Techniques for smart and secure 5G softwarized networks

Laurent Ciavaglia¹ · Prosper Chemouil² · Bruce Maggs³

Published online: 12 September 2019

© Institut Mines-Télécom and Springer Nature Switzerland AG 2019

The automation of 5G networks and services delivery is becoming critical. All major industries are rapidly digitizing and automating their businesses and will increasingly rely on the best of breed 5G networks empowered by cloud platforms and connectivity services supporting a similar level of business agility and flexibility. CSP (Communications Service Provider) service delivery and network management automation is thus becoming critical for handling the increase in overall complexity and scale of operations created by the transformation of 5G networks into a programmable, software-driven, service-based architecture. Going forward, unprecedented operational agility will be required to support new business opportunities enabled by technology enablers, such as network slicing. The goal is thus to have all operational processes and tasks (e.g. service creation, fulfilment, assurance, and optimization) executed automatically and enabled at the required scale and total cost of ownership.

This special issue discusses some of these important challenges, highlighting a set of selected best papers from the ICIN 2018 conference addressing a wide range of topics from cloud services, optimization, availability to 5G security frameworks, and controls.

Eight conference papers have been invited to submit an extended version of their initial work to contribute to this special issue. The review process helped to guarantee the quality of the form and the content, and ensure the scientific and technical correctness, while at the same time providing useful feedback to improve or complement the articles. Hereafter, we provide a summary of each paper in this special issue.

The first article from Tlili et al. “DAReSch: Deadline-Aware Request Scheduling for Cloud Storage Services” presents a deadline-aware data request scheduling scheme, called DAReSch, that aims at scheduling data requests in order to minimize data transfer times and to meet the deadlines specified by the users. The authors show their mechanism outperforms current reference solution (OpenStack python-swiftclient) for Swift users even with stringent deadline requirements. They envisage for their future work to investigate a negotiation-based system that finds an agreement between users and storage providers in order to assign the appropriate deadline to each request depending on the priority of the requested data.

The second article titled “Algorithms for the Design of 5G networks with VNF-based Reusable Functional Blocks” from Chiaraviglio et al. received the Best Paper Award at the ICIN 2018 conference and tackles problem of designing a 5G network composed of Virtual Network Function (VNF)-based entities, called Reusable Functional Blocks (RFBs). RFBs provide a high level of flexibility and scalability, which are recognized as core functions for the deployment of the forthcoming 5G technology. The authors formulate the problem of minimizing the total costs of a 5G network composed of RFBs and physical 5G nodes, which is a NP-Hard, and derive two algorithms, called SFDA and 5G-PCDA, to tackle it. The results provided in the article clearly show the trade-offs that emerge between (i) the total costs incurred by the installation of the 5G equipment, (ii) the percentage of users that are served, and iii) the minimum downlink traffic provided to the users.

In the third article “The Controller Placement Problem for Robust SDNs against Malicious Node Attacks considering the Control Plane with and without Split-Brain”, Santos et al. investigate the controller placement problem (CPP) to determine the number and location of the SDN controllers in order to find a CPP solution that maximizes the control plane robustness against a given number of malicious node attacks. For different malicious node attacks, based on node centrality metrics and corresponding to different attacker’s strategies, they evaluate the previous solutions to determine the ones that maximize the network robustness, considering the SDN

✉ Laurent Ciavaglia
laurent.ciavaglia@nokia.com

Prosper Chemouil
prosper.chemouil@ieee.org

¹ Nokia, Nozay, France

² IEEE ComSoc, 92320 Châtillon, France

³ Duke University, Akamai Technologies, Cambridge, MA, USA

control plane operating with or without split-brain. Their conclusions highlight that the split-brain does not always provide the best robust CPP solutions due to its feature of requiring a minimum number of connected controllers (which must be over half of the total number of them) to be operational.

In the fourth article, Behrad et al. provides “A Survey on Authentication and Access Control for Mobile Networks: from 4G to 5G”. The upcoming 5G networks are expected to support a set of multiple requirements and use cases, raising the expectations in terms of improved user experience while at the same time facing the challenge to provide high levels of security by considering a variety of security aspects, such as authentication and access control mechanisms. The current protocol in 4G designed to address security is 4G AKA. It presents some weaknesses and vulnerabilities that negatively affect operators’ networks and their subscribers’ security. In designing an authentication and access control mechanism for 5G, it is crucial to evaluate both 4G AKA’s weaknesses and the new requirements of 5G and architectural solutions brought by the 3GPP.

Alashaikh et al., in the fifth article, outlines mechanisms for the “Embedded Network Design to Support Availability Differentiation”. They describe the problem of how to provide, in a cost-efficient manner, high levels of availability and service differentiation in communication networks, along with the strategy to embed in the physical layer topology a high availability set of links and nodes termed the spine. The spine enables through protection, routing and cross layer mapping, the provisioning of differentiated classes of resilience with varying levels of end-to-end availability. Here we present an optimization model formulation of the spine design problem, considering link availability and the cost of upgrading link availability. The design problem seeks to minimize the cost while attaining a desired target flow availability. Extensive numerical results illustrate the benefits of modifying the availability of a subset of links of the network to implement quality of resilience classes.

In the sixth article which received the Best Demo Award at the ICIN 2018 conference, titled “Resource Management of Cloud-Enabled Systems using Model-free Reinforcement Learning”, Jin et al. highlight the growing challenge of controlling virtualized system behavior in complex dynamically evolving environments. The authors examine the applicability of a new management paradigm based on Reinforcement Learning approach, where no preliminary specification of the system model is required. The article concludes with the results of experimentation on a 5G network slice that hosts with cloud-based applications in a multi-agent Reinforcement Learning setting, demonstrating the value of information

exchange between learning agents, and discusses the technical challenges that need to be addressed in this emerging field.

The seventh article “Multi-cloud Cooperative Intrusion Detection System: Trust and Fairness” from Abusitta et al. investigates the vulnerability to intelligent cyber-attacks of the recent cloud computing systems due to their increased sophistication. The article builds on recent works in cloud security which have shown that a cooperation among cloud-based IDSs can enhance their accuracy. However, there are two main challenges associated with the existing cooperative IDSs, which are related to trust and fairness assurance. To tackle these challenges, the authors propose a cooperative cloud-based IDS framework that (1) enables IDSs to distributively form trustworthy IDSs communities by advancing a trust-based hedonic coalitional game, which allows IDSs to increase their individual detection accuracy in the presence of untrusted IDSs, and (2) formulates a fairness assurance mechanism as a Stackelberg game between the well-behaving IDSs and the selfish ones that frequently send consultation requests to other IDSs, and at the same time do not answer other IDSs’ consultation requests. Experimental results show the effectiveness of the proposed approach in terms of enhancing the accuracy of detection and achieving the fairness among IDSs in terms of benefits obtained through cooperation.

The article “Automotive Virtual Edge Communicator (AVEC) with Vehicular Inter-agent Service Orchestration & Resourcing (ViSOR)” from Copeland et al. is the eighth article and concludes the set of articles of this special issue. The article focuses on the scenario of critical communications, in which relief teams must have assured connectivity, not only within the team but also across different service agencies in the area. Since emergency agencies and essential services always send service cars to affected zones, advanced technologies and computing resources aboard these vehicles can be pooled together to boost network capacity temporarily, just where it is crucially needed. These vehicles become Automotive Virtual Edge Communicators (AVECs). They are managed by a Vehicular Inter-agency Service Orchestration & Resourcing (ViSOR) system that creates transient proximity-based “trust circles” to manage novel cooperative hosting, opportunistic virtualization, and “car-sourcing” of crisis zone data. This study evaluates the feasibility of this challenging but highly rewarding concept and identifies gaps in emerging technologies.

Good reading!

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.