Optimizing networks of multi satellites operations for KOMPSAT series

Se-Chul Park[1], Dae-Hwan Hyun[2], Myung-Sin Lee[3], Hwan-Jong Chu[4], Dae-Won Chung[5], Eun-Kyu Kim[6]
Korea Aerospace Research Institute (KARI), Eoeun-dong, Daejon, Korea, 305-333

Korea Aerospace Research Institute (KARI hereafter) successfully launched KOMPSAT 2 in 2006 and its operation has been proven very stable without any failure so far. The launches of KOMPSAT 3 and 5 are currently scheduled for 2012 and hence additional mission control system for these will be added to the current control system which is only dedicated for KOMPSAT 2. Each individual control system includes large number of servers, workstations and PCs and is very high in its complexity due to the many network segments in it. Also antennas and timing equipments for each individual control system are shared between them. The network system for the operation of the series of KOMPSATs requires optimization of variable factors such as network segments policy control to eliminate unnecessary network traffic and access control policy for the shared antennas and timing equipments. In this paper, I would like to discuss the network optimization process and result for the KOMPSAT 2 that is currently in service and also the overall design and analysis of future optimization of the network for the time when KOMPSAT 3 and 5 are in operation.

I. Introduction

The Korea's second multipurpose satellite KOMSAT2 was launched on July 2006 and has been operated and completed its mission successfully and currently doing its extended mission out of its lifetime. The system for the multi satellite operation has been developed for the operations of KOMSAT 3 and 5 that are scheduled to be launched in 2012. Therefore KARI puts its first step on the first ever multi mission operations phase, which also means the increase in the number of satellite operation equipments and the network facilities to support it. In terms of network, the increase in the number of network equipments causes the difficulty in management of each equipment, which shows the possibility that the operation system can be vulnerable to security threats due to the equipment setup error and careless management. In this paper, multi satellite control network design and implementation are discussed not just in consideration of quantitative increase of the equipments but in consideration of security and optimization

.

II. Case study

DoE is US Department of Energy whose network structure is a good example of the federal computer usage environment and 6 to 7 DoE WANs are interconnected as described in Figure 1 and are called ESNet(Energy Science Network). SNet is high performance communication line and works as a connection line to deliver the information that needs administrative support and security. It was designed based on VPN structure and configured to be placed on top of the ESNet layer for the security purpose. The main communications network of DoE is divided into 3 Enclaves that are Red network, Yellow network, and Green network according to the security level in each Enclave. Red network is an Enclave that handles the extremely confidential information and its security is maintained by strictly controlling the access only possible through the virtual private network on the top layer.

[1] System Administrator, LEO Satellite Mission Operations Team
[2] Senior System Administrator, LEO Satellite Mission Operations Team
[3] Senior Operation Controller/Training Officer, LEO Satellite Mission Operations Team
[4] Operation Engineer, LEO Satellite Mission Operations Team
[5] Head of LEO Satellite Mission Operations Team
[6] Director of Satellite Operations Division

Yellow network also deals with the security sensitive information that is less serious than Red network and hence has relatively less strict security policy. The access to Yellow network is only possible through DMZ area that is installed for the protection of information of DoE on ESNet. Finally the Green network is an Enclave that handles all the relatively non security sensitive information such as all the public information and web information and is also protected by the DMZ area. The main trend of the current network security is to divide the network into many enclaves for management according to the security level and apply the defense-in-depth to the enclave that has the top security level.

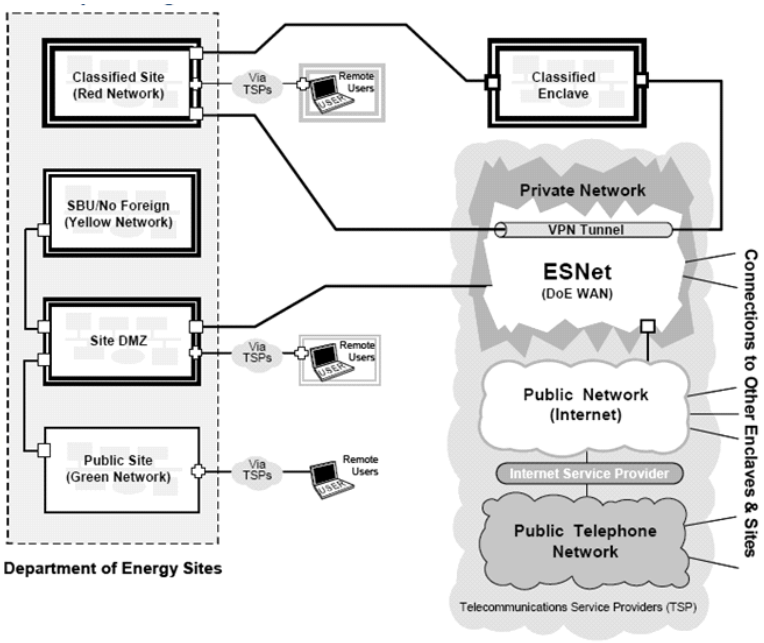

Figure 1. Network description of the DoE

III. Network designs for KOMPSAT series

Satellite operation system, as shown in Figure 2, is categorized into 3 enclaves according to the security level and the element that is most vulnerable to the internal and external threat is designated as Red-network area. The system that has higher security level than general systems but has less security level than Red-network is allocated in the Yellow-network. Flight support system and image processing system belong to the Yellow-network. Finally, the system that has frequent data communication and relatively low security level is allocated to DMZ and Server Farm and NMS system that is for the efficient management of the satellite operation system network are such examples.

Figure 3 is a design of the network interface with MCE and other satellite operations related systems for KOMPSAT2, KOMPSAT3 and KOMSTSAT 5. The data exchange of the MCE of each satellite with other systems is possible without any restriction because it does not go through any Network security equipment and the hazardous traffic and the access from the unauthorized users can be prevented by placing network security equipments in the communications link with external antenna site and external data server. The advantage of such system is that the number of network security equipments used is less than the equipments needed for the network design that we are going to mention later. This means the relatively lower cost for the network equipments maintenance and possible saving on equipment management. Also the traffic monitoring and control are relatively simple because the network traffic control is carried out by the main central firewall and the scalability for the future system can be accomplished just by the physical addition of the system to the firewall ports. The satellite operating system(MCE) that must be most protected from the external threats, however, cannot be considered as a security enhanced element since it is applied the same level of security settings as the other elements in the internal networks. Due to the shortcomings, this network design needs to be modified in security perspective.

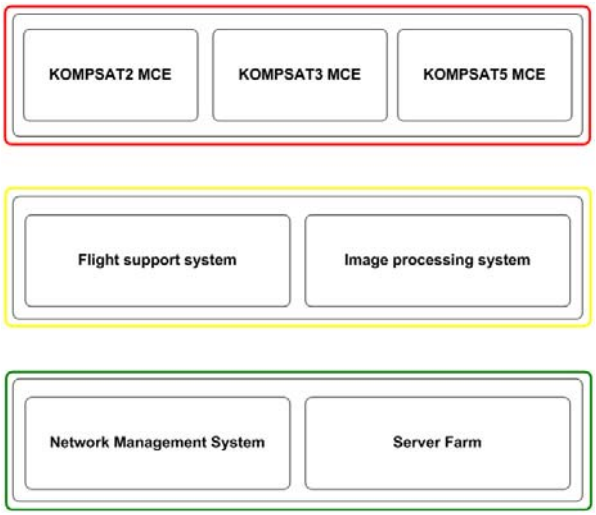

Figure 2. Enclaves of the KOMPSAT series networks

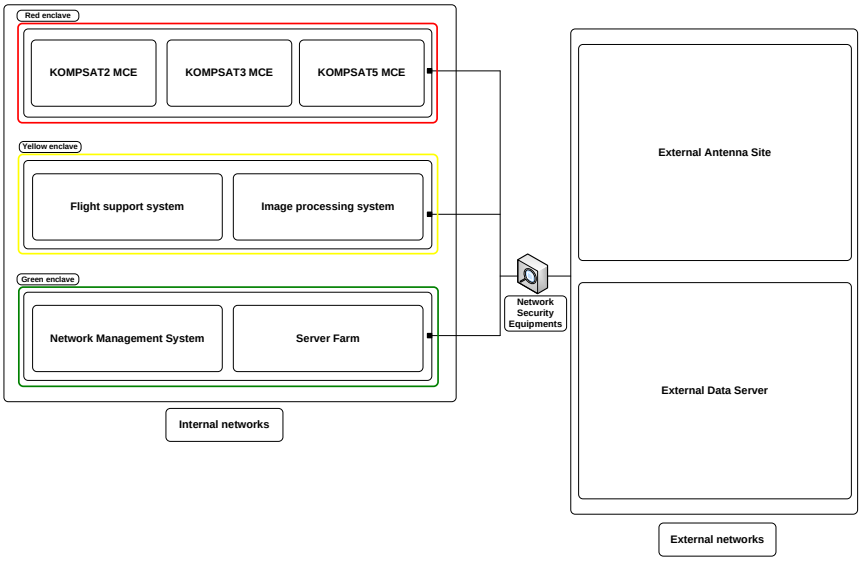

Figure 3. Design of the network #1

Figure 4 is the modified design of Figure 3 by changing the configuration of the link to increase network security. External network interface area was separately made to prevent the direct access to the MCE of each satellite due to the fact that the Figure 3 design allows the direct access to the MCE that must be most protected from the external network and all the network and system equipments to access to and from the external network are placed.

Also it blocks the hazardous traffic and the access from the harmful users by making the inward and outward traffic go through each network security equipment as the design in Figure 3 shows. The whole area of internal network enclave, however, can be accessed from external network due to the lack of network security equipments in the internal network when external network security equipments are passed by external threats. Therefore it has the same security problem as resides in the design in Figure 3.

Figure 5 is a network design that is in consideration of network security and optimization and the security feature is enhanced by placing network security equipments between each enclave link. The security of the DMZ enclave that has frequent data communication with outside is maintained by network security equipments as described in Figure 3 and 4 and the Red, Yellow and Green enclaves are only accessible to the external users only through DMZ. Therefore the access from the external users to the satellite MCE in Red enclave is impossible because of the four

network security equipments that must be passed by the users from the outside for the access. This minimizes the chances of the possible security problem due to the network security equipment failure.

The design in Figure 5 contains the relatively more network security equipments than other designs and hence seems to need more personnel and cost. However the same personnel and cost as in design #1 and #2 are required to manage the design by integrating and managing the large number of network security equipments through NMS(network Management System) located in Green enclave. The network components of each network security equipment and individual system are shown in Table 1.

The control and management of the network resources and security in multi satellite operations environment by utilizing the existing workforce are now possible due to the design of the system to efficiently manage and allocate network security equipments.

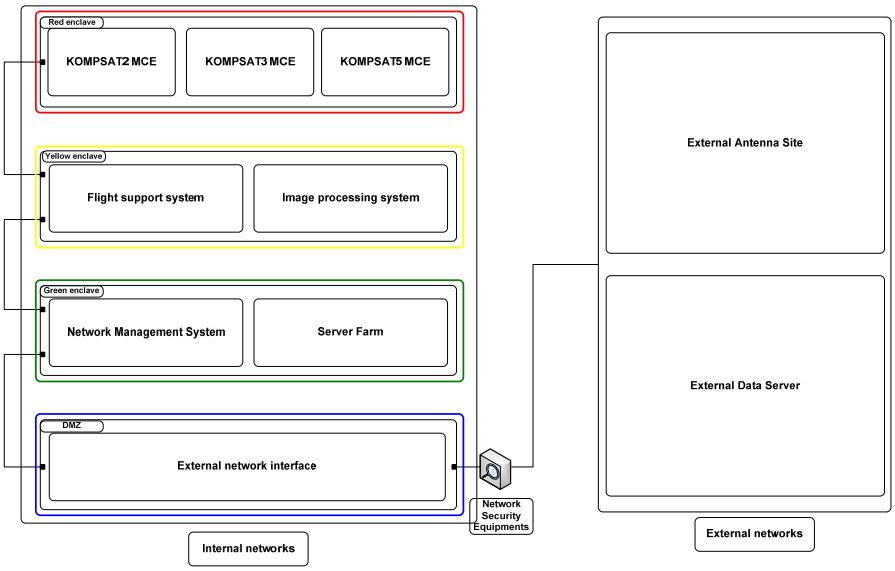

Figure 4. Design of the network #2

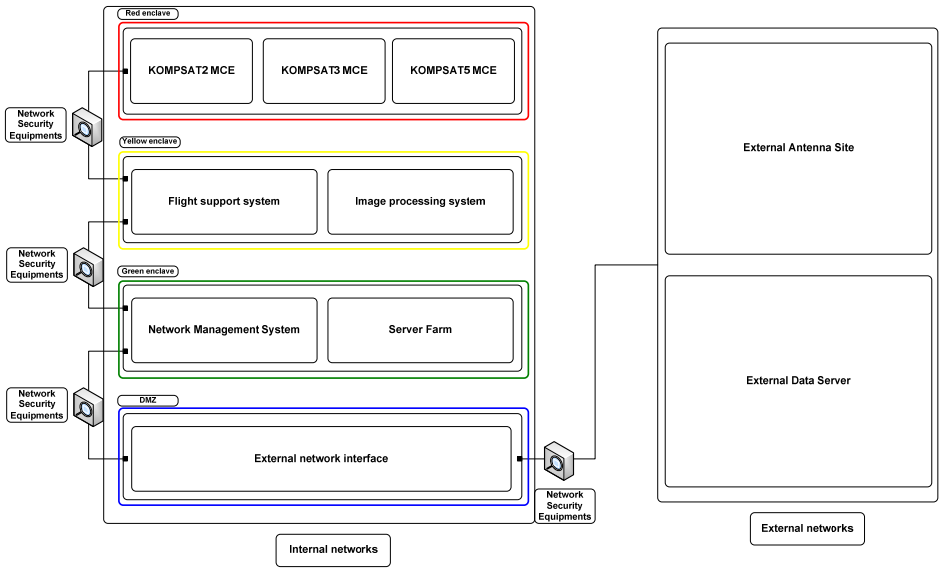

Figure 5. Design of the network #3

Table 1. Details of the Network security equipments

System	Location	Role
Router	Network Boundary	First packet filtering
Firewall 1	Network Boundary	Second packet filtering
Firewall 2	Network Boundary	Third packet filtering
Firewall 3	Network Boundary	Contents filtering
VPN	Network Boundary	Packet capsulation
UTM	Network Boundary	Contents filtering, Anti-viruses
N-IDPS	Network Boundary	Network traffic monitoring
Nessus	Each enclave	Vulnerability monitoring

IV. Conclusion

In this paper, we described network optimisation of satellite operation system for KOMPSAT2, KOMPSAT3 and KOMPSAT5. We designed network architecture like Figure 5 that has advances in cost and security with other network architecture and we are going to apply that network architecture to the KOMPSAT 3 and KOMPSAT5 satellite operation system. After that we are going to research on network virtualisation that reduces network equipments, network complexity and maintenance cost.

Appendix A
Acronym List

KOMPSAT KOrean MultiPurpose SATellite
NMS Network Management System
UTM Unified Threat Management
VPN Virtual Private Network

References

[1] S. Kent, "IP Encapsulating Security Payload (ESP)", RFC2406, November 1998
[2] S. Kent, "IP Authentication Header", RFC 2402, November 1998.
[3] Stephen Northcutt,'Inside Network Perimeter Security 2nd edition', Sams Publishing, March 04 2005.