Editorial

Network Security and Management in SDN

Zhiping Cai¹, **Chengchen Hu²**, **Kai Zheng³**, **Yang Xu⁴**, and **Qiang Fu⁵**

¹College of Computer, National University of Defense Technology, Changsha 410073, China

²Xi'an Jiaotong University, Xi'an 710049, China

³Huawei Technologies, Shenzhen 518129, China

⁴New York University, New York City, NY 11201, USA

⁵Victoria University of Wellington, Wellington 6140, New Zealand

Correspondence should be addressed to Zhiping Cai; zpcai@nudt.edu.cn

Received 17 February 2018; Accepted 20 February 2018; Published 4 June 2018

Copyright © 2018 Zhiping Cai et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Software Defined Networking (SDN) enables flexible deployment and innovation of new networking applications by decoupling and abstracting the control and data planes. It has radically changed the concept and way that we build and manage networked systems and reduced the barriers to entry for new players in the service market. Recently, SDN has been widely studied and applied to facilitate network management and the development of network security systems. However, the separation of control and data planes makes SDN vulnerable to security threats. Attackers can monitor and tamper network management information and disrupt network communication by implementing man-in-the-middle attacks, saturation attacks, Denial of Service (DoS) attacks, and so forth. Therefore, it is important to analyze the vulnerability and design defense mechanisms for securing SDN-based systems. In this special issue, we have selected nine papers that address such technical issues.

B. Han et al. propose a cross-plane distributed DoS (DDoS) attack defense framework in SDN, called OverWatch, which exploits collaborative intelligence between data plane and control plane with high defense efficiency. They develop a collaborative DDoS attack detection mechanism, which consists of a coarse-grained flow monitoring algorithm on the data plane and a fine-grained machine learning based attack classification algorithm on the control plane. J. Ye et al. apply the support vector machine classification algorithm to judge the network traffic and detect the DDoS attack. T. Wang et al. also try to address the DoS attack problem. They propose a lightweight and fast DoS detection and mitigation system

for SDN, called SDNManager. The SDNManager employs a novel dynamic time-series model which greatly improves bandwidth prediction accuracy. They also propose a dynamic controller scheduling strategy to ensure the global network state optimization and improve the defense efficiency.

Y. Zhou et al. discovered a novel inference attack targeted at SDN/OpenFlow network, which is motivated by the limited flow table capacities of SDN/OpenFlow switches and the following measurable network performance decrease resulting from frequent interactions between data and control plane when the flow table is full. They also propose two possible defense strategies for the discovered vulnerability, including a routing aggregation algorithm and a multilevel flow table architecture. C. Qi et al. present a game-theoretic model to analyze the security performance of SDN architectures. This model can represent several kinds of player information, simulate approximate attack scenarios, and quantitatively estimate systems' reliability. Their experimental results and analysis reveal diverse defense mechanisms adopted in dynamic systems, which have different effects on security improvement.

W. Fu et al. analyze the forwarding procedure and identify the performance bottleneck of SDN software switches. An FPGA-based mechanism for accelerating and securing SDN switches, named FAS, is proposed to take advantage of the reconfigurability and high-performance advantages of FPGA. FAS improves the performance as well as the capacity against malicious traffic attacks of SDN software switches by offloading some functional modules. Y. Lee et al. propose

Duo, an intrusion tolerant system in SDN, which can reduce exposure time without consuming computing resources. Duo classifies traffic into benign and suspicious traffic with the help of SDN/NFV technology that also allows dynamically forwarding the classified traffic to different servers. By reducing exposure time of a set of servers, Duo can decrease exposure time on average.

C. Zhang et al. propose Kuijia, a robust traffic engineering system for data center WANs, which relies on a novel failover mechanism in the data plane called rate rescaling. The victim flows on failed tunnels are rescaled to the remaining tunnels and put in lower priority queues to avoid performance impairment of aboriginal flows. Real system experiments show that Kuijia is effective in handling network faults and significantly outperforms the conventional rescaling method. Y. Shi et al. propose CHAOS, an SDN-based moving target defense system. A Chaos Tower Obfuscation (CTO) method is proposed to depict the hierarchy of all the hosts in an intranet and define expected connections and unexpected connections. Moreover, they develop fast CTO algorithms to achieve a different degree of obfuscation for the hosts in each layer. The proposed approach makes it very easy to realize moving target defense in networks.

*Zhiping Cai
Chengchen Hu
Kai Zheng
Yang Xu
Qiang Fu*