A Framework for SFC Integrity in NFV Environments

Lucas Bondan[1 2], Tim Wauters[2], Bruno Volckaert[2], Filip De Turck[2], and Lisandro Zambenedetti Granville[1]

[1] Institute of Informatics (INF) – Federal University of Rio Grando do Sul – Brazil
[2] Department of Information Technology (INTEC) – Ghent University – Belgium
Email: {lbondan, granville}@inf.ufrgs.br, {tim.wauters, bruno.volckaert, filip.deturck}@intec.ugent.be

Abstract. Industry and academia have increased the deployment of Network Functions Virtualization (NFV) on their environments, either for reducing expenditures or taking advantage of NFV flexibility for service provisioning. In NFV, Service Function Chainings (SFC) composed of Virtualized Network Functions (VNF) are defined to deliver services to different customers. Despite the advancements in SFC composition for service provisioning, there is still a lack of proposals for ensuring the integrity of NFV service delivery, *i.e.,* detecting anomalies in SFC operation. Such anomalies could indicate a series of different threats, such as DDoS attacks, information leakage, and unauthorized access. In this PhD, we propose a framework composed of an SFC Integrity Module (SIM) for the standard NFV architecture, providing the integration of anomaly detection mechanisms to NFV orchestrators. We present recent results of this PhD regarding the implementation of an entropy-based anomaly detection mechanism using the SIM framework. The results presented in this paper are based on the execution of the proposed mechanism using a realistic SFC data set.

Keywords: Service Function Chaining, Network Functions Virtualization, Anomaly Detection

1 Introduction

Network Functions Virtualization (NFV) was proposed to deal with the virtualization of network functions usually performed by dedicated hardware devices (*e.g.,* firewalls, session border controllers, load balancers) [1]. In NFV, Virtual Network Functions (VNF) are connected to each other, composing Service Function Chainings (SFC) for service delivery. Any anomaly in SFC operation, such as missing elements, misconfiguration, and redirection, could lead to the interruption of the service delivery and, in some cases, could indicate attacks to the network. For this reason, in this PhD, we propose an additional SFC Integrity Module (SIM) to the NFV architecture [2]. SIM is a framework that allows the implementation of different anomaly detection mechanisms and the integration

of such mechanisms into any NFV network under the control of NFV Orchestrators (NFVO). In this PhD, our focus resides in: (*i*) the applicability of existent and new anomaly detection mechanisms for SFC integrity in NFV environments, (*ii*) how to integrate such mechanisms to the NFV Management and Orchestration (MANO) architecture [3], and (*iii*) the evaluation of anomaly detection solutions in realistic NFV scenarios using the proposed SIM framework.

1.1 Motivation

In virtualized environments, vulnerabilities and exploits can lead to different SFC threats, since virtualization elements of NFV environments are susceptible to exploits. Examples of exploitable elements are container engines [4], hypervisors [5], and virtual machines [6]. Therefore, solutions have been proposed to detect anomalies in different NFV elements, such as VNFs [7], NFV services [8], and SLA violations [9]. However, there is still a lack of proposals dealing with security and integrity issues in the context of SFC [10]. In this PhD, we consider both the lack of solutions for SFC integrity and the potential vulnerabilities of NFV environments as research opportunities to be properly explored. To do so, we first investigated and proposed a framework that allows the implementation of anomaly detection techniques based on the NFV MANO information model.

2 SFC Integrity Framework

The NFV MANO architecture does not consider security-related tasks to protect functions and services. In this PhD research, we seek to guarantee the integrity of SFC operation for service delivery. Our proposal is designed to operate in NFV networks ruled by NFVOs according to the standard NFV MANO architecture.

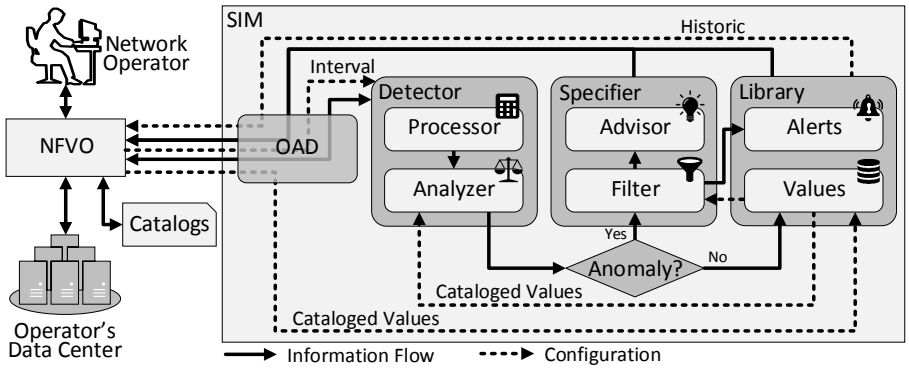


Fig. 1. Detailed SIM architecture [2] – The SIM communicates directly with NFVOs, using standard northbound APIs for requesting information regarding NFV elements operation and also to forward the results of the anomaly detection analysis.

2.1 Proposed Approach

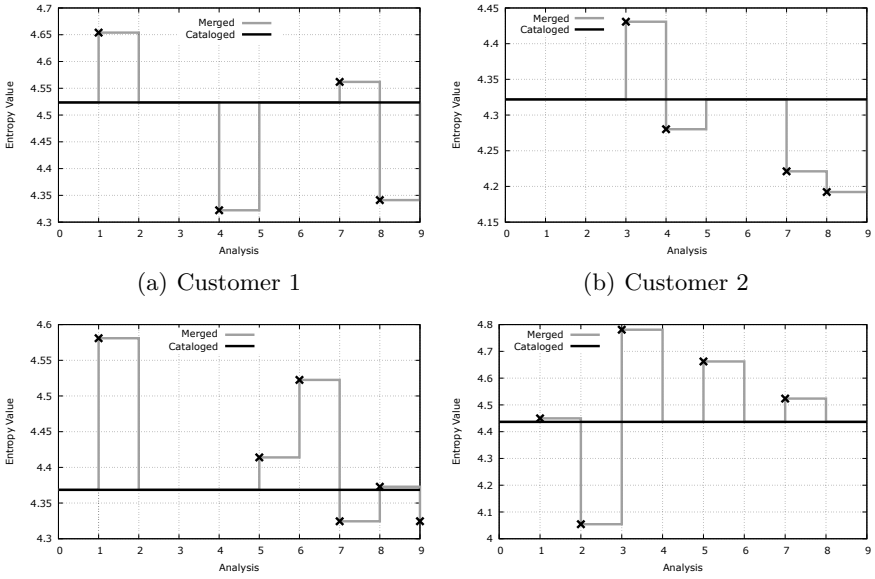
The NFVO sends cataloged and monitored information to an Orchestrator Abstraction Driver (OAD), depicted in Fig. 1 along with all SIM internal components. The information is then processed and analyzed according to the anomaly detection mechanisms implemented in the Detector component. If no anomalies are detected, the results are stored in the Library for further access. Otherwise, the results are filtered using the Filter module to specify the sources of such anomalies. Once identified, SIM stores it in the Library and forwards a report message to NFVO with the filtered results and suggestions from the Advisor module for overcoming such anomalies, *e.g.,* turn off unregistered VNFs.

2.2 Methodology

SIM was designed with specific elements for processing, analyzing, and filtering, enabling the design and implementation of different anomaly detection mechanisms. In this paper, we advance our first investigation using entropy-based anomaly detection [2] in two ways: (*i*) evaluating our solution using realistic NFV data sets [11] and (*ii*) improving the entropy-based anomaly detection mechanism to work with the current data set. These improvements enabled us to analyze each customer individually, increasing the accuracy of the anomaly detection mechanism. The data set was generated based on realistic information regarding the number of network functions composing SFCs on lager scale enterprise networks (with around 100 VNFs) [11]: 2 to 7 VNFs per SFC, mostly 2 to 5 [12]. So the number of VNFs for a given customer follows a truncated power-low distribution with exponent 2, minimum 2 and maximum 7. Following enterprise reports, anomalies were injected in the data set with a likelihood of 60% [13]. We considered three anomaly types: (*i*) unregistered SFCs, (*ii*) missing SFCs, and (*iii*) unauthorized changes in the SFC, such as additional or missing VNFs.

2.3 Results Obtained

Fig. 2 shows the entropy results of the anomaly detection mechanism considering 4 customers with different sets of SFCs. The detector creates a merged list with cataloged and monitored information. As the number of elements with low probability increases in the list, *i.e.,* highly uncertain elements, the merged entropy changes, indicating a disorder in the monitored elements. The merged entropy varies according to the number and type of anomalies detected (represented by markers). In our experiments, anomalies of type (*i*) and (*ii*) decreased the entropy value, since they involve adding or subtracting information, while anomalies of type (*iii*) (changes in existing values) increased the entropy value. It may lead to situations where anomalies of type (*i*) and (*ii*) cancel the entropy variations caused by anomalies of type (*iii*) and vice-versa. Despite rare to occur, this problem should be properly addressed to avoid false negatives. With the two-level approach of SIM (detection and filtering) it is possible to avoid false negatives with fine-grained filters comparing monitored and cataloged information. After each analysis the entropy values go back to normal (cataloged).



(a) Customer 1 (b) Customer 2

(c) Customer 3 (d) Customer 4

Fig. 2. Entropy results per customer. When anomalies occur (represented by markers), the entropy values varies, according to the amount of anomalies and their type.

3 Conclusions and Future Work

This PhD aims to propose efficient solutions for maintaining the integrity of service delivery in NFV environments. As first step, we proposed a SIM framework that allows the implementation of different anomaly detection mechanisms to analyze the network operation. The SIM modular architecture has the ability to operate with different NFVOs, requiring only to adapt one specific block. For future research, we foresee the following topics as good directions to follow.

Detection on different information levels. SIM was designed to operate at different levels of information. In this way, we foresee the possibility to analyze information regarding real-time resource consumption by virtual machines (*e.g.,* CPU, RAM, disk) and network information (*e.g.,* SFC traffic flows, bandwidth).

Evaluation of different detection mechanisms and network scenarios. Different anomaly detection mechanisms could be more suitable for a given network scenario, according to its characteristics. Analyzing the operation of different mechanisms in different environments will lead to important insights.

Deployment on production networks. Our results are based on realistic data sets generated according to real-world observations. However, production networks may present unpredicted behaviors, such as communication problems between NVFOs and other network elements. In this way, analyzing SIM operation in production networks is another important step of this PhD.

4 Acknowledgements

This research was performed partially within the FWO project "Service-oriented management of a virtualised future internet".

References

1. Chiosi, M., et al.: Network Functions Virtualisation (NFV). White Paper 1, ETSI NFV ISG (2012) available at: https://portal.etsi.org/NFV/NFV_White_Paper.pdf.
2. Bondan, L., Wauters, T., Volckaert, B., Turck, F.D., Granville, L.Z.: Anomaly Detection Framework for SFC Integrity in NFV Environments. In: IEEE Conference on Network Softwarization (NetSoft). (jul 2017 (to appear))
3. Quittek, J., et al.: Network Functions Virtualisation (NFV) - Management and Orchestration. White paper, ETSI NFV ISG (2014)
4. Combe, T., Martin, A., Pietro, R.D.: To Docker or Not to Docker: A Security Perspective. IEEE Cloud Computing **3**(5) (Sept 2016) 54–62
5. Thongthua, A., Ngamsuriyaroj, S.: Assessment of hypervisor vulnerabilities. In: International Conference on Cloud Computing Research and Innovations (ICCCRI). (May 2016) 71–77
6. Wang, Z., Yang, R., Fu, X., Du, X., Luo, B.: A shared memory based cross-vm side channel attacks in iaas cloud. In: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). (April 2016) 181–186
7. Giotis, K., Androulidakis, G., Maglaris, B.S.: A scalable anomaly detection and mitigation architecture for legacy networks via an openflow middlebox. Security and Communication Networks **9** (Oct 2015) 1958–1970
8. Xilouris, G.K., Kourtis, M.A., Gardikis, G., Koutras, I.: Statistical-based Anomaly Detection for NFV Services. In: IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). (2016) (To appear)
9. Sauvanaud, C., Lazri, K., Kaâniche, M., Kanoun, K.: Anomaly Detection and Root Cause Localization in Virtual Network Functions. In: IEEE International Symposium on Software Reliability Engineering (ISSRE). (Oct 2016) 196–206
10. Briscoe, B., et al.: Network Functions Virtualisation (NFV) - NFV Security: Problem Statement. White paper, ETSI NFV ISG (2014)
11. Rankothge, W., Le, F., Russo, A., Lobo, J.: Data Modelling for the Evaluation of Virtualized Network Functions Resource Allocation Algorithms. Computing Research Repository (CoRR) **abs/1702.00369** (2017) Available at: http://arxiv.org/abs/1702.00369.
12. Sherry, J., Hasan, S., Scott, C., Krishnamurthy, A., Ratnasamy, S., Sekar, V.: Making Middleboxes Someone else's Problem: Network Processing As a Cloud Service. In: ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. (2012) 13–24
13. Anstee, D., Bowen, P., Chui, C., Sockrider, G.: Worldwide infrastructure security report. Technical report, Arbor Networks (2017) Available at: https://www.arbornetworks.com/insight-into-the-global-threat-landscape.