



POLITECNICO DI TORINO
Repository ISTITUZIONALE

Formal assurance of security policies in automated network orchestration (SDN/NFV)

Original

Formal assurance of security policies in automated network orchestration (SDN/NFV) / Yusupov, Jalolliddin. - (2020 May 29), pp. 1-130.

Availability:

This version is available at: 11583/2850616 since: 2020-10-30T11:29:12Z

Publisher:

Politecnico di Torino

Published

DOI:

Terms of use:

Altro tipo di accesso

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

Formal assurance of security policies in automated network orchestration (SDN/NFV)

Jaloliddin Yusupov

Nowadays, networks are evolving rapidly, and the need for more dynamic and automated network management is taking a significant role in defining the direction of this evolution. The new paradigms that are drastically changing the rules of the game are Software Defined Networking (SDN) and Network Function Virtualization (NFV). Despite the undeniable great benefits like scalability and flexibility they bring, these technologies also pose new issues regarding misconfigurations and security flaws since they rely upon external input to compose service graphs, to configure the virtual network functions (VNFs) and in order to enforce policies.

In this regard, traditional formal techniques have been proven to be a reliable means for verification, i.e. to discover such issues. However, the use of these techniques requires familiarity with mathematical foundations, where extensive training and expertise are required from network engineers to apply such methods. Other issues that have to be considered in virtualized networks are the need to use resources efficiently and the need to have automated procedures that let the administrators keep the pace with such rapidly evolving systems. The problem of efficiently placing the network functions across data centers can be solved by means of combinatorial approaches, but such approaches lack the formal verification part. In fact, in the literature, these two classes of problems have traditionally been addressed separately. A thorough search of the relevant literature yielded that reliable delivery of network services with a formal assurance about the network safety and security properties, providing at the same time efficient allocation of the resources and good automation, remains an open problem of greatest importance to be tackled in future research.

In this dissertation, we present our contributions to this field of research, which includes our proposed modeling framework and optimized verification and refinement technique. In particular, the modeling framework allows users to automatically extract formal specifications from the source of network function applications, which is then converted into the compatible input format of different formal network analysis tools. In this way, we contribute to overcome the lack of familiarity with the formal notations. We utilize these formal models to formulate the joint virtual network placement and formal verification problem as a maximum satisfiability modulo theory problem (MaxSMT). Using this formulation, we target various instances of the problem in the cloud, 5G RAN, and industrial networks. In addition to the objectives discussed by the existing approaches, our model is able to encode more expressive constraints including the modeling of the forwarding behavior of the network functions, configuration parameters, and security policies. This approach, being formal, provides high confidence that the intended network security policies are correctly enforced.