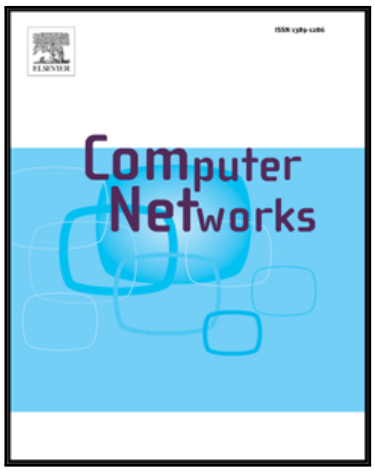

Security and Performance of Software-defined Networks and Functions Virtualization

David Hausheer , Oliver Hohlfeld , Stefan Schmid , Guofei Gu

PII: S1389-1286(18)30145-2
DOI: 10.1016/j.comnet.2018.03.025
Reference: COMPNW 6452

To appear in: *Computer Networks*

Please cite this article as: David Hausheer , Oliver Hohlfeld , Stefan Schmid , Guofei Gu , Security and Performance of Software-defined Networks and Functions Virtualization, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.03.025

Security and Performance of Software-defined Networks and Functions Virtualization

Software-Defined Networking (SDN) and Network Function Virtualization (NFV) are envisioned to drastically change network operations and management by introducing unprecedented flexibility. SDN outsources and consolidates the control of data plane elements and introduces open interfaces between these layers, while NFV abstracts network functions from dedicated hardware to virtual machines running on commodity hardware. Together, the SDN and NFV paradigms enable a simpler, more efficient, and cheaper network operation and management.

However, softwarization also introduces new challenges, especially in terms of performance and security. For example, the composition of functions in complex software stacks that can run on arbitrary platforms instead of vendor-provided, dedicated hardware introduces major performance challenges. Moreover, e.g., the outsourcing of network control or the relocation of network functions to cloud services creates new challenges on data privacy and network security.

These two central challenges of softwareized networks are the topic of this special issue of the Computer Networks' Journal Special Issue on "Security and Performance of Software-defined Networks and Functions Virtualization". It provides an overview on original, high-quality papers that present, analyze, and discuss new solutions related to these challenges.

On one hand, security aspects include mechanisms that improve the security and privacy in SDN/NFV, e.g., solutions that enable the validation, verification and certification of network functions. On the other hand, the SDN and NFV paradigms enable in turn new ways to implement security mechanisms, e.g. the mitigation of DDoS attacks. At the same time, performance aspects of SDN/NFV include performance measurement and monitoring (e.g., performance benchmarking and standards) as well as mechanisms to improve the performance (e.g., mechanisms to achieve high packet processing performances in virtualized environments). Additionally, economic and management aspects related to these challenges need to be considered as well. These aspects include, e.g., the design of energy efficient NFV networks, algorithms controlling the function placement, services offerings enabled by SDN/NFV (e.g. to improve the end-user experience), or techno-economic aspects (e.g. pricing and business models).

Overall, this Special Issue had received 54 submissions, from which 8 papers were subject to early rejects or had been withdrawn. The remaining papers underwent a rigorous review process, with at least 3 reviews per paper. Based on these reviews which were discussed in detail, the guest editors finally accepted 7 papers for publication (acceptance rate 13%).

This Special Issue starts with one paper that addresses security aspects of SDN/NFV. Specifically, the paper entitled *"On Detecting Compromised Controller in Software Defined Networks"* proposes a method to detect compromised controllers through the collection of packet traces in the data plane. In particular, the authors implement and evaluate a machine learning approach, relying on different features and classifiers.

The remaining papers in this Special Issue tackle performance aspects of SDN/NFV. Starting with performance measurement and monitoring, the second paper of this issue entitled *"Detecting Heavy Flows in the SDN Match and Action Model"* describes a new approach for large flow detection in high throughput traffic streams. It can differentiate between heavy flows, elephant flows, and bulky flows. The approach proposed detects large flows with high accuracy and presents a good tradeoff between control plane traffic and the number of required flow table space. The paper additionally investigates efficient packet sampling of large flows and shows how the proposed algorithms can be adapted to a distributed monitoring that scales with the number of SDN switches.

The third paper entitled *"Methodology, Measurement and Analysis of Flow Table Update Characteristics in Hardware OpenFlow Switches"* provides a performance analysis methodology for SDN switches to help designing efficient controllers. The methodology, which has been tested in experiments with several OpenFlow hardware switches, is based on sending flow table updates to the