Anomaly Detection Framework for SFC Integrity in NFV Environments

Lucas Bondan[*†], Tim Wauters[†], Bruno Volckaert[†], Filip De Turck[†], Lisandro Zambenedetti Granville[*]
[*]Institute of Informatics – Federal University of Rio Grande do Sul – Brazil
[†]Department of Information Technology (INTEC) – Ghent University – Belgium
Email: {lbondan, granville}@inf.ufrgs.br, {tim.wauters, bruno.volckaert, filip.deturck}@intec.ugent.be

***Abstract*—With the increasing deployments of Network Functions Virtualization (NFV) in both industry and academia, it becomes necessary to design mechanisms for keeping the integrity of Service Function Chains (SFC) responsible for NFV services delivering. Despite the advances in the development of management and orchestration for NFV, solutions to keep SFCs resilient to well-known and zero-day threats are still much needed. In this paper, we introduce a framework for deploying anomaly detection techniques for SFC in NFV environments. Our framework consists of a set of functional blocks with well-defined functions, composing an additional SFC Integrity Module (SIM) for the standard NFV architecture. The proposed SIM enables NFV orchestrators to analyze NFV elements and perform suggested actions with the goal of keeping service integrity in the network. The results obtained through the evaluation of a Proof-of-Concept implementation show that the proposed framework is able to properly detect different types of anomalies using entropy-based detection techniques.**

***Index Terms*—network functions virtualization, service function chaining, services integrity, anomaly detection**

I. Introduction

Introduced by the European Telecommunications Standards Institute (ETSI), the concept of Network Functions Virtualization (NFV) is already a reality in computer networks [1]. NFV deals with the virtualization of network functions usually performed by dedicated hardware devices, such as load balancing, Deep Packet Inspection (DPI), and firewalling. In NFV, service provisioning is achieved by chaining Virtual Network Functions (VNF) to compose Service Function Chains (SFC). Both industry and academia are taking advantage of NFV and SFC for boosting innovation and providing flexibility in network service provisioning and management [2].

Many solutions for NFV Management and Orchestration (MANO) emerged recently, mainly focused on service life-cycle management. However, there still are many challenges in NFV MANO not properly addressed [3]. Among them, SFC integrity is extremely important for service delivery [4]. SFCs are vulnerable to many types of exploits, such as unauthorized reconfiguration of VNFs (for denial of service or unauthorized privilege for specific users), flow redirection, and duplication. Despite its importance, there currently is no focus on SFC integrity solutions for network safety and guaranteeing the proper operation of SFCs in NFV environments.

Taking into account the security of NFV deployments, ETSI created a working group focused on NFV security issues, evidencing the importance of protecting NFV environments. The literature in the area lists several vulnerabilities related to different virtualization approaches that can be exploited for malicious purposes [5] [6]. Moreover, undisclosed vulnerabilities (so-called zero days) are under constant investigation by security firms [7]. However, there is a lack of solutions for guaranteeing the integrity of SFC deployments against exploits of potential known and unknown vulnerabilities. Malicious users take advantage of network operators' assumption that following network security best practices will keep their environment protected against malicious behaviors.

978-1-5090-6008-5/17/$31.00 © 2017 IEEE

In this paper, we propose an anomaly detection framework for SFC deployments in operators' data centers, using SFC models based on ETSI NFV MANO network service catalogs [8]. Our solution interacts with NFV Orchestrators (NFVO) to provide reactive resiliency executing operations like stopping anomalous VNFs, deploying new valid VNFs, stopping anomalous redirected traffic, and detecting re-chained SFCs. Moreover, the proposed solution is based on two views: (*i*) a general SFC view, which results from monitoring the entire SFC operation and the interactions among its elements (*e.g.,* connection points, member VNFs, virtual links); and (*ii*) a VNF view, which is computed from analyzing local information regarding VNFs operation (*e.g.,* connection points, dependencies, localization).

We consider an operator network scenario as presented by the ETSI NFV security group, where the same organization that operates the VNFs deploys and controls the resources. As main contributions of our work, we highlight: (*i*) an SFC anomaly detection solution, (*ii*) the proposal of an *SFC Integrity Module* (SIM) for the NFV MANO architecture, and (*iii*) an information model based on the NFV MANO network service register. Results obtained based on a Proof-of-Concept (PoC) implementation show that the proposed framework is able to properly detect different types of anomalies using entropy-based detection techniques.

The remainder of this paper is organized as follows. In Section II, we provide the background, related work, and motivation for this work. In Section III, we present the proposed SIM framework in detail. In Section IV, we detail the design of the SIM PoC developed to validate the proposed framework. The evaluation performed to validate the SIM framework is presented and discussed in Section V. Finally, our conclusions and perspectives for future work are discussed in Section VI.

II. Background and Related Work

The ETSI NFV Industry Specification Group was established aiming at a consensus for interoperability and management of Virtualized Network Functions (VNFs), creating the concept of NFV [1]. As the NFV concept evolved, it became an enabler for flexible service deployment, delivery, and management [2]. Essentially, NFV decouples network functions from dedicated hardware to run as software in commercial-of-the-shelf (COTS) servers as VNFs.

The NFV architecture presents a Management and Orchestration (MANO) plane designed to handle operations related to services and functions life-cycle management, a well as resource sharing [8]. The central element in NFV MANO is the NFVO, responsible for deploying and monitoring functions and services. In NFV, service delivery is provided by connecting VNFs through SFCs (or VNF Forwarding Graphs – VNFFG – according to ETSI's nomenclature), enabling automated provisioning of network services with different characteristics. Taking into account the importance of SFC for service delivery, the Internet Engineering Task Force (IETF) created a working group focused on defining an architecture for SFC operation [9].

Despite all its benefits, NFV has challenges to be overcome, from small NFV deployments [10] to performance issues [11], but especially MANO-related issues [3]. The CloudNFV project [12] provides an architecture for deploying and managing VNFs in a cloud environment using open standards. TeNOR [13] is an NFVO designed for supporting NFV as a Service (NFVaaS), focusing on automated deployment and configuration of services and resource sharing optimization for VNF hosting. In the same way, Maestro [14] is the first NFVO that considers the internal composition of VNFs for selecting their best deployment setup on wireless networks.

Despite NFV MANO solutions properly address the challenges they aim for, there are still a lack of proposals for dealing with security and integrity of NFV deployments, especially in the context of SFC [4]. Lee and Shen [15] proposed a path self-recovery scheme for SFCs, without taking into account anomalies on the SFC elements. Examples of exploitable elements are container engines [5], hypervisors [6], and Virtual Machines (VM) [16].

In NFV environments, vulnerabilities and exploits can lead to different types of malicious behavior for compromising the integrity of SFC operation. Examples of such malicious behavior are information redirection and duplication, Denial of Service (DoS), and unauthorized privileges for specific users. However, there is still a lack of proposals for guaranteeing SFC integrity in NFV scenarios. In this paper, we propose an anomaly detection framework, detailed in the next section. To the best of our knowledge, the SIM framework proposed in this paper is the first SFC integrity approach for NFV.

III. SFC Anomaly Detection Framework

The framework proposed in this paper is based on the addition of a new module called SIM in the NFV MANO architecture, as depicted in Figure 1. The SIM communicates directly with the NFVO, using standard northbound APIs of the NFVO to request information regarding NFV elements operation and to forward the results of the anomaly detection.

Operations and Business Support Systems (OSS/BSS) are responsible for enforcing access control rules in data centers shared with different network operators. NFVO is the NFV element responsible for bringing intelligence to service provisioning and composition processes, directly interacting with VNF Managers (VNFM) for managing the VNF operation life-cycle. In the same way, the resource sharing orchestration among different virtualized elements is performed by the NFVO through the Virtual Infrastructure Managers (VIM).

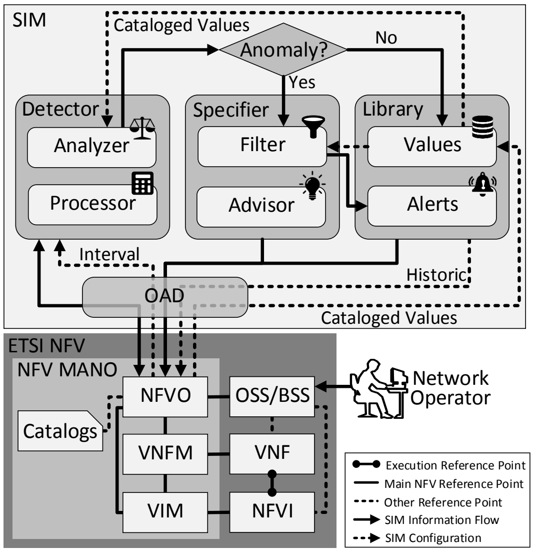


Figure 1. SIM architecture and its internal components

We designed SIM detached from NFVO to make it independent of the NFVO implementation. Therefore, any NFVO should be able to communicate and operate with SIM using standard northbound APIs. Moreover, SIM is a modular framework, providing flexibility for implementing different anomaly detection techniques. SIM can be directly configured by network operators. However, the most suitable approach is controlling and configuring SIM through NFVO, taking advantage of management interfaces already provided by NFVO.

As depicted in Figure 1, network operators configure services through OSS/BSS and NFVO, as well as SFCs and VNFs responsible for delivering network operators services. According to the NFV architecture, the NFVO must deal with all responsibilities regarding services' life-cycle management [8]. To do so, NFVO manages services, SFCs, and VNFs available through a catalog with information regarding their operation. For deploying a new VNF, the network operator should first catalog it. Once deployed, VNFs operation should be monitored and registered by NFVO. SIM is composed of four functional components, described in detail as follows.

Orchestrator Abstraction Driver (OAD): Responsible for handling all communication between NFVO and SIM. Since SIM was designed to operate with any NFVO, SIM should be able to adapt its communication to fit their northbound APIs. OAD hosts the communication functions of the NFVO being used. To change the NFVO or communicate with multiple NFVOs, only the OAD component needs to be modified, avoiding changes and bringing flexibility to SIM operation.

Detector: Requests and receives information regarding SFCs and VNFs operation to/from NFVO, as well as performs the anomaly detection technique implemented. This component can be configured in two different ways: oriented (*i*) by *events*, where SIM requests and analyzes SFCs and VNFs information only when a new event related to these elements is signalized by NFVO; and (*ii*) by *polling*, in which SIM periodically looks for anomalies based on a predefined time interval. The Detector component is composed of two modules. The first one is the *Processor* module, responsible for processing the information acquired from NFVO and formatting it for the anomaly detection techniques. The second module is called *Analyzer* and it uses the processed information to identify potential anomalies based on cataloged values. If an anomaly is detected, results are forwarded to the Specifier component. Otherwise, the Library component stores the results and the NFVO is notified about the absence of anomalies.

Specifier: Identifies the anomalous elements and selects the most appropriate action to be taken. The main reason for separating the anomaly detection from its specification is to save time and computational resources. To do so, a *Filter* module is defined for filtering the anomalies from the list of monitored elements. After identifying the anomalous elements, the *Advisor* module evaluates which is the most appropriated action to be taken to overcome the anomalies and sends an alert message to the NFVO. The suggestion can be based on both predefined sets of actions and learning mechanisms, depending on the implementation of the Advisor module. After selecting the action, the Specifier component sends a notification containing the information regarding the anomalous elements to the Library. The final choice of whether the apply or not the suggested actions and possible impacts of such actions lies with the NFVO.

Library: Stores the anomaly detection technique results and forwards them to the NFVO when queried. The *Alerts* module handles information regarding alerts generated by the Specifier, which can also be used by the network operator to generate reports regarding the historical occurrence of anomalies in the data center. In the same way, the *Values* module handles the results of analyses that did not detect any anomaly. These values can be used as the baseline for further analyses depending on the anomaly detection technique implemented in the Detector component, or they can be re-evaluated when new anomaly detection techniques are implemented, enabling the detection of previously undetected anomalies [17].

IV. Anomaly Detection Mechanism

In this section, we provide the details related to the design of a SIM Proof-of-Concept (PoC), developed to evaluate the proposed framework. In Subsection IV-A, we present the anomaly detection technique implemented to validate SIM operation. Then, in Subsection IV-B, we present and discuss the information regarding NFV elements under analysis.

A. Anomaly Detection Technique

The choice for a specific anomaly detection technique depends on the network scenarios and monitored information. [17]. Techniques that require supervised training or statistical modeling regarding network operation may not be suitable for NFV scenarios due to their dynamic behavior. However, information theory-based techniques do not require training data sets or statistical models to operate, as required by classification and statistic-based techniques. Moreover, information theory-based techniques are less complex than spectral theory-based techniques, which usually demand high processing capabilities to run in acceptable time.

Based on information theory techniques, we implemented a Shannon's Information Entropy anomaly detection technique into the Detector component. The decision for using Shannon's entropy is based on the type of information monitored and the proven effectiveness of using entropy for detecting anomalies on network environments [18]. Disorders in the data set of monitored elements handled by NFVO indicate anomalies in the operation of NFV elements. The computational cost of calculating the entropy is smaller than comparing element by element (diff). Only if the entropy changes, the filtering process will be started to identify where the anomaly occurs. The two-level approach of SIM (detection and filtering) also improves the accuracy and avoids false negatives alarms, two known issues of entropy-based detection mechanism [19].

B. Monitored Information

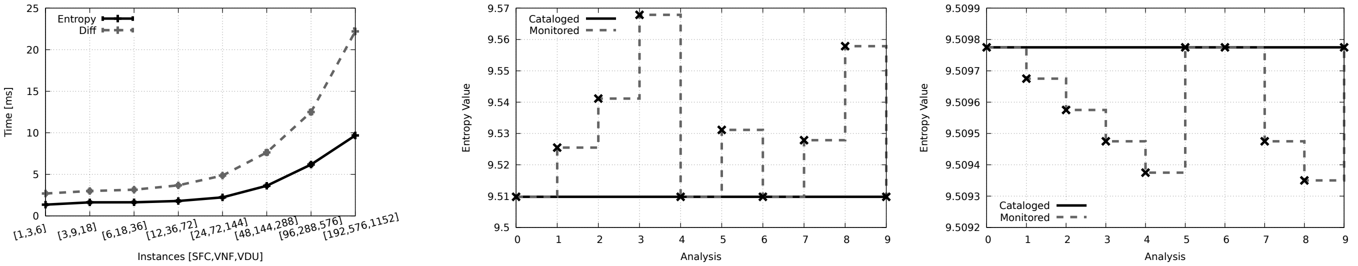
After defining the types of anomalies to be detected and the anomaly detection technique, the final step is selecting which information will be monitored and analyzed. The information monitored determines which types of anomalies and possible threats the system will be able to detect. We based the PoC design on the information model proposed by ETSI NFV MANO [8]. This information model provides a hierarchical structure for NFV elements, composing a tree for cataloging information regarding the operation of SFCs, VNFs, Virtual Deployment Units (VDU – VNFs' execution elements, like virtual machines or containers), among others. For the PoC implementation, we selected the information regarding (*i*) SFC operation (identifier, connection points, virtual links, and member VNFs); and (*ii*) VNF operation (identifier, connection points, virtual links, member VDUs, localization, and VDU dependencies). Although VDU-specific information, such as resource consumption, is not handled in this paper, it can be easily achieved using SIM framework by adding a new third view in the SFC operation to handle VDU information.

V. SIM Framework Validation

In this section, we present the evaluation of SIM based on the definitions presented in the previous section. First, we present and discuss the results obtained through an experimental evaluation of the PoC in Subsection V-A. Then, in Subsection V-B, we analyze the trace of anomalies detected and the actions suggested by SIM PoC.

A. Entropy Result Analysis

Our first evaluation is regarding the time spent by the anomaly detection technique in analyzing the data set. We compared the time expended for calculating the entropy with the time needed for directly comparing cataloged information stored in NFVO catalogs with monitored information obtained from the running NFV elements by NFVO (Diff). We varied the number of instantiated elements, from 1 SFC to 384, each one composed of 3 VNFs and up to 3 VDUs. The results are depicted in Figure 2(a). All experiments have been repeated until we achieved a confidence level of 99%.



(a) Execution time comparison

(b) Anomalous elements detected

(c) Missing elements detected

Figure 2. Evaluation results: Execution time comparison of entropy-based anomaly detection vs extracting differences (Diff) (a); and comparison of entropy value changes when detecting anomalous (b) and missing (c) elements

The entropy-based technique was faster than extracting the difference between monitored and cataloged information for all number of instances (deployed elements) evaluated. As we can observe in Figure 2(a), although both execution times are close to each other for small deployments (*e.g.,* above 6 SFCs, 18 VNFs, 36 VDUS), as the number of instances increases, the entropy presents a less accentuated growth. For this reason, entropy is considered a light-weight anomaly detection technique, suitable for performing the first evaluation of the monitored information for detecting anomalies. When the entropy indicates an anomaly, more complex mechanisms for filtering such anomalies can be applied. This configuration fits in the SIM framework, where the entropy-based technique was implemented in the Detector component, allowing us to implement more sophisticated filters in the Filter module. The advantage of this approach is executing sophisticated heavy-weight algorithms (*e.g.,* Diff) only when an anomaly is detected by the entropy analysis, saving time and computational resources when no anomalies are detected. The drawback, however, is that when anomalies are detected by the entropy analysis, the filtering process should be performed after the entropy calculation, increasing the total execution time.

The second experiment is related to the effectiveness of using entropy for detecting anomalies. For this experiment, we randomized the occurrence of anomalous events in the data set to analyze the changes in the entropy value. The data set is composed of information regarding 150 SFCs, each one composed of 3 VNFs, totaling 450 VNFs. We defined a probability of 60% of occurrence for each anomaly, each one being able to occur up to 5 times in each analysis. Considering that every disorder in the monitored information characterizes an anomaly, the anomalies detected represent 100% of the anomalies inserted in the data set. We measured the overall entropy of the monitored information with randomized anomalies and compared with the unchanged cataloged entropy value. In Figure 2(b), we show the changes in the entropy value when anomalous elements are detected in the data set, while Figure 2(c) shows the entropy when some information of the monitored elements is missing.

As can be observed in Figure 2, the entropy value changes significantly more when anomalous elements are present (Figure 2(b)) than when cataloged elements are missing on the monitored data set (Figure 2(c)). It highlights the difference in the magnitude order of the changes in the entropy value when anomalous and missing elements are detected in the data set and is directly related to the amount of information cataloged in the NFVO. This behavior is especially interesting for our scenario for two main reasons. First, it is impossible for anomalous and missing elements to *cancel* or hide each other in the final entropy value. Second, it is usually worse when an intruder element is found in the network than when there is a missing one. An intruder element (non-cataloged) may indicate a higher threat, such as information leakage, while a missing one usually indicates a DoS. By analyzing these differences, more sophisticated actions could be suggested to NFVO when more dangerous behavior is detected.

B. Anomaly Detection Analysis

For this evaluation, we recorded the anomalies and the actions suggested by SIM to NFVO during the anomaly detection analysis. The recorded values of the tracking can be observed in Tables I and II for uncataloged and missing elements detection, respectively. Tracking these data sets allow us to verify what anomalies were detected, as well as the actions suggested by the SIM PoC Advisor module to NFVO.

When no anomalies occur, SIM sends a standard report to NFVO without any suggested action, as occurs in analyses $0, 4, 6,$ and 9 of Table I, and on $0, 5, 6,$ and 9 of Table II. With regard to the anomalies summarized in Table I, when an anomalous VNF is detected (analyses $1, 2, 3, 5,$ and 8), SIM sends the results of the anomaly detection and suggests NFVO to shutdown the anomalous VNFs. An uncataloged VNF in the middle of an SFC may indicate several threats, such as DoS attacks, flow duplication for obtaining private information, and unauthorized access to services. In the same way, uncataloged virtual links (analyses 5 and 7) and connection points (analyses 7 and 8) may also indicate flow duplication and unauthorized access, as well as unauthorized privilege for users accessing services means of by a side connection.

In the case where missing VNF are detected (all anomalies presented in Table II), the immediate standard action is to re-instantiate the missing VNF to avoid interruption in delivering the services composed of the missing VNF. For missing connection points (analyses $2, 3, 4, 7,$ and 8) and missing virtual links (analysis 4), the suggested action is restarting the connections lost and re-chaining the virtual link, respectively. The most common threat characterized by missing elements is a DoS attack, where one or more SFC elements are turned off or reconfigured for overthrowing service delivery.

Table I
ANOMALOUS ELEMENTS TRACE AND SUGGESTED ACTIONS

Analysis	Anomalies	Possible Threat	Suggested Action
0, 4, 6, 9	None	–	None
1, 2, 3	Uncataloged VNFs (1, 2, 4)	DoS, flow duplication, unauthorized access	Shutdown VNFs
5	Uncataloged virtual link (1) and VNF (1)	DoS, flow duplication, unauthorized access, unauthorized privilege	Remove & trace virtual link, shutdown VNF
7	Uncataloged virtual link (1) and connection point (1)	Flow duplication, unauthorized access, unauthorized privilege	Remove & trace virtual link, remove connection point
8	Uncataloged connection point (1) and VNF (2)	DoS, flow duplication, unauthorized access, unauthorized privilege	Remove connection point, shutdown VNF

Table II
MISSING ELEMENTS TRACE AND SUGGESTED ACTIONS

Analysis	Anomalies	Possible Threat	Suggested Action
0, 5, 6, 9	None	–	None
1	Missing VNF (1)	DoS	Re-instantiate VNF
2, 3, 7, 8	Missing VNFs (1, 2, 2, 2) and connection point (1, 1, 1, 2)	DoS	Re-instantiate VNFs, restart connections
4	Missing VNF (2), connection point (1), and virtual link (1)	DoS	Re-instantiate VNFs, restart connections, re-chain

The Advisor module implemented was configured with a predefined set of standard suggested actions, according to the type of anomaly detected. However, smarter mechanisms may be implemented in the Advisor for suggesting more precise actions to NFVO. For example, machine learning techniques can be implemented to learn over time what is the best action to be executed based on the history of anomalies detected. Complementarily, fine-grained conclusions can be obtained, such as uncovering the origins of a DoS attack by analyzing the missing elements and the last access to these elements.

VI. Final Remarks and Future Work

In this paper, we presented the SIM framework capable of monitoring and maintaining SFC integrity in NFV environments. SIM was designed to be easily adaptable to operate with different NFVOs, and its modular architecture enables the implementation of different anomaly detection and filtering techniques. The choice of such techniques should fulfill network operators' needs for their NFV environment and the information available in such an environment. We implemented an entropy-based anomaly detection technique based on Shannon's entropy to validate SIM operation. The results obtained confirm the entropy-based technique as a suitable solution for detecting anomalies using some elements of the information model proposed by the ETSI NFV MANO group. As future work, we consider extending the SIM views to include VDU information, such as resource consumption. In addition, more advanced anomaly detection techniques can be implemented and evaluated, as well as different filtering mechanisms, according to the network scenario and threats to be detected.

VII. Acknowledgements

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

References

[1] M. Chiosi *et al.*, "Network Functions Virtualisation (NFV)," ETSI NFV ISG, White Paper 1, 2012, available at: https://portal.etsi.org/NFV/NFV_White_Paper.pdf.

[2] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 236–262, Firstquarter 2016.

[3] R. Mijumbi, J. Serrat, J. l. Gorricho, S. Latre, M. Charalambides, and D. Lopez, "Management and orchestration challenges in network functions virtualization," *IEEE Communications Magazine*, vol. 54, no. 1, pp. 98–105, January 2016.

[4] B. Briscoe *et al.*, "Network Functions Virtualisation (NFV) - NFV Security: Problem Statement," ETSI NFV ISG, White Paper, 2014.

[5] T. Combe, A. Martin, and R. D. Pietro, "To Docker or Not to Docker: A Security Perspective," *IEEE Cloud Computing*, vol. 3, no. 5, pp. 54–62, Sept 2016.

[6] A. Thongthua and S. Ngamsuriyaroj, "Assessment of hypervisor vulnerabilities," in *International Conference on Cloud Computing Research and Innovations (ICCCRI)*, May 2016, pp. 71–77.

[7] "Zero-Day Danger: A Survey of Zero-Day Attacks and What They Say About the Traditional Security Model," FireEye, White Paper, 2015.

[8] J. Quittek *et al.*, "Network Functions Virtualisation (NFV) - Management and Orchestration," ETSI NFV ISG, White Paper, 2014.

[9] P. Quinn and U. Elzur, "Network Service Header," Internet Engineering Task Force, Internet-Draft draft-ietf-sfc-nsh-10, Sep. 2016, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-ietf-sfc-nsh-10

[10] L. Bondan, C. R. P. d. Santos, and L. Z. Granville, "Management requirements for ClickOS-based Network Function Virtualization," in *International Workshop on Management of SDN and NFV Systems (ManSDN/NFV) collocated with the International Conference on Network and Service Management (CNSM)*, Nov 2014, pp. 447–450.

[11] L. Bondan, C. R. P. dos Santos, and L. Z. Granville, "Comparing Virtualization Solutions for NFV Deployment: A Network Management Perspective," in *IEEE Symposium on Computers and Communication (ISCC)*, June 2016, pp. 669–674.

[12] J. Soares, M. Dias, J. Carapinha, B. Parreira, and S. Sargento, "Cloud4NFV: A platform for Virtual Network Functions," in *IEEE International Conference on Cloud Networking (CloudNet)*, Oct 2014, pp. 288–293.

[13] J. F. Riera, J. Batallé, J. Bonnet, M. Días, M. McGrath, G. Petralia, F. Liberati, A. Giuseppi, A. Pietrabissa, A. Ceselli, A. Petrini, M. Trubian, P. Papadimitrou, D. Dietrich, A. Ramos, J. Melián, G. Xilouris, A. Kourtis, T. Kourtis, and E. K. Markakis, "TeNOR: Steps towards an orchestration platform for multi-PoP NFV deployment," in *IEEE NetSoft Conference and Workshops*, June 2016, pp. 243–250.

[14] A. G. Dalla-Costa, L. Bondan, J. A. Wickboldt, C. B. Both, and L. Z. Granville, "Maestro: An NFV Orchestrator for Wireless Environments Aware of VNF Internal Compositions," in *IEEE International Conference on Advanced Information Networking and Applications (AINA)*, Tamkang University, Taipei, Taiwan, Mar. 2017 (to appear).

[15] S. I. Lee and M. K. Shin, "A self-recovery scheme for service function chaining," in *International Conference on Information and Communication Technology Convergence (ICTC)*, Oct 2015, pp. 108–112.

[16] Z. Wang, R. Yang, X. Fu, X. Du, and B. Luo, "A shared memory based cross-vm side channel attacks in iaas cloud," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, April 2016, pp. 181–186.

[17] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 15:1–15:58, Jul. 2009.

[18] A. S. da Silva, J. A. Wickboldt, L. Z. Granville, and A. Schaeffer-Filho, "ATLANTIC: A framework for anomaly traffic detection, classification, and mitigation in SDN," in *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, April 2016, pp. 27–35.

[19] P. Berezinski, B. Jasiul, and M. Szpyrka, "An Entropy-Based Network Anomaly Detection Method," *Entropy*, vol. 17, no. 4, pp. 2367–2408, 2015.