

다중위성운영을 위한 네트워크 구성 방안 연구

백현철¹ · 장인식² · 이상정^{3,†} · 김병철³ · 이재용³¹한국항공우주연구원²(주) AP위성³충남대학교

Network Configuration Study for Multi-Satellite Operations

Hyun Chul Baek^{1,†}, In Sik Jang², Sang Jeong Lee³, Byung Chul Kim³, Jae Yong Lee³¹Korea Aerospace Research Institute²Asia Pacific Satellite Incorporated³Chungnam National University

Abstract

Integration of satellites with diverse missions, such as broadcast-communication, earth, meteorological and marine observations, and navigation, is vulnerable. The problems of the currently constructed ground station network were analyzed by constructing the test environment. Based on this, we designed a network that was capable of operating multiple satellites by one ground station. In addition, we proposed an interface and network configuration method with domestic and foreign ground stations. The network linking the domestic and foreign ground stations was composed of KREONET (Korea Research Environment Open Network) and GLORIAD (Global Ring Network for Advanced Application Development) of the KISTI (Korea Institute of Science and Technology Information). The internal network consists of VPN (Virtual Private Network), DMZ (De-Militarized Zone), and 1-way USB and so forth. By constructing the network by using the proposed method, harmful data, such as virus inflow and infection, can be blocked.

초 록

방송·통신, 지구관측, 기상관측, 해양관측, 그리고 항행 등 서로 다른 임무를 가지고 있는 위성들을 통합 운영하는 것은 보안에 취약하다. 현재 구성된 지상국 네트워크의 문제점은 시험 환경을 구축하여 분석하였다. 이를 바탕으로 하나의 지상국에 의해서 여러 개의 위성을 운영할 수 있는 네트워크를 설계하였다. 또한, 국내외 지상국과의 인터페이스 및 네트워크 구성방안을 제안하였다. 국내외 지상국과 연동하는 네트워크는 국가과학기술연구망과 글로벌과학기술협업연구망으로 구성하였다. 내부 네트워크는 방화벽, 가상사설망, DMZ, 1-way USB 등으로 구성하였다. 제안된 방법으로 네트워크를 구축하면 바이러스 유입 및 감염 등 유해 데이터를 차단할 수 있다.

Key Words : Multi-Satellite Operation(다중위성운영), Security Network(보안네트워크), Virtual Private Network(가상사설망), 1-way USB System(단방향 USB 시스템)

1. 서 론

저궤도위성의 특성상 한반도에 위치한 지상국은 공간적, 시간적 제약을 극복하기 위해 해외에 위치한 지

상국을 활용하여 위성에 명령을 전송하거나, 위성의 영상을 수신하고 있다. 또한, 정지궤도 위성도 초기 운영 및 거리 측정 등의 목적으로 해외지상국을 활용하고 있으며, 달 탐사를 위해 심우주 네트워크(DSN; deep space network)와 연계하여 임무 수행을 준비하고 있다. 하지만, 위성이 많아지고, 임무가 다양하고 복잡해질수록 체계적인 네트워크 구성과 관리가 필수적으로 요구된다. 특히 방송·통신, 지구관측, 기상관측,

Received: Jul. 30, 2018 Revised: Jun. 20, 2019 Accepted: Jul. 09, 2019

† Corresponding Author

Tel: +82-42-821-6582, E-mail: eesjl@cnu.ac.kr

© The Society for Aerospace System Engineering

해양관측, 그리고 항행까지 서로 각기 다른 임무를 가지고 있는 위성들을 하나의 네트워크로 구성하는 것은 관리와 보안 측면에서 어려움에 직면할 수 있으므로 어떻게 하면 효율적으로 네트워크를 구성하고, 관리할 것인가에 대해 충분한 분석이 필요하다. 이를 위해 세계 주요 우주 운영기관들의 네트워크 현황을 살펴보면, 미국항공우주국(NASA; National Aeronautics and Space Administration) 네트워크는 근지구 네트워크(NEN; near Earth network), 우주 네트워크(space network), 그리고 심우주 네트워크(DSN)로 구분하고, 이를 통해 100개 이상의 우주 임무를 지원하고 있고, 유럽우주기관(ESA; European Space Agency)은 기관 소속의 10 여개 지상국과 계약을 통한 전 지구적 네트워크를 구축하여 운영하고 있다. 이와 같이 해외 우주운영 기관들은 기관 소유의 지상국, 계약을 통한 상용 지상국 활용, 그리고 기관 간의 협업을 통한 상호 지상국 활용을 위해 전 지구적 네트워크(global ground network)를 구축하여 운영하고 있다[1,2]. 이에 본 논문에서는 현재 구성된 지상국 네트워크의 문제점을 도출하고, 시험 환경을 구축하여 분석하였다. 이를 바탕으로 국가 우주개발 계획에 따른 국내 위성 수요에 부합할 수 있도록, 하나의 지상국에 다중 위성운영을 위한 네트워크 설계와 국내·외 지상국과의 인터페이스 및 네트워크 구성을 제안하였다.

2. 국내·외 네트워크 구성 방안

2장에서는 국내의 지상국과 관제 및 탑재체 데이터 인터페이스를 위한 구성요소를 서술하였고, 가상사설망과 첨단연구망 활용방안에 대해서 기술하였다.

2.1 관제데이터 네트워크 인터페이스

위성을 발사하여 초기 안정화 및 성능 검증을 수행하는 과정에서 국내 지상국 이외에도 해외 지상국을 활용해야 하므로 네트워크 성능을 최적 상태로 유지할 수 있도록 설계하는 것이 중요하다. 저궤도위성 S-Band를 기준으로 살펴보면, 위성으로 전송되는 명령은 가변적인 대역폭 2 Kbps ~ 4 Kbps를 가지며, 위성의 상태데이터는 2.048 Kbps, 4.096 Kbps를 가지므로

국내외 지상국과의 네트워크 전송대역폭은 최소 64 Kbps를 가져야 한다[3]. 위성 발사 초기 안정화의 중요성을 고려한다면, 네트워크 안정성이 가장 좋은 전용회선을 활용하여 구축하는 것이 가장 합리적이다. 전용회선은 하루 24시간, 1년 365일 동안 100% 성능을 유지하기 때문에 안정성은 높은 반면, 상대적으로 고가이므로 초기 운영 기간을 제외하고는 사용을 제한한다. 이를 보완하기 위해 안정성과 비용 대비 효율성이 높은 ISDN(integrated service digital network)으로 백업회선을 구축할 수 있지만, 기존 가입자만 서비스를 제공해 주고, 신규 가입을 더 이상 받지 않기 때문에 추가적으로 사용하기 어렵고, 가까운 미래에 서비스 제공을 하지 않을 것으로 예상된다. 이를 대체하기 위해 가상사설망(VPN; virtual private network)을 기반으로 인터넷망을 활용한 백업라인을 구축하여 운영하는 것이 바람직하다. Figure 1은 전용회선, 백업회선, VPN 등을 이용한 관제데이터의 네트워크 인터페이스 구성도를 나타낸다. 각각의 회선은 방화벽을 통해 지상국과 데이터를 주고받는다.

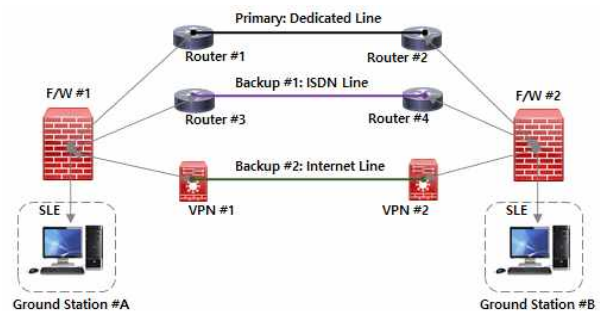


Fig. 1 Control data network interface

2.2 영상데이터 네트워크 인터페이스

위성 발사 후 안정화 단계를 지나면, 위성 탑재체의 데이터를 수신하고, 활용하는 방안에 대해서 고려해야 한다. 탑재체 중에서 대용량의 저궤도위성 X-Band를 활용한 위성영상은 RHCP(right-handed circular polarization)/LHCP(left-handed circular polarization) 2대의 편파와 I 채널 및 Q 채널을 활용하여 640 Mbps의 데이터를 전송하고 있다[4]. 실시간으로 위성영상 데이터를 처리 및 전송하기 위해서는 최소 네트워크 대역폭이 640 Mbps보다 넓어야 하고, 위성영상을 수신

하는 안테나에서 수신시스템까지 광케이블 혹은 Cat.5e 이상의 네트워크 케이블(1 Gbps 지원)로 연결해야 한다는 것을 의미한다. 하지만, 해외 지상국의 경우 640 Mbps의 전송로를 확보한다는 것은 비용 대비 효율성 등을 고려하면, 쉬운 문제가 아니다. 이를 위해 저궤도위성의 경우 해외 지상국을 통해 위성영상을 수신하고, 전송하기 위해 45 Mbps의 전송로를 활용하고 있는데, 이는 저궤도위성이 지구를 1회 선회할 때 약 95분으로 산정하고, 위성영상데이터를 7분 다운로드 하였을 때 다음 교신이 이루어지기 전까지 처리 및 전송할 수 있는 시간을 고려한 최적의 설계를 수행한 것이다. 하지만 45 Mbps 전용회선을 구성한다는 것은 비용 대비 효율성이 떨어져 구축 및 사용하기 힘든 실정이다. 그래서 효율적인 가상사설망을 활용한 인터넷 망으로 45 Mbps의 네트워크를 구성하였으며, 소프트웨어인 고성능파일전송솔루션(ASPERA)를 활용하여 전송 대역폭을 보장하고 있다.

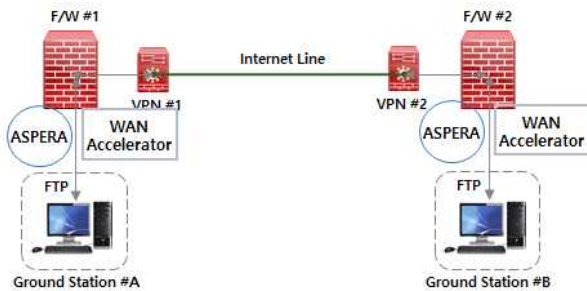


Fig. 2 Payload data network interface

고성능파일전송솔루션은 패스프 프로토콜(FASP; fast and secure protocol) 기반으로 기존 인프라를 활용하여 FTP(file transfer protocol), HTTP(hyper text transfer protocol) 그리고 Window CIFS(common internet file system)과 같은 전통적인 파일 전송 기술을 사용하여 파일 전송 시 발생하는 병목현상을 제거한다. 또한, 파일 용량, 전송 거리, 네트워크 상태에 관계없이 대용량 데이터를 전송할 수 있는 최적의 솔루션으로 열악한 네트워크 환경 하에서도 대역폭 제어와 보안·안정성을 강화해주는 역할을 한다. 국내외 지상국과 고속대용량 네트워크를 구성할 때, 소프트웨어 기반을 고성능파일전송솔루션과 하드웨어 기반의 WAN 가속기(wide area network

accelerator)를 활용하는 방법으로 네트워크를 구축할 수 있다[5]. Figure 2는 ASPERA 소프트웨어를 사용한 지상국간 영상데이터 네트워크 인터페이스이다.

2.3 가상사설망(VPN; virtual private network)

1999년 12월에 다목적실용위성 1호를 발사하는 시점에서 국내의 지상국 네트워크 구성은 64 Kbps의 전용회선과 ISDN을 활용하는 것이 최적의 솔루션이었으나, 2018년 현재 전용회선을 활용하여 해외 지상국과 연결하는 것은 안정성이 최우선인 S-Band 통신에 국한되고 있다. 위성영상과 같이 대용량 데이터를 고속으로 전송하기 위해서는 전용회선을 사용하는 것보다 인터넷을 활용하는 것이 이상적이지만, 위성영상은 보안이 요구되므로 제약사항이 발생한다. 이를 만족하기 위해 가상사설망을 활용하면, 보안 및 안정성을 확보할 수 있다.

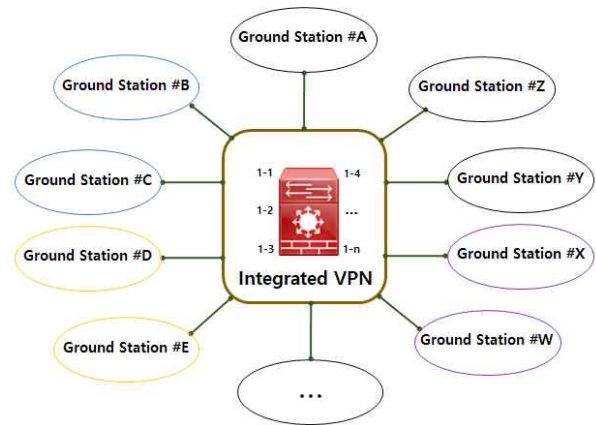


Fig. 3 Virtual Private Network modularization

가상사설망은 일반 인터넷망을 터널링 방식으로 구성하여 마치 내부 사설망 혹은 전용선 같이 이용하는 방식으로 IP Sec(internet protocol security)과 SSL(secure socket layer)을 이용하여 데이터를 처리한다. 암호화는 128 Bits의 평문(암호문) 블록을 암호(복호)화하여 동일한 길이의 암호문(평문)을 만드는 대칭키 방식의 블록암호 알고리즘인 ARIA(Academy & Research Institute & Agency)와 AES(Advanced Encryption Standard)를 주로 사용하고, 키 길이와 라운드 변환은 ARIA 128 Bits, 192 Bits 및 256 Bits에 12회, 14회 및 16회 그리고 AES 128 Bits, 192 Bits 및 156 Bits에 10회, 12회 및 14회를 수행한다. 암호 알고리즘과 키 길이에 따라 보안 등급이 달라지므로 보안

측면에서는 유리하지만, 역설적으로 높은 수준의 암호화는 전송 및 처리속도 저하를 가져온다. 이를 개선하기 위해 성능이 좋은 장비를 사용해야하며, 각 위성별 요구되는 전송 속도를 만족하면서 암호화 수준을 높이는 방법으로 최적화가 필요하다.

또한, 초기 가상사설망을 구축할 때는 1 : 1의 개념을 적용하였으나, 시간이 지남에 따라 가상사설망을 활용해야 하는 국내·외 지상국의 증가로 1 : N의 모듈식 개념을 적용하여 구성하는 것이 가장 효율적인 방법이다. Figure 3은 여러 지상국을 연결하는 VPN을 모듈화 한 것으로 모듈화 VPN 구성할 경우 고려사항은 가상사설망의 안정화 및 관리 효율성을 위해 이중화 시 가능한 동일 밴더사의 제품으로 구성해야 한다. 이는 동일한 설정 값을 갖는데도 다른 밴더사의 제품과는 호환이 되지 않는 경우가 종종 발생하여 문제가 발생 하는 것을 사전에 대비하기 위한 것이다.

2.4 첨단 국가과학기술연구망

한국과학기술정보연구원(KISTI; Korea Institute of Science and Technology Information)에서는 수요자 중심의 과학기술정보자원 구축 및 관리를 위해 국가과학기술연구망(KREONET; Korea Research Environment Open NETWORK)과 글로벌과학기술협업연구망(GLORIAD; Global Ring Network for Advanced Application Development)을 구축하여 국가 차원의 첨단정보인프라를 활용한 연구개발 업무를 지원하고 있다[6].

KREONET은 IP 네트워크와 광전용 사설 네트워크(optical private network)를 통한 하이브리드형 네트워크 환경을 제공하며, 다중 장애 대비, 다중 경로 구성이 가능한 “Mesh & Several Ring”으로 망을 구성하여 운영 중에 있다. 또한, 네트워크 장비로 유입되는 패킷이 올바른 물리적 포트로 출력될 수 있도록 경로를 설정, 관리 및 해제하는 기능의 “L1 Control Plane” 기술적용하고 있고, 다중 장애 극복, 네트워크 관리자를 위해 복잡한 네트워크 구성 변경이나 장비들의 이동하지 않아도 다른 포트들로부터 트래픽을 받을 수 있게 설정을 할 수 있는 “Any to Any” 서비스를 제공한다. 그리고 모든 노드에서 과장을 식별할 수 있는 관 기반 운영 관리 툴인 “Wavelength Tracker” 기능으로 전 구간 광 품질 추적, 관리, 운영이 가능한

회선 운영 기술을 적용하여 대용량 데이터의 고속 전송을 요구하는 사용자에게 최적의 네트워크 성능을 제공한다. KREONET은 연구용의 인터넷망을 제공하는 범용연구서비스망과 통신사업자가 제공하는 전용회선 개념의 첨단연구서비스망으로 구분할 수 있고, GLORIAD망은 한국, 미국, 중국, 러시아, 캐나다, 네덜란드, 북유럽 5 개국 등 15 개국이 공동으로 참여하여 지구를 10 G급 환형 광 네트워크로 연결하는 글로벌 연구망으로 전 세계 80여 개국 27,700개의 네트워크를 직접 연동하여 글로벌 협업 환경을 지원한다. 현재 해외 지상국과의 데이터 송·수신을 위해 KREONET과 GLORIAD를 사용 중에 있다. Figure 4는 KREONET과 GLORIAD의 협업 연구망을 나타내고 있다.



Fig. 4 National Science and Technology Research Network of KISTI

3. 지상국 내부 네트워크 구성 방안

3장에서는 다중위성운명을 위해 지상국 내부 네트워크를 위한 서버 팜, 단방향 USB 시스템, DMZ 등 구성요소에 대해서 서술하였다.

3.1 망형 토폴로지를 활용한 네트워크 구성

방송·통신, 지구관측, 기상관측, 해양관측, 그리고 항행까지 서로 각기 다른 임무를 가지고 있는 위성들을 하나의 네트워크로 구성하는 것은 운영, 관리 및 보안 측면에서 비효율적이다. 또한, 위성운영에 필수적인 시스템들을 가상화를 통해 대폭 감소시켰지만, 여전히 많은 수의 시스템이 운영되고 있다. 이와 같이 많은 시스템 구축을 위해 L2급 스위치를 활용하여 가상랜

(VLAN; Virtual LAN)으로 나누어 현재 운영 중에 있는 지구관측위성들과 운영 준비 중인 저궤도위성 및 정지궤도위성들을 하나의 네트워크에 하위로 다수의 네트워크를 구성하는 것이 효율적일 수 있다. 또한, 여러 개의 스위치를 하나로 그룹화하여 논리적으로 하나의 스위치(L2/L3)처럼 동작할 수 있는 버추얼 새시(virtual chassis; 마치 물리적으로 하나의 새시와 같이 논리적인 기능을 제공하여 스위치 상호 간에 하나의 구조로 결합 시켜주는 프로토콜)를 적용하여 대역폭 확장 및 안정적인 백업을 구성할 수 있다.

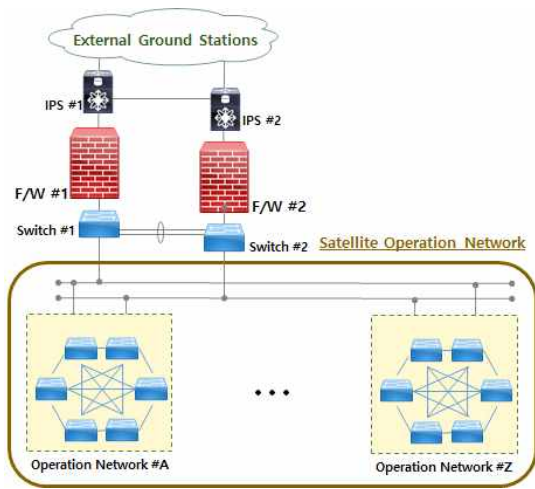


Fig. 5 Mesh network configuration for multi-satellite operation

또한, 위성운영 네트워크를 POD(plain old data) 기반 망형(mesh) 형태로 구축하면, 물리적 연결에 구애받지 않고, 네트워크 최적 경로로 트래픽 라우팅과 지연 시간이 짧은 “Any to Any” 연결이 가능하여 다중위성운영 네트워크 관리 측면에서 유연하게 적용할 수 있고, 기민한 대응과 비용 최소화를 실현할 수 있다는 장점을 가질 수 있다. Figure 5는 다중위성운명을 위해 각 위성마다 운영 시스템을 분리하고, 위성운명을 위한 지상국 내부 네트워크 구성은 망형 토폴로지 형태로 구성한 그림이다.

3.2 서버 팜 구성

다중위성을 운영하면 위성별 상태 데이터와 전송 명령, 그리고 영상 데이터 등 대용량 데이터가 산출된다. 이를 효율적으로 관리하기 위해 데이터 서버 혹은 스

토리지와 같은 대용량 데이터 저장장치가 요구되는데, 이를 각각의 위성마다 데이터 서버와 스토리지를 구성할 경우 유지·관리에 많은 비용과 노력이 필요하게 된다. 이를 개선하기 위해 서버 팜을 구성하여 데이터 서버와 스토리지 등을 구축하여 다중위성의 데이터들을 저장하는 것이 관리 측면과 비용 측면에서 효율적인 방법이다. 결과적으로 다중위성운영 네트워크와 분리하여 집단화된 서버 그룹을 구성하고, 이를 기반으로 각 데이터 서버들 중 어떤 데이터 서버의 서비스가 중단되더라도 다른 데이터 서버가 즉시 대체할 수 있도록 구성하여 서비스 중단을 막을 수 있어 데이터 서버의 안정화에 유용하다. Figure 6은 위성운영 네트워크와 별도로 구성된 서버 팜을 나타낸다.

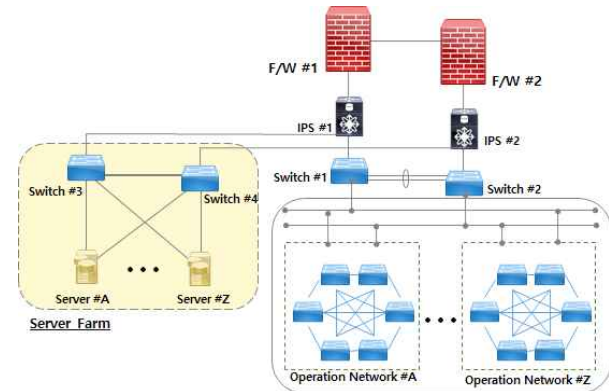


Fig. 6 Configuration of server farm

3.3 단방향 USB 시스템 구성

위성을 운영하는 네트워크는 일반 사용자가 접근할 수 없는 단독망으로 구축하여 폐쇄적으로 운영하고 있다. 또한, 운영을 위해 필수적인 프로그램을 제외하고, MS Office, 한글 등과 같은 다른 응용 프로그램도 설치를 제한하고 있다. 이는 일반 사용자에 의한 데이터의 무분별한 입·출입 방지, 프로그램의 취약점 및 악성코드를 이용한 해킹, 바이러스 유입 방지 등 보안을 강화하기 위한 방법이다. 그러나 다중위성을 운영하는 과정에서 발생할 수 있는 데이터 처리를 위해서 폐쇄망에 접근하여 데이터를 반출해야 한다. 이를 위해 인가된 USB(universal serial bus)와 2 가지 이상의 바이러스 검출 소프트웨어를 활용하는 등 다양한 방법을 취하고 있지만, 악성코드나 바이러스 등이 유입될 수

있는 구조적 한계를 가지고 있다. 이를 극복하기 위해 외부로부터 바이러스 등으로부터 안전하고, 내부의 데이터를 보다 쉽게 반출할 수 있는 단방향 USB 시스템을 활용하여 폐쇄망의 데이터를 사용자망으로 전송하여 데이터를 분석하고, 활용할 수 있도록 구성할 수 있다. 서버의 보안은 방화벽 설치로 인가되지 않은 사용자와 장치에 대한 접근을 차단하고, 안티 바이러스 소프트웨어를 설치하여 바이러스 및 악성 프로그램의 서버 감염을 차단한다. 소프트웨어는 주기적으로 업데이트를 수행하고, 서버 로그 관리를 통해 인증되지 않은 사용자 및 장치의 접근 여부를 식별하고, 데이터에 대한 보안 강화를 위해 파일 형태의 전송이 아닌 암호화된 패킷 형태로 전송한다. 서버와 단방향 USB 시스템의 전송 포트는 범용 포트가 아닌 임의의 포트 선정하고, ID 인증 방식을 통해 인가된 사용자에게만 데이터를 전송할 수 있도록 보안을 강화하여 운영의 안정성 및 효율을 증대시킬 수 있다[7,8]. Figure 7은 단방향 USB 시스템의 구성으로 각 서버에는 인증을 위한 별도의 프로그램과 안티바이러스 프로그램을 설치하고, 시스템이 설치된 장소에는 시건장치 등의 물리적 보안으로 단방향 시스템은 인가되지 않은 사람이 접근하지 못하도록 구성해야 한다.



Fig. 7 Configuration of 1-way USB system

3.4 DMZ을 포함한 방화벽 구성

방화벽은 신뢰 수준이 서로 다른 네트워크 구간들 사이에 위치하여 신뢰 수준이 낮은 네트워크로부터 오는 해로운 트래픽이 신뢰 수준이 높은 네트워크로 오지 못하도록 막는 역할을 수행한다. 네트워크 관리자 입장에서 높은 신뢰도를 갖는 구간은 내부 네트워크 구간이고, 낮은 신뢰도를 갖는 구간을 인터넷 구간 또는 외부 네트워크 구간이라 볼 수 있다. 이중화된 방화벽을 구축하고, 해외지상국과 연동하기 위한 전용선 구간과 인터넷 구간을 구분하여 각각 라우터와 IPS(intrusion prevention system), 가상사설망 등을

거처 방화벽으로 연결하도록 구성해야 한다. 이는 인터넷을 통해 유입되는 바이러스 혹은 유해 데이터를 차단하여 다른 해외지상국에 영향을 미치지 않도록 해야 하고, 다중위성운영 네트워크는 방화벽 내에서 자유로이 데이터를 제공할 수 있도록 해야 하며, 확장성을 고려하여 구성해야 한다. 또한, DMZ(Demilitarized Zone)을 통해 내부 네트워크와 외부 네트워크 사이에 서브넷을 구성하여 외부 네트워크에서의 침입으로부터 내부 네트워크를 보호하고, 서버의 경우도 각각의 망에 단독으로 구성하기 보다는 서버 팜을 통해 서버들을 구성하고, 적절한 서버를 통해 다중위성데이터를 저장 및 백업하도록 설계하면, 향후 발사될 위성들의 데이터 저장 공간도 확보할 수 있어 효율적인 방법이 될 것이다. Figure 8은 하나의 지상국에서 다중위성 운영을 위한 망형 구조의 위성별 네트워크와 서버팜, 모듈화된 VPN, 단방향 USB 시스템, DMZ 등의 모든 구성 요소를 포함한 지상국 내부 네트워크 구성이다.

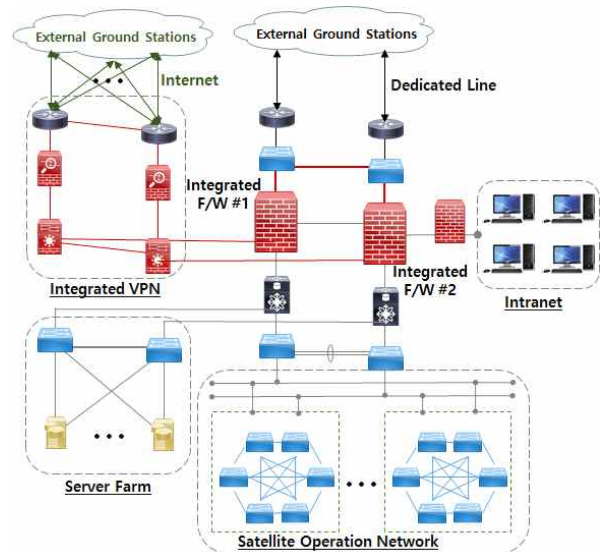


Fig. 8 Ground station network configuration for multi-satellite operations

4. 다중위성운영을 위한 네트워크 구성 시험

4장에서는 2장 및 3장에서 제시한 구성 방안을 활용하여 다중위성운영을 위한 데이터 인터페이스 시험 환경을 구성하고, 시험 환경 구축에 대해 기술하였다.

4.1 통합 방화벽 시험 환경 구성 및 구축

방화벽을 외부로부터 접근되는 네트워크의 유일한 접속 포인트에 설치하여 네트워크를 통해 드나드는 모든 트래픽이 방화벽을 통과하게 함으로써 외부의 접근을 승인된 트래픽만으로 제한 할 수 있어 보안 접근 정책 관리 및 강화를 용이하게 할 수 있다. 기존에 구성된 방화벽을 이중화된 통합 방화벽으로 구축하기 위해 Figure 9와 같이 시험 환경을 구축하였다.

테스트베드 구축 시 스위치간 포트 설정 및 라우팅 테이블(routing table), 방화벽 정책 등의 충돌 방지를 위해 포트 구성 및 라우팅 테이블 설정, 방화벽 정책 등을 새롭게 설정하였다.

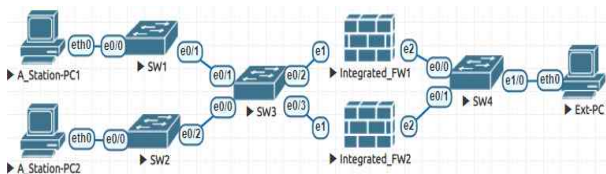


Fig. 9 Test Bed of Integrated Firewall

4.2 통합 가상사설망 시험 환경 구성 및 구축

가상사설망 연결을 구성하는 가장 중요한 요소인 VPN 터널링 프로토콜은 크게 VPN 연결 지점 간에 오가는 데이터 패킷의 암호화, VPN 터널의 생성 및 관리, 그리고 암호화 키 관리를 수행한다. 터널링 프로토콜은 데이터가 전송 네트워크를 통과할 수 있도록 하는 라우팅 정보를 포함한 헤더와 데이터를 캡슐화한다. 캡슐화된 프레임은 헤더에 추가되어 있는 라우팅 정보를 기반으로 인터넷과 공중망을 경유하여 터널의 목적지로 전송되고, 목적지에 도달하면 디캡슐화되어 최종 층(layer)로 향하게 된다. 이는 기존의 전용회선의 경우 보안성이나 품질 면에서는 인터넷 망에 비해 뛰어날 수도 있으나, 직접 전용망을 구축하거나 통신사업자에게서 전용망을 임대하고 이를 연결하기 위한 전용 네트워크 장비를 도입하는데 막대한 비용이 소요된다. 이를 개선하기 위해 가상사설망을 사용하였고, 초기 가상사설망을 구축하기 위해 “End to End”에 1 : 1 개념으로 구축하여 운영하고 있었다.

하지만, 위성의 증가와 더불어 국내외 지상국의 증가로 인하여 더 이상 1 : 1 개념의 구성보다는 1 : N 개념의 구성이 다중위성운명을 위해 더 효율적이 방안

이다. 이를 위해 기존에 구성된 VPN을 이중화된 통합 VPN으로 구축하였고, Figure 10은 구축된 시험 환경이다.

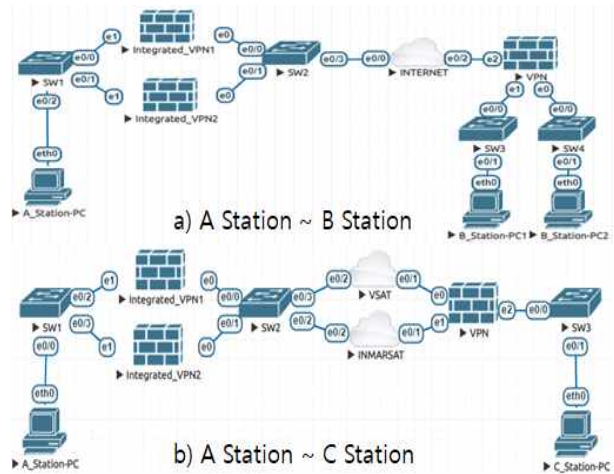


Fig. 10 Test Bed of Integrated VPN

통합 VPN 시험 환경 구축 시 네트워크 주소 변환기능(NAT; network address translation)의 문제점을 방지하기 위해 모든 시스템의 IP 주소를 재 할당하여 구축하였다. 또한 라우팅 테이블 충돌 방지를 위해 라우팅 테이블을 새로 설정 하였다. 통합 방화벽과 통합 VPN의 시험 환경을 Figure 11과 같이 구축하였다.



Fig. 11 Test Bed with Integrated Firewall and Integrated VPN

4.3 첨단연구망을 이용한 네트워크 구축 및 시험

국내 신규 지상국을 구축하기보다는 기존 지상국과 첨단연구망·범용연구서비스 네트워크를 활용하여 위성 영상과 같은 대용량 데이터를 고속으로 전송해 줄 수

있는 환경을 구축하고, 해외지상국은 GLORIAD를 활용하여 네트워크를 구성하면, 고 비용의 신규 지상국 구축비용을 줄이고, 대용량의 위성영상 데이터를 효율적으로 전송할 수 있다. 이는 기존 전용회선의 보안성과 VPN의 장점을 모두 충족할 수 있는 좋은 방안임에 틀림없다. 4.1절과 4.2절에 구축한 시험 환경을 기반으로 데이터 전송 시험을 수행하였다. 시험을 위해 KISTI와 협력하여 지상국간에 1 Gbps의 첨단연구망을 구축하였고, Figure 12와 같이 데이터 전송 시스템을 설치한 후 시험을 수행하였다. 네트워크 토폴로지는 다중 위성운명을 위해 지상국 A는 망형(mesh type), 지상국 B는 계층형(tree type) 구조를 기반으로 Table 1의 조건과 같이 보안장비를 아무것도 사용하지 않은 경우, 방화벽만 사용하는 경우, 방화벽과 VPN을 설정한 경우, 방화벽과 VPN, ASPERA 소프트웨어를 모두 사용한 4 가지 경우로 데이터를 전송하여 네트워크의 속도 측정을 수행하였다.

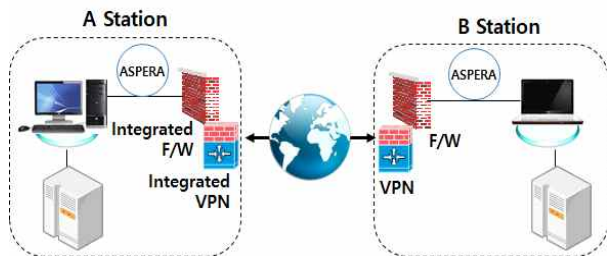


Fig. 12 Data transmission test configuration using 1 Gbps research network

Table 1은 데이터 전송 시험 10회를 수행한 평균 결과 값을 나타낸 것으로 1 Gbps 망을 구성한 후 아무런 조건 없이 시험을 수행한 결과 “up” 일 때 980 Mbps, “down” 일 때 990 Mbps의 전송 속도를 얻을 수 있다. 이를 기반으로 방화벽만 설정 후 시험을 수행하면, “up” 일 때 830 Mbps, “down” 일 때 844 Mbps의 전송 속도를 보이며, 방화벽에 128 bits 블록 암호화 알고리즘 ARIA를 탑재한 가상사설망을 추가로 설정하면, “up” 일 때 223 Mbps, “down” 일 때 242 Mbps로 현저히 감소하는 것을 확인할 수 있다.

일반적으로 VPN을 사용할 경우 10% ~ 20% 감소가 나타나지만, KISTI에서 회선을 직접 포설하여 운영하는 것이 아니라 KT 등과 같은 회선사업자를 통한 임대회선을 이용하여 첨단연구망을 구성하여 전송 속도의 차이가 발생하는 것으로 추정된다. 또한, 현재의 회선을 활용하여 전송 속도 향

상을 위해 암호 알고리즘을 AES 128 Bits로 설정한 ASPERA를 활용하여 시험한 결과 “up” 일 때 390 Mbps, “down” 일 때 485 Mbps의 전송 속도를 얻을 수 있었다.

Table 1 Data transmission measurement result using 1 Gbps research network

Test Condition	Station	Link	Average Rate (10 회)
-	A to B	UP	990 Mbps
		Down	980 Mbps
F/W	A to B	Up	830 Mbps
		Down	844 Mbps
F/W + VPN	A to B	UP	242 Mbps
		Down	223 Mbps
F/W + VPN + ASPERA	A to B	UP	390 Mbps
		Down	485 Mbps

Figure 13은 Table 1의 데이터를 그래프로 나타낸 것이며, 동일 조건으로 다른 망 구성에서 시험을 수행한다면, 다른 결과를 얻을 수 있을 것으로 예상된다. 이에 향후 전송 속도 향상을 위해 암호화 알고리즘에 따른 속도 측정 등 최적화 연구를 진행할 계획이다.

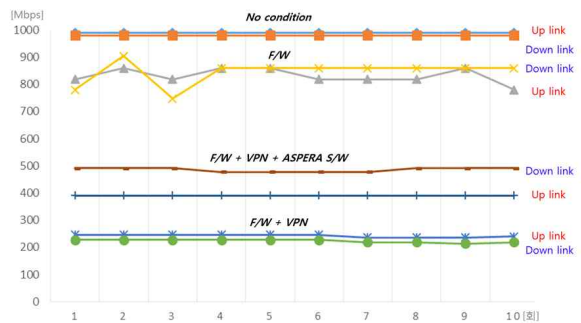


Fig. 13 Data transmission measurement result using 1 Gbps research network

5. 결 론

본 논문에서는 방송·통신, 지구관측, 기상관측, 해양관측, 그리고 항행까지 서로 각기 다른 임무를 가지고 있는 위성들을 효과적으로 운영하기 위한 네트워크 구축 방안에 대해서 제시하였다. 저궤도위성의 특성상 한반도에 위치한 지상국만을 활용하는 것은 공간적, 시간적 제약이 발생하기에 이를 극복하기 위한 방법으

로 해외지상국을 활용하고 있다. 세계 주요 우주 운영 기관인 미국항공우주국(NASA), 유럽우주기관(ESA)들도 기관 소유의 지상국, 계약을 통한 상용 지상국 활용, 그리고 기관 간의 협업을 통한 상호 지상국 활용을 위해 전 지구적 네트워크(global ground network)를 구축하여 운영하고 있다. 우리도 이를 반영하여 국내외 지상국을 신규로 구축하기보다는 기존 지상국을 활용하고, 세계 주요 우주 운영 기관과 협업하거나, 계약을 통한 상용 지상국을 활용하는 것이 효율적이다. 이를 위해 네트워크 구성은 첨단연구망·범용연구서비스망을 활용하여 위성영상과 같은 대용량 데이터를 고속으로 전송해 줄 수 있는 환경을 구성하는 것이 합리적인 방법이다. 또한, 지상국 네트워크 구성은 방화벽을 외부로부터 접근되는 네트워크는 하나의 접속 포인트로 두어 네트워크를 통해 드나드는 모든 트래픽이 방화벽을 통과하게 함으로써 외부의 접근을 승인된 트래픽만으로 제한 할 수 있어 보안 접근 정책 관리가 용이하고, 국내외 지상국 데이터 인터페이스를 위해 1 : N 가상사설망을 구성하면, 접점을 최소화할 수 있고, 관련 접점을 집중적으로 관리할 수 있어 보안 강화 및 유지보수 비용을 최소화 할 수 있다. 여기에 추가로 서버 팜을 통한 데이터 관리, DMZ 기능 등을 이용하여 지상국 네트워크를 구성하면, 운영 친화적인 네트워크 환경을 구축할 수 있다. 이를 위해 기반이 될 수 있는 방화벽과 가상사설망을 구축하기 위해 시험 환경을 구성하였고, 이에 따른 문제점들을 해결 후 이중화 시험 환경을 구축하였다. 하지만, 모든 국내외 지상국과 연동은 시간이 필요하며, 이를 위해 네트워크 품질 향상을 위한 연구는 계속 진행할 것이다.

후 기

본 연구는 한국항공우주연구원의 “위성임무관제사업”의 지원을 받아 수행되었습니다.

References

- [1] J. B. Lee et al., “Analysis of global ground station trend,” *Current Industrial and Technological Trends in Aerospace*, vol. 3, no. 1, pp. 90-107, 2005.
- [2] M. S. Lee et al., “Satellite ground station network status of space agency,” *Current Industrial and Technological Trends in Aerospace*, vol. 12, no. 1, pp. 177-185, 2014.
- [3] H. Y. Baek et al, “Introduction to Multi-Satellite Operation at KARI Ground Station” *SpaceOps AIAA-2006-5890*. 2006.
- [4] J. I. Kim et al, “Design and Development of Polar Integrated Ingestion System for KOMPSAT-2/3/5”, *Korea Society of Satellite Technology Vol.6 No.1*. 2015.
- [5] ASPERA High-speed file transfer software homepage, <https://asperasoft.com>, accessed June 2018.
- [6] Korea Institute of Science and Technology Information homepage, <https://www.kisti.re.kr>, accessed June 2018.
- [7] I. S. Jang et al., “A study on the internal network and external network interworking using the one-way USB system,” *Proc. of Symposium of the Korean Institute of Communications and Information Sciences 2014*, pp. 617-618, 2014.
- [8] I. S. Jang et al., “Development of the operation maagement system for LEO satellite operation and improvement plan for next phase,” *Proc. of SpaceOps Conference 2014*, AIAA-2014-1651, 2014.
- [9] H. Y. Baek et al, “A Study on the application of Virtual Private Network for Satellite Image Data Transmission”, *Proc. of Symposium of Korea Society of Satellite Technology Vol.4 No.1*. 2018..