FraSeR: a Framework for Segment Routing in NFV Environments

Rafael Hengen Ribeiro and Burkhard Stiller

Communication Systems Group CSG, Department of Informatics IfI,
University of Zürich UZH
Binzmühlestrasse 14, CH—8050 Zürich, Switzerland
{ribeiro,stiller}@ifi.uzh.ch

Abstract. Segment Routing (SR) is a source routing protocol that allows several operations to be made by intermediate nodes employing instructions, called segments, into packet headers. However, SR is not straightforward to be implemented in current networks, since it requires modifications. This paper proposes the FraSeR framework, that integrates SR into Network Function Virtualization (NFV) environments to facilitate the deployment of high-level policies with centralized control. A use case illustrates FraSeR's ability to enforce security policies in an NFV scenario.

Keywords: Segment Routing · Security policies · hSDN · NFV· Routing

1 Introduction

Segment Routing (SR) defines a source routing protocol that allows several operations to be made at intermediate nodes by inserting instructions, called segments, into the packet header [7]. The SR mechanism allows for deviating packets from their original planned routes, complementing a traditional Interior Gateway Protocol (IGP) [7], such as Open Shortest Path First (OSPF), by adding new routing capabilities, for instance, to avoid congested paths. SR also enables proper integration and chaining of different Virtual Network Functions (VNF) in Network Function Virtualization (NFV) environments [14], facilitating to enforce policies between them. SR allows, for instance, enforcing policies by steering traffic through a set of intermediate VNF solely by putting routing information into the packet header.

Although SR is a powerful mechanism, it is not straightforward to be implemented in existing NFV environments, since it requires network functions, such as firewalls, to be modified to make them SR-aware [1]. In general, SR rules need to be manually inserted into routers that will process them, turning difficult for operators to deploy them. This complexity in SR management leads to higher manual effort and can increase operational costs. A few efforts addressed the integration of SR with a centralized controller, such as ROSE [17], which neither offers an interface for high-level policies nor can it be easily integrated with VNFs. As of today, no research was conducted to both (i) create a unified SR

environment providing centralized management to implement high-level policies for SR and at the same time (*ii*) integrating SR with existing NFV environments.

Thus, this work proposes a framework, called FraSeR, to enable operators to integrate SR applications in NFV environments using high-level directives, focusing on "enforcing security policies". Furthermore, this framework provides a management interface connected to a controller, which refines directives into SR policies and deploys them to devices in the underlying infrastructure. The management interface provides a centralized view and control of the entire system, facilitating to insertion of new rules and managing the existing ones. Moreover, FraSeR benefits from different efforts in SR-aware VNFs, such as [1], [2], [13], allowing to integrate them with with Layer 3 (L3) routers in traditional networks.

The outline of this paper is as follows: First, Section 2 introduces SR, NFV, and Software-Defined Networking (SDN) concepts and discusses related work. While Section 3 outlines the framework proposed, Section 4 details the use case by focusing on security policies. Finally, Section 5, summarizes the approach and pitches future work.

2 Background and Related Work

The source routing protocol SR introduces for the Internet Protocol (IP) packet headers a segment of intermediate forwarding nodes (e.g., routers), allowing to route packets accordingly to the segment in the packet header [7]. Therefore, SR might be used as a mechanism to deviate packets from their original routes planned, for example, avoiding congested paths. SR can be implemented in IPv4 or IPv6 networks [7]. SR for IPv4 networks relies on Multiprotocol Label Switching (MPLS) headers, while Segment Routing over IPv6 (SRv6) is based on the use of an IPv6 extension header called Segment Routing Header (SRH), as defined by RFC 8754 [6].

NFV decouples the software implementation of network functions from the underlying hardware by leveraging virtualization technologies and commercial off-the-shelf programmable hardware, such as general-purpose servers, storage, and switches [8]. NFV allows for the design and implementation of complex and composite network services by concatenating physical or virtualized components (e.g., VNF), creating a Service Function Chaining (SFC) [8]. The NFV paradigm benefits from SDN to improve the flexibility and simplicity of networks [12]. SDN brought innovation to networks by separating the data plane and control plane [12]. The control plane is logically centralized and allows operators to program the behavior of their network. In contrast, the data plane is only responsible for the forwarding behavior, executing all rules implemented in the control plane. The SDN paradigm relies on a South-Bound Interface (SBI) protocol, such as OpenFlow, to make the control plane communicate with the data plane.

Currently, alternatives to SDN, such as hybrid Software Defined Networks (hSDN) [10], are studied to integrate SDN programming capabilities with existing legacy networks, taking advantage of the SDN potential without requiring the replacement of current devices. Different architectures were proposed [10],

including the use of SBI protocols, such as the Path Computation Element Protocol (PCEP) [16], to make traditional routers communicate with a controller.

Although SDN provides flexibility, the capabilities of programmable networks are not achievable for end-users unless higher-level abstractions are provided [3]. A higher-level abstraction is achieved by using intents, which are high-level abstract declarations written by network operators to specify the desired network behavior [4]. Efforts, such as Lumi [9], were made to use intents for network management. Lumi proposed a refinement process from high-level natural language intents into the deployment of network rules.

As there are no known solutions so far, which implement an SR framework for NFV environments with centralized control and support for high-level policies, only recent efforts including SR and NFV are considered as related work. In a recent effort, [14] implements an SR data plane for IPv4 networks. Created SR paths assist the network integration of VNFs. A prototype allows to set up SR paths via PCEP to enable traffic making use of VNF chains. Although this implementation helps create SR tunnels for NFV environments, it is limited to IPv4 networks supporting MPLS. Furthermore, SRv6 was explored in [15] bringing VNF chaining to a public cloud provider as well as deploying and measuring SRv6 for VNF chain performance. Despite the use of SRv6, manual tunnels are used without a centralized controller. In addition, other approaches addressed problems related to scalability in NFV orchestration [5]. Concerning specific VNF implementations of SR, different solutions propose the design and prototyping of specific VNF to make them SR-aware. These include a SR-aware proxy [13], Firewalls [1], and Intrusion Detection Systems (IDS).

3 Overview of the Approach

FraSeR comprehends a conceptual architecture (*cf.* Figure 1) of a framework to help operators enforce high-level policies using intents in current NFV environments. The proposed approach combines (i) a management interface for operators to express very high-level intents, (ii) an underlying infrastructure combining layer 3 (L3) routers with VNFs, (iii) a lightweight controller that refines the expressed intents into SR-policies and deploys them in the corresponding devices. In addition, this architecture uses hSDN concepts, relying on standardized protocols, such as PCEP, as SBI to make routers communicate to the controller.

At the North end of the architecture, a network operator uses a management interface to specify intents that are derived into SR policies to enforce SFC. After specifying a policy, the controller refines it and embeds an SR rule into the ingress router, which inserts segments, represented by s_i, corresponding to VNF_i, into the packet header of transit packets. For instance, an operator might specify a policy to enforce all packets coming from R_1 to pass through the sequence of VNFs $<\text{VNF}_1, \text{VNF}_n>$ before proceeding to R_n. Then, the controller refines this policy and deploys an SR policy to insert segments (VNF_1, VNF_n and R_n) into the ingress router R_1 (*cf.* Figure 1).

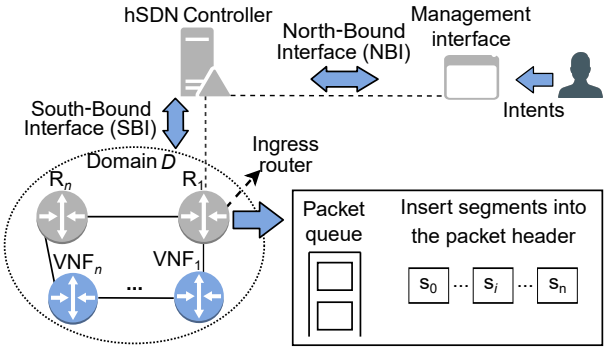

Fig. 1. Concept of an SR-based NFV Framework

The enforcement of an SFC for a packet coming from a domain D is represented by $(D) \mapsto \{\text{VNF}_1, ..., \text{VNF}_n\}$, where VNF_i represents a VNF that the packet should pass through before reaching its destination. The packet, in this case, should pass for all the VNFs in the specified sequence. Note that the operator does not need to specify the intermediate routers as the controller is aware of the topology and considers them in the path computation. In addition, the deployment of these policy enforcements should work on both IPv4 (SR/MPLS) and IPv6 (IPv6 SRH) networks, and the framework will provide a base for both implementations.

4 Use Case: SRv6 for Security Policy Enforcement

As NFV environments in general comprise heterogeneous functions with different levels of security and trust, it is essential to ensure confidentiality and integrity according to different types of traffic. That can be achieved by enforcing security policies in these environments by employing security labels [11].

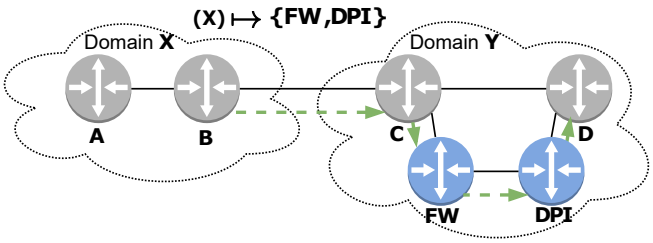

Fig. 2. Domains X and Y; X Determines an Untrusted Domain

Herewith this framework, by means of SR, helps explicitly to enforce security policies through labels, steering traffic into different security VNFs. For instance, suppose that an operator wants to implement a security policy indicating that all traffic from an untrusted domain X must pass through a FireWall (FW) and a DPI in sequence, formally $P = (X) \mapsto \{FW, DPI\}$ (*cf.* Figure 2).

The deployment of the aforementioned policy is divided into three steps. First, *(i)* the framework refines this policy at the controller level, identifying the SR policy's intermediate nodes and the target ingress node. In this case (*cf.* Figure 2), the ingress node for domain Y will be the router C. Then, *(ii)* the controller computes an SR path that results in a sequence of segments $S =< FW, DPI, D >$, representing VNFs Firewall (FW) and DPI, and the router D, respectively, to be inserted into the ingress router C. This SR path will be applied for all packets p_i coming from X with a destination in domain Y. Lastly, *(iii)* the routing algorithm will be complemented with SR to route all packets according to this policy, *i.e.*, forward packets from router C to Firewall and DPI instead of going directly to router D. This behavior is exemplified in Figure 2 by the green dashed arrows, indicating the packet route.

5 Summary and Next Steps

This paper proposed FraSeR, a Framework for Segment Routing (SR) in Network Function Virtualization (NFV) environments. FraSeR enables the specification of high-level intents for SR through a management interface, allowing, for instance, the enforcement of security policies. This approach's prototype is currently under development and a use case illustrates how the framework can enable the enforcement of security policies in an NFV environment.

Next steps includes *(i)* the full-fledged support for intent-level languages at the management interface, *(ii)* a robust leader election mechanism to be used for the controller, and *(iii)* the use of SRv6 network programmability as defined in RFC 8986, allowing for very complex policies to be implemented.

Acknowledgements

While this work was inspired by the industrial collaboration of the CSG with RUAG Schweiz AG in the context of the Harmonia project, it was supported partially by *(a)* the University of Zürich UZH, Switzerland and *(b)* the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement No. 830927, the CONCORDIA project. The authors would like to thank RUAG's team and the CSG for their valuable feedback. Special thanks go to Muriel Franco for his valuable contributions to this work.

References

1. A. Abdelsalam, S. Salsano, F. Clad, P. Camarillo, C. Filsfils: SERA: Segment Routing Aware Firewall for Service Function Chaining Scenarios. In: 2018 IFIP Networking Conference (IFIP Networking) and Workshops. Zurich, Switzerland, May 2018, pp. 46–54
2. A. Abdelsalam, S. Salsano, F. Clad, P. Camarillo, C. Filsfils: SR-Snort: IPv6 Segment Routing Aware IDS/IPS. In: 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). Verona, Italy, November 2018, pp. 1–2

3. S. Arezoumand, K. Dzeparoska, H. Bannazadeh, A. Leon-Garcia: MD-IDN: Multi-Domain Intent-Driven Networking in Software-Defined Infrastructures. In: 2017 13th International Conference on Network and Service Management (CNSM). IEEE, Tokyo, Japan, November 2017, pp. 1–7
4. M. Behringer, M. Pritikin, S. Bjarnason, A. Clemm, B. Carpenter, S. Jiang, L. Ciavaglia: Autonomic Networking: Definitions and Design Goals. RFC 7575, RFC Editor, June 2015
5. V. Eramo, F. G. Lavacca, T. Catena, M. Polverini, A. Cianfrani: Proposal and Investigation of a Scalable NFV Orchestrator Based on Segment Routing Data/Control Plane. In: 2018 14th International Conference on Network and Service Management (CNSM). IEEE, Rome, Italy, November 2018, pp. 426–431
6. C. Filsfils, D. Dukes, S. Previdi, J. Leddy, S. Matsushima, D. Voyer: IPv6 Segment Routing Header (SRH). RFC 8754, RFC Editor, March 2020, http://www.rfc-editor.org/rfc/rfc8754.txt
7. C. Filsfils, N. K. Nainar, C. Pignataro, J. C. Cardona, P. Francois: The Segment Routing Architecture. In: 2015 IEEE Global Communications Conference (GLOBECOM). IEEE, San Diego, CA, USA, February 2015, pp. 1–6
8. B. Han, V. Gopalakrishnan, L. Ji, S. Lee: Network Function Virtualization: Challenges and Opportunities for Innovations. IEEE Communications Magazine **53**(2), 90–97, 2015
9. A. S. Jacobs, R. J. Pfitscher, R. H. Ribeiro, R. A. Ferreira, L. Z. Granville, W. Willinger, S. Rao: Hey, Lumi! Using Natural Language for Intent-Based Network Management. In: 2021 USENIX Annual Technical Conference (USENIX ATC 21). USENIX Association, July 2021
10. S. Khorsandroo, A. G. Sanchez, A. S. Tosun, J. M. A. Rodríguez, R. Doriguzzi-Corin: Hybrid SDN Evolution: A Comprehensive Survey of the State-of-the-Art. Computer Networks **192**, 107981, 2021
11. X. Li, V. Kashyap, J. K. Oberg, M. Tiwari, V. R. Rajarathinam, R. Kastner, T. Sherwood, B. Hardekopf, F. T. Chong: Sapper: A Language for Hardware-Level Security Policy Enforcement. In: 19th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS). Salt Lake City, UT, USA, February 2014, pp. 97–112
12. J. Matias, J. Garay, N. Toledo, J. Unzilla, E. Jacob: Toward an SDN-enabled NFV architecture. IEEE Communications Magazine **53**(4), 187–193, 2015
13. A. Mayer, S. Salsano, P. L. Ventre, A. Abdelsalam, L. Chiaraviglio, C. Filsfils: An Efficient Linux Kernel Implementation of Service Function Chaining for Legacy VNFs Based on IPv6 Segment Routing. In: 2019 IEEE Conference on Network Softwarization (NetSoft). Paris, France, June 2019, pp. 333–341
14. C. Portegies, M. Kaat, P. Grosso: Supporting VNF Chains: An Implementation Using Segment Routing and PCEP. In: 2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN). Paris, France, 2021, pp. 1–5
15. F. Spinelli, L. Iannone, J. Tollet: Multi-Cloud Chaining with Segment Routing. In: 2020 IFIP Networking Conference (Networking). IEEE, Paris, France, July 2020, pp. 514–518
16. J. Vasseur, J. Le Roux: Path Computation Element (PCE) Communication Protocol (PCEP). RFC 5440, RFC Editor, March 2009, http://www.rfc-editor.org/rfc/rfc5440.txt
17. P. L. Ventre, M. M. Tajiki, S. Salsano, C. Filsfils: SDN Architecture and Southbound APIs for IPv6 Segment Routing Enabled Wide Area Networks. IEEE Transactions on Network and Service Management **15**(4), 1378–1392, 2018