Network configuration for multi-satellite operations in a network isolation environment for enhanced security

Hyun Chul Baek[1], Tae Geun Son[1]
Korea Aerospace Research Institute, P.O. Box 113 Yuseong, Taejeon, 305-600, Korea

Cyber security threats exploit vulnerable points of the software and detour security products and malware. In order cope with such cyber-attacks, efforts are put forth to upgrade security policies regularly by establishing information protection systems (Firewall, IDS, IPS, anti-Ddos, etc.), security solutions (EMS, SIEM, etc.), Patch Management System (PMS), and anti-virus systems. However, vulnerabilities remain, such as the exchange of malware-infected data, intentional data leakage by employees, etc. Network isolation strategies to protect the internal system have been introduced to address external attacks such as virus, hacking, Denial of Service (DoS), etc. Network isolation or network separation strengthens security by blocking any external access. As it restricts the scope of malware operation, damages can be minimized. A bi-direction data transfer system to strengthen physical security is designed to support the physical layer and data link layer, different from application-based systems that also support the OSI 7 Layer. In addition, bi-direction data transfer systems can cope with problems of the existing 1-way systems when they fail to receive a response (ACK) after data transmission, such as transmission data error, loss, receiver malfunction, etc. As such, bi-direction data transfer systems support Error Correcting Codes (ECC) for file transmission as they utilize a physical layer, detect receiver troubles by the line monitoring function, and provide buffering and retransmission functions. This study suggests a network design and operation method to improve enhanced physical security and work efficiency in such ways as preventing hacking attempts and viruses from outside by addressing problems among ground station networks operating multi-satellites and establishing a ground network isolation and connection systems so that multi-satellites are operated stably by multiple ground stations.

I. Introduction

Cyber security threats have advanced into various types: Advanced Persistent Threats (APT) to attack a certain target for various purposes persistently; phishing, pharming, and smishing to snatch personal information and money; ransomware aiming at individuals' assets; and large-scale cyber-attacks to manipulate the Internet of Things (IoT). Cyber security threats exploit vulnerable points of software, detour security products, and malware. In order to cope with such cyber-attacks, efforts are put forth to upgrade security policies regularly by establishing information protection systems (firewall, IDS, IPS, Anti-Ddos, etc.), security solutions (ESM, SIEM, etc.), Patch Management Systems (PMS), and anti-virus systems. However, vulnerabilities remain, such as the exchange of malware-infected data and intentional data leakage by employees. Network isolation strategies to protect the internal system have been introduced to address external attacks such as viruses, hacking, and Denial of Service (DoS). Network isolation or network separation strengthens security by blocking any external access. As it restricts the scope of malware operation, damages can be minimized. On the other hand, bi-direction data transfer systems have been introduced and applied to networks for multi-satellite operations to address this problem since network isolation may decrease work efficiency and convenience. Before such bi-direction data transfer systems were introduced, the Universal Serial Bus (USB) and 1-way systems were applied to inter-network data transmission, but these involved problems since data transmitted between networks increased as satellite use rates increased. The administrator suffered inconvenience as the use rate increased, and the efficiency decreased as the process became complicated. A bi-direction data transfer system to strengthen physical security is designed to support the physical layer and data link layer, different from application-based systems that also support the OSI 7 Layer. In addition, bi-direction data transfer systems can cope with problems of the existing 1-way systems when they fail to receive a

response (ACK) after data transmissions, such as transmission data error, loss, and receiver malfunction. Furthermore, bi-direction data transfer systems support Error Correcting Codes (ECC) for file transmission as they utilize a physical layer, detect receiver troubles by the line monitoring function, and provide buffering and retransmission functions. Integrated multi-satellite operation networks based on network isolation and connection technology are classified as the satellite operation network for satellite control, the satellite information network to receive, handle, and distribute satellite images, and the Di-Militarized Zone (DMZ) network for external contact points. The interface with ground bases for satellite control domestically and abroad consists of a dedicated line and high-tech research networks (KREONET, Korea Research Environment Open NETwork). For transmission of large-volume data, such as satellite images, virtual private networks (VPN: IPSec, SSL, and MPLS) are utilized. This study suggests a network design and operation method to improve enhanced physical security and work efficiency by preventing hacking attempts and viruses from outside, addressing problems among ground station networks, operating multi-satellites, and establishing a ground network with national satellites that integrates network isolation and connection systems so that multi-satellites are operated stably through multiple ground stations

II. Network Security Threats

A. Types of hacking attacks and major hacking techniques

As technology advances, hacking attacks and attempts increase with less knowledge required for such hacking attacks than before. Since hacking tools are widely distributed, there is no need to acquire all of the knowledge required for hacking; as a result, the number of hacking invaders, such as script kids, increases. Moreover, attack types are advancing from mere attempts to such complex attacks as social engineering and APT. Indeed, there are a variety of hacking types. While simple system bugs were used in such attacks in the past, upgraded attack methods that need various levels of knowledge, such as a network system and applied system, are currently used. As the Internet advances, anyone can easily share hacking information or execution codes. Hackers with various hacking purposes attempt to acquire system authority or information and utilize their attacks to paralyze e-commerce (e.g., DoS attack) or express their political goals. Hacking is advancing so that remotely controllable agent-type back doors are installed to attack other systems. Figure 1 shows various types of hacking attacks. Another prominent feature of recent hacking attacks is to aim at a particular system or network to detour the security system. Automated tools such as Internet “worms” and Windows-attacking tools have also been developed. Encrypted communication methods and tunneling techniques between an attacker and its agent are used to secure their concealment. As hacking techniques and methods advance, variant attacks are being used, becoming more and more complicated. Specifically, the primary hacking techniques are port scan, password cracking, sniffing, spoofing, buffer overflow, DoS/D-DoS, phishing, and SQL injection. Pharming is used depending on mobile environments. Smishing and Mobile DoS (M-DoS) aim at basic desktop environments, while more advanced and wireless environment attack techniques have emerged. As cloud environments are spread, hacking techniques different from existing ones, such as side chain attacks, add more danger. Research on new defensive techniques, such as homomorphism encryption, is urgently needed to create countermeasures.

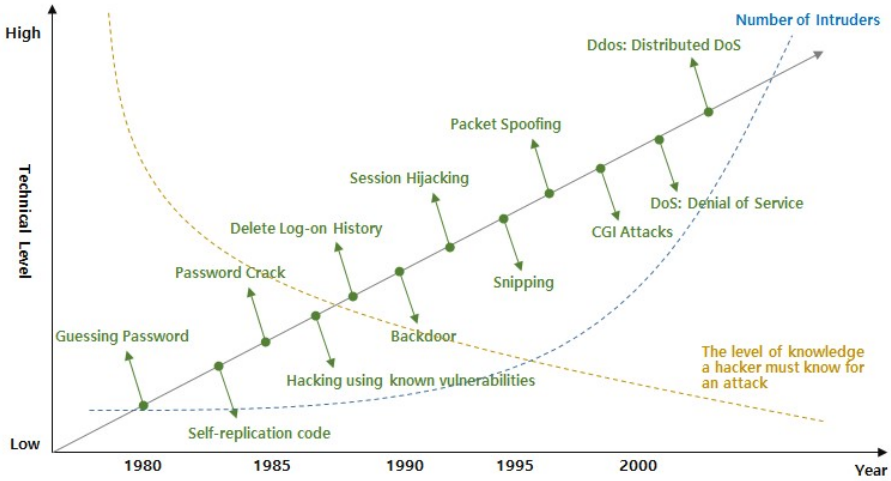

Figure 1. Changes in hacking attack trends

B. Ways to Respond to Attacks on TCP/IP Weak Points

TCP/IP, which is most commonly used in Internet environments, consists of the Transmission Control Protocol (TCP) and packet communication protocol IP (Internet Protocol), as illustrated in Figure 2. TCP is the transmission layer to deliver reliable data, while IP is the network layer that designates the address (departure and destination) and the path. When TCP/IP was first designed, there was little security awareness (necessity). As the "Best Effort" protocol, TCP/IP involves many security weak points since it includes no cross-certification procedures or confidentiality-secured procedures. The IP header includes packet fragmentation and reassembly information, source ID, and destination IP. However, there is no section to check or verify if the address is accurate. The TCP header does not include any section to check the port information. When the header information is examined for security reasons, the receiving part's mutual certification and transmitting part are not defined. There is no procedure to guarantee the integrity of transmitted data, such as encryption. Although TCP/IP is designed with the concept of "Best Effort" and has maintained its leading position on the Internet, this protocol involves weak points regarding certification and confidentiality. These are attacking types that utilize TCP/IP weak points, including spoofing, sniffing, SYN flooding, teardrop, and ICMP·ARP·NTP·IPv6·HTTPS attacks. To respond to such attacks, version updates that complement existing security and weak points are crucial. Hacking attacks, such as Zero-day Attacks that aim at the status before such updates, are also increasing, and, in response, various intelligent security devices and systems to prevent unknown attacks are currently utilized. R&D is also necessary to make up for weak security points in IPv6 environments of IoT service

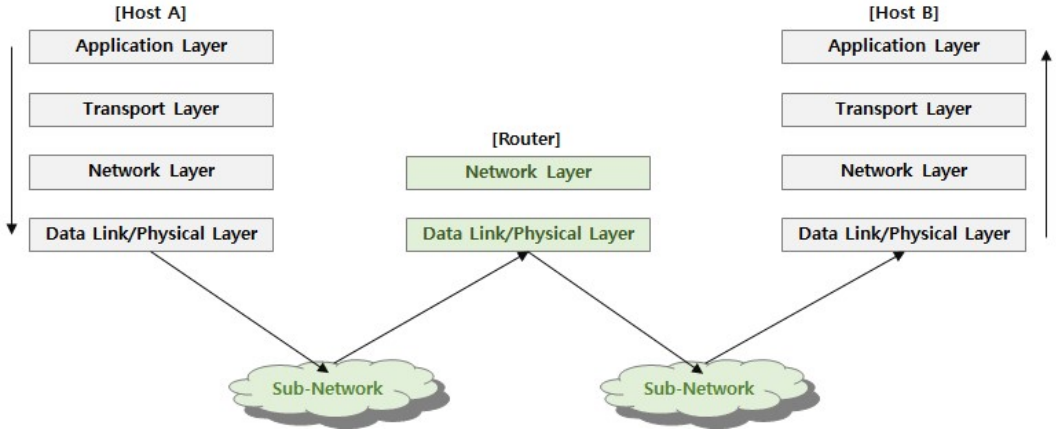

Figure 2. TCP/IP Structure

C. Network Security Vulnerability

Various security solutions that tighten the security policy are adopted to cope with cyber-attacks, including information protection systems such as firewalls and intrusion detection systems, integrated security management systems, and security information and event management systems. A firewall is located at the border between networks, filtering packets based on the IP information (L# header) and port information (L4 header) of the packet departure point and destination. In other words, a firewall limits communication only to permitted IPs and ports and blocks IPs and ports that are not designated, blocking illegal intrusions from outside. In addition, it features packet inspection and Network Address Translation (NAT) functions. The intrusion preventive system is installed in a network section or in each host, such as a server, detecting packet data patterns and blocking harmful traffic. While a firewall analyzes header information, the IPS inspects packet data and performs both detection and blocking. The error detection rate of the IPS is not relatively high since it detects mostly known patterns of misuse. However, the detection rate increases in the case of abnormality detection since unknown attacks are also detected and blocked. Therefore, it is crucial to monitor the average traffic in a normal situation and establish the proper threshold for each situation regarding abnormality detection. Recently, there were cases of hacking security devices, using their vulnerable versions of firmware, laundering the IP, and misusing it as a transit. An attacker accessed the backdoor of the victimized devices, activated the Virtual Private Network (VPN) function, and attempted hacking attacks on other spots. As such, security devices involved limitations in coping with various attacks that use such malware. Moreover, there were attempts to access regularly from outside in a specific IP range, and there were logs that tried

to transmit a large amount of data. Some policy management problems most often found among security devices were excessive permission policy, two-way policy input, security violation policy, and log deactivation. Such policies lead to unnecessary access to the internal network, causing a severe security threat. As shown in Figure 3, even if the security equipment was managed according to the established operating procedures, it was difficult to judge whether the policy may lead to a security problem in actual operating environments.

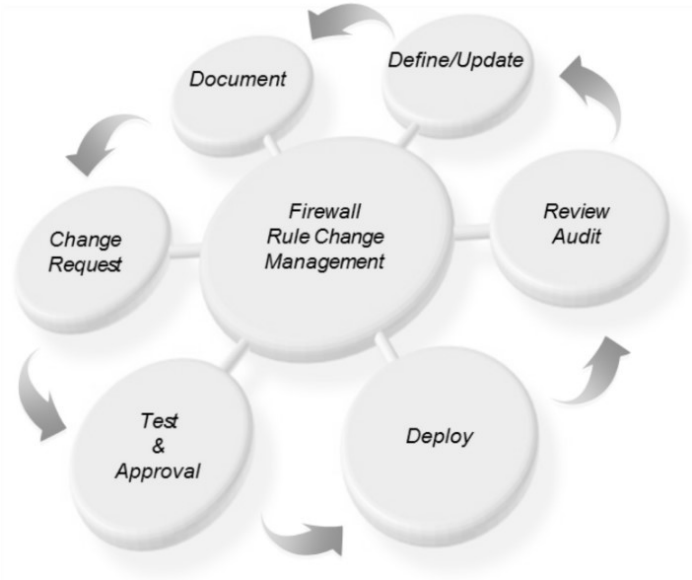

Figure 3. Security equipment operation procedures and management

D. Structural vulnerability of the network

As the security functions were upgraded, the integrated network was designed to integrate separate networks for each satellite in consideration of satellites that were expected to be launched. The integrated multi-satellite network was divided into the operation network to control the satellite and the information network to receive images from the satellite. There was a firewall between the operation network and the information network to manage the different types of inter-network data interfaces. The satellite operation network uses a dedicated line for an external access interface and a high-tech research network. The satellite information network utilizes the VPN to transmit extensive data. As shown in Figure 4, structural problems were observed in establishing an integrated multi-satellite operation network. Before the network integration, each network was operated by different administrators, and different administrators configured new network accesses. The security issues of each network section were examined in advance, but in terms of integration, the network was connected from inside to outside in some sections while the network was connected from outside to inside in some sections

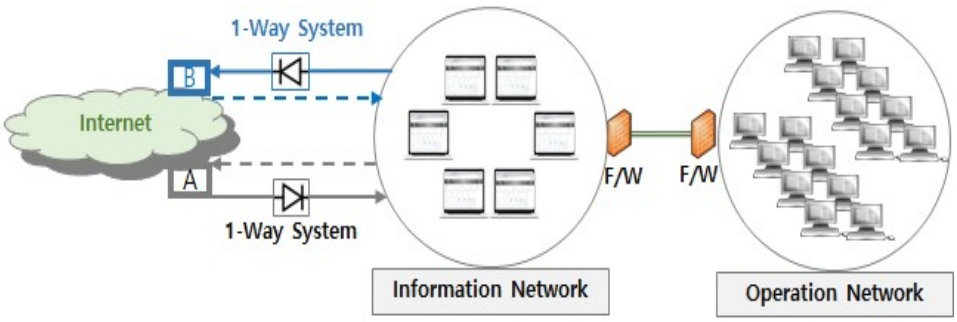

Figure 4. Structural vulnerability of the integrated network

E. Secure USB vulnerability

If data transmission is required between a particular task area and an Internet area, a separate configuration for file transmission is required in the case of network separation. Even if network separation is implemented, intrusions still involve "Black Hole" vulnerability issues. Even permitted USB memory devices are operated, as shown in Figure 5, and thus there can be attempts to exchange data infected with malware and bring them inside. Some files downloaded from outside may not be checked regarding virus infection when the data are transmitted into the business network, and as a result, the internal system is infected with a virus. There is also a risk of data leakage by internal workers. A series of procedures are implemented to fulfill a satellite's missions. For example, imaging and mission plans reflect a user's request for imaging. Commands to be transmitted to the satellite are generated and sent via the antenna. A data interface is required to receive status and image data from a satellite, process them, and provide them to users. In addition, an overseas station needs to reserve antenna operation via the network and provide the mission plan and schedule so that images can be received. A secure USB method was used to transmit such data in separate network environments where data were transmitted from outside to inside, employing a one-way system, or from inside to outside. However, as the number of satellites and the quantity of data to be transmitted increased at stations at home and abroad, the inconvenience among actual users inevitably increased. Particularly, virus checks and security procedures were required when a user accessed the system with a USB method, even if it was a secure USB device. Additionally, inefficient tasks increased since related records should be kept.

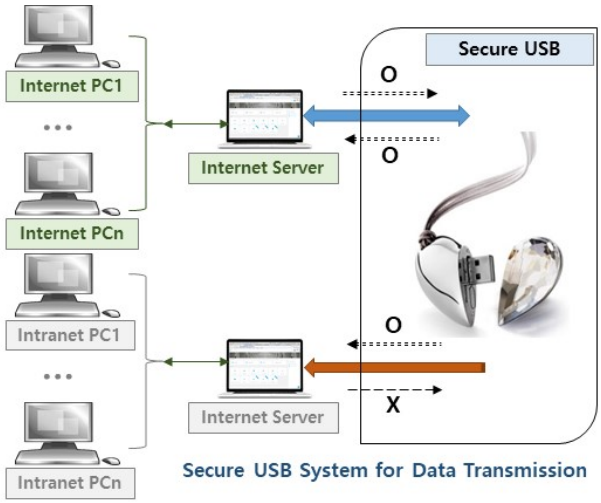

Figure 5. Secure USB use and management

III. A Network for Multi-Satellite Operation

A. The bi-direction data transfer system

To address the network's structural problems and cope with the secure USB vulnerability and user work inefficiency, the bi-direction data transfer system needs to be established. The bi-direction data transfer system adopts two-way data transmission using 2 sets of the one-way system, as illustrated in Figure 6. In general, a one-way system cannot receive responses (ACK) after data transmission and thus cannot cope with transmission data errors and loss and receiver disorders. In contrast, the two-way bi-direction data transfer system can support the Error-Correcting Code (ECC) for file transmission by utilizing a physical line and detect receiver errors by using the line detection function with data retransmitted after buffering. In addition, security policy configuration and management in both primary and reverse directions are performed through a physical line in the control area, which is an advantage in terms of security and integrated management. As shown in Table 1, it is possible to transmit all the data in the primary direction, while in the reverse direction, only text files are transmitted to a limited extent so that harmful traffic from outside can be blocked.

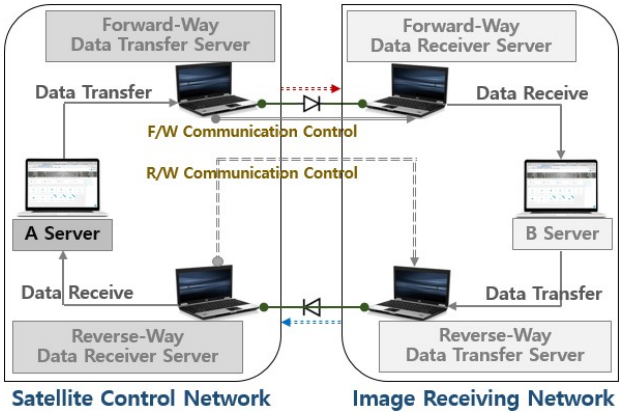

Figure 6. Data transmission employing the bi-direction data transfer system

Table 1. The file filtering function of the bi-direction data transfer system

Classification	Description
Extension filtering	- Filtering based on the extension (.exe, .com, .pdf, etc.)
MIME-Type and Content-Type	- Filtering on the MIME form 1) Multipart-related/Multipart MIME type - Filtering on the content types 1) XML Media type 2) Application type 3) Auto/Video type 4) Text type 5) File type (MS word, etc.)
File Signature	Filtering through file header analysis (execution/document/image/video file, etc.)
Malware	Malware detection through the dual engine
Suspicious code	Analysis of execution files or document files through an internal code and a malware diagnosis (static analysis)

B. Way to enhance the inter-network data transmission rate

TCP-based inter-network data transmission was performed for inter-network data transmission, but due to the low transmission rate, it was inappropriate to transmit large-quantity data such as satellite images. To cope with this problem, the UDP proxy server was established to increase the transmission rate. The proxy server supports clients in accessing sub-systems of another network indirectly. It is an intermediate communication bridge between the server and the client. The goal of the server is to transmit data at high speed to clients only using the proxy rather than transmitting requests to the server via the intermediate cache with the server unconnected. The proxy may consist of either the TCP or UDP. The central communication used to be performed mainly by the TCP method. This was because transmission reliability was relatively high as it was connected in the 1-to-1 (Unicast) way. Currently, however, the UDP has also secured the reliability sufficiently, although it is not as high as the TCP. In addition, it is possible to transmit more information than the TCP; thus, the UDP is utilized to transmit such information in real time, as in streaming. This was applied to the bi-direction data transfer system, but it could not secure the desired transmission bandwidth. To address this problem, the Non-Internet Protocol Networking (Non-IP) method was adopted, as shown in Figure 7, and it was possible to gain minimal bandwidth to transmit satellite images. Non-IP is a new concept of network protocol designed to support various new and advanced 5G services efficiently instead of the existing TCP/IP system. The TCP/IP protocol was designed as a text-based user interface instead of dynamic media such as audio and video. Computers and terminals communicate with one another at a fixed position. However, as the telecommunication system advanced and various related services were added,

TCP/IP was no longer the optimal system to provide advanced services of 5G. As Non-IP Networking was applied, securing the transmission rate of 500 Mbps in the bi-direction data transfer system became possible

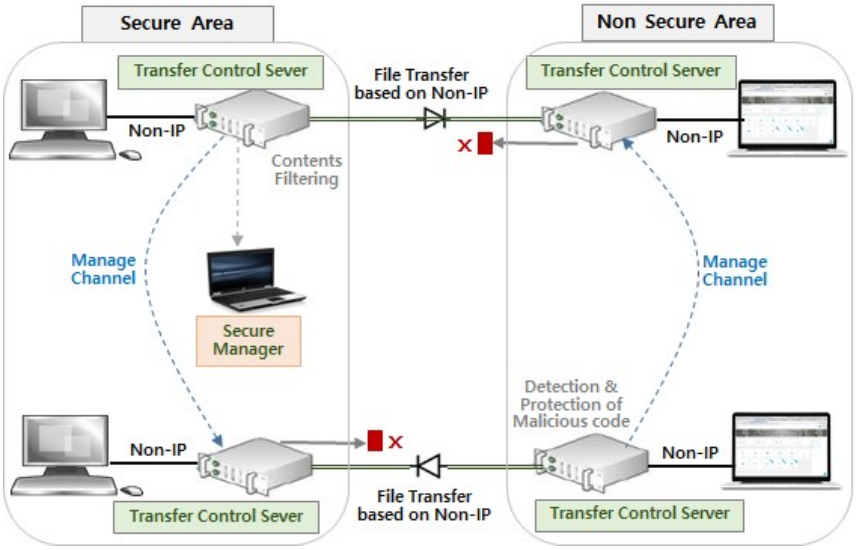

Figure 7. Bi-direction way data transmission of Non-IP

C. National satellite ground network configuration for multi-satellite operation

For efficient multi-satellite operation, the national satellite ground network was established. The national satellite ground network consists of the satellite operation network, satellite information network, and DMZ network. The satellite operation network transmits commands to a satellite and enhances the security of contact points with external entities through the dedicated line and KREONET to receive satellite status data. Ordinary users have no access to this system. The satellite information network consists of a dedicated line for storing, processing, and distributing images from a satellite, KREONET, and VPN. The contact points from external entities, except the primary system, are blocked by means of the dedicated line and KREONET. Data are distributed through the DMZ network among institutions that cannot utilize the dedicated line and KREONET, as shown in Figure 8.

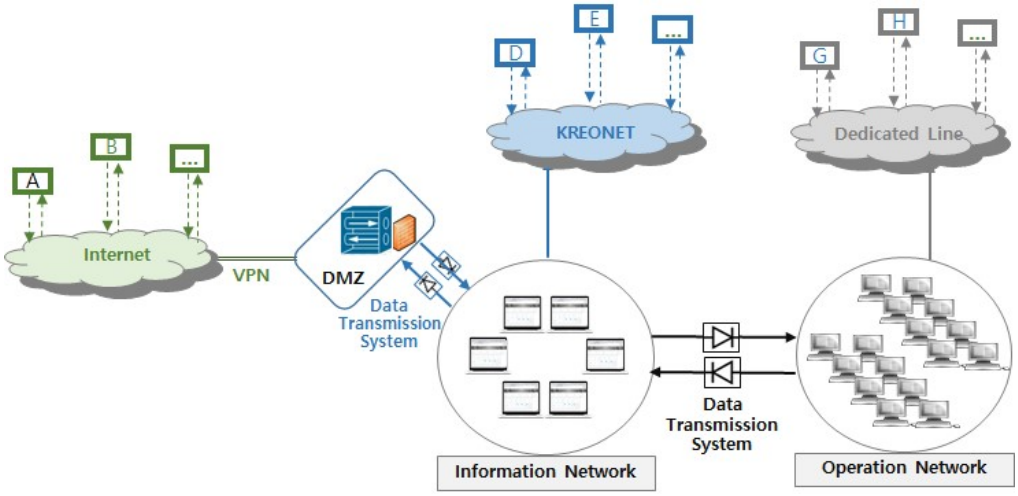

Figure 8.Network configuration for multi-satellite operation

The network configuration for multi-satellite operation is based on the network separation guide in 2008, through which it was possible to block any external access through network separation, limit the dynamic range of malware, minimize the possible damage, and protect internal data securely. Although security is enhanced through network separation, the network separation from external entities decreases work efficiency and convenience. The two-way data transmission system was developed to address this problem, and the CC-certified two-way bi-direction data transfer system was introduced to enhance security and work efficiency. The two-way bi-direction data transfer system utilizes a physical line to support file transmission and Error Correcting Code (ECC), monitor lines, detect receiver errors, resume transmission after buffering, and secure integrated management in the security area. In utilizing such advantages, the two-way bi-direction data transfer system was configured between the satellite operation network and satellite information network to perform as the data interface. In addition, the bi-direction data transfer system was configured between the satellite information network and DMZ network to act as the interface with ground stations at home and abroad and transmit data. Data transmission is performed via the VPN (IPsec) tunneling function of DMZ-based ground stations to focus on increasing security.

IV. Conclusion

To cope with cyber-attacks, the following systems were established for regular upgrading of the security policy: information protection system (firewall, IDS, IPS, Ddos, etc.), security solution (ESM, SIEM etc), patch management system (PMS, Patch Management System), and anti-virus system. However, there remained vulnerable points, such as the exchange of malware-infected data and intentional data leakage by internal employees. For this reason, the network separation method was introduced. The network separation (or network isolation) system blocks external access to enhance security, thereby minimizing damage by limiting the operation range of malware. However, this network separation may decrease work efficiency and convenience. To address this challenge, the bi-direction data transfer system was introduced and applied to the network for multi-satellite operation. Before the bi-direction data transfer system was introduced, inter-network data transmission was performed by applying the secure Universal Serial Bus (USB) and 1-way system. As the quantity of data transmitted between networks increased in line with the increase of satellite and frequency use, procedural complexity and operator inconvenience issues augmented. In utilizing this network separation method and the inter-network system, the integrated multi-satellite operation network divided the system into the following sections: Satellite Operation Network, Satellite Information Network for satellite image acceptance, processing, and distribution, and di-militarized zone network for external contact points. The network for ground stations at home and abroad for satellite control and the network with major institutions consisted of a dedicated line and high-tech research network (KREONET, KISTI). The DMZ-based virtual private network was used as the interface to transmit large-volume satellite video data to institutions that did not use a dedicated line. As a result, problems of ground networks for the multi-satellite operation were solved. As the network separation method and inter-network system were established for the stable operation of multiple satellites in different ground stations, work efficiency and physical security level against hacking and virus infection were improved.

Appendix A
Acronym List

DMZ	Di-Militarized Zone network
DoS	Denial of Service
ECC	Error Correcting Codes
EMS	Element Management System
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
KREONET	Korea Research Environment Open NETwork
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation

Non-IP	Non-Internet Protocol
NSGN	National Satellite Ground Network
OSI	Open Source Initiative
PMS	Patch Management System
SIEM	Security Information and Event Management
SIN	Satellite Information Network
SON	Satellite Operation Network
SSL	Secure Socket Layer
USB	Universal Serial Bus
VPN	Virtual Private Network

References

[1]Hyun Chul Baek, Tae Geun Son, Min A Kim and Jung Nam Jun, "Technology Trends of Network Separation & Data Transmission System", *Current Industrial and Technological Trends in Aerospace*, Vol. 20, No. 2, Dec. 2022, pp. 120.

[2]Hyun Chul Baek, Tae Geun Son, Gyeoul Lee and Myung shin Lee, "A study on the data transfer between different networks using Non-IP networking", *The Korean Society for Aeronautical & Space Sciences*, 2022 KSAS Fall Conference, 16 Nov. 2022, pp. 215.

[3]Hyun Chul Baek, Tae Geun Son, Jae Hyoung Park and Myung shin Lee, "Data Transmission in UDP and Non-IP methods", *The Korean Space Science Society*, Vol. 31, No.2, Oct. 2022, pp. 79.