SDN 기반의 OpenStack 네트워킹을 위한 Virtual TAP 설계 및 구현

정세연 [1], 유재형 [2], 홍원기 [1]

[1] 포항공과대학교 컴퓨터공학과

[2] 포항공과대학교 정보통신대학원

{jsy0906, styoo, jwkhong}@postech.ac.kr

Design and Implementation of Virtual TAP for SDN-based OpenStack Networking

Seyeon Jeong[1], Jae-Hyoung Yoo[2], James Won-Ki Hong[1]

[1]Department of Computer Science and Engineering, POSTECH

[2]Graduate School of Information Technology, POSTECH

요 약

오늘날 트래픽 규모의 증가 및 향상된 QoS(Quality of Service)에 대한 요구와 함께 클라우드 서비스가 널리 보급됨에 따라 서버 리소스의 효과적인 사용을 가능하게 하는 가상화 기술이 주목받고 있다. 본 연구에서는 기존 하드웨어 TAP(Test Access Port) 장치가 가상 링크(virtual link)를 통해 전달되는 가상 머신(Virtual Machine) 간 패킷을 복제하는데 사용될 수 없다는 문제점을 해결하기 위한 방안으로 가상 스위치에서 동작하는 Virtual TAP(vTAP)을 제안한다. 이를 위해 Port mirroring 또는 SPAN(Switched Port Analyzer)과 같은 기존 스위치의 기능을 이용할 수 있지만, 대량의 트래픽을 처리해야하는 환경(예, 데이터센터, NFV 등)에서 성능 저하 및 수동 설정에 따른 에러를 야기할 수 있다. 따라서, 본 연구에서는 ONOS(Open Network Operating System) SDN(Software-Defined Networking) 컨트롤러를 기반으로 제어되는 OpenStack 네트워크 환경에서 DPDK(Data Plane Development Kit)로 가속화된 Open vSwitch 에서 동작하는 vTAP 의 구현 및 설계를 기술하며, 제안하는 방법의 성능을 검증한다.

Ⅰ. 서 론

기존 하드웨어 TAP(Test Access Port) 장치는 EPC(Evolved Packet Core)와 같은 시스템의 각 네트워크 링크에 배치되어 통과하는 패킷을 전기적으로 복제하며, 각 TAP 장치에서 복제된 패킷은 NPB(Network Packet Broker)에서 aggregate 되어 IDS(Intrusion Detection System) 및 트래픽 analyzer 등으로 전달된다. 이러한 하드웨어 TAP 기반 패킷 모니터링 방식은 성능을 보장하지만 CAPEX 를 수반하며, 특히 오늘날 보편적인 서버 가상화 환경에서 가상 머신(Virtual Machine, VM) 및 가상 스위치 기반 가상 네트워크 환경 내부에서 발생하는 패킷을 복제하는데 사용될 수 없다. 반면, 본 연구에서 제안하는 Virtual TAP(vTAP)은 기존 TAP 장치의 소프트웨어 구현으로서, 서버 가상화 환경에서 가상 머신 간 트래픽을 패킷 수준에서 모니터링할 수 있게 한다.

우리는 기존 연구[1]에서 KVM(Kernel-based Virtual Machine) 기반의 서버 가상화 환경에서 OpenFlow 의 그룹 테이블(Group Table) 기능을 이용하여 가상 스위치에서 vTAP 을 구현하였으며, 패킷 복제 속도 측면에서 Port mirroring 기반 구현과 성능을 비교하였다. 또한, 개별 스위치 단위의 수동 설정이 필요한 Port mirroring 과는 달리, 제안된 방식은 SDN(Software-Defined Networking) 컨트롤러를 이용하여 복제 대상 패킷 플로우를 유연하게 특정짓고 중앙집중화된 방식으로 TAP 정책을 관리할 수 있음을 보였다. 본 연구에서는 기존 연구의 vTAP 설계를 확장하여 SDN 컨트롤러로 제어되는 OpenStack 네트워킹 환경(예, 데이터센터)에서 동작하도록 구현한다. 이를 통해 OpenStack VM 간 트래픽을 패킷 수준에서 모니터링할 수 있음을 보이고 실험을 통해 성능을 검증한다.

Ⅱ. 관련 연구

학계에서는 주로 데이터센터와 같은 대규모 (SDN) 네트워크의 모니터링 및 트래픽 엔지니어링을 위해 패킷 복제 기능을 활용하는 연구가 다수 존재한다 [2]. 이들 연구에서는 Port mirroring 을 통해 물리 스위치를 경유하는 패킷만 모니터링 하는 반면, 본 연구에서는 가상 스위치(OVS) 수준에서 패킷을 복제하여 호스트 서버 내부의 가상 머신 간 트래픽을 모니터링한다.

근래 네트워크 관리에 머신 러닝(Machine Learning) 기술을 접목하는 연구가 활발해짐에 따라, 일부 연구에서는 패킷 수준 데이터를 학습해 침입탐지 기능 등을 강화한다 [3]. 이를 위해 패킷 수준 데이터를 고속으로 제공하는 방안으로 본 연구의 DPDK(Data Plane Development Kit) 기반 가속화된 패킷 복제 기능이 활용될 수 있다.

Ⅲ. 제안하는 방법

그림 1 은 본 연구에서 제안하는 SDN 기반으로 운용되는 OpenStack 환경에서 VM 인스턴스 간 패킷 모니터링을 위해 OVS 가상 스위치 기반으로 vTAP 기능을 구현한 시스템의 구조를 보인다. 제안하는 구조는 크게 (1)OpenStack 네트워킹과 ONOS 컨트롤러 및 이를 연동하기 위한 ONOS 어플리케이션의 집합인 SONA(Simplified Overlay Network Architecture)와 [4], (2)vTAP 정책의 적용 및 관리를 위한 사용자 인터페이스 역할의 vTAP 어플리케이션으로 구성된다.

SONA 는 ONOS 의 주요 어플리케이션 중 하나로서, 일반적으로 Neutron 및 Open vSwitch 에이전트 기반으로

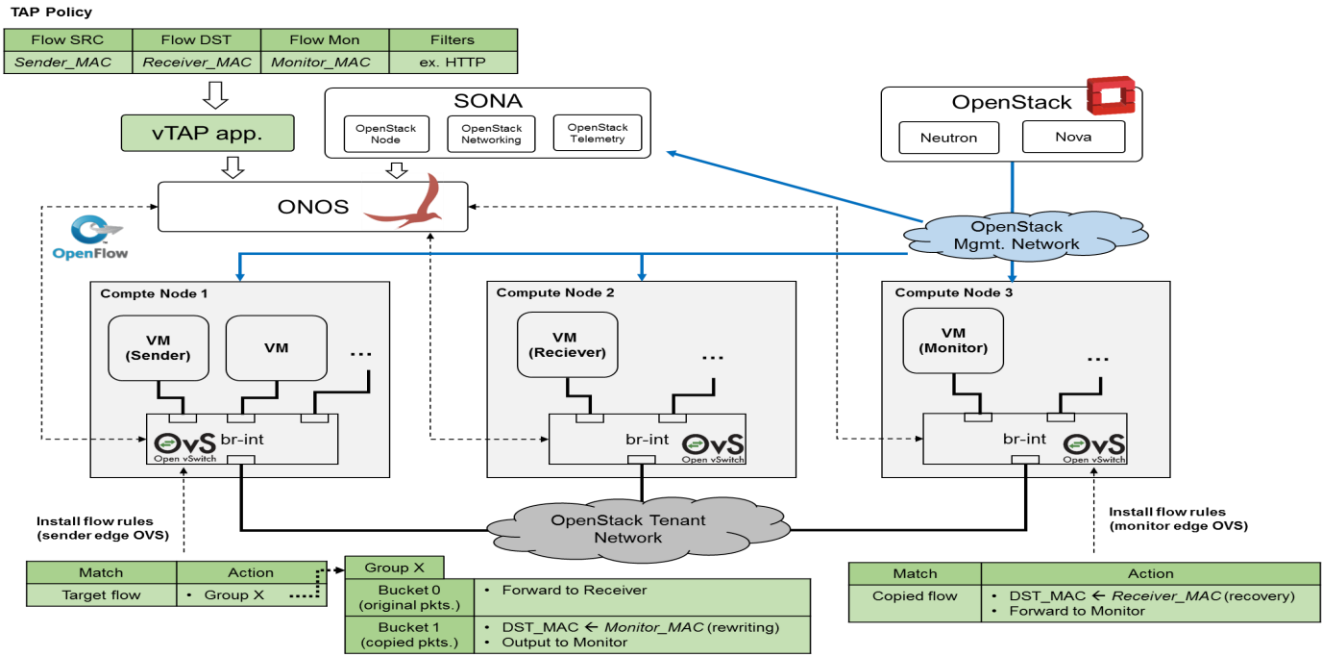

그림 1 SDN 기반 OpenStack 네트워킹에서 동작하는 vTAP 시스템 구조

동작하는 OpenStack 네트워킹을 ONOS 컨트롤러를 통해 SDN 기반으로 동작시켜 트래픽 엔지니어링 및 네트워크 정책 제어(예, vTAP)를 용이하게 한다. 본 연구에서는 SONA(ONOS 1.13 버전)와 OpenStack(Pike 버전) Nova 및 Neutron 소스 코드를 일부 수정해서 SONA 및 제안된 vTAP 어플리케이션을 통해 Compute 노드의 DPDK 기반 OVS(OVS-DPDK)에 패킷 복제 정책을 적용한다.

제안하는 vTAP 어플리케이션은 네트워크 관리자가 복제를 원하는 패킷 플로우를 출발지(source), 목적지(destination), 모니터링 목적지(monitor), 패킷 필터(filter) 수준에서 명세한 정책(그림 1 의 TAP Policy)을 ONOS API 및 OpenFlow 를 이용하여 관련 엣지(edge) 스위치(OVS)에 플로우 룰(flow rule) 형태로 반영한다. 출발지 엣지 스위치에 설치된 플로우 룰은 복제 대상 (원본) 패킷을 매칭시켜 그룹 테이블로 전달하며, 해당 그룹 테이블은 (1) 원본 패킷을 목적지로 그대로 전송하며 (2)원본 패킷을 복제하여 라우팅 정보(IP 또는 MAC 주소)를 수정, 모니터링 목적지로 전달한다. 모니터링 목적지의 엣지 스위치는 복제 패킷을 수신하여 라우팅 정보를 원상태로 복구시킨 뒤 모니터링 목적지로 전달한다.

Ⅳ. 실험

제안된 vTAP 의 성능 평가를 위해 네트워크 공격 트래픽이 유입될 때 원본 패킷 수신지(Receiver) 및 복제 패킷 수신지(Monitor)에 설치된 각 Suricata IDS 에서 생성되는 alert 의 개수를 비교하였다 (그림 2). Receiver 및 Monitor 는 2 개의 vCPU 와 2GB 메모리가 할당된 OpenStack VM 인스턴스이며, 1 개의 전용 CPU 코어가 할당된 OVS-DPDK 에서 패킷 복제 및 포워딩이 동시에 수행된다. 실험 결과에서 50 Mbps 까지는 동일한 alert 개수를 보이며 복제 패킷에 대한 IDS 분석의 정확도를 보장하지만, 100 Mbps 이상에서는 양쪽 모두 감소된 alert 개수를 보였다. 이는 분석할 패킷 개수가 증가하면서 IDS 의 리소스 점유율이 늘어나게 되고 그 결과 VM 의 패킷 drop 비율이 증가하면서 IDS 분석 정확도가 감소하였기 때문이다. 또한 패킷 복제 과정을 거치지 않고 상대적으로 빠르게 전달되는 원본 패킷을 수신하는 Receiver 에서 패킷 drop 비율이 더 높았다. 향후 연구에서 수신측 VM 에서도 DPDK 를 사용하여 패킷 처리를 위한 전용 리소스를 할당, IDS 가 사용하는 리소스와 isolation 하는 방법 등을 통해 발견된 문제점을 보완할 예정이다.

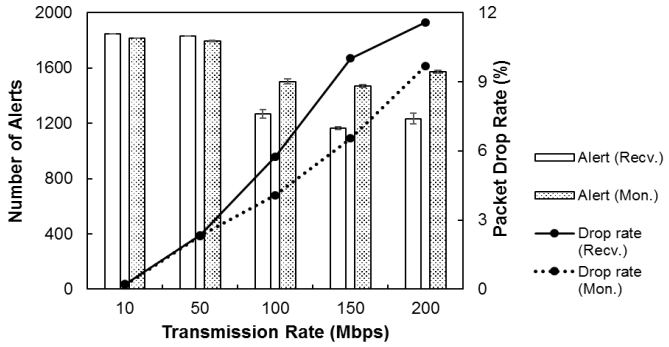

그림 2 IDS 에서 생성된 Alert 개수 비교

Ⅴ. 결론

본 논문에서는 OpenStack 환경에서 VM 인스턴스 간 패킷 모니터링을 위해 SDN 컨트롤러에서 패킷 복제 정책(추상화, 중앙집중화)을 설정하여, 가상 스위치에서 패킷 복제 기능을 수행하는 vTAP 의 구조를 설계하고 구현 과정을 설명하였다. 또한, IDS 를 활용한 유스케이스를 통해 OpenStack 환경에서의 사용 가능성과 성능을 평가하였다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [2018-0-00749, 인공지능 기반 가상 네트워크 관리기술 개발]

참 고 문 헌

[1] Jeong, Seyeon, et al. "OpenFlow-based virtual TAP using open vSwitch and DPDK." NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018.

[2] Liu, Guyue, et al. "NetAlytics: Cloud-Scale Application Performance Monitoring with SDN and NFV." Proceedings of the 17th International Middleware Conference. ACM, 2016.

[3] Abubakar, Atiku, and Bernardi Pranggono. "Machine learning based intrusion detection system for software defined networks." Emerging Security Technologies (EST), 2017 Seventh International Conference on. IEEE, 2017.

[4] ONOS wiki, "SONA: DC Network Virtualization," 2018. [Online]. https://wiki.onosproject.org/display/ONOS/SONA%3A+DC+Network+Virtualization