ShadeNF: A Platform for Online Network Function Verification

Yu Sun
Binghamton University
ysun59@binghamton.edu

Hui Lu
Binghamton University
huilu@binghamton.edu

Abhinav Srivastava
Frame.io
abhinav@frame.io

Cong Xu
IBM Research Austin
xucong@us.ibm.com

ABSTRACT

The correct implementation of network policies (e.g., routing, NAT, VPNs, load balancing, and IDS/IPS) for underlying network functions is *critical*, as it determines the security, availability and performance of a production network. However, it is notoriously known that making sure network policies are correctly implemented is challenging, even for basic reachability policies. This becomes more challenging in cloud environments featured with SDN-enabled NFV, where multiple tenants are hosted with *richer* in-network services in the form of chained, virtualized network functions with dynamic, customized network policies.

To address this problem, existing approaches have been proposed to model network behaviors, generate synthetic network traffic, and verify intended network policies. However, these solutions face a fundamental challenge in SDN-enabled NFV — lack of capturing *dynamics* of the production system. For example, virtual network functions (running in virtual machines) can be arbitrarily composed to realize service chaining on the fly; the chained network functions create more complex unpredictable network policies. Further, the on-demand cloud service model compounds this complexity with dynamic loads and varying network function requirements.

One (seemingly straightforward) solution may be to extend existing network models to capture dynamic system behaviors, and thus generate test traffic with broader coverage. However, despite the possibility of doing so, such model-based approaches will easily result in *state-space explosion*, which will take extensive time for completing a simple network verification task even for a small network. On the other hand, focusing on a subset of "intended" polices may reduce the state space, but could fail to catch some critical sources of violations in practice — in most cases, it is even hard (or impossible) to know the intended polices without really operating network functions in a production environment (e.g., with improvised changes in NFV configurations/policies).

Ideally, conducting network verification in a *live* production environment — complementary to model-based verification approaches — is attractive, as production traffic captures the most *exact, realistic* dynamic state of the system that model-based verification tools cannot provide. However, doing so brings potential risks of impacting or even damaging a live production environment, as mis-configured "inline" test network functions could wrongly manipulate network traffic — numerous network outrages are actually caused by (tiny) mis-configurations of a live production system. It becomes more problematic in multi-tenant cloud, as such misbehaviors could impact other tenants.

In this paper, we present **ShadeNF**, a novel online verification platform for testing in-cloud network functions in a *production-like* environment, without disrupting the live production system. ShadeNF enables such a production-like test environment (i.e., the shadow system) with an exact clone of the production network functions (to be tested), which captures the dynamic state and vulnerabilities of the live production system. Further, ShadeNF delicately steers live production traffic to the shadow system as the test traffic, which captures the dynamic state of the production workloads. The actual verification is operated in a completely isolated environment with desired resources (e.g., CPU, memory and storage), thus not interfering with the production system.

We make three key contributions in ShadeNF: First, ShadeNF introduces a new *live, consistent* snapshot approach to clone chained, dependent network functions by leveraging programmable SDN virtual switches. This approach both preserves a consistent snapshot and reduces performance overhead with *no* modifications to VMs software and legacy network flows. Second, to capture the dynamics of the production workloads, ShadeNF creates a new traffic forwarding plane, which selectively, unidirectionally steers the production traffic to the test system with new "programmable forwarding pipes". These forwarding pipes also enable the *auto-chaining* of arbitrary network functions. Last, to explore broader test coverage, ShadeNF advances existing model-based approaches by taking patterns of real production traffic into consideration — ShadeNF populates synthetic test traffic with realistic traffic patterns that are captured and provided automatically.

We have implemented a ShadeNF platform prototype upon OpenStack. Our evaluation in a real cloud testbed shows that: (1) ShadeNF captures the dynamics of a production system without affecting the production system; (2) ShadeNF can effectively detect a variety of policy violations.

CCS CONCEPTS

• **Networks**; • **Network services** → Network monitoring; Cloud computing; Programmable networks;

KEYWORDS

Network function virtualization, Software-defined networking, Cloud computing, Network verification

SoCC '18, October 11–13, 2018, Carlsbad, PA, USA
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-6011-1/18/10…$15.00
https://doi.org/10.1145/3267809.3275467