have diverse mechanisms for every specific scenario, which means the identification of suspicious traffic patterns (defined by security operators and expressed in the security policy) is very important. Thus, the management of security policies is central to intra-DCN security. Management of security policies includes policy definition [29], [30], policy compilation [31], [32], policy assignment [33], [34], policy optimization [35], [36], policy deployment [37], [38], and policy lookup [39], [40]. Some research has described several roadmaps ahead, but so far no consensus has been reached.

5 The Three Stages

Security is mostly a defensive practice that takes charge of policy enforcement. From the perspective of control theory, articulate system design is required to meet application requirements, where sensors and actuators are versatile for real time response, and feedback is essential to constantly adapt the situational changes and improve control quality. Many security approaches targeting the SDN-based cloud DCN have been proposed and can be evaluated in the well-known PDR lifecycle model.

5.1 Protection Stage

In the protection (or planning) stage, the key to intra-DCN security is to design a suitable architecture that both satisfies the security management requirements and is future-proof to a certain extent.

Unlike traditional DCN, SDN has a global view of the cloud DCN, and thus enables security mechanisms to be deployed in a distributed and dynamic manner. Two aspects need to be weighed in this phase: where to place security functions and how to manage security policies.

Regarding the placement of security functions, SDN and NFV devices are orthogonal [41]. **Table 1** shows the main differences between SDN and NFV. SDN focuses on network forwarding, mainly for traffic delivery. It performs stateless processing of L2-L3 network traffic at the packet level according to network topology. By contrast, the basic responsibility of NFV is network monitoring, and it is also responsible for security, measurement, and optimization. NFV conducts stateful and deep inspection of L4-L7 network traffic at the flow level according to resources and policies.

▼Table 1. Orthogonality of SDN and NFV

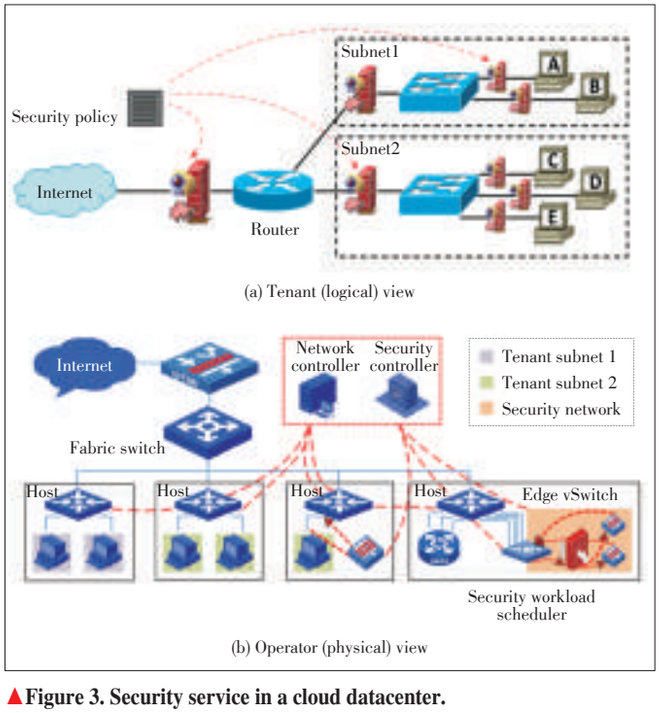
	Forwarding	Monitoring
Task	Delivery	Security, measurement, optimization
Logical object	Packet	Flow
Physical object	L2-L3, Header	L2-L7, Header + Payload
Basis	Topology	Resource, policy
State	Stateless	Stateful
Manner	Local autonomy	Global governance
Device	NIC, hub, switch, router	Middlebox
Algorithm	Routing origination, Routing lookup	Packet classification, pattern matching, AppID, traffic management

NIC: Network Interface Card AppID: Application Identification

Conventionally, SDN and NFV devices are managed by different administrators. Tualatin [11] is designed according to orthogonal principles and provides efficient security in a cloud datacenter. Networking devices and security devices are separately managed by their corresponding controllers (**Fig. 3**). Considering both flexibility and performance, Tualatin decouples the security scenarios into intra-VN, inter-VN, and access-VN and uses hardware and software co-design to meet different security requirements.

There have also been proposals of pushing all middleboxes, mostly network security functions, to the edge of intra-DCN [42] or implementing security inspected in off-path control plane [43]. However, the authors of this paper do not believe this will solve the problem all together.

Security policies can be enforced with changing [44] or respecting [33] forwarding policies. Security policy enforcement combined with forwarding policies can easily introduce performance impact on the data plane, while security policy enforcement based on forwarding policy has clear design boundary and thus simplifies control plane structure.



▲Figure 3. Security service in a cloud datacenter.

5.2 Detection Stage

In the detection (or runtime) stage, network security functions are used to discover and defend security attacks.

In Fig. 3, intra-VN security depends on traffic statistics generated by NetFlow on software switches to enable heavy-load security inspections. Both ACL and QoS policies are deployed on software switches. For inter-VN security, Tualatin chains multiple security services within a standalone virtual network. Tualatin introduces a security workload scheduler for load balancing and function composition and exposes fine-grain APIs for flow slice to support micro-segmentation. For access-VN, hardware UTM or NGFW can be leveraged for common security inspections for multiple tenants. This helps with the sharing of computing resources of security devices.

To efficiently implement these detection engines, virtualized middleboxes need to be redesigned in a consolidated way. RouteBricks [45] reveals the curtain of high-speed packet processing on commodity servers. CoMB [46] consolidates middlebox functions and re-implements them on an X86 platform. These works demonstrate the possibility of high-performance middleboxes on commodity servers, which lays the foundation for NFV. OpenGate [47] proposes the architecture for distributed middlebox processing. It takes full advantage of different hardware platforms to tackle the challenges of L2-L3 and L4-L7 processing, which helps to optimize middlebox performance.

For all these hardware accelerated or software virtualized functions to cooperate effectively and achieve high performance, major breakthroughs in policy management technology is necessary.

5.3 Response Stage

In the response (or feedback) stage, security events, action results, clues of potential threats, statistical and behavioral anomalies are collected. The collected information is analyzed with special tools, including machine learning and big data, to find new threat signatures or models [48], previously unknown vulnerabilities [49], and ways to improve security back to the protection stage. Within industry, security information and event management (SIEM) advancements can definitely be leveraged on this front [50].

6 Conclusion

Modern DCN for cloud computing has made great progress in terms of architecture evolution, and now SDN and NFV are leading the way forward. Therefore, SDN security is critical for

the proliferation of multifarious cloud services.

Despite the extrinsic nature of various emerging threats—especially those introduced by virtualization and multi-tenancy—the essence of network security is still unchanged. Beginning with the well-known PDR model, this paper has discussed the latest threats categorized by the CIA matrix as well as network security advancements.

In the area of intra-DCN security, this paper emphasizes the central role of security policies in the evolution of novel security mechanisms, including network virtualization and isolation, intrusion and extrusion prevention, and attack defense and mitigation. From security architecture to particular algorithms, from theory to practice, from academia to industry, there have been more and more proposals and developments around different aspects of policy management, such as definition, compilation, assignment, optimization, deployment and lookup.

Besides the management of security policy, other notable challenges and opportunities have unveiled promising directions in the green field of DCN security. We argue that there is yet no sign of framework consensus or approach convergence in the near future for SDN based cloud DCN security, and we expect key developments in distributed policy, service chaining, as well as visualization and troubleshooting tools.

References

[1] R. N. Mysore, A. Pamboris, N. Farrington, *et al.*, "PortLand: a scalable fault-tolerant layer 2 data center network fabric," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 4, pp. 39-50, 2009. doi: 10.1145/1592568.1592575.

[2] D. A. Joseph, A. Tavakoli, and I. Stoica, "A policy-aware switching layer for data centers," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 4, pp. 51-62, 2008. doi: 10.1145/1402958.1402966.

[3] Forbes. Predicting Enterprise Cloud Computing Growth [Online]. Available: http://www.forbes.com/sites/louiscolumbus/2013/09/04/predicting-enterprise-cloud-computing-growth/

[4] U.S. Government Publishing Office. Public Printing and Documents - Coordination of Federal Information Policy - Information Security - Definitions [Online]. Available: http://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542/content-detail.html

[5] W. Schwartau. "Time based security," New York, USA: Interpact Press, 1999.

[6] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, "A survey of securing networks using software defined networking," *IEEE Transactions on Reliability*, vol. 64, no. 3, pp. 1086-1097, Sept. 2015. doi: 10.1109/tr.2015.2421391.

[7] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Communications Surveys & Tutorials*, vol. PP, no. 99, p. 1, Jul. 2015. doi: 10.1109/comst.2015.2453114.

[8] I. Alsmadi and D. Xu, "Security of software defined networks: a survey," *Computers & Security*, vol. 53, pp. 79 - 108, Sep. 2015. doi: 10.1016/j.cose.2015.05.006.

[9] J. François, L. Dolberg, O. Festor, and T. Engel, "Network security through software defined networking: a survey," in *Proc. Conference on Principles, Systems and Applications of IP Telecommunications*, Chicago, USA, 2014, p. 6. doi: 10.1145/2670386.2670390.

[10] Cisco Systems. Cisco Global Cloud Index: Forecast and Methodology, 2014-2019 [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html

[11] X. Wang, Z. Liu, B. Yang, Y. Qi, and J. Li, "Tualatin: towards network security service provision in cloud datacenters," in *IEEE 23rd International Conference on Computer Communication and Networks (ICCCN)*, Shanghai, China, 2014, pp. 1-8. doi: 10.1109/icccn.2014.6911782.

[12] *Virtual Extensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Llayer 2 Networks over Layer 3 Networks*, IETF RFC 7348, Aug. 2014.

[13] *Service Function Chaining (SFC) Architecture*, IETF RFC 7665, Oct. 2015.

[14] S. Jain, A. Kumar, S. Mandal, *et al.*, "B4: experience with a globally-deployed software defined wan," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 3-14, 2013. doi: 10.1145/2486001.2486019.

[15] C. Hong, S. Kandula, R. Mahajan, *et al.*, "Achieving high utilization with software-driven WAN," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 15-26, 2013. doi: 10.1145/2486001.2486012.

[16] Akamai. Q2 2015 State of the Internet—Security Report [Online]. Available: https://www.stateoftheinternet.com/resources-cloud-security-2015-q2-web-security-report.html

[17] J. Mudigonda, P. Yalagandula, J. C. Mogul, B. Stiekes, and Y. Pouffary. "NetLord: a scalable multi-tenant network architecture for virtualized datacenters," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 62-73, 2011. doi: 10.1145/2018436.2018444.

[18] T. Koponen, K. Amidon, P. Balland, *et al.*, "Network virtualization in multi-tenant datacenters," in *Proc. 11th USENIX Symposium on Networked Systems Design and Implementation*, Seattle, USA, Apr. 2014.

[19] X. Wang, Z. Liu, Y. Qi, and J. Li, "LiveCloud: a lucid orchestrator for cloud datacenters," in *Proc. IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom)*, Los Alamitos, USA, pp. 341-348, Dec. 2012. doi: 10.1109/cloudcom.2012.6427544.

[20] A. Bremler-Barr, Y. Harchol, D. Hay, and Y. Koral, "Deep packet inspection as a service," in *Proc. 10th ACM International on Conference on Emerging Networking Experiments and Technologies*, Sydney, Australia, pp. 271-282, 2014.

[21] Z. A. Qazi, C. Tu, L. Chiang, *et al.*, "SIMPLE-fying middlebox policy enforcement using SDN," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 27-38, 2013. doi: 10.1145/2486001.2486022.

[22] S. Fayazbakhsh, L. Chiang, V. Sekar, M. Yu, and J. Mogul, "Enforcing network-wide policies in the presence of dynamic middlebox actions using FlowTags," in *Proc. 11th USENIX Symposium on Networked Systems Design and Implementation*, Seattle, USA, Apr. 2014, pp. 533-546.

[23] A. Gember, A. Krishnamurthy, S. St. John, *et al.*, "Stratos: a network-aware orchestration layer for middleboxes in the cloud," University of Wisconsin-Madison, Madison, USA, Tech. Rep., 2013.

[24] A. Gember, R. Viswanathan, C. Prakash, et al., "OpenNF: enabling innovation in network function control," in *Proc. ACM Conference on SIGCOMM*, Chicago, USA, pp. 163-174, 2014. doi: 10.1145/2619239.2626313.

[25] W. Liu, X. Qiu, P. Chen, *et al.*, "SDSA: a programmable software defined security platform," in *Proc. International Conference on Cloud Computing Research and Innovation*, Biopolis, Singapore, Oct. 2014, pp. 101-106.

[26] A. Mahimkar, J. Dange, V. Shmatikov, H. Vin, and Y. Zhang, "dFence: transparent network-based denial of service mitigation," *Proc. 4th USENIX Symposium on Networked Systems Design and Implementation*, Cambridge, USA, Apr. 2007, pp. 327-340.

[27] JE Belissent, "Method and apparatus for preventing a denial of service (DoS) attack by selectively throttling TCP/IP requests," U.S. Patent No. 6,789,203. 7, Sep. 2004.

[28] J. Ioannidis and S. M. Bellovin, "Pushback: router-based defense against DDOS attacks," in *Proc. Network and Distributed System Security (NDSS) Symposium*, San Diego, USA, Feb. 2002. doi: 10.5353/th_b3017330.

[29] T. L. Hinrichs, N. Gude, M. Casado, J. C. Mitchell, and S. Shenker, "Practical declarative network manage," in *Proc. 1st ACM SIGCOMM Workshop on Research on Enterprise Networking*, Barcelona, Spain, Aug. 2009, pp. 1-10. doi: 10.1007/978-3-540-92995-6_5.

[30] C. Prakash, J. Lee, Y. Turner, *et al.*, "PGA: using graphs to express and automatically reconcile network policies," in *Proc. ACM Conference on Special Interest Group on Data Communication*, London, UK, Aug. 2015, pp. 29-42. doi: 10.1145/2785956.2787506.

[31] N. Foster, R. Harrison, M. J. Freedman, *et al.*, "Frenetic: a network programming language," *ACM SIGPLAN Notices*, vol. 46, no. 9, pp. 279-291, 2011. doi: 10.1145/2034773.2034812.

[32] C. Monsanto, J. Reich, N. Foster, J. Rexford, and D. Walker, "Composing software-defined networks," in *Proc. 10th USENIX Symposium on Networked Systems Design and Implementation*, Lombard, USA, Apr. 2013. doi: 10.1016/b978-0-12-416675-2.00014-0.

[33] N. Kang, Z. Liu, J. Rexford, and D. Walker, "Optimizing the 'one big switch' abstraction in software-defined networks," in *Proc. Ninth ACM Conference on Emerging Networking Experiments and Technologies*, Santa Barbara, USA, Dec. 2013, pp. 13-24. doi: 10.1145/2535372.2535373.

[34] X. Wang, W. Shi, Y. Xiang, and J. Li, "Efficient network security policy enforcement with policy space analysis," *IEEE/ACM Transactions on Networking*, 2016. doi: 10.1109/tnet.2015.2502402.

[35] A. R. Curtis, J. C. Mogul, J. Tourrilhes, *et al.*, "DevoFlow: scaling flow manage-

ment for high-performance networks," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 254-265, 2011. doi: 10.1145/2018436.2018466.
[36] P. Kazemian, G. Varghese, and N. McKeown, "Header space analysis: static checking for networks," in *Proc. 9th USENIX Symposium on Networked Systems Design and Implementation*, San Jose, USA, Apr. 2012, pp. 113-126.
[37] M. Reitblatt, N. Foster, J. Rexford, C. Schlesinger, and D. Walker, "Abstractions for network update," in *Proc. ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, Helsinki, Finland, Aug. 2012, pp. 323-334. doi: 10.1145/2377677.2377748.
[38] W. Zhou, D. Jin, J. Croft, M. Caesar, and P. Godfrey, "Enforcing customizable consistency properties in software-defined networks," in *Proc. 12th USENIX Symposium on Networked Systems Design and Implementation*, Oakland, USA, Apr. 2015, pp. 73-85.
[39] B. Vamanan, G. Voskuilen, and T. Vijaykumar, "EffiCuts: optimizing packet classification for memory and throughput," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 207 - 218, 2011. doi: 10.1145/1851182.1851208.
[40] Y. Qi, L. Xu, B. Yang, Y. Xue, and J. Li, "Packet classification algorithms: from theory to practice," in *Proc. 28th Conference on Computer Communications*, Rio de Janeiro, Brazil, Apr. 2009, pp. 648 - 656. doi: 10.1109/infcom.2009.5061972.
[41] J. McCauley, A. Panda, M. Casado, T. Koponen, and S. Shenker, "Extending SDN to large-scale networks," Open Networking Summit, Research Track, Santa Clara, USA, 2013.
[42] S. Ratnasamy and S. Shenker. Quick Overview of SDN/NFV Research at Berkeley [Online]. Available: http://onrc.stanford.edu/protected% 20files/Day1/6.% 20Overview% 20of% 20SDNv2% 20Architecture% 20and% 20Related% 20Efforts.pdf
[43] S. Shin, P. Porras, V. Yegneswaran, *et al.*, "FRESCO: modular composable security services for software-defined networks," in *Proc. 2014 Workshop on Security of Emerging Networking Technologies*, San Diego, USA. doi: 10.14722/sent.2014.23006.
[44] M. Yu, J. Rexford, M. J. Freedman, and J. Wang. "Scalable flow-based networking with DIFANE," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 351-362, 2011. doi: 10.1145/1851182.1851224.
[45] M. Dobrescu, N. Egi, K. Argyraki, *et al.*, "RouteBricks: exploiting parallelism to scale software routers," in *Proc. ACM SIGOPS 22nd Symposium on Operating Systems Principles*, Big Sky, USA, 2009, pp. 15 - 28. doi: 10.1145/1629575.1629578.
[46] V. Sekar, N. Egi, S. Ratnasamy, M. Reiter, and G. Shi, "Design and implementation of a consolidated middlebox architecture," in *Proc. 9th USENIX Symposium on Networked Systems Design and Implementation*, San Jose, USA, Apr. 2012, pp. 24-24.
[47] Y. Qi, F. He, X. Wang, *et al.*, "OpenGate: towards an open network services gateway," *Computer Communications*, vol. 34, no. 2, pp. 200-208, 2011.
[48] M. V. Mahoney and P. K. Chan, "Learning nonstationary models of normal network traffic for detecting novel attacks," in *Proc. Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Edmonton, Canada, 2002, pp. 376-385. doi: 10.1145/775047.775102.
[49] W. Fan, M. Miller, S. Stolfo, W. Lee, and P. Chan, "Using artificial anomalies to detect unknown and known network intrusions," *Knowledge and Information Systems*, vol. 6, no. 5, 2004, pp. 507-527. doi: 10.1109/icdm.2001.989509.
[50] N. B. Anuar, M. Papadaki, S. Furnell, and N. Clarke, "An investigation and survey of response options for intrusion response systems (IRSs)," in *IEEE Information Security for South Africa*, Johannesburg, South Africa, 2010, pp. 1-8. doi: 10.1109/issa.2010.5588654.

Manuscript received: 2015-12-01

Biographies

Zhi Liu (zhi-liu12@mails.tsinghua.edu.cn) is currently a PhD candidate at Department of Automation, Tsinghua University, China. He received his BS degree from Department of Automation, Tsinghua University in 2012. His research interests include software-defined networking, cloud datacenter network, and performance optimization for networking algorithms and systems.

Xiang Wang (xiang-wang11@mails.tsinghua.edu.cn) received his PhD degree in 2015 from Department of Automation, Tsinghua University. He received his MS degree from the School of Software Engineering, University of Science and Technology of China in 2010 and BS degree from the School of Telecommunication Engineering, Xidian University, China in 2007. His research interests include software-defined networking, distributed system, and performance issues in computer networking and system architectures.

Jun Li (junl@tsinghua.edu.cn) received his PhD degree in Computer Science from New Jersey Institute of Technology (NJIT), USA, and MS and BS degrees in Control and Information from Department of Automation, Tsinghua University. He is currently a professor at Tsinghua University, and Executive Deputy Director of the Tsinghua National Laboratory for Information Science and Technology. Before rejoined Tsinghua University in 2003, he held executive positions at ServGate Technologies, which he co-founded in 1999. Prior to that, he was a senior software engineer at EXAR and TeraLogic. In between of his MS and PhD studies, he was an assistant professor then lecturer in the Department of Automation, Tsinghua University. His current research interests mainly focus on networking and network security.