네트워크 기능 가상화 관리 및 오케스트레이션 기능과 보안★

김현철*

요 약

최근 몇 년 동안 네트워크 인프라의 설계, 관리, 그리고 운영하는 방식은 새로운 기술들과 구성 방식들의 등장으로 끊임없이 진화하고 있다. 이러한 거대한 추세를 반영하고 이러한 신기술들이 제공하는 막대한 경제적인 이득과 유연성을 기반으로 소프트웨어 정의 네트워킹 (SDN)과 네트워크 기능 가상화 (NFV)가 핵심요소로 등장하였다. SDN/NFV는 네트워크 인프라의 민첩성을 대폭 향상시켜 네트워크 운영자나 서비스 제공자로 하여금 게이트웨이, 라우터, 그리고 로드 밸런서와 같은 자신만의 네트워크 기능들을 일반적인 하드웨어 상에서 구현 가능하게 하였다. SDN/NFV를 통하여 네트워크 서비스의 설계, 제공 및 운용이 동적으로 지원 가능하게 되었다. NFV에서 MANO는 이러한 가상 인프라 관리자 (VIM)나 가상 네트워크 기능 관리자 (VNFM)와 같은 소프트웨어 관리자들의 오케스트레이션을 지원한다. 본 논문에서는 이러한 NFV MANO의 내용을 체계적으로 살펴보고 가상화 환경에서의 보안체계를 제안하고 있다.

Management, Orchestration and Security in Network Function Virtualization

Hyuncheol Kim*

ABSTRACT

The design, management, and operation of network infrastructure have evolved during the last few years, leveraging on innovative technologies and architectures. With such a huge trend, due to the flexibility and significant economic potential of these technologies, software defined networking (SDN) and network functions virtualization (NFV) are emerging as the most critical key enablers. SDN/NFV enhancing the infrastructure agility, thus network operators and service providers are able to program their own network functions (e.g., gateways, routers, load balancers) on vendor independent hardware substrate. They facilitating the design, delivery and operation of network services in a dynamic and scalable manner. In NFV, the management and orchestration (MANO) orchestrates other specific managers such as the virtual infrastructure manager (VIM) and the VNF Manager (VNFM). In this paper, we examine the contents of these NFV MANO systematically and proposes a security system in a virtualized environment.

Key words : Network Function Virtualization, Management, Orchestration

접수일(2016년 2월 15일), 수정일(1차: 2016년 2월 29일), 게재확정일(2015년 3월 3일)

★ 이 논문은 2015년도 남서울대학교 학술연구비 지원에 의해 연구되었음.

* 남서울대학교 컴퓨터학과 교수

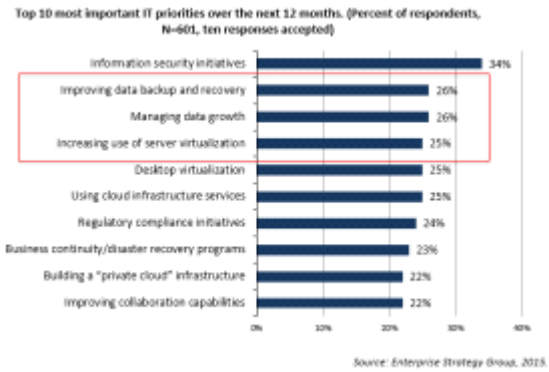
1. 서 론

현재의 네트워크는 몇몇 기초적인 문제로 인하여 고품질, 대규모, 대용량 서비스 제공이 어려운 구조이다. 우선 지금까지 네트워크 서비스를 제공하기 위한 대부분 장비의 내부 구조를 살펴보면 각각의 개별 장비에서 제어플레인, 데이터플레인, 그리고 관리플레인 기능을 독립적으로 수행하는 형태로 발전해왔다. 또한 장비에서 수행하는 대부분의 기능이 서로 중복되는 분산구조 형태로 운영이 되어왔다. 그러나 이러한 분산구조 형태에서는 네트워크 구성이 변경되는 경우 라우터, 스위치, 방화벽, 인증장비 등 해당되는 모든 장비에 변경된 정책과 설정은 입력해야하기 때문에 변경시간이 오래 걸리고 신속하게 서비스를 제공할 수 없다는 단점이 있다 [1][2].

한편 지금까지의 전통적인 네트워크 인프라 구성은 코어스위치를 중심으로 하단에 분산스위치를 두고, 또 그 하단에 액세스 스위치로 구분되는 전통적인 3단(Tier) 구조였다. 이러한 3Tier 구조는 일반적으로 North-South 트래픽이라고 하며 초기 인터넷 트래픽의 특징에서와 같이 내부 트래픽보다는 인터넷 트래픽과 다른 네트워크로 전달되는 트래픽이 많다는 전제에 기반하고 있다. 그러나 최근 인터넷트래픽의 많은 부분을 처리하고 있는 데이터센터의 트래픽은 East-West 트래픽이 대부분을 이루고 있기 때문에 이를 처리하기 위한 네트워크 인프라의 변경이 요구되고 있다 [3][4].

이처럼 네트워크 인프라가 고품질, 지식 기반 서비스 및 솔루션을 제공하기 위해 네트워크는 컴퓨팅과 융합하여 개방화, 가상화, 소프트웨어화로 진화하고 있으며 대표적인 기술이 SDN (Software Defined Networking) 및 NFV (Network Function Virtualization)이다. NFV는 네트워크 사업자가 기존의 네트워크 하드웨어 장비들을 가상화해 데이터센터, 네트워크 노드 및 가입자 장비에 위치시킬 수 있는 표준 하드웨어 상에서 네트워크를 구축할 수 있게 하는 것을 목표로 한다 [5][6][7].

SDN/NFV를 통하여 네트워크 서비스의 설계, 제공 및 운용이 동적으로 지원 가능하게 되었고 NFV에서 MANO는 이러한 가상 인프라 관리자 (VIM)나 가상 네트워크 기능 관리자 (VNFM)와 같은 소프트웨어 관리자들의 오케스트레이션을 지원한다 [8][9]. 본 논문에서는 이러한 NFV MANO (Management and Orchestration)의 내용을 체계적으로 살펴보고 가상화 환경에서의 보안체계를 제안하고 있다.



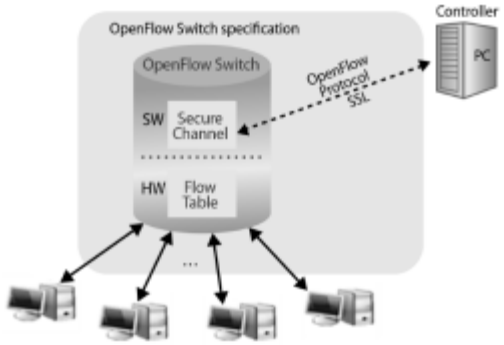
(그림 1) IT 사업의 우선순위 분석

2. 관련연구

2.1 SDN/OpenFlow

SDN은 초기 스탠퍼드 대학 캠퍼스 네트워크를 소프트웨어 기반으로 바꾸기 위해 시작되었지만 기존 네트워크 인프라에서 제공하지 못했던 운영의 효율성과 확장성, 그리고 가용성 등의 제공 가능성을 확인하면서 통신서비스 사업자와 서비스 제공자로부터 큰 주목을 받고 있다.

기존 네트워크 트래픽은 네트워크의 모든 상황을 알 수 없는 개별 네트워크 장비의 연산에 의해 경로가 결정되기 때문에 특정 구간에는 엄청난 부하가 발생할 수 있지만 동일한 경로의 다른 구간에는 아무 트래픽도 흐르지 않는 경우가 빈번하게 발생할 수 있다. 이를 해결하기 위해 구글에서는 WAN Fabrics를 도입하였고 WAN Fabrics의 핵심 기술이 SDN/OpenFlow이다.



(그림 2) OpenFlow 시스템 구성

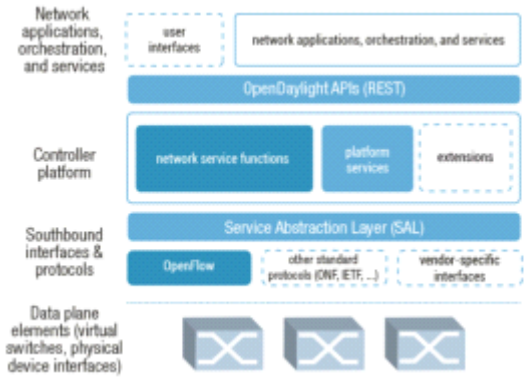
(그림 2)에서와 같이 OpenFlow를 이용하면 장비 업체나 종류에 관계없이 네트워크 장비의 플로우 테이블을 개방형 프로토콜에 따라서 손쉽게 프로그래밍 할 수 있다. 또한 기존의 인터넷 트래픽에 영향을 주지 않으면서 다양한 네트워킹 기술을 시험할 수 있다. 이는 새로운 라우팅 프로토콜, 보안 모델, 어드레싱 방법, 그리고 IP를 대체할 수 있는 새로운 인터넷 기술개발 환경을 제공한다.

2.2 OpenDaylight

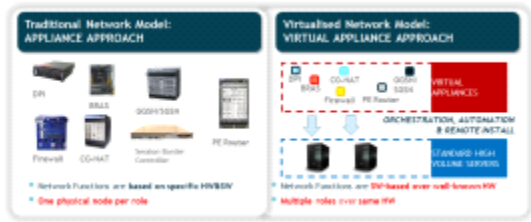
기존 네트워크 장비 제조사들이 주축이 되어 만든 OpenDaylight는 (그림 3)에서와 같이 SDN Platform을 제공 기술로 Controller는 물론 Southbound API를 제공한다. OpenDaylight의 특징은 Southbound API를 확대하여 OpenFlow가 아니더라도 동작을 할 수 있도록 한다는 점이다. 이는 벤더들이 소유하고 있는 기존의 검증된 다양한 솔루션들을 SDN Platform 에서도 그대로 사용하고자 함이다.

3. NFV와 보안

기존의 네트워크에서는 서비스 제공 단위요소를 하드웨어 기준으로 구분하였다. 그러나 이러한 방식은 적시적소에 자원을 배치할 수 없기 때문에 자원의 낭비와 막대한 운영비용을 필요로 하였다. 이러한 문제를 해결하기 위해 NFV는 (그림 4)에서와 같이 가상화를 기반으로 자원의 이동과 배치를 용이하게 하여 물리적 자원을 최소화하여 네트워크 서비스의 효율성을 향상시키고 시스템의 복잡성을 감소시켜 저가로 서비스를 제공하는 것에 초점을 두고 있다. 또한 NFV가 반드시 SDN을 사용하는 것은 아니지만 NFV과 SDN는 밀접하게 상호 보완적인 관계이다.



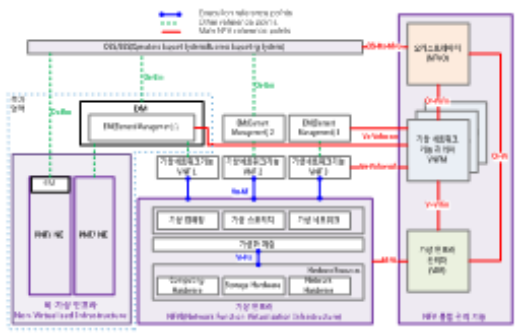
(그림 3) OpenDaylight 프레임워크



(그림 4) NFV 개념도

3.1 NFV 구조

ETSI NFV ISG에서는 (그림 5)에서와 같이 NFVI (Network Function Virtual Infrastructure), VNF, MANO로 구성되는 NFV 참조 기능 구조를 정의하였고 구현 위주 이슈 도출 및 벤더와 통신사업자간의 상호 운용성에 초점을 맞추어 추가적인 표준화 작업을 진행하고 있다. 특히 모바일 분야에서 NFV 구현이 활발하게 이루어지고 있다.



(그림 5) NFV 참조 모델과 역할

NFV는 상용 서버에서 가상 네트워크 기능을 소프트웨어적으로 구현하기 때문에 성능 문제가 대두되었고 인텔 DPDK (Data Plane Development Kit), Open On-Load, Netmap, ODP (Open Data Plane) 와 같은 다양한 DPA (Data Plane Acceleration) 기술이 공개되었다.

3.2 OPNFV

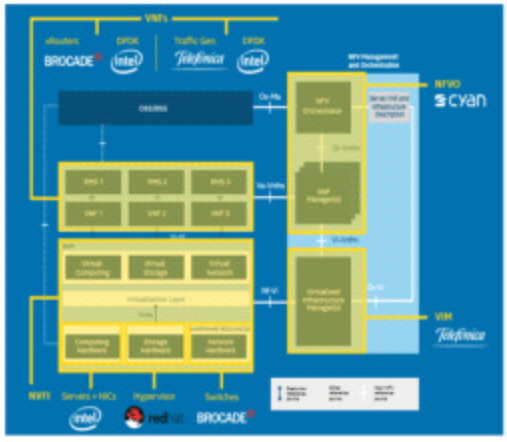
OPNFV 프로젝트는 NFV 기술의 진화와 확산을 목적으로 ETSI NFV 구조 프레임워크를 따르는 공개 소프트웨어 기반의 NFV 참조 플랫폼을 선도적으로 개발하는 것이며, 동시에 기존의 관련 공개 소프트웨어 프로젝트와의 융합을 통하여 NFV 서비스를 더욱 활성화 하는 것도 포함한다.

따라서 OPNFV 프로젝트 결과물을 통하여 NFV 솔루션을 설치하고 시험검증 할 수 있으며 실제 NFV를 구축할 때 시스템 통합을 위한 참조모델로서 활용할 수 있다. 이를 통하여 OPNFV는 다양한 네트워크 서비스의 유스케이스와 서비스 특성에 맞는 NFV 솔루션을 각자 개발할 수 있는 참조 플랫폼을 제공한다.

3.3 MANO

네트워크 기능 가상화를 통하여 네트워크 서비스를 구성, 제어, 관리하기 위한 NFV 프레임워크의 MANO는 통합적인 계층적 관리를 위하여 인프라 자원을 관리하는 VIM (Virtual Infrastructure Manager)과 VNF를 관리와 이를 통합하는 오케스트레이터로 구성되어 있다. 기존의 장비에 대해서는 기존의 방식에 따라서 장비의 EM (Element Management) 등을 통해서 직접 관리가 필요하기도 하다.

MANO 규격의 목적은 NFV를 구성하는 기능 블록들을 정의하고, 각 기능 블록이 제공해야 하는 기능, 여러 기능 블록간 인터페이스 및 상호 교환되는 정보 모델을 포함하는 NFV 기능 구조를 정의하는 것이다.



(그림 6) MANO와 종단간 NFV 시연구조

(표 1) NFV에서 잠재적인 보안 위협

① 토폴로지 Validation과 Enforcement
② 관리지원 인프라의 가용성
③ 보안 부트/크래쉬
④ 성능 Isolation
⑤ 사용자/테넌트 AAA
⑥ 인증된 시가 서비스
⑦ 클론 이미지에서의 사설키
⑧ 다중 관리자 Isolation
⑨ 가상 테스트와 모니터링을 이용한 백도어

3.4 NFV와 보안

NFV의 동적인 특징을 반영하기 위해 다음과 같은 두 가지 보안 위협은 반드시 고려되어야 한다. 우선 서로 다른 가입자의 서비스나 서비스 기능은 반드시 서로 분리되어 보호되어야 한다. 또한 NFVI는 가입자 서비스로부터 독립되어 보호되어야한다. 아울러 서비스 도입의 탄력성을 확보하기 위해서는 동일한 서비

스를 구성하는 기능들이 동일한 물리적인 자원 내에 설치되어서는 안 된다. 이러한 내용을 반영하여 ETSI 보안전문가그룹에서 정의한 NFV 관련 잠재적 보안 위협은 (표 1)과 같다 [10].

4. 결 론

기존의 네트워크 구조에서 네트워크 장비는 각각의 하드웨어 자원으로 구성된다. 그러나 이러한 하드웨어는 상이한 전용기술을 필요로 하며 장비설치 공간과 전력, 비용 등이 발생하게 된다. 또한 새로운 네트워크를 구성할 때마다 새로운 기술을 사용하는 장비를 설치해야 하는 문제점이 있다. 이러한 문제를 해결하기 위한 것이 NFV이며 NFV는 가상 환경 구성을 통해 네트워크 트래픽 구간을 줄이고 또한 물리적인 제약도 줄일 수 있다.

본 연구에서 제안하는 가상화 기반 관련 연구에서와 같이 SDN과 NFV를 접목하면 NFV에 의해 만들어진 가상화된 네트워크 장비로의 트래픽을 SDN을 이용해 제어할 수 있게 된다. 필요한 트래픽만 특정 네트워크 장비로 보내고 일반 트래픽은 SDN을 이용해 노드 간 직접 트래픽으로 전환하는 등의 효율적 네트워크 정책을 적용할 수 있게 되어 보다 능동적으로 네트워크를 구성할 수 있게 된다.

참고문헌

[1] A. Checko et al., “Cloud Ran for Mobile Networks – A Technology Overview,” IEEE Commun. Surveys & Tutorials, vol. 17, no. 1, 2015, pp. 405 - 26.

[2] R. Mijumbi et al., “Network Function Virtualization: State-of -the-Art and Research Challenges,” IEEE Commun. Surveys & Tutorials, no. 99, 2015, pp. 1.

[3] ETSI NFV ISG, “ETSI Network Functions Virtualisation (NFV) Industry Standards (ISG) Group Draft Specifi cations,” http://docbox.etsi.org/ISG/NFV/Open, Dec. 2014, accessed May 26, 2015.

[4] ETSI GS NFV-MAN 001, “Network Functions Virtualisation (NFV); Management and Orchestration,” http://www.etsi.org/, Dec. 2014

[5] K. Ogaki et al., “Integrating Heterogeneous It/Network Management Models Using Linked Data,” Proc. 2013 IFIP/IEEE Int’l. Symp. Integrated Network Management, May 2013, pp. 768 - 71.

[6] J. Cardoso et al., “Cloud Computing Automation: Integrating USDL and TOSCA,” LNCS. Springer 2013, vol. 7908, pp. 1 - 16.

[7] D. R. Lopez, “OpenMANO: The Dataplane Ready Open Source NFV MANO Stack,” Proc. IETF 92 Meeting Proc., Dallas, TX, Mar. 2015.

[8] N. Chowdhury et al., “Virtual Network Embedding with Coordinated Node and Link Mapping,” Proc. IEEE INFOCOM 2009, April 2009, pp. 783 - 91.

[9] R. Mijumbi et al., “Design and Evaluation of Algorithms for Mapping and Scheduling of Virtual Network Functions,” Proc. IEEE Conf. Network Softwarization, Univ. College London, April 2015.

[10] ETSI ISG NFV, “ETSI GS NFV-SEC 001 V1.1.1: Network Functions Virtualisation (NFV); NFV Security; Problem Statement,” October 2014.

[저 자 소 개]

김 현 철 (Hyuncheol Kim)

1990년 2월 성균관대학교 학사
1992년 2월 성균관대학교 석사
2005년 8월 성균관대학교 박사
2006년 9월 ~ 현재 남서울대학교 컴퓨터학과 교수

email : hckim@nsu.ac.kr