국가연구망의 발전방향 및 차세대 국가연구망 보안

이 명 선*, 조 부 승**, 박 형 우***, 김 현 철****

요 약

최근 광네트워킹 기술의 급격한 발전, SDN (Software-Defined Network) 및 NFV (Network Function Virtualization)로 대두되는 네트워크의 소프트웨어화, 그리고 단순한 고성능연결서비스를 포함한 연구협업을 가능하게 하는 플랫폼으로써의 연구망 등 인터넷 서비스을 포함한 연구망에서는 급격한 변화가 진행되고 있다. 이에 슈퍼컴과 함께 국가과학기술경쟁력을 대표하는 국가연구망의 향후 발전방향을 선진 국가연구망의 비교분석 및 사회가 요구하는 연구망의 역할 변화에 맞추어 조망해본다. 또한 국가연구망 백본의 40Gbps 및 100Gbps급 초광대역 네트워크화, 대용량의 데이터를 고속으로 전송하기 위한 Science DMZ 기반의 망분리, 마지막으로 BRO 기반 프로그래머블 가능한 캠퍼스 네트워크 Lastmile 보안 환경 구축 방안을 제시한다.

Developement Strategy for the National Research Network and Next Generation Network Security

Myoungsun Lee*, Buseung Cho**, Hyoungwoo Park***, Hyuncheol Kim****

ABSTRACT

With repid development of optical networking technology, Software-Defined Network (SDN) and Network Function Virtualization (NFV), high performance networking service, collaboration platform that enables collaborative research globally, drastically National Research Network (NRN) including Internet Service has changed. Therefore we compared and analyzed several world-class NRNs and took a view of future development strategy of the NRN. Also we suggest high speed security environment in super high bandwidth network with 40Gbps and 100Gbps optical transmission technology, network separation of NRN with Science DMZ to support high performance network transmission for science big data, building security environment for last-mile in campus network that supports programmability of IDS using BRO framework.

Key words : Software-Defined Network (SDN), Network Function Virtualization (NFV), National Research Network(NRN), BRO, Science DMZ, Security

접수일(2016년 10월 27일), 게재확정일(2016년 12월 9일)

★ 본 논문은 미래창조과학부 소프트웨어 기반의 첨단과학기술연구망 구축과 서비스 사업에 의하여 연구되었음.

* 한국과학기술정보연구원/첨단연구망서비스실
** 한국과학기술정보연구원/첨단연구망서비스실,. 교신저자(Corresponding author)
*** 한국과학기술정보연구원/첨단연구망서비스실
**** 남서울대학교/컴퓨터학과

1. 서 론

최근 광네트워킹 기술의 급격한 발전, 소프트웨어 정의 네트워크(Software-Defined Network, SDN)로 대두되는 네트워크의 소프트웨어화, 그리고 단순한 고성능연결서비스를 포함한 연구협업을 가능하게 하는 플랫폼으로써의 연구망 등 인터넷 서비스를 포함한 연구망에서는 급격한 변화가 진행되고 있다[1]. 이는 인공지능 혹은 거대과학 연구에서의 빅데이터 처리(대용량 데이터 전송기능 포함)가 요구되는 데이터 집중형과학(Data-Intensive Science)의 출현, 오픈사이언스로 대표되는 과학적 패러다임의 변화 등에서 요구되는 연구망의 역할 또한 변화하고 있다[2]. 특히 국가연구망은 미래 연구 환경인 사이버연구환경을 구현하기 위한 사이버인프라스트럭처의 핵심요소로써, 국가연구망의 전송속도 및 기능 측면에서의 고도화와 함께, 연구데이터에 대한 보안에 대한 요구 또한 지속적으로 증가하고 있으며, 이러한 기술의 발전에 부합하는 보안 기술 및 보안 프레임워크 또한 필요하다.

이에 슈퍼컴과 함께 국가과학기술경쟁력을 대표하는 국가연구망의 향후 발전방향을 선진 국가연구망의 비교분석 및 사회가 요구하는 연구망의 역할 변화에 맞추어 조망해본다. 이에 따른 국가 연구망의 기술적 그리고 사회적 변화에서 연구 데이터의 보안, 연구자의 보안을 위한 차세대 보안 환경에 대해 기술적 요구사항 및 고려사항 등을 알아본다. 본 논문의 2절에서는 각 대륙별 선진 국가연구망에 대한 12가지 부문에 대한 비교 분석을 통해 시사점을 분석해보고 3절에서는 다양한 국내외적인 이슈와 접목하여 국가연구망의 발전방향에 대해 제시한다. 그리고 4절에서는 발전하는 국가연구망에서의 40G/100G 이상으 초고대역폭 연구망에서의 보안, Science DMZ로 대표되는 망분리, 마지막으로 Bro 기반 IDS를 통한 가입자단 보안 환경 구성 등 차세대 보안 이슈 및 고려사항 등을 제시한다.

2. 선진 국가연구망 비교분석

2.1 국가연구망 비교대상 및 비교분석 항목

선진 국가 연구망에 대한 비교분석을 위해 각 대륙별 국가를 대표하는 연구망을 선정함은 물론 현재 연구망의 운영 수준 및 발전 가능성을 토대로 GEANT, APAN, GLIF 등 세계적인 연구망 커뮤니티에서의 선도적인 활동성을 고려하였다. GLORIAD, TEIN 등 글로벌 연구망은 국가연구망에서의 공통적인 비교대상으로 판단할 수 없어 제외하였다.

[표1] 선진 국가연구망 비교 대상

순서	국가연구망	국가/대륙
1	Internet2/ESnet	미국/북미
2	CANARIE	캐나다/북미
3	SURFnet	네덜란드/유럽
4	GEANT	유럽
5	SINET/JGN-X	일본/아시아
6	AARNET	호주/오세아니아

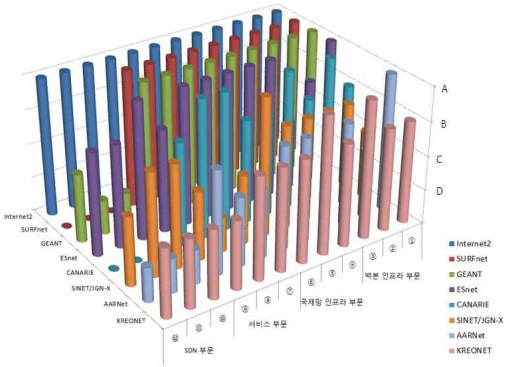
비교대상으로는 크게 국내망 인프라, 국제망 인프라, 서비스, 소프트웨어 정의 네트워크(SDN) 부분으로 진행하되, 아래 표와 같이 총 12개 세부항목을 대상으로 비교 분석 하였다[3][4][5][6][7][8][9][10][11].

[표2.] 선진 국가연구망 비교분석항목

① 광 기반 국내 백본 인프라 수준
② 하이브리드 네트워크 서비스 수준
③ 연구망 트래픽 교류를 위한 유연한 서비스 구현 수준
④ 국제망 인프라 구축 및 유지 수준
⑤ 국제망 연동 수준
⑥ 국제망 서비스 수준
⑦ 연구망 서비스 수준
⑧ 협업 플랫폼 수준
⑨ 연구지원 다양성 수준
⑩ SDN 네트워크 하드웨어 인프라 수준
⑪ SDN 네트워크 소프트웨어 인프라 수준
⑫ 응용/서비스 및 연구협력 수준

22 선진 국가연구망 비교분석 결과 및 시사점

선진 국가연구망을 크게 4개 부문으로 그리고 총 12개의 세부항목으로 비교 평가한 결과, 결과적으로 미국의 연구교육망인 Internet2가 최상위 수준으로 평가되었으며, 국가과학기술연구망(KREONET)은 인프라부문과 서비스부문에 대해서는 전반적으로 최상위 수준의 80%정도에 해당하는 수준으로 평가되었으며, SDN부문은 60%수준으로 나타났다.



[그림 1]선진 국가연구망 비교평가

먼저 국가연구망 백본인프라 부문에서 Internet2, SURFnet, GEANT 등의 경우, 전체 백본에 대한 Dark Fiber를 소유하고 있거나, 5년 이상의 장기적인 임대를 통해 확보함으로써 최근 단일 람다기준 40Gbps/100Gbps급 전송기술을 통해 테라급이상 거의 무한대의 대역폭을 확보함은 물론 하이브리드 네트워크 아키텍처를 기반으로 ESnet의 OSCARS와 같은 온디멘드(On-demand) 동적 대역폭 할당 시스템을 구축하여 운영하고 있다.

국제연구망 백본인프라에서는 ESnet을 비롯한 선진연구망에서는 대륙간 다수의 100Gbps급 국제연구망을 구축함으로 물론 GLIF의 대륙간 람다교환노드 역할을 수행하는 Key GOLE operator로써의 역할을 수행하고 있다[12]. 또한 소프트웨어 정의 네트워크 아키텍처를 토대로 프로그래머블한 국제 연구망의 운영은 물론 국제망에 대한 동적자원할당 시스템을 운영하고 있다.

다음으로 서비스 부문에서는 Internet2, SURFnet 등에서 Internet2 NET+ 등의 클라우드 서비스, InCommon 등의 ID Federation 서비스, perfSONAR등을 기반으로 한 성능측정서비스 등 다양한 응용지원서비스를 제공함은 물론 연구망 중심의 협업 플랫폼을 자체 개발하여 활용하고 있다.

마지막으로 SDN부문의 경우, Internet2 등에서는 100G급 SDN 인프라를 구축하여 프러덕션 기반의 서비스로 제공하고 있으며, 개방형 제어기를 기반으로 한 다양한 응용서비스를 개발하여 운영에 활용하고 있다.

3. 국가연구망 발전방향

3.1 국가 사회구성의 필수적 인프라에 맞는 국가연구망의 지속가능한 성장모델 마련

이미 유럽에서는 GEANT2020, NORDUNET2020 등의 미래 연구망의 비전 및 발전방향으로 국가연구망은 단순히 타분야 및 산업을 돕는 단순한 연구분야의 컴퓨터 네트워크가 아닌 사회를 구성하는 필수 기반 인프라(Communication Common)로써의 역할을 강조하고 부각하고 있다[13][14]. 특히 국내에서는 국가초고성능컴퓨팅육성법 제정(2012)에 의해 국가초고성능컴퓨팅기반서비스체제 구축을 위한 핵심 인프라로써의 국가슈퍼컴퓨터와 국가연구망을 핵심 자원으로 지정하여 과학기술경쟁력을 견인하는 중장기적인 국가 연구 인프라로써의 역할을 강조하고 있다. 또한 최근 광네트워킹 기술의 획기적인 발전을 통한 지속적인 국가연구망 백본의 가속화 그리고 고도화와 더불어 40Gbps/100Gbps 이상의 lastmile 접속, Science DMZ, SDN 등의 최신 기술을 적용한 캠퍼

스 네트워크의 고도화를 통한 국가 연구망 기반의 혁신적인 네트워크 연구 환경이 마련되어야 한다[10].

그러나 국가연구망은 국가슈퍼컴퓨팅 등 타분야에 비해 이미 첨단 네트워크 기술로써 많이 알려지거나 향유하고 있는 기술로 인식되어 새로운 사회적, 기술적, 국가적 이슈화를 하지 못하고 있는 것이 현실이다. 최근 선택과 집중, 단기성과 창출 위주의 정부정책 그리고 국가 R&D 전체 예산삭감 영향으로 점차 국가연구망에 투자되는 예산이 점차적으로 감소 추세에 직면하고 있어, 이러한 어려운 여건을 해소하기 위하여, 지속적으로 고성능화를 위한 국가연구망 인프라의 확충과 더불어 유지보수 비용의 절감 등 효과적인 국가연구망 운영 전략이 필요하다. 즉 총체적인 국가 R&D를 지원하는 지속성장 가능한 국가연구망 성장 모델에 대한 발굴 및 수립이 필요하다.

3.2 국가연구망 이용자 커뮤니티 스스로 지속적 성장 가능한 커뮤니티 지원 및 신규 서비스 개발

최근 유럽연구망 GEANT의 30주년 기념행사에서 10년 후 GEANT의 발전은 현재 GEANT 사용자 커뮤니티 지원을 통해 커뮤니티 스스로 지속적인 생존과 활동을 할 수 있도록 해야 함을 강조하였다. 즉 국가 연구망 커뮤니티의 지속적인 성장은 국가연구망 자체 성장과 직결된다. 국가연구망은 전통적으로 첨단 네트워크 분야의 기술적인 리더십을 핵심가치로 현재까지 추진되고 있으며, 이와 더불어 국가연구망 이용자 커뮤니티 스스로 활성화되어 발전할 수 있는 이용자 정책 개발 및 체계적인 수행이 절실히 필요하다.

전 세계 국가연구망에서는 또한 최근 “Science engagement"를 통한 기존에 국가연구망에 대해 각기 다른 뷰를 가지고 있는 캠퍼스 전산담당자, 보안담당자, 연구자, 네트워크 개발자 등 다양한 국가연구망 관련 당사자 간의 단순한 요구사항의 수집을 통한 지원이 아니라 필요시 연구자의 연구프로세서에 대한 분석 및 이에 대한 지원 등 긴밀한 협업 환경이 요구되고 있다. 이는 대개 국가연구망 백본 운영기관과 국가연구망 가입기관 즉 캠퍼스네트워크 상호간의 동반성장을 통해 인프라 수준의 격차, 기술 수준 격차 등에 대한 해소 또한 필요한 상황이다.

현재 국가연구망 서비스는 기존의 고성능 네트워크 연결형 서비스를 넘어, 4K/8K 이상의 초고화질 기반의 원격화상협업, 통합적 그리고 자동화된 이용자 네트워크 환경 관리 및 네트워크 운영/관리 자동화, 글로벌무선로밍서비스(eduroam) 등의 부가 서비스 확대가 지속적으로 요구되고 있으며, 특히 국가연구망 백본 네트워크와 가입자 네트워크간 lastmile 연동 속도가 기존의 최대 1Gbps/10Gbps에서 40Gbps/100Gbps급 이상으로 초고속화되고 있는 상황에서 초광대역환경에서의 차세대 보안 서비스 및 다양한 보안 이슈에 유연하게 대응 가능한 프로그래머블한 사용자레벨의 보안환경이 필요하다.

3.3 글로벌 연구망 협력체계를 확대하여 연구망 리더 그룹간 파트너쉽 강화

유럽 스위스에 위치한 유럽입자물리연구소(CERN)의 강입자충돌기 (Large Hadron Collider, LHC)에서 발생한 실험데이터를 전세계의 그리드 컴퓨팅자원이 공동협업하여 처리하는 WLCG (Worldwide LHC Computing Grid)에서의 국제 연구망 기반의 협력 활동, 차세대핵융합실험로 국제열핵융합실험로(International Thermonuclear Experimental Reactor, ITER), 한국형핵융합연구로 (Korea Superconducting Tokamak Advanced Research, KSTAR) 등 차세대 핵융합실험로 기반 글로벌 협업연구 등 초소속 국제 연구망을 필요로하는 거대 과학 기술 협업연구는 지속으로 늘어가고 있다. 특히 글로벌 협업 연구에서는 페타급 스케일의 연구데이터의 이동에서부터 엑사급 스케일의 연구데이터의 이동이 요구되어 이를 지원하는 글로벌 연구망의 구축 및 운영협업은 필수적이다.

대표적으로 2005년부터 한국, 미국, 캐나다, 러시아, 중국, 네덜란드, 북유럽 국가 연구망간 협력을 통해 지

국 북반구를 10Gbps급 링으로 국제 연구망을 구성하는 글로리아드 (GLObal RIng network for Advanced Application Development, GLORIAD)가 대표적이며, 현재는 첨단 네트워크 인프라 중심의 글로리아드 협력을 넘어 R&D 응용분야별 글로벌 협업을 위한 중재자/매개체로써의 역할을 수행하고 있으며 이러한 흐름은 가속화될 것으로 예상된다[16]. 특히 기존 글로리아드 참여기관과 기본적인 협력관계를 바탕으로 협력-아젠다의 재구성 및 그 외 글로벌 연구망 기관과 협력 관계 구축 강화를 통해 지속적으로 요구되는 글로벌 연구망에 대한 수요를 대응해야 한다. 특히 글로벌 연구망 세계는 기본적으로 각 국가 연구망의 인프라 그리고 기술적 헌신 (contribution)에 의한 활동이 전제되며,기존 글로리아드 중심의 기술 및 응용의 리더십을 점차 아시아, 중동, 아프리카, 중남미 등 저개발 국가에 대한 리더십 발휘 또한 요구된다.

3.4 클라우드 등 소프트웨어 기반의 플랫폼 서비스가 가능한 소프트웨어 중심 서비스체계로의 전환

국가연구망은 고성능 네트워크 연결성 서비스 제공은 물론 최근 요구되는 클라우드 형태의 소프트웨어 플랫폼에 대한 국가연구망 서비스 추진이 필요하다. 이는 기존 전통적인 하드웨어 중심의 폐쇄적 네트워크 환경에서 점차 개방형 OS를 기반으로 하는 소프트웨어 중심의 개방형 네트워크를 통해 현재보다 개선된 네트워크의 유연성과 확장성을 강화하여 클라우드 등 다양한 소프트웨어 중심의 서비스 요구에 대응 가능한 환경이 필수적이다. 물론 기존의 하드웨어 중심의 국가연구망 인프라의 견고하고 안정된 서비스를 토대로 점차적으로 소프트웨어 기반으로 국가연구망로의 전환이 요구된다. 더불어 소프트웨어 중심의 연구망에서는 기존 하드웨어 중심의 연구망에 비해 망의 안정성을 극대화하기 위한 다중 OS의 클러스터 매커니즘과 같은 다양한 가용성 보장 매커니즘이 적용되어야 하며, 특히 하드웨어 중심의 닫힌 네트워크 환경에 비해 개방형 소프트웨어를 사용함으로써 발생하기 쉬운 보안 위협이 증가될 가능성이 높아 이에 대한 대응방안 또한 마련되어야 한다.

최근 외국은 물론 국내에서도 정부 혹은 민간에서의 클라우드 서비스에 대한 활성화 추진과 함께 보안성 및 안정성이 요구되는 과학기술 빅데이터(Big Data)의 보관, 유통, 접근 등이 용이한 사설 클라우드 환경 마련이 국가연구망의 활용과 더불어 동시에 고려되어야 한다. 이를 통해 국가연구망 기반 통합 서비스 플랫폼으로써의 연구망 서비스 개발이 가능하고, 이는 결국 향후 국가연구망의 CAPEX (Capital Expenditures)와 OPEX (Operating Expenses)에 대한 획기적 절감을 가져올 것으로 예상된다.

3.5 The Fourth Paradigm: Data-Intensive Scientific Discovery 가속화 및 제4차 산업혁명 대응

과학기술 연구방법론 측면에서 경험을 기반으로 한 연구(1000년전)에서 이론을 기반으로 한 연구(수백년전)로 변하였으며, 근현대에 들어 계산과학 연구에서 현재는 데이터집약형 연구기법으로 전환되고 있다. 이는 최근 유럽최대입자연구소의 강입자충돌기에서 발생한 데이터를 기반으로 한 “힉스입자의 발견” 그리고 최근 LIGO (Laser Interferometer Gravitational-Wave Observatory) 실험을 통한 “중력파의 검출” 등이 대표적인 예이다. 이러한 데이터집약형 과학에서의 연구는 과학기술 빅데이터의 집약/모델링, 협업/가시화, 분석/데이터마이닝, 공유 등을 위한 초고성능 빅데이터 전송과 연구패턴에 맞는 빅데이터 처리를 위한 어플리케이션 플랫폼을 필요로 한다. 이를 위해 지난 몇 년간 유럽과 미국에서는 e-science를 지원하는 슈퍼컴과 국가연구망을 포함한 지속가능한 사이버인프라스트럭처(e-infrastructure)의 구축을 지속적으로 추진하고 있다. 이러한 흐름은 고에너지물리분야 뿐만 아니라 차세대에너지원에 대한 연구인 차세대핵융합실

험로 국제열핵융합실험로(ITER)/한국형핵융합연구로(KSTAR) 및 천문우주분야 SKA (Square Kilometre Array) 등 대형 실험 장비에서 발생하는 빅데이터에 대한 초고속 유통이 반드시 요구되며, 단순히 국가연구망 자원을 넘어 슈퍼컴퓨팅, 클라우드컴퓨팅 등 다양한 자원과의 긴밀한 연계 또한 필요로 한다. Open Science 또한 이와 비슷한 움직임으로 데이터에 대한 개방을 통한 접근 그리고 협업을 통한 과학의 흐름을 대변한다고 볼 수 있다.

제1차 산업혁명(기계적 생산, 증기기관), 제2차 산업혁명(대량생산, 전기에너지), 3차 산업혁명(컴퓨터 제어 자동화), 제4차 산업혁명(인공지능, 빅데이터)

또 다른 움직임으로 1차, 2차, 3차 산업혁명은 인간의 손과 발을 기계가 대체하여 자동화를 이룬 반면, 4차 산업혁명은 인공지능의 출연으로 사람의 두뇌를 대체하는 시대에서 빅데이터를 전송하고, 융합과 초연결을 네트워크를 통해 가능하게하고 있다. 또한 다학제적 접근을 기반으로 한 IT, BT, NT의 융합연구는 물론 문화에 이르는 사회전반에 이르는 융합을 통해 새로운 가치를 창조하며, 이에 대한 국가연구망의 역할은 반드시 고려되어야 한다.

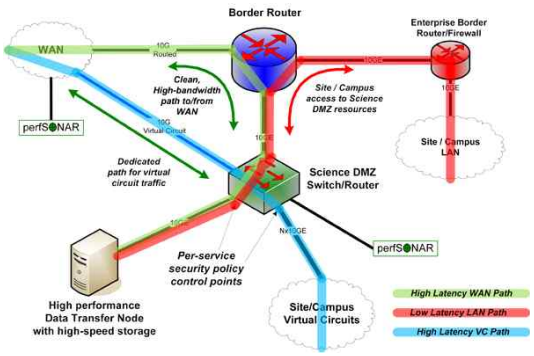
4. 차세대 네트워크 보안 이슈 및 고려사항

4.1 40Gbps 및 100Gbps급 초광대역 네트워크 보안

최근 40Gbps/100Gbps급 이상의 네트워크 고속화와 더불어 이에 대한 침입차단시스템(IDS), 침입방지시스템(IPS), DDOS 차단시스템 등의 보안 장비에 대한 개발이 진행되고 있다. 보통 이러한 고성능 보안장비는 NON-BLOCKING 모드에서 기본적으로 10G*N으로의 CPU 코어별 로드밸런싱(Load-Balancing)을 통해 성능을 구현하고 있다. 이는 10Gbps 이상의 플로우 사이즈가 큰 빅플로우(Elepant Flow)에 대해서는 대응이 불가한 상황이다. 최근 argus 플로우 기반의 40Gbps/100Gbps급 네트워크에서의 passive 기반의 플로우 수집 및 이에 대한 처리 방법이 고안되어 시험을 통해 가능성을 보여주고 있다. argus 플로우는 argus 플로우에 대한 병렬 생성 그리고 클라우드 등 확장 가능한 계산 및 저장 노드를 통해 확장성(Scalibility)를 최대한 높일 수 있는 유연한 구조의 시스템 설계를 통해 가능하다. 특히 PF_RING 등 고속 패킷 캡쳐링을 적용함으로써 손실율없이 패킷을 수집하여 분석할 수 있는 환경이 마련되어야 한다.

4.2 Science DMZ 기반 망분리

Science DMZ의 개념은 캠퍼스 네트워크에서의 일반적인 비즈니스 플로우와 과학기술빅데이터의 고속전송을 필요로 하는 빅데이터 기반 연구 플로우를 구분하여, 해당 특성에 맞는 보안 정책 수립 및 수행을 목적으로 한다. 즉 비즈니스 플로우에 대해서는 방화벽 필요시 웹방화벽 적용 등의 엄격한 보안 정책을 적용하고, 빅데이터 기반의 플로우에 대해서는 ACL 등의 초고속 전송환경에서도 동작 가능한 보안 매커니즘을 적용하는 것이다[17].

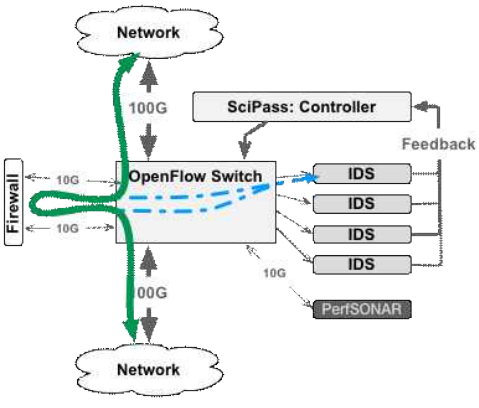


[그림 2] Science DMZ 기본 모델

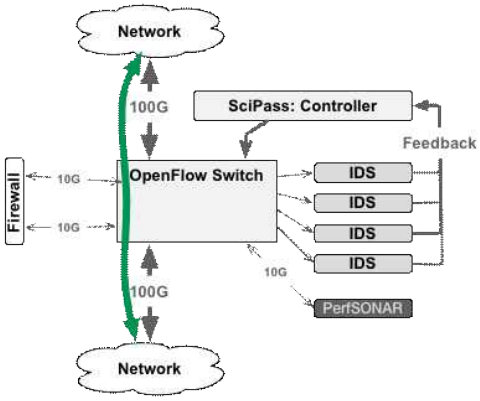
즉 캠퍼스 네트워크에 대해 사용목적에 맞는 망분리를 통해 40Gbps/100Gbps로 고속화되어가는 캠퍼스 네트워크에서의 효율적인 보안 정책을 수립하고 적용하는 것이다. 물론 종단간 이미 신뢰를 기반으로 하는 연결은 가상 회선(Virtual Circuit) 형태로 캠퍼스 네트워크 내부까지 직접 연결한다. 이를 통해 성능이 보장된 네트워크 보안 환경을 구축할 수 있다. 이는 슈퍼컴퓨팅환경, 다중클러스터기반의 클라우드 환경 등 다양한 환경에서 변형 적용 가능한 유연한 구조를 지닌다.

4.3 BRO 기반 프로그래머블 가능한 캠퍼스 네트워크 Lastmile 보안 환경 구축

Bro 네트워크 보안 모니터는 전통적인 IDS와는 차별되는 네트워크 분석 프레임워크로써, 최근 사이버인프라스트럭처에 보안을 위해 다양한 과학 연구에 활용되고 있다. 특히 대학, 연구기관, 슈퍼컴퓨팅센터 및 오픈 사이언스(Open Science) 등 고성능 환경에서 스크립팅 언어로 모니터링 정책 구현은 물론 전통적인 시그너처에 의존하여 특정 행위에 대한 감지뿐만 아니라 유연한 구조로 높은 수준의 시멘틱 분석까지 가능한 프레임워크이다[18][19][20].



[그림 3] 정상 트래픽 플로우를 처리하는 Scipass



[그림 4] 바이패스(bypass)를 수행하는 Scipass

현재 오픈 소스 기반의 개방형 인터페이스를 통해 접근 가능하여 최근 이슈가 되고 있는 SDN과의 결합을 통해 프로그래밍 가능한 보안환경을 구현할 수 있다. 이를 통해 캠퍼스 네트워크에서 발생하는 동적인 보안 환경을 제어할 수 있는 프레임워크를 제공함은 물론 다양한 보안 환경을 확장성있게 구현 가능하다. 현재 Global NOC 등에서 진행되고 있는 Scipass 프로젝트 등에서 Science DMZ에서 동작하는 방화벽을 동적으로 제어가능하게 함은 물론 확장성을 제공하여 100Gbps에 이르는 고대역의 네트워크 환경에서도 동작가능하게 구현 가능하다.

단, 추가적인 고려사항으로 OpenFlow 기반의 SDN 스위치가 연구망 백본과 연동된 캠퍼스 네트워크의 경계라우터(Border Router) 앞단에 위치해야 경계라우터의 부하를 Scipass를 통해 줄여줄 수는 있다. 이 경우, 고성능 OpenFlow 스위치의 가용성이 보장되어야 캠퍼스 네트워크 백본 전체의 안정성을 보장할 수 있으며, 이를 위해 SDN 스위치의 이중화 및 제어기를 이중화 등이 추가적으로 고려되어야 한다.

5. 결 론

본 논문에서 네트워킹 기술의 급격한 발전과 함께, 리를 토대로 데이터집중형과학을 지원하는 선진 국가연구망의 비교분석을 토대로 국가연구망의 발전방향

을 제시하였다. 또한 초고속화, 글로벌화, 소프트웨어화 및 플랫폼화 되어가는 국가연구망의 차세대 보안 환경에 대해 제시하였다. 국가연구망 백본의 초광대역화에 따른 초고속 보안 솔루션이 필요로 하지만 최근 Science DMZ 기반 망분리 및 BRO를 토대로 한 캠퍼스 네트워크 즉 사용자 네트워크에서의 보안 환경이 필수적으로 요구되며, 이에 대한 대응이 필요하다.

참고문헌

[1] McKeown, Nick, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. "OpenFlow: enabling innovation in campus networks." ACM SIGCOMM Computer Communication Review 38, no. 2, 2008

[2] Tony Hey, Stewart Tansley, Kristin Tolle, The Fourth Paradigm: Data-Intensive Scientific Discovery“, Microsoft Research, 2009.10.16

[3] Internet2, http://www.internet2.edu/

[4] ESnet, http://es.net/

[5] CANARIE, https://www.canarie.ca/

[6] SURFnet, https://www.surf.nl/

[7] GEANT, http://www.geant.org/

[8] SINET, https://www.sinet.ad.jp/

[9] JGN-X, http://www.jgn.nict.go.jp/

[10] AARNET, https://www.aarnet.edu.au/

[11] KREONET, http://www.kreonet.net/

[12] GLIF, http://glif.is/

[13] GEANT Expert Group, “Knowledge without Borders-GEANT2020 as the European Communications Commons“, European Commission, 2011.10

[14] NORDUnet, “The Role of NREN's in 2020”, 2011

[15] Inder Monga, Eric Pouyoul, Chin Guok, "Software-Defined Networking for Big-Data Science - Architectural Models from Campus to the WAN“, 2012 SC Companion: High Performance Computing, Networking, Storage and Analysis (SCC), 2012

[16] Kwangjong Cho, SeongHae Kim, HyeakRo Lee, “GLORIAD-KR and Its Advanced Applications”, 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT), 2010

[17] Dart, Eli, Lauren Rotman, Brian Tierney, Mary Hester, and Jason Zurawski. "The science dmz: A network design pattern for data-intensive science." Scientific Programming 22, no. 2, 2014

[18]Edward Balas, AJ Ragusa, “SciPass: a 100Gbps capable secure Science DMZ using OpenFlow and Bro”, Supercomputing 2014 conference (SC14), 2014

[19] SciPass https://github.com/GlobalNOC/SciPass

[20] Vern Paxson “Bro: A System for Detecting Network Intruders in Real-Time” Computer Networks, 31(23-24), pp. 2435-2463, 1999

[著者紹介]

이 명 선 (Myungsun Lee)
1982년 2월 아주대학교 전자공학 학사
1996년 8월 한남대학교 컴퓨터공학 석사
2005년 2월 한남대학교 컴퓨터공학 박사
email : mslee@kisti.re.kr

조 부 승 (Buseung Cho)
2000년 2월 성균관대학교 전기전자 및 컴퓨터공학 학사
2002년 8월 균관대학교 전기전자 및 컴퓨터공학 석사
email : bscho@kisti.re.kr

박 형 우 (Hyoungwoo Park)
1981년 2월 서울시립대학교 전자공학 학사
1994년 2월 성균관대학교 정보통신공학 석사
1997년 2월 성균관대학교 정보통신공학 박사
email : hwpark@kisti.re.kr

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