편집위원 : 이순석 (ETRI)

SDN에서 데이터 경로 설계에 대한 고려 사항

윤현식, 강경순, 김학서, 박혜숙
한국전자통신연구원

요 약

오늘날 미래인터넷 기술의 하나로서 SDN이 클라우드 서비스, 모바일 서비스, 스마트 TV, 빅데이터 및 사물지능통신 등의 새로운 서비스를 제공할 수 있는 개방형 플랫폼으로 주목받고 있다.

본고에서는 이러한 SDN 망을 구축함에 있어서 제어 인터페이스, QoS, 멀티캐스트, 이동성 및 네트워크 보안 측면에서 고려해야 할 사항들을 살펴본다. 기존 네트워크의 근본적인 문제점으로 인해 발생한 복잡성 및 성능 저하 요인들이 SDN의 장점을 활용하여 해결될 수 있으며, 이에 본고에서 제시된 고려 사항들이 큰 역할을 할 것이다.

Ⅰ. 서 론

오늘날 클라우드 서비스, 모바일 서비스, 스마트 TV, 빅데이터 및 사물지능통신 등 다양한 분야에서 새로운 서비스의 활성화를 위해 네트워크 인프라의 지원에 대한 요구가 증가하고 있다.

이는 기존의 폐쇄적인 네트워킹 환경에서 개방형 네트워킹 환경으로의 변화를 요구하고 있으며, 이에 OpenFlow 기반의 SDN(Software-Defined Networking) 기술이 주목받고 있다[1].

SDN은 네트워크 제어 기능이 패킷 포워딩 기능과 분리되어 직접적으로 프로그래밍 가능한 네트워크 구조이며, 이를 통해 애플리케이션과 네트워크 서비스들에게 네트워크 인프라가 추상화되도록 한다. 그리고 이러한 추상화를 통해서 네트워크 운용자는 네트워크 설계 및 운용을 간략화할 수 있다. 또한, SDN에서 네트워크 장치들은 기존의 복잡한 프로토콜을 구현 및 동작시킬 필요가 없이 단순히 제어 장치로부터의 명령만을 수행하면 되므로 간략화될 수 있다. SDN의 구조는 〈그림 1〉에 제시되었다 [2][3].

네트워크 추상화 이외에 SDN은 보편적인 네트워크 서비스를 구현하는 것을 가능하게 하는 API(Application Programming Interface)들을 지원한다. 그리고, 상기의 보편적인 네트워크 서비스는 라우팅, 멀티캐스트, 보안, 접근 제어, 대역폭 관리, 트래픽 제어, 품질 보장(QoS), 프로세서 및 저장 용량 최적화, 에너지 사용 및 정책 설정 등이 있다.

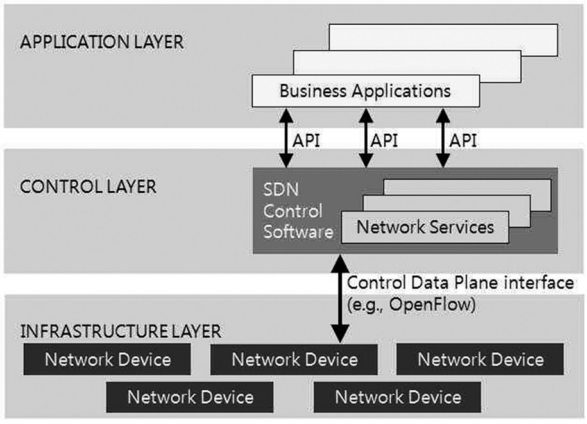

그림 1. SDN 구조

OpenFlow는 SDN 구조의 네트워크 제어 평면과 포워딩 평면 간에 정의된 최초의 표준 인터페이스이며, 컴퓨터의 CPU와 같이 외부 애플리케이션에 의해 네트워크 장치의 포워딩 평면을 프로그램하는 함수로서 인식될 수 있다.

OpenFlow는 미리 정해진 규칙에 따라서 트래픽을 구분할 때 플로우의 개념을 사용하므로 더 정밀한 트래픽 제어 기능을 제공하며, 네트워크가 애플리케이션 또는 사용자 레벨에서의 변화에 실시간으로 대응할 수 있게 한다.

OpenFlow 시스템은 〈그림 2〉와 같이 제어 장치 (Controller)와 OpenFlow 스위치(Switch)로 구성되며, 제어 장치와 OpenFlow 스위치 간에는 보안 채널 상에서 동작하는 OpenFlow 프로토콜에 의해서 스위치 제어 정보가 교환된다. 그리고 OpenFlow 스위치는 패킷을 룩업하고 전달하는 플로우 테이블들과 그룹 테이블로 구성되며, 외부 제어 장치와의 통신을 위한 OpenFlow 채널을 포함한다[4].

OpenFlow 기술은 대부분의 이더넷 스위치와 라우터에서 방화벽, NAT(Network Address Translation), QoS(Quality of Service) 기능 구현을 위해 기존에 사용하고 있는 플로우 테이

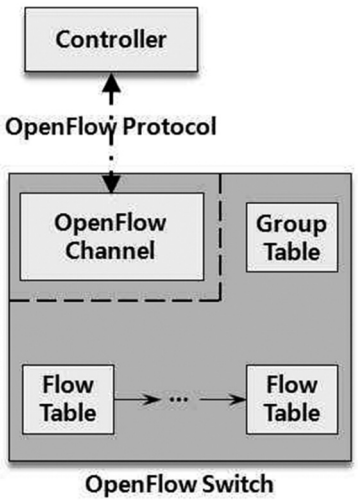

그림 2. OpenFlow 시스템 구성 요소

블에 개방형 프로토콜을 사용해서 프로그래밍할 수 있는 환경을 제공하며 이는 최근에 요구되는 다양한 요구 사항들을 개발할 수 있는 새로운 인터넷 기술 개발 환경을 제공한다.

이에 본고에서는 첫째, SDN 관련 표준화 동향과 업체 동향을 살펴보고, 둘째 OpenFlow 기반의 SDN 구축 시에 데이터 경로를 설계함에 있어서 고려되어야 할 사항들을 여러 서비스 관점에서 제시하고자 한다.

Ⅱ. 관련 연구

SDN 관련해서 한편으로는 ONF, IETF 및 ITU-T 등의 표준화 기구들에서 관련 규격의 표준화 작업이 진행되고 있으며, 다른 한편으로는 가상화, 컴퓨팅 서버 및 네트워크 장비 업체들이 SDN 기술에 대한 연구를 강화하고, 자사 제품에 적용하고 있다. 이에 관련된 연구 동향을 살펴 보고자 한다.

1. 표준화 동향

스탠포드 대학의 주도로 시작된 OpenFlow 기술의 상용화를 촉진시키기 위해서 2011년 3월 비영리 표준화 단체인 ONF(Open Networking Foundation)가 만들어졌다. ONF는 네트워킹 기술을 컴퓨팅 기술로 재해석하고 시장이 요구하는 표준화 및 솔루션을 빠르게 제공하는 것을 목표로 한다.

ONF는 Deutsche Telekom, Facebook, Google, Microsoft, Verizon, Yahoo에 의하여 설립되어 이들 회사들이 이사회 멤버를 이루었으며, 여기에 HP, IBM, Dell, Cisco, Juniper, Brocade, Extreme Networks, Netgear, Riverbed Technology, A10 Networks, VMware, ZTE Corporation, Huawei 등 다양한 ICT(Information and Communications Technology) 글로벌 기업들이 회원사로 참여하고 있다. 아울러 우리나라에서는 SKT, KT, 삼성, 한국전자통신연구원(ETRI)이 회원사로 참여하고 있다.

ONF에서는 Technical WG(Working Group)에서 표준화를 주도하고 있으며, 2010년 OpenFlow 1.0 규격이 나온 이후로 2012년 4월에 1.3 규격까지 완료된 상황이다.

대표적인 국제적 표준화 기구인 ITU-T(ITU's Telecommunication Standardization Sector) 에서는 TSAG(Telecommunication Standardization Advisory Group) 중에서 SG(Study Group) 13에서 SDN을 논의할 예정이다. SG 13에서는 주로 FN(Future Network)과 관련된 주제를 다루고 있으며, 이러한 주제 아래 SDN을 앞으로 다루어야 할 이슈로 지정하여 논의할 계획이다.

IETF(Internet Engineering Task Force)는 2011년 11월에 개최된 제82차 회의에서 SDN(Software Driven Networks) BoF(Birds of a Feather)를 개최하였으며, SDN BoF는 네트워크 장비를 제어하는 소프트웨어와 애플리케이션이 소통할 수 있도록 SDN 관리자(Orchestrator)와 API 등을 표준화하는 것을 목표로 한다. 제1차 SDN BoF 회의에서는 SDN 기술 표준을 추진하기 위한 기술적 이슈와 주문형 대역폭, 데이터센터, 클라우드 서비스 등을 포함하는 활용 사례들이 발표되었다.

제82차 IETF 회의에서는 SDN BoF 뿐만 아니라 VPN4DC BoF, ALTO WG, L3VPN WG, L2VPN WG 등 다수의 새로운 BoF와 기존 WG에서 SDN 관련 기술이 주요 항목으로 다루어졌다[5].

2. 업체 동향

Google은 ONF의 표준화 움직임이 시작되기 전부터 OpenFlow 개발을 시작하였으며, 2010년 자사의 글로벌 데이터센터들을 연결시켜 주는 'G-Scale 네트워크'라는 이름으로 OpenFlow 프로젝트를 시작하였다. Google은 인터넷 및 데이터센터 연결을 위한 2개의 백본망이 있는데 관리에 어려움이 있었으며, 이를 해결하기 위해 중앙 집중화된 네트워킹이 가능한 OpenFlow를 도입했다고 설명하였다. 아울러 OpenFlow 진화에 상당한 투자를 하고 있으며, 수백 명의 엔지니어 인력을 투입하고 있다.

HP는 ONF의 창립 멤버로서 OpenFlow 표준화에 앞장서서, 하드웨어, 소프트웨어, 관리 프로세스 간소화를 통한 네트워크 운영 비용의 감소를 위해 노력하고 있다. 현재 60개 지역의 테

스트베드에 자사의 제품(Procurve 5400)을 판매하고 있는데, 이는 테스트베드 제품의 95%를 차지하고 있다. 또한 HP는 이들 시험 결과들을 반영하여 장비 기능과 성능 개선에 활용하고 있다. 16종의 OpenFlow 지원 상용 스위치를 출시하고 있으며, 곧 FlexNetwork 아키텍처 기반의 모든 스위치로 OpenFlow 지원을 확장할 계획이다.

Big Switch Networks사는 스탠포드 대학에서 OpenFlow 1.0을 개발한 주축 인력들이 설립한 회사로서, OpenFlow 기반 소프트웨어를 개발하고 있으며 2012년 1월에 오픈 소스 기반의 OpenFlow 제어 프로그램인 Floodlight를 발표하였다. 또한 2012년 6월에는 기존 Legacy 스위치/라우터들과 연동성을 제공하는 OpenFlow기반 Overlay SDN을 발표하였으며 현재 8개의 스위치 회사와 7개의 애플리케이션 제어 프로그램을 공동 개발중이다.

NEC는 ONF의 이사회 멤버인 NTT Communications를 고객으로 두고 OpenFlow 연구를 꾸준하고 지속적으로 수행하는 기업으로서 OpenFlow와 Legacy 기능을 혼합한 하이브리드 솔루션인 'ProgrammableFlow'라는 제품을 출시하였다. 국내 업체보다 4-5년은 앞서는 것으로 판단되는 NEC는 이 분야에 더 많은 투자를 계획하고 있다.

Cisco는 ONF의 표준 제정에 동참하고 자사의 데이터센터 장비인 Nexus 시리즈에 SDN을 지원하기 위한 개발에 착수하였음에도 불구하고 OpenFlow 지원에는 소극적인 모습을 보이고 있다. Cisco는 대신에 All Layer API화를 통해 Cisco ONE(Open Network Environment)로 차별화할 것을 강조하고 있다. 즉 경쟁 업체들이 말하는 OpenFlow 기반의 SDN이 아닌 인텔리전트 네트워크가 추가된, 프로그램화 가능한 네트워크로 시장에 접근하고 있다.

이들 상기의 업체 외에도 Pica8은 데이터센터와 클라우드 컴퓨팅 환경에서 사용되는 자사 제품에 OpenFlow 기술을 포함할 계획을 가지고 있으며, 라드웨어는 부하 분산, 보안 정책 등 다양화가 가능한 서비스 지원 플랫폼을 OpenFlow기반으로 지원하는 솔루션을 시연하였다.

Ⅲ. SDN에서 데이터 경로 설계에 대한 고려 사항

본고에서는 SDN망 구축 시에 고려해야 할 여러 가지 사항들 중에서 특히 데이터 경로 설계에 대한 고려 사항을 살펴 보고자 한다. SDN에서의 제어 인터페이스, QoS, 멀티캐스트, 이동성 및 네트워크 보안 관점에서의 고려 사항을 알아 본다.

1. 제어 인터페이스

SDN 구조에서 하나의 제어 장치로 얼마나 많은 네트워크 장치를 관리할 수 있으며, 제어 장치의 성능 문제없이 효율적으로 네트워크 장치를 관리하는 방안에 대한 연구가 진행되고 있다[6].

이를 참고하여 SDN 제어 장치들이 네트워크 장치를 효과적으로 제어하기 위해 고려되어야 할 사항들은 다음과 같다.

첫째, SDN 제어 장치가 몇 개의 네트워크 장치들을 관리할 것인가 하는 확장성이 고려되어야 한다. SDN 제어 장치와 네트워크 장치가 1:1로 동작하면 많은 수의 제어 장치가 필요하게 된다. 반면 하나의 제어 장치가 많은 네트워크 장치들을 관리하면 제어 장치의 성능 및 제어 장치 고장 시에 많은 네트워크 장치들의 관리 부재를 유발한다. 따라서 하나의 SDN 제어 장치로 제어할 수 있는 적절한 네트워크 장치 수에 대한 고려가 있어야 한다.

둘째, 제어 장치와 네트워크 장치 간에 정보 전달의 실시간성이 보장되어야 한다. SDN 제어 장치에서 생성된 플로우 정보는 제어 장치가 관리하는 네트워크 장치에 실시간으로 전달되어 네트워크 트래픽의 전달에 활용되어야 한다. 플로우 정보의 전달에 지연이 발생하면 트래픽 전달에 오류가 발생할 수 있으므로 이에 대한 방안이 고려되어야 한다.

셋째, 제어 장치와 네트워크 장치 간의 플로우 정보 전달을 위한 제어 경로 구성 방안이 고려되어야 한다. 제어 장치와 네트워크 장치 간의 경로는 별도로 구성될 수도 있고, 트래픽 전달을 위한 데이터 경로와 혼용해서 사용할 수도 있다. 만약 제어 경로가 데이터 경로와 혼용해서 사용되는 경우에는 제어 경로의 대역폭을 보장하는 방안이 고려되어야 한다.

마지막으로 SDN 제어 장치의 중단 없는 동작을 위하여 SDN 제어 장치의 이중화 또는 다른 제어 장치로의 이전 메커니즘을 통한 가용성을 확보하는 방안이 고려되어야 한다. 만일 이중화가 된다면 이중화된 제어 장치 간의 동기화 및 절체 메커니즘이 필요하다. 이중화가 되어 있지 않은 경우에는 정상 동작하는 다

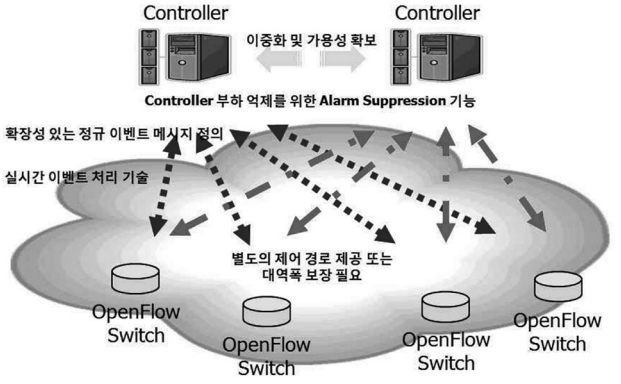

그림 3. M:N 구조의 신뢰성 있는 이벤트 메시지 전달 방안

른 제어 장치가 이상이 발생한 제어 장치를 백업하는 메커니즘이 고려되어야 한다. 〈그림 3〉에 M 개의 제어 장치들이 N 개의 네트워크 장치들을 관리하는 경우의 신뢰성 있는 이벤트 메시지 전달 방안을 제시하였다.

2. QoS

일반적으로, QoS 보장 기술은 단대단 특징을 요구하는 기술로서, 개별적으로 폐쇄형 망을 운용하는 기존 네트워크 환경에서는 그 품질 보장이 어렵다는 특징이 있다.

SDN 기술은 이러한 폐쇄적 망 환경을 개방형으로 탈바꿈시킴으로써, 근 20년 넘게 지속되어온 QoS 보장 관련 문제를 근본적으로 해결할 수 있는 기술로 활용될 수 있을 것이다[7].

본고에서는 SDN에서 단대단 QoS를 보장하기 위해 고려되어야 할 사항들을 다음과 같이 제시한다.

첫째, 각각의 네트워크 장치들에서 제공 가능한 플로우 엔트리 개수의 제약이 고려되어야 한다. OpenFlow 기술은 패킷의 포워딩을 위해 플로우 정보를 사용하며, 하나의 플로우는 12-tuple 정보로 구분된다. 그러나, 플로우 정보의 사용은 패킷 포워딩을 위한 플로우 엔트리 개수가 대폭 증가하는 문제점이 있다[8]. 일례로 12-tuple 사용시 한 가입자 내에서도 적게는 수 개에서 많게는 수십 개의 플로우가 생성될 수도 있다. 이와 같은 경우 가능한 한 많은 플로우 엔트리를 제공하는 것이 중요하지만, TCAM 메모리의 제약으로 인해 한계가 있다. 따라서 일반적인 Best Effort 서비스의 경우에는 소스, 목적지 주소를 기반으로 한 Aggregate 플로우로 관리하여 서비스하는 것이 바람직하며, 품질 보장형 서비스의 경우에는 5-tuple 이상의 헤더 정보를 이용하여 좀 더 세분화된 마이크로 플로우로 관리하여 서비스하는 것이 바람직하다.

둘째, SDN을 구성하는 데 사용되는 네트워크 장치들의 성능 차이로 인한 문제점이 고려되어야 한다. 일례로 OpenFlow 제품군별 지원 가능한 플로우 엔트리의 개수는 Brocade MX 제품의 경우에는 4,000 개까지 지원하지만, NEC PF5820의 경우에는 750 개까지만 가능하다. 〈그림 4〉는 각 제품별로 지원하는 플로우 엔트리 수의 차이로 인해 발생할 수 있는 성능 저하 문제를 단적으로 보여 주고 있으며, OFS #1, OFS #2를 통해 목적지로 가는 모든 트래픽들은 성능 저하 문제를 겪을 수 있음을 나타내고 있다. 이와 같이 SDN을 구성하는 네트워크 장치들의 성능이 다른 경우에는 데이터 경로 설정 시에 지원 가능한 특징(예, 12-tuple 플로우 엔트리 수)을 정확히 파악한 후, 최솟값을 가정하여 데이터 경로를 설정하여야 한다.

셋째, 패킷 손실 이외에 지연 및 지터와 같은 다양한 QoS 파

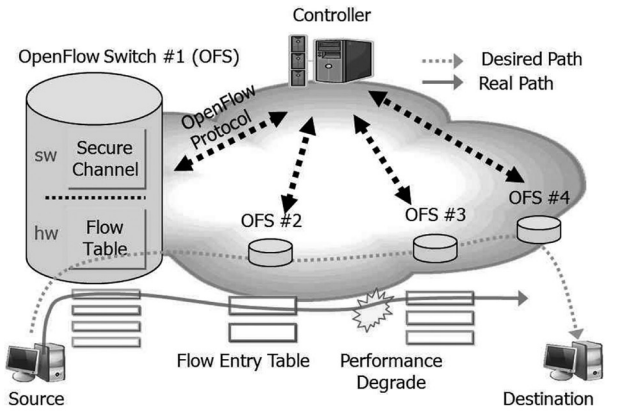

그림 4. 플로우 엔트리 수 차이에 의한 성능 문제

라메터들을 지원하는 방안이 고려되어야 한다. 이를 위해서는 큐잉 기능과 스케쥴링 기능이 함께 제공되어야 하지만, 현재까지는 단순 큐잉 기능만이 제공되고 있다[4][7].

마지막으로 캐리어 망에 적용될 경우에 기본 요구 사항인 50ms의 장애 복구 시간을 만족하는 방안이 고려되어야 한다. 최근의 연구 논문에 따르면 SDN기반으로 캐리어 망을 구축하는 경우에 위의 요구 사항을 만족하기에 어려움이 있다[9].

3. 멀티캐스트

멀티캐스트 기술은 IPTV 방송 서비스, 화상 회의 서비스 등의 고수익 핵심 서비스들의 기반 기술임에도 불구하고 아직도 망 자원 낭비 요소를 많이 가지고 있으며, 망 운용의 복잡성을 제공하고 있다.

기존의 멀티캐스트 방법은 PIM-SM(Protocol Independent Multicast - Sparse Mode) 및 IGMP (Internet Group Management Protocol) 프로토콜의 동작에 의해서 멀티캐스트 트리를 구성한 후 서버에서 가입자로 멀티캐스트 패킷을 전송하는 방법을 이용하는데, 멀티캐스트 트리는 단방향성을 가지므로 망 이용 효율이 떨어지며, 각 노드가 다수 개의 멀티캐스트 패킷을 복사하는 것은 노드의 부하를 증가시키고, 마지막으로 PIM-SM은 망의 안정성을 위협하는 요소가 된다.

이에 OpenFlow 기반의 SDN의 장점을 활용하여 효율적으로 멀티캐스트 서비스를 제공하는 방법에 대한 연구가 진행되고 있다[10].

이를 참고하여 SDN에서 멀티캐스트 서비스를 효율적으로 제공하기 위해 고려되어야 할 사항들은 다음과 같다.

첫째, SDN의 중앙 집중적인 제어 기능을 활용해서 멀티캐스트 전송 경로를 구축하는 방법이 제공되어야 한다. SDN에서는 제어 장치가 네트워크의 구성 정보를 가지므로 PIM-SM과 같은 멀티캐스트 프로토콜의 동작 없이도 멀티캐스트 경로를 구

축하는 것이 가능하다.

둘째, 망 자원의 이용 효율을 향상시키는 방법으로 멀티캐스트를 제공하는 방법이 고려되어야 한다. 기존에는 PIM-SM과 같은 프로토콜의 동작에 의해 트리(Tree) 구조로 구성되었지만, 링(Ring) 구조와 같은 다른 토폴로지를 가지는 멀티캐스트 경로를 구성하는 방법도 가능하다. 〈그림 5〉와 같이 링 구조로 멀티캐스트 트리를 구성할 경우에는 기존의 트리 구조가 단방향성이고 하향 대역폭만을 활용하는 것에 비해 양방향성을 제공하면서 상 · 하향 대역폭을 고루 활용하는 것이 가능하다.

셋째, 망 노드에서 멀티캐스트 트래픽을 적절한 부하를 가지고서 처리할 수 있는 방법이 고려되어야 한다. 기존에 망 노드에서 멀티캐스트 패킷을 복사 및 전달하는 과정은 패킷 처리 부하를 증가시키며, 특히 패킷 복사 개수가 증가하는 경우에 노드의 패킷 처리 성능을 저하시키는 요소가 되었다. 이에 멀티캐스트를 수행함에 있어서 패킷 복사를 최소화할 수 있는 방안이 고려되어야 한다.

마지막으로 멀티캐스트를 수행함에 있어서 QoS 및 장애 탐지 등의 부가 기능이 제공될 수 있는 방안이 제공되어야 한다. 현재의 멀티캐스트 프로토콜은 QoS나 장애 탐지 등의 기능을 제공하지 않는 반면, SDN에서는 중앙 집중적인 제어를 활용해서 QoS가 보장되는 경로를 설정하는 것이 가능하며 링 구조의 멀티캐스트 방법을 제공하는 경우에는 패킷 송신 단말이 최종적으로 멀티캐스트 패킷을 수신하므로 장애 탐지가 가능하다.

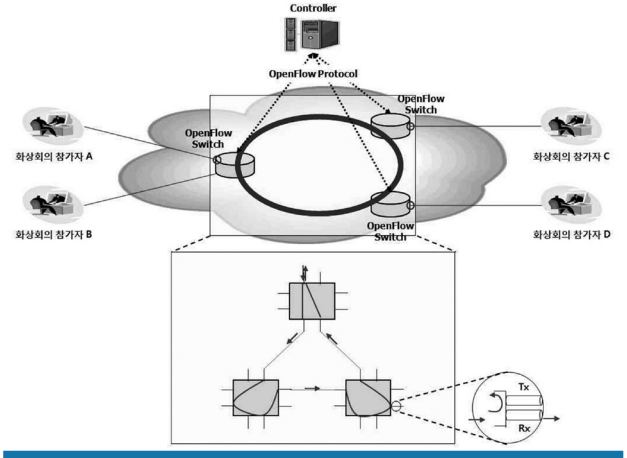

그림 5. SDN에서의 화상 회의 서비스

4. 이동성

이동성 기술은 단말의 이동에도 불구하고 끊김 없는 연결을 제공하기 위한 기술로서 일반적으로 WiFi 기반의 무선랜 상에서 제공되며, 관련 규격은 IETF의 MIPv6(Mobile IPv6), DSMIP(Dual-Stack Mobile IP) 및 PMIP(Proxy Mobile IP) 등이 있다.

기존의 이동성 제공 방법은 단말 또는 단말을 대신한 망 노드가 HA(Home Agent)와 이동에 대한 정보를 교환하는 것에 의해 단말과 HA간에 터널을 생성하며, 단말에게 전달되는 모든 정보가 HA를 통해서 단말에게 전달되도록 하였다.

그러나, 기존의 방법은 단말의 이동에 따른 빠른 경로의 재설정에 어려움이 있었고, HA가 단말로 전달되는 모든 트래픽을 처리해야 하므로 확장성에 문제가 있었으며, 이동성 기능을 제공하기 위해 단말과 관련 망 노드에 다양한 이동성 관련 규격들을 구현해야 하므로 복잡성이 증가하였다.

이에 OpenFlow 기반의 SDN의 장점을 활용하여 효율적으로 이동성 서비스를 제공하는 방법에 대한 연구가 진행되고 있다[10].

이를 참고하여 SDN에서 이동성 서비스를 효율적으로 제공하기 위해 고려되어야 할 사항들은 다음과 같다.

첫째, SDN의 중앙 집중적인 제어 기능을 활용해서 단말의 이동 시에 신속히 경로를 재구성하는 방법이 제공되어야 한다. SDN은 제어 장치가 네트워크의 구성 정보를 가지므로 이동성 프로토콜 없이도 단말까지의 경로를 신속히 재구성하는 것이 가능하다. 또한, 제어 장치에서 데이터 경로만을 설정하므로 HA와 같이 단말로 향하는 모든 데이터를 처리해야 하는 부담도 없다.

둘째, 다양한 무선 인터페이스를 가지는 이동통신망에서의 적용 방법 또는 이동통신망과의 연동 방법이 고려되어야 한다. 현재 이동성 프로토콜은 주로 WiFi 기반의 무선랜 환경을 가정하고 있으며, 이에 SDN에서는 〈그림 6〉과 같은 새로운 서비스의 창출을 위해 다양한 무선 인터페이스 기반의 이동통신망에서의 적용 방법이 고려되어야 한다.

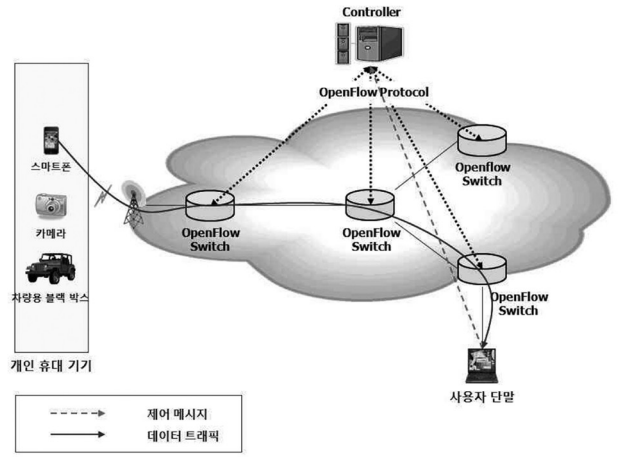

그림 6. SDN에서의 개인 휴대 기기 정보 저장 방법

마지막으로 QoS가 보장되는 이동성을 제공하는 방법이 고려되어야 한다. 특히 다른 무선 인터페이스를 제공하는 이동통신망 간의 이동 시에도 QoS를 최대한 보장해 줄 수 있는 방안이 검토되어야 한다.

5. 네트워크 보안

최근의 DDoS(Distributed Denial of Service) 공격과 관련해서 네트워크 보안의 중요성은 증가하고 있으며, 이와 관련해서 SDN 기반의 네트워크 보안 제공 방안이 연구되고 있다 [11][12][13].

이를 참고하여 SDN에서 네트워크 보안 기능을 제공하기 위해 고려되어야 할 사항들은 다음과 같다.

첫째, SDN 제어 장치와 네트워크 장치 간의 통신을 위한 안전한 보안 메커니즘이 고려되어야 한다. 제어 장치에서 네트워크 장치로 설정된 플로우 정보에 의해 네트워크 트래픽이 전달되므로 올바른 플로우 정보의 전달은 매우 중요하다. 따라서 SDN 제어 장치와 네트워크 장치 간에는 보안이 유지되는 정보 전달 매커니즘이 필요하다.

둘째, 기존 네트워크에서 구축된 DDoS 방어 시스템/침입 탐지 시스템/침입 방지 시스템과 같은 공격 대응 시스템과의 연동 방안이 고려되어야 한다.

셋째, DDoS 공격을 탐지 및 방어하는 방안이 고려되어야 한다. 이와 관련하여 제어 장치에서 네트워크 장치의 통계 정보를 수집하여 공격의 탐지 및 방어를 하는 방안이 있고, 네트워크 장치 내에 DDoS 공격 탐지 및 방어 기능을 구현하는 방안도 있다.

이상의 사항들을 고려한 SDN에서의 네트워크 보안 제공 방법이 〈그림 7〉에 제시되었다.

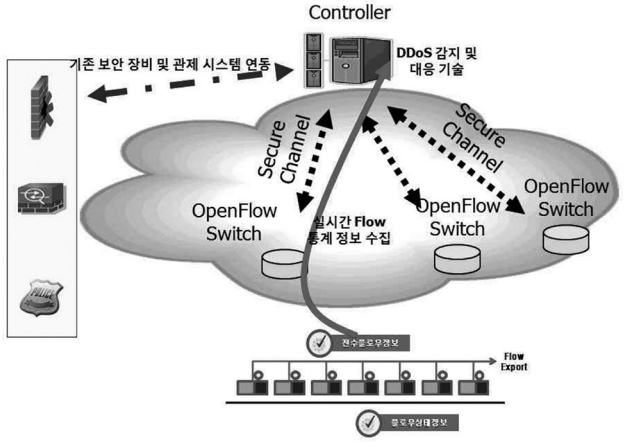

그림 7. SDN에서의 네트워크 보안 제공 방법

이상에서 SDN망 구축 시에 데이터 경로 설계에 대한 고려 사항을 요약하면 〈표 1〉과 같다.

표 1. SDN에서 데이터 경로 설계 시의 고려 사항

기능	고려 사항
제어 인터페이스	• 제어 장치가 관리하는 네트워크 장치 개수에 대한 확장성 제공 • 제어 장치와 네트워크 장치 간의 정보 전달의 실시간성 제공 • 제어 장치와 네트워크 장치 간의 플로우 정보 전달을 위한 제어 경로 구축 방안 • SDN 제어 장치의 중단없는 동작을 위한 가용성 확보 방안
QoS	• 제공 가능한 플로우 엔트리 개수의 제약 해소 방안 • 다양한 성능을 가진 네트워크 장치 간의 연동 방안 • 다양한 QoS 파라메터 지원 방안 • 캐리어 망 적용 방안
멀티캐스트	• SDN의 중앙 집중적 제어를 이용한 멀티캐스트 전송 경로 구축 방안 • 망 자원 이용 효율 향상 방안 • 망 노드 부하 감소 방안 • QoS 및 장애 탐지 등의 부가 기능 제공
이동성	• SDN의 중앙 집중적 제어를 이용한 빠른 경로 재설정 방안 • 다양한 무선 인터페이스 지원 방안 • 이종망간 이동성 제공
네트워크 보안	• 제어 장치와 네트워크 장치 간의 통신을 위한 보안 메커니즘 제공 • 기존의 공격 대응 시스템과의 연동 방안 • DDoS 공격 탐지 및 방어 방안

Ⅳ. 결 론

클라우드 서비스, 네트워크 가상화, 스마트 TV 등의 최근 우리의 일상 생활을 변화시키는 새로운 서비스들은 네트워크 분야의 지원을 요구하고 있으며, 이러한 요구 사항을 만족하기 위해 기존의 폐쇄형 네트워크에서 개방형 네트워크로의 변화가 활발히 연구되고 있다.

개방형 네트워크로 변화하기 위한 방안으로 OpenFlow 기반의 SDN 기술이 주목받고 있으며, ONF를 필두로 IETF, ITU-T 등의 표준화 기구에서 표준화 논의가 활발히 진행중이다. 또한 다양한 업체에서 SDN의 요소 기술과 서비스를 개발 및 적용하고 있다.

이에 본고에서는 이러한 SDN망을 구축함에 있어서, 데이터 경로 설계 시에 고려해야 할 사항을 제어 인터페이스, QoS, 멀티캐스트, 이동성, 네트워크 보안 측면에서 살펴보고, 세부 항목을 제시하였다.

그 중요한 내용을 요약하면, 제어 인터페이스 관련해서는 확장성과 가용성을 고려해야 하고, QoS 관련해서는 플로우 엔트리 개수의 제약과 네트워크 장치 간의 연동성을 고려해야 하며,

멀티캐스트 관련해서는 망 자원 이용 효율, 망 노드의 부하 등을 고려해야 한다. 아울러 이동성 관련해서는 다양한 무선 인터페이스 지원이 고려되어야 하고 네트워크 보안 관련해서는 기존의 공격 대응 시스템과의 연동이 고려되어야 한다.

본고의 고려 사항을 반영해서 SDN망을 구축하면, 새로운 서비스의 요구 사항을 만족하는 개방형 서비스 플랫폼 역할을 담당하는 망 인프라가 구축될 것으로 확신한다.

참 고 문 헌

[1] 윤빈영, 이범철, Dan Pitt, "미래 네트워킹 기술 SDN," 전자통신동향분석, 제27권 제2호, pp. 129-136, April 2012.

[2] ONF, "Software-Defined Networking: The New Norm for Networks," ONF White Paper, April 2012.

[3] ONF, "OpenFlow: Enabling Innovation in Campus Networks," ONF White Paper, March 2008.

[4] ONF, "OpenFlow Switch Specification," ONF Specification, Sept. 2012.

[5] 임용재, 백선경, 김동철, 연승준, "네트워크의 패러다임 전환: OpenFlow," PM Issue Report 2012, 제1권 이슈1, 2012.

[6] Enterasys, "Software Defined Networking(SDN) in the Enterprise," (http://www.enterasys.com / company /literature/SDN_tsbrief.pdf).

[7] Balazs Sonkoly, et al, "On QoS Support to Ofelia and OpenFlow," in Proc. Of European Workshop on Software Defined Networks, pp. 109-113, Oct. 2012.

[8] Pagiamtzis Kostas, Sheikholeslami Ali, "Content-Addressable Memory (CAM) Circuits and Architectures: A Tutorial and Survey," IEEE Journal of Solid-State Circuits, vol. 41, no. 3, pp. 712-727, March 2006.

[9] Dimitri Staessens, et al, "Software Defined Networking: Meeting Carrier Grade Requirements," in Proc. Of IEEE Workshop on Local & Metropolitan Area Networks(LANMAN), Oct. 2011.

[10] KoK-Kiong Yap, Te-Yuan Huang, Ben Dodson, Monica S.Lam, Nick McKeown, "Towards Software-Friendly Networks," APSys 2010, pp. 49-53, August 2010.

[11] Matthew Pascucci, "Software-defined networking: Exploring SDN security pros and cons," (http://searchsecurity.techtarget.com/tip /Software-defined-networking-Exploring-SDN-security-pros-and-cons).

[12] Phillip Porras, et al, "A Security Enforcement Kernel for OpenFlow Networks," HotSDN 2012, pp. 121-126, August 2012.

[13] Rodrigo Braga, et al, "Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow," 35th Annual IEEE Conference on Local Computer Networks, pp. 408-415, Oct. 2010.

약 력

윤 현 식

1993년 경북대학교 전자공학과 공학사
1995년 경북대학교 전자공학과 공학석사
1995년~2000년 LG정보통신 선임연구원
2000년~현재 한국전자통신연구원 책임연구원
관심분야: 네트워크 프로토콜, 이동성 기술, SDN

강 경 순

1998년 원광대학교 컴퓨터공학과 학사
2000년 동국대학교 컴퓨터공학과 석사
2000년~현재 한국전자통신연구원 선임연구원
관심분야: 운영체제, QoS, SDN

김 학 서

1999년 충북대학교 이학석사
2000년~현재 한국전자통신연구원 선임연구원 근무
관심분야: 네트워크 아키텍쳐, QoS, traffic engineering, SDN

박 혜 숙

1992년 경성대학교 전산통계학과 이학사
1994년 부산대학교 전자계산학과 이학석사
2005년 충남대학교 컴퓨터과학과 이학박사
1994년~현재 한국전자통신연구원 책임연구원
관심분야: 네트워크 QoS, 플로우 라우터, 가상사설클라우드 기술