Editorial

Amitava Biswas*

Cisco Systems,
San Jose, 95134, CA, USA
Email: amitavabiswas@ieee.org
*Corresponding author

Chen Liu

Utopia Compression Corp.,
Los Angeles 90064, USA
Email: chenliu419@gmail.com

Inder Monga

Lawrence Berkeley National Laboratory Energy Sciences Network,
Lawrence Berkley National Lab (Livermore),
1 Cyclotron Road, Mail stop 50A-3111, Berkeley, CA 94720, USA
Email: imonga@es.net

Kashinath Basu

Department of Computer Science,
Oxford Brookes University,
Oxford, OX3 0BP, UK
Email: kbasu@brookes.ac.uk

Michael Bredel

California Institute of Technology and CERN,
CH-1211 Geneve 23, Switzerland
Email: michael.bredel@cern.ch

Biographical notes: Amitava Biswas is currently at Cisco Systems, California, USA.

Chen Liu is employed at Utopia Compression Corp., Los Angeles, USA.

Inder Monga is currently at Lawrence Berkeley National Laboratory Energy Sciences Network, Lawrence Berkley National Lab (Livermore), Berkeley, California, USA.

Kashinath Basu is a Senior Lecturer in the Department of Computing and Communication Technologies at Oxford Brookes University, UK. He has over 16 years of research experience in the field of computer networking. He has published several papers in conferences and journals and has co-authored a number of books. He is actively involved in the organising and programme committees of conferences and research publications. He is frequently invited as a guest speaker in various academic and business events. He obtained both his PhD and BS in Computer Science from the Oxford Brookes University, UK.

Michael Bredel is currently at California Institute of Technology and CERN, Geneve, Switzerland.

For last few years, there has been a tremendous growth in data traffic due to high adoption rate of mobile devices and cloud computing. Internet of things (IoT) will stimulate even further growth. This is increasing scale and complexity of telecom/internet service provider (SP) and enterprise data centre (DC) compute and network infrastructures. As a result, managing these large network-compute converged infrastructures is becoming complex and cumbersome. To cope up, network and DC operators are trying to automate network and system operations, administrations and management (OAM) functions. OAM includes all non-functional mechanisms which keep the network running.

By removing human operators from the lower levels of the management loop (e.g., using an automated system to analyse network alarms/events and take corrective action), improved operational and economic efficiencies and operational scalability is being achieved. This kind of network management automation is reducing capital and operation expenditures; this in turn is driving down cost, stimulating service demand, increasing revenues and maintaining profitability. New paradigms like software defined network (SDN), software defined infrastructure (SDI), network function virtualisation (NFV), and automation of network and system management operations is helping in achieving these business objectives. From this viewpoint, SDN and NFV can be considered as milestones in this roadmap of automated OAM for large scale infrastructures.

Centralisation of control plane in a SDN controller avoids the need to have human operators to manage large number of network devices individually. By virtue of centralisation, SDN can implement various automated network management and control plane logic. Similarly, many large internet application providers have implemented home grown non-traditional automated network and system management systems at their DCs. On the other hand, NFV approach by telecom SPs, is proposing to address some of the manageability-at-scale problems with virtual network devices running on generic hardware. This will replace large variety of specialised network device hardware, simplify and bring in operational efficiencies. For all these paradigms, the key success factors are intelligent software, its programmability to implement complex logic at low cost and scaling opportunities through elasticity at different time scales.

However, with increase in scale, complexity and increased role of software driven approaches, engineering performance becomes very important. In addition, such software centric infrastructures also become more vulnerable to cyber attacks and intrusions. This is well-known as ‘increase of attack surface’ in cyber security parlance. So this problem of cyber-security and robustness becomes as important as the core functional requirements.

Therefore, this special issue aims to show case some new ideas and research for enabling automation, performance and security of software-based network systems.

The first article – 'SmartRegion: a region-based, distributed approach to software defined networks', authored by Farrahi Moghaddam et al., proposes a region-based packet routing framework to improve network scalability in a SDN.

The second one – 'Towards an automated framework to instantiate virtual networks in OpenFlow-based infrastructures', authored by Doriguzzi-Corin et al., proposes a software framework to automate instantiation of virtual networks in OpenFlow-based physical network infrastructures.

The third one – 'An agent-based framework for production software defined networks', authored by Izard et al., proposes a software framework to ease development of an uniform SDN-based offering.

The fourth article – 'Mitigating the controller performance bottlenecks in software defined networks', authored by Caba and Soler, addresses the controller performance bottleneck challenge in SDNs, by proposing use of optimal configurations.

The fifth article – 'Analysis of an application delivery platform for software defined infrastructures', authored by Gupta et al., characterised the behaviour of an application-to-SDN interface that enables performance management in an application delivery network (a SDI). Their goal is to investigate what causes such system to behave sub-optimally.

The last article – 'Critical analysis of layer 2 network security in virtualised environments', authored by Bull and Matthews, investigates effect of MAC flooding attack on virtual switches in some commonly used hypervisors that are used in DCs.