Editorial

Stephane Maag

Department of Networks and Mobile Multimedia Services,
Institut Mines-Telecom/Telecom SudParis,
CNRS UMR 5157, Evry, France
Email: stephane.maag@telecom-sudparis.eu

Biographical notes: Stephane Maag received his PhD in Computer Science in 2002 and Habilitation à Diriger des Recherches in 2011 from the University Paris Sud XI, France. He was recruited by National Institute of Telecommunications in 2002 as an Assistant Professor, joined the CNRS UMR 5157 Samovar in 2003. Since 2013, he has been a Full Professor at Telecom SudParis. His research interests mainly focus on the testing and monitoring of communicating systems in particular IP-based networks. He leads and participates in several international collaborative research projects (ITEA3, H2020, ICT Asian, etc.). He also chaired several conferences and workshops in the domain of network testing and monitoring. He did supervise more than ten PhD thesis and 20 MSc students. He has published several papers (>60) in high ranked international conferences (INFOCOM, ICWS, ASE, etc.) and journals (*ACM Computing Surveys*, *IEEE/ACM Transaction on Networking*, etc.).

1 Introduction

The last decade has seen revolutionary evolution in telecommunications (3G/4G, LTE, etc.), mobile networks (MANETs, sensors, Wifi, etc.), internet of things, etc. While deploying, configuring, operating, securing and managing such networks is today costly and time consuming, it is expected to drastically become even more in the near future.

These networks tend to converge and to interwork within their own contexts and new interoperability standards. However, while there are many advantages in providing such hybrid networks, their management, configuration and validation need to be addressed. Although some methodologies and tools have been established in the past for this purpose in telecommunication networks, the dynamicity, heterogeneity and complexity of next-generation networks (NGN) make the monitoring and management of their components much more complex.

Low-level interfaces on a per-device basis are currently used for the management of networks. Nevertheless, in these large-scale heterogeneous mobile NGN, such interfaces become tough to reach, configure and control. Furthermore, many of the existing approaches lack controllability, scalability and testability in operational networks. Similarly, existing end-to-end monitoring applications usually depend on low-level network activity information such as MIB parameters, interface logs, traffic counters or signatures.

Therefore, a major challenge is the way of monitoring these distributed outputs to provide a global knowledge of real-time network operations and then efficiently managing these next-generation networks.

This special issue of the *IJSSC* on network management and monitoring contains new original papers as well as extended versions of the best papers from the International Workshop on Network Management and Monitoring (NetMM) hosted in Barcelona, Spain, on March 2013. This special issue is an opportunity for researchers and industry experts to present their novel and innovative methodologies, techniques, tools and real-life experiences concerning NGN management and monitoring.

2 Content of this issue

There are five papers in this special issue, all of them studying specific aspects (methodologies, tools and applications like security) of network management and monitoring.

The first paper proposed by A. Bashar presents a Bayesian networks-based admission control (BNAC) approach for implementing a call admission control solution. The core of the BNAC system is a Bayesian network (BN) decision support system for call admission control in NGN environments. BN is compared qualitatively to other machine learning approaches in the context of network management. The paper focuses on the performance evaluation of the BNAC system using packet delay, packet loss, queue size, and blocking probability to quantify performance achievable over a baseline scenario and peak operational conditions.

In the second paper, X. Che and S. Maag proposes a logic-based passive testing approach to test in a formal way the protocol performance requirements provided by protocol standards or experts in specifying time related protocol properties. They aim at checking these properties on real execution traces. Based on a new monitoring algorithm, a prototype is developed and experienced. Their proposed technique is evaluated through a set of IMS/SIP properties (tackling the conformance and performance) and execution traces.

Copyright © 2015 Inderscience Enterprises Ltd.

The authors of the third paper, F.B. Abreu et al. introduce an attack detection approach based on monitoring and rules for ensuring security constraints. The monitoring area is recent and improvements with respect to detection capabilities are interesting in that paper. The approach relies on the analysis of the protocol routing behaviour by processing the traces produced by each node which outputs routing events are correlated between nodes to detect potential intrusions. The authors perform a virtualised mesh network platform that consists of virtual nodes executing the BATMAN routing protocol in order to identify malicious routing traffic diffused by an attacker through the network.

In the fourth paper, the research area of model driven development for context-aware application development and management on service platforms is studied. S. Hammoudi et al. propose a new approach named context aware model driven development (COMODE) in order to focus on the development of context-aware applications. They define and experiment an explicit approach based on a model transformation technique to integrate context information into business logic at model level. Through separation of concerns (business and context), the authors improve the reuse, adaptability and management of system context information.

In the fifth paper, O. Rodas and M.A. To present a scalable classification-based hybrid method for intrusion prevention systems (IPS) based on a distributed monitoring methodology. The authors aim at managing the processing of all the authentication logs over different IPS in order to make decisions in real time about what can be considered as a legitimate intrusion. Various scenarios are presented and emulated with Dockemu, a cutting-edge network emulation tool they developed. The approach is experimented through brute force attacks within an attacking botnet to an SSH service which logs are correlated in a central node in real-time. Log information is correlated with a customised format, filtered and stored in MongoDB by collaborative intrusion detection systems.

Through this special issue, we illustrate diverse facets of network management and monitoring, the inherent challenges, methodologies and specifically their applications. We believe that these aspects provide new insights and ideas to researchers and developers, inspiring readers to provide new contributions in this research field.

Acknowledgements

The guest editor would like to thank Dr. Fatos Xhafa (Technical University of Catalonia, Spain), Editor-in-Chief of *IJSSC*, Dr. Ilsun You (Korean Bible University, Korea), executive editor of *IJSSC*, and Dr. Aniello Castiglione (University of Salerno, Italy), managing editor of *IJSSC*, for giving us the possibility to organise the special issue as well as their great support. The guest editor also thank the reviewers for their fruitful comments allowing here to provide high quality research papers.