INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT
Int. J. Network Mgmt 2014; **24**: 219–220
Published online 29 June 2014 in Wiley Online Library (wileyonlinelibrary.com) DOI: 10.1002/nem.1872

Editorial

Flow-based approaches in network management: recent advances and future trends

Ramin Sadre,[1,*†] Anna Sperotto,[2] Rick Hofstede[2] and Nevil Brownlee[3]

[1]Aalborg University, Aalborg, Denmark
[2]University of Twente, Enschede, The Netherlands
[3]The University of Auckland, Auckland, New Zealand

The continuous increase of line speeds and throughput in modern computer networks has considerably stimulated the usage of aggregation-based monitoring techniques for network management in the past years. Amongst those, flow-based approaches have become extremely popular among researchers and operators due to the wide availability of hardware and software flow exporters and their quasi-standardized exporting formats, such as NetFlow or IPFIX. While flow-based monitoring was originally used for simple diagnosing and accounting purposes, researchers are now proposing flow-based approaches for a wide range of application fields, such as intrusion detection, traffic classification, and resource management.

Several trends can be identified in flow-based monitoring. First of all, we observe more and more attempts to close the gap between packet-based and flow-based monitoring. As the latter was originally proposed as an efficient and scalable alternative to Deep Packet Inspection (DPI) in high-speed networks, the most recent flow exporters allow for enriching flow data with application-layer information, for example. It can be expected that this will lead to new approaches and solutions for network management problems. Second, IPFIX is evolving towards a generic protocol for exporting structured data. For example, the IPFIX Working Group has investigated the use of IPFIX for exporting SNMP Management Information Base (MIB) variables. Another example was showcased at the IETF-87 meeting, where room temperatures were exported to a central collection point using IPFIX. Since IPFIX is a push protocol, it will provide an effective way for network managers to continuously collect information from remote hosts. Finally, new environments, such as Clouds and Software Defined Networks (SDN), demand new flow-based solutions for their monitoring and management. OpenFlow, the most prominent protocol for SDN, is flow-based, highlighting the need for network managers to monitor and understand trends in flows through their networks.

Thus, the goal of this Special Issue of the *International Journal on Network Management* is to present innovative flow-based approaches and solutions for network management tasks, as well as new methods and technologies for the generation, processing and analysis of flow information. The articles in this Special Issue present research results and a survey on the usage of flow-based approaches, and on the design and implementation of high-speed monitoring devices.

A total of 22 submissions was received for this Special Issue, for which we wish to thank all authors. Three papers did not go through the full review process because they were identified early as out of scope. Each of the remaining 19 papers received at least three independent reviews. In total, 47 reviewers participated in the review process. Based on their reviews, seven papers were finally selected for publication.

*Correspondence to: Ramin Sadre, Computer Science Department, Aalborg University, Denmark.
†E-mail: rsadre@cs.aau.dk

The first paper, by Moreno *et al*., proposes and validates a flexible architecture for the monitoring of high-speed networks using off-the-shelf systems. The second paper, by Jusko *et al*., presents a unified solution to identify Peer-to-Peer (P2P) communities through the analysis of flow data. Groléat *et al*. present in the third paper the design of a real-time and flow-based traffic classifier for high-speed networks. The fourth paper, by Foremski *et al*., presents a flow-based classifier that, by inspecting DNS traffic, is able to classify a highly significant portion of network traffic. Paper number five, by Asai *et al*., proposes a network application profiling framework based on traffic causality graphs and demonstrates its accuracy for application identification. In the sixth paper, Marat Zhanikeev proposes a new and lock-free shared memory design for high-speed traffic capturing on multicore systems and studies its performance. Finally, the seventh paper, by Drăsar *et al*., surveys state-of-the-art flow-based anomaly detection methods, and proposes a new classification of detection methods and a new taxonomy of network anomalies.

The guest editors of this Special Issue wish to acknowledge the excellent work that has been performed by the reviewers, who have spent a considerable amount of their time providing high-quality reviews. We would also like to extend our thanks to the editorial board of IJNM, and in particular to James Hong and Aiko Pras for the great opportunity and their support in editing this Special Issue. Last but not least, we thank production editor Jovelyne Sotoya, Wiley, for her help.

The work on this Special Issue was partly funded by FLAMINGO, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

DOI: 10.1002/nem