International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8676-8680

Real-time Monitoring Technique Using SFC Classifier in NFV Environment

Sang-Min Shin[1] and Gu-In Kwon[2*]
Department of Computer Engineering, Inha University, 100 Inharo, Nam-Gu, Incheon 22212, Korea.

*(*Corresponding author)*
[2]ORCID: 0000-0003-0065-4330

Abstract

Network services which handle large-scale traffic require stability and security for the network. Traffic management for efficient traffic processing is also becoming an important issue. NFV (Network Function Virtualization) architecture has been developed to provide a flexible and effective framework to handle this issue and SFC (Service Function Chaining) technique which can configure a single network service by combining network traffic with requirements has been studied.

In this paper, we propose a monitoring technique using RCC (Recyclable Counter with Confinement) based SFC classifier for efficient traffic management in SFC. The proposed technique can manage network security functions efficiently for abnormal traffic changing in real time and makes managing traffic better.

Keywords: NFV, SFC, Traffic, Classifier, Monitoring

INTRODUCTION

Due to the widespread uptake of mobile internet environment, data traffics to support is increasing. As a result, data traffic is explosively increasing. In addition, the types of traffic that can occur in this environment are changing from a vertical structure to a horizontal traffic structure [1]. These changes mean that the number of network functions and services must be diversified, and NFV technology has emerged to deal with these issues. NFV is a technology that virtualizes network resources to control and manage network functions in network equipment flexibly [2], among which SFC technology is attracting attention as a network service that utilizes virtualized network resources based on user's demand [3].

The SFC classifies the network traffic including the user's demand and determines the order of the network functions to be performed, and forms the order of the network functions into one chain, thereby supporting a more efficient network service [3]. At the initial entrance of the external traffic, which is the first step, an SFC classifier is constructed which classifies the chain of the traffic according to the user's request [4]. The SFC classifier is informed by the NFV MANO (Management And Orchestration) outside the SFC domain of the Network Function Chain that is configured according to the user's demand and specific policy [5][6]. After classification for Service Function Chain, SFC classifier encapsulates the Service Function Path and passes it to the corresponding Service Function Forwarder. Traffic reaches a Service Function through an encapsulated Service Function Path and is provided with a network service.

SFC support large-scale traffic processing, which includes network security features such as firewalls and DPI (Deep Packet Inspection) for network stability and security. However, if you add network security features such as DPI to all service function chains, you must use one service function, which means that you need to provide a lot of overload and slow network service.

In this paper, we propose a technique to provide the network security function flexibly according to the changing traffic conditions in real time by monitoring the amount of traffic flowing through the RCC [7] based SFC classifier in the SFC domain do.

This thesis is comprised of as follows: 'BACKGROUND INFORMATION' section explains the background knowledge related to the research including SFC, RCC, and DPI; 'PROPOSAL' section propose a traffic monitoring and management technique based SFC classifier; 'CONCLUSION AND FUTURE RESEARCH' section describes the conclusion of this research and the future work.

BACKGROUND INFORMATION

1. SFC Architecture

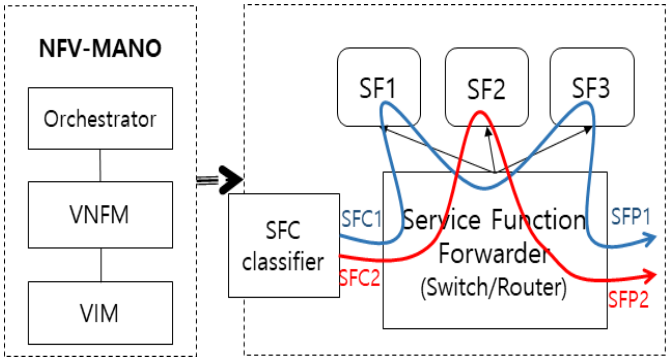

Figure 1: SFC Architecture

In 2015, the SFC WG (Working Group) established standards for the overall structure of SFC through the standard RFC 7665 - Service Function Chaining Architecture document [4]. We also defined the SFC Orchestration structure based on NFV MANO (Management And Orchestration) [5][6] to form a service function chain.

[Fig. 1] shown the structure of the SFC including NFV-MANO. This structure is largely divided into an domain of NFV-MANO which provides formation information of a service function chain and an SFC domain which classifies incoming traffic and provides a service function.

1.1 NFV-MANO

NFV-MANO is a service function that enables the Orchestrator to perform services according to its needs through Virtual VNFM (Network Function Manager), which manages the virtualized resources of the service function, and VIM (Virtualized Infrastructure Manager), which manages the virtualized infrastructure.

1.2 Service Function Chain (SFC)

It is a logical path that specifies the essential service feature set that should be applied to the traffic and the order of the functions to be executed. In [Fig. 1], we can see the path that SFC1 and SFC2 provide different network services.

1.3 SFC Classifier

The SFC Classifier offer the Classification and encapsulation.

classifies and encapsulates the external traffic including the user's demand according to the formed service function chain information.

1.4 Service Function Path (SFP)

The SFP is the path through which traffic is actually delivered, and is the result of mapping service functional resources and physical service nodes on the physical network.

1.5 Service Function Forwarder (SFF)

The SFF delivers the traffic to one or more connected service functions according to the information delivered in the SFC encapculation.

1.6 Service Function (SF)

The SF is an element responsible for a specific network service of the received packet. It can be embedded in physical network elements and implemented as virtual elements. Multiple service features may appear in the same management domain.

2. RCC (Recyclable Counter with Confinement)

RCC is a recycling counter for fast and accurate aggregation of traffic per large-scale real-time flow using a small amount of memory [7]. This counter model consists of two main processes to solve the memory limit and the speed limit: 1) Use a small amount of memory possible by resetting and recycling the memory block you are using. 2) By limiting the virtual vector used in the counter to one word, fast access is possible.

[Fig. 2] shown the two data structures of the RCC. The RCC consists of one for the probabilistic counter (A, the randomized counter) and one for the deterministic accumulator (B , the hash table). Using these two data structures, the RCC reuses a portion of the memory space of Counter A and accumulates the virtual vector in the hash table of Counter B. This structure allows one memory access to the encoding and one hash operation, and three times memory access to the decoding and two hash operations to perform the desired operation more fastly. As a result, it enables real-time detection of up to as high loader/down.

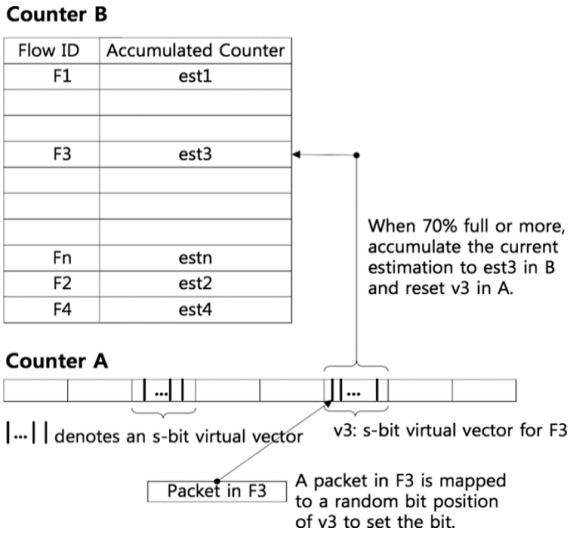

Figure 2: Step of Reinforcement Learning

3. DPI (Deep Packet Inspection)

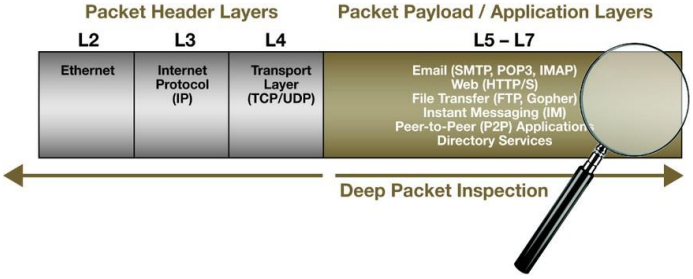

Figure 3: Analysis of DPI Technology by Packet Layer

Deep packet inspection is used to analyze the internal information of the packets in the traffic and classify the incoming data types to control the network traffic [8]. DPI collects/analyzes not only the entire network layer but also the behavior of packet application programs.

[Fig. 2] shown how DPI analyzes packets according to their packet layer. Through this analysis, DPI perform SLA (Service Level Agreement) which performs peering traffic control and finds abnormal bandwidth users and applies the appropriate usage policy [8]. In addition, it guarantees QoS (Quality of Service) based on traffic control and bandwidth allocation, and protects against attacks from viruses and malicious users through fine-grained data stream inspection [9]. While DPI has advantages of being utilized for network security and traffic adjustment, the DPI has a disadvantage in that it slows down the analysis of the header and data payload of the packet and can provide a slower network service.

PROPOSAL

Monitoring Using SFC Classifier

Network stability and network security within the SFC area where large-scale traffic is connected are necessary to ensure proper response to abnormal traffic and high quality of service .Traffic security and management are handled through one of the service functions, DPI, and the existing SFC classifier forms a deep packet inspection in the service function chain. This means that a service function with a long execution time is added to the traffic changing in real time, and this causes a lot of waste on the traffic having many requests and continuous connection. In this paper, we propose a traffic management technique that adaptively adds DPI to the service function chain based on the amount of traffic in real-time. By adding RCC to SFC classifier, our proposed technique can measure the packet amount in light and efficient way. And we introduce a case of traffic management based on the change of abnormal traffic.

1. RCC-based SFC classifier

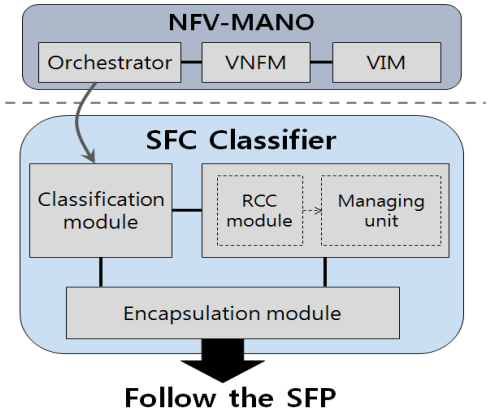

Figure 4: RCC-based SFC classifier structure

[Fig. 4] shown the structure of the RCC-based SFC classifier that measures the amount of packets at the initial inflow of traffic. The classifier consists of three modules: Classification module, RCC module, and Encapsulation module.

1.1. Classification Module

It is the first module to process traffic when it receives traffic, and it classifies the traffic by receiving the service function chain information of the traffic requirement from the NFV-MANO's Orchestrator. The Orchestrator receives service function information and instances required from the VNFM, mapping service functions to the infrastructure, and allocates hardware resources to form a service function chain. The Classification module is connected with the RCC module and the Encapsulation module to transmit the information of the determined service function chain and corresponding traffic.

1.2. RCC Module

The RCC module measures the amount of packets of traffic corresponding to information in the determined service function chain. The statistical information about the change of the measured traffic and the end of the connection is transmitted to the managing unit, which is used for the traffic reclassification and processing of the same requirement traffic again after the end of the connection. The RCC module is also connected to the Classification and Encapsulation module to give information on the amount of traffic and information on reclassification requests.

1.3. Encapsulation Module

The encapsulation module includes an encapsulation process in which each traffic that has receive the traffic classification and measurement of the amount of packets is processed through a service function path in the SFC domain. As the last step of the SFC classifier, the encapsulated traffic through this module identifies the service function path and receives the network service through the SFC element.

The order of traffic flow in the SFC classifier is as follows:

1) The first incoming traffic is classified into the service function chain through the Classification module.

2) Measure the amount of packets corresponding to classification through RCC module.

3) The encapsulation module encapsulates the service function path information in the corresponding traffic.

2.Handling of Abnormal Traffic

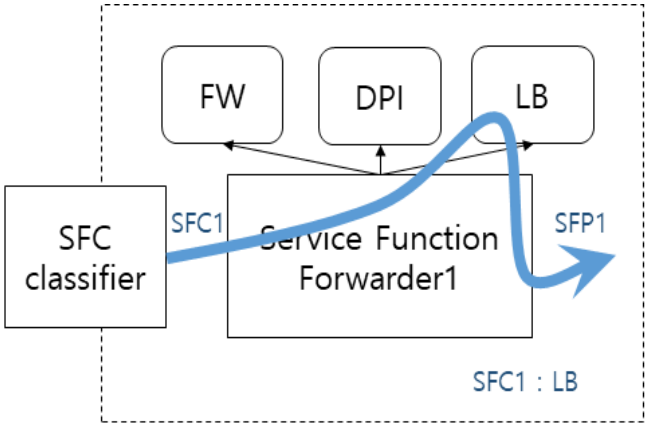

Figure 5: Growing abnormal traffic

[Fig. 5] shown the result of rapidly growing traffic in real time.

Initially, SFC1 is provided with the LB (Load Balancer) service function. The traffic of the SFC classifier increases rapidly at a certain point in time, and the RCC module of the SFC classifier calculates the packet amount of the corresponding traffic in real time to detect the increase of the abnormal traffic. The RCC module give the information of the increased traffic to the connected Classification module, and based on the transmitted traffic information, the Classification module forms the service functional chain as a path to visit the DPI first by reclassifying the traffic.

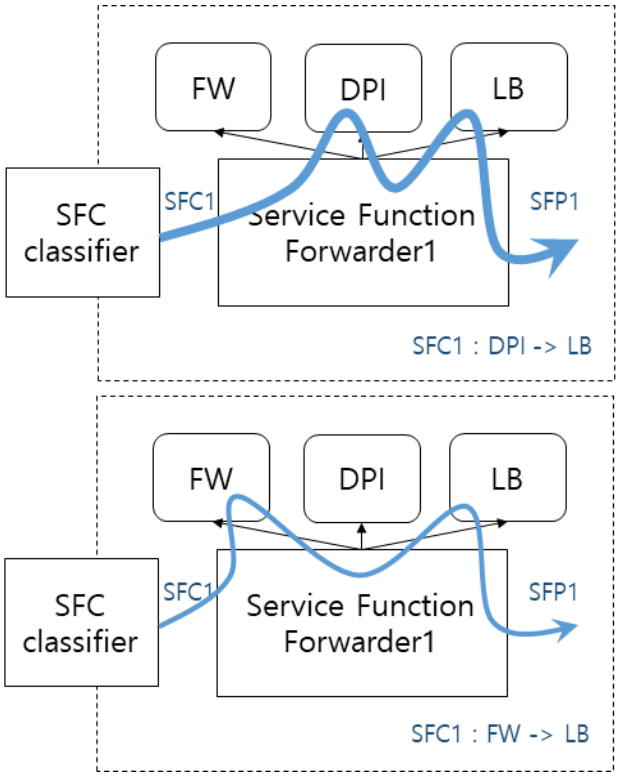

Figure 6 : Growing abnormal traffic handling

[Fig. 6] shown the result of the changed service function chain.

In the top part of [Fig. 6], the SFC1 receives the LB after the DPI first as a result of the changed Chain. DPI detects malicious attacks through packet inspection of corresponding traffic and strengthens network security against attack traffic including FW (Firewall) according to network policy. Thereafter, the FW can block malicious attack traffic and see that SFC1 is restored to normal traffic.

If the SFC1 that only receives the Load Balancer in [Fig. 5] initially visits the DPI first, it results in waste compared to the service provided in the network service through the deep packet inspection. However, when the traffic is processed by the SFC classifier proposed in this paper, it is possible to provide the network security function to the users lighter and more efficiently than the existing technique by using memory and high speed operation which are advantages of RCC.

CONCLUSION AND FUTURE RESEARCH

In this paper, we propose an effective traffic management technique using RCC-based SFC classifier to manage real-time incoming traffic in NFV environment. This technique adds RCC to the SFC classifier, which is the first stage of the SFC domain, with small memory access and fast operation, and measures the amount of traffic and forms a network security function according to the amount of traffic. This can provide efficient traffic management in terms of network stability and security with lower load and faster response times than before. In the future research, management method will be studied on the same traffic that comes back after the connection is terminated by using a managing unit in the RCC Module that has statistical information of the traffic.

ACKNOWLEDGEMENTS

This work was supported by the National Research Foundation of Korea (NRF) grant funded by Korea government (MSIP) (no. NRF-2015R1A2A2A01003501).

REFERENCES

[1] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, *103*(1), 14-76.

[2] Han, B., Gopalakrishnan, V., Ji, L., & Lee, S. (2015). Network function virtualization: Challenges and opportunities for innovations. *IEEE Communications Magazine*, *53*(2), 90-97.

[3] Medhat, A. M., Taleb, T., Elmangoush, A., Carella, G. A., Covaci, S., & Magedanz, T. (2017). Service Function Chaining in Next Generation Networks: State of the Art

and Research Challenges. *IEEE Communications Magazine*, *55*(2), 216-223.

[4] Halpern, J., & Pignataro, C. (2015). *Service function chaining (sfc) architecture*(No. RFC 7665).

[5] ETSI, N. (2014). Network Functions Virtualisation (NFV); Management and Orchestration. *NFV-MAN*, *1*, v0.

[6] Mechtri, M., Ghribi, C., Soualah, O., & Zeghlache, D. (2017). NFV Orchestration Framework Addressing SFC Challenges. *IEEE Communications Magazine*, *55*(6), 16-23.

[7] Nyang, D., & Shin, D. (2016). Recyclable counter with confinement for real-time per-flow measurement. *IEEE/ACM Transactions on Networking*, *24*(5), 3191-3203.

[8] Chaudhary, A., & Sardana, A. (2011, April). Software based implementation methodologies for deep packet inspection. In *Information Science and Applications (ICISA), 2011 International Conference on* (pp. 1-10). IEEE.

[9] Yu, F., Chen, Z., Diao, Y., Lakshman, T. V., & Katz, R. H. (2006, December). Fast and memory-efficient regular expression matching for deep packet inspection. In *Architecture for Networking and Communications systems, 2006. ANCS 2006. ACM/IEEE Symposium on* (pp. 93-102). IEEE.