메세지 인증 코드 기법을 이용한 위성명령 보안 메카니즘 설계

o
홍기용*, 최완식*, 이호진*, 김동규**

한국전자통신연구소*
위성통신기술연구단

아주대학교**
컴퓨터공학과

Design of Command Security Mechanism for the Satellite Using Message Authentication Code

K. Y. Hong*, W. S. Choi*, H. J. Lee*, D. K. Kim**

Satellite Comms. Technology Division*
ETRI

Department of Computer Engineering**
AJOU University

ABSTRACT

For the secure control of the communication satellite, security mechanisms should be employed on the ground station as well as on the spacecraft. In this paper, we present a security architecture for the spacecraft command security of the communication satellite. An authentication mechanism is also proposed using message authentication code (MAC) based on the Data Encryption Standard (DES) cryptosystem.

Keywords: Satellite, Spacecraft command Security, Authentication, DES

1. Introduction

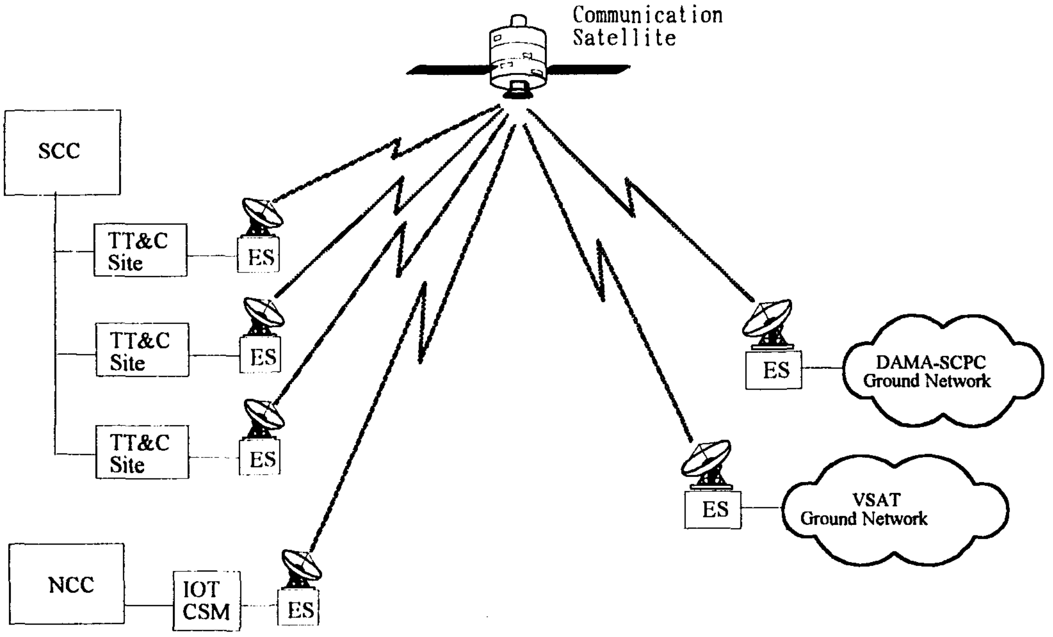
Currently, communication services utilizing communication satellite are rapidly growing. Satellite systems also tend to extend their connectives towards data communication networks, PSTN(Public Switched Telephone Network), and many kinds of ground network systems such as VSAT and DAMA-SCPC System [1,12,13,14,16]. To provide the continuous communication service via satellite, the spacecraft and its resources should be securely controlled by the authorized ground station, that is, spacecraft control center(SCC). Because of the increased attacks by hackers, it is required to provide the security mechanisms into the communication satellite system [1,3,4,5,6,7,8,9,10,15]. The SCC should also have the capabilities to protect the spacecraft command sent to the communication satellite for the desired control [1,10,15]. The communication satellite could be designed to provide the authentication mechanism for the uplink spacecraft command using Data Encryption Standard(DES) [11]. The command authentication facility(CAF) could be incorporated with the TC&R(Telemetry, Command, and Ranging) subsystem of the communication satellite. For the authentication of the spacecraft command, the CAF calculates the message authentication code(MAC) by encrypting the received command based on the DES.

In this paper, we present the designed authentication scheme for the communication satellite. Security enhanced system architecture is proposed for the SCC and the satellite. The formal authentication protocol is also presented using DES cryptosystem.

2. Authentication Mechanism for the Satellite

2.1 Network Configuration

Satellite communication network consists of the satellite and various kinds of ground components such as TT&C(Telemetry, Tracking, and Commanding) site, NCC(Network Control Center), terrestrial communication networks based on VSAT(Very Small Aperture Terminal) and DAMA-SCPC(Demand Assignment Multiple Access - Single Channel Per Carrier) [12,13,14,15,16]. An overall configuration of satellite communication network including the satellite is illustrated on figure-1. The SCC performs the telemetry acquisitions via TT&C site for the real time monitoring of the satellite. It also sends the commands to the satellite for the desired controls. To prevent unauthorized commanding, the SCC should protect the issued spacecraft commands prior to the transmission of it through the TT&C site.

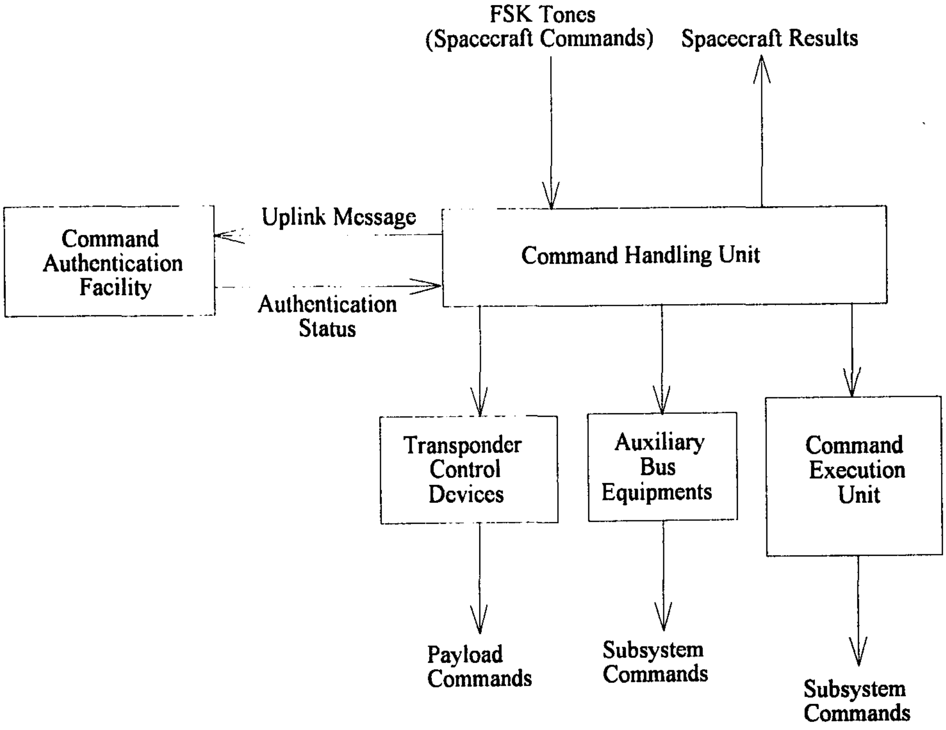


SCC : Satellite Control Center
TT&C : Telemetry, Tracking, and Commanding
NCC : Network Control Center
IOT : In-Orbit-Test
CSM : Communication System Monitoring
ES : Earth Station

<Figure-1> Overall configuration of satellite communication network

2.2 Architecture of TC&R Subsystem with Security

The TC&R subsystem consists of the command handling unit (CHU), transponder control devices (XCD), auxiliary bus equipments (ABE), and command processor (CEU). For the spacecraft command security of the satellite, the CAF(command authentication facility) is incorporated with the TC&R (Telemetry, Command, and Ranging) subsystem illustrated on figure-2. The CHU receives the FSK tones as the spacecraft commands sent from the ground station. If the secure mode is set, the CHU sends the received command message to the CAF for the command authentication. The CAF calculates the MAC relating the uplink message and verifies the validity of the command message. The only valid command can be routed to the designated devices to execute the command. The destination of the command is one of the subsystems that are AOCS (Attitude and Orbit Control Subsystem), payload subsystem, and other subsystem.



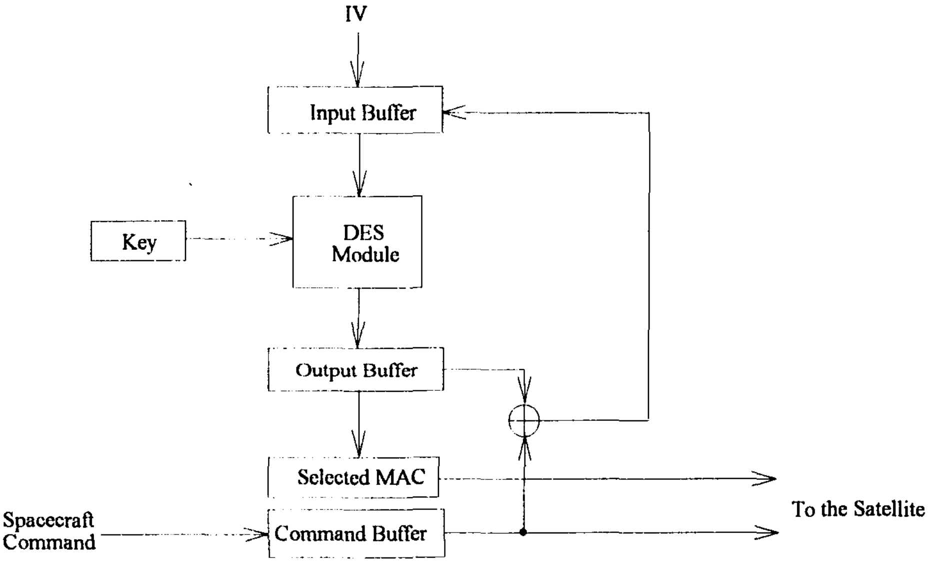
<Fig > Functional Block Diagram of TC&R Command Security

The spacecraft command structure for the satellite could consist of SYNC word, command handling unit address, flag, OpCode, and checksum fields. The flag field means that there is a checksum in the spacecraft command. If the flag is set to clear, the command does not include the checksum field. If the TC&R subsystem operates in the protection mode, the MAC would be appended to the end of the spacecraft command for the authentication.

3. Design of Authentication Protocol for the Satellite

3.1. MAC Scheme of the Spacecraft Command

Algorithm of calculating the MAC is designed using the DES cryptosystem based on the CFB (Cipher Feedback) mode [11]. The DES module operates twice for the MAC calculation in this scheme as shown figure-2. The first encryption is performed to encrypt the input buffer as a plaintext filled with the IV (Initial Value) by the encryption key. In the next encryptions, the output value of the previous encryption will be exclusive ORed with the spacecraft command. The result will be used for the next input. The MSB k bit-portion of the second output, encrypted by the same key, will be selected for the MAC. The MAC will be appended to the issued spacecraft command structure prior to transmitting it.



<Figure-2> Scheme of MAC Calculation for the Spacecraft Command

3.2 Authentication Protocol

After launching the satellite, SCC(Satellite Control Center) and TT&C(Telemetry, Tracking, and Commanding) site should keep tracking the predesigned mission scenario of a spacecraft. In the transient phase such as transfer and drift orbit, SCC should be responsible for issuing spacecraft command to the communication satellite in order to put spacecraft into the normal operational phase. SCC and TT&C sites continue to receive and analyze telemetry, and send telecommand for supporting communication service by maintaining the desired attitude and orbit of spacecraft in the normal operational phase. Also, NCC performs monitoring and control of communication payload in this phase. For secure control of the communication satellite, the adopted security mechanisms should protect sensitive spacecraft command and information against attacks because there are insecure RF links. In this section, we present the formal design of authentication protocol that can be employed directly to both SCC and communication satellite for efficient real time processing. Authentication enables SCC to make an authenticator, i.e., a MAC, to be used to verify the authenticity. When the communication satellite receives a spacecraft command, it should check the validity of the command whether it should be executed or not. The following mechanism is the designed authentication protocol based on the DES excluding third party KMC(Key Management Center) for spacecraft command and telemetry processing in real time.

● Notations

▶ $E_K[\,]$	: Encryption Function of DES Cryptosystem with Key K
▶ $D_K[\,]$	: Decryption Function of DES Cryptosystem with Key K
▶ MK	: Master Key
▶ WK_X	: Working Key of ID X
▶ A	: Unique ID of the Satellite Control Center
▶ SAT	: Unique ID of the Communication Satellite
▶ TC	: Telecommand
▶ TM	: Telemetry
▶ SCMD	: Spacecraft Command
▶ ASTAT	: Authentication Status
▶ SEQ_X	: Sequence Number of Valid Telecommand This value should be kept on storage of both ID X and ID SAT
▶ $\{\ \}$	: Concatenation

Let us assume that only one master key MK is kept on the tamper-proof storage of the satellite as well as on that of the SCC. Initially, the master key should be loaded into the satellite securely before launching, and only known to the authorized control center. A working key WK is a key for the encryption process in order to generate an authenticator, i.g., MAC. The MAC can be a k-bit selected output of final ciphertext that is calculated by means of DES CFB mode. The master key can be used as a key encryption key for the purpose of encrypting a working key. The working key is a data encryption key in order to generate a MAC relating to sensitive spacecraft command. The followings are authentication protocol based on the DES cryptosystem;

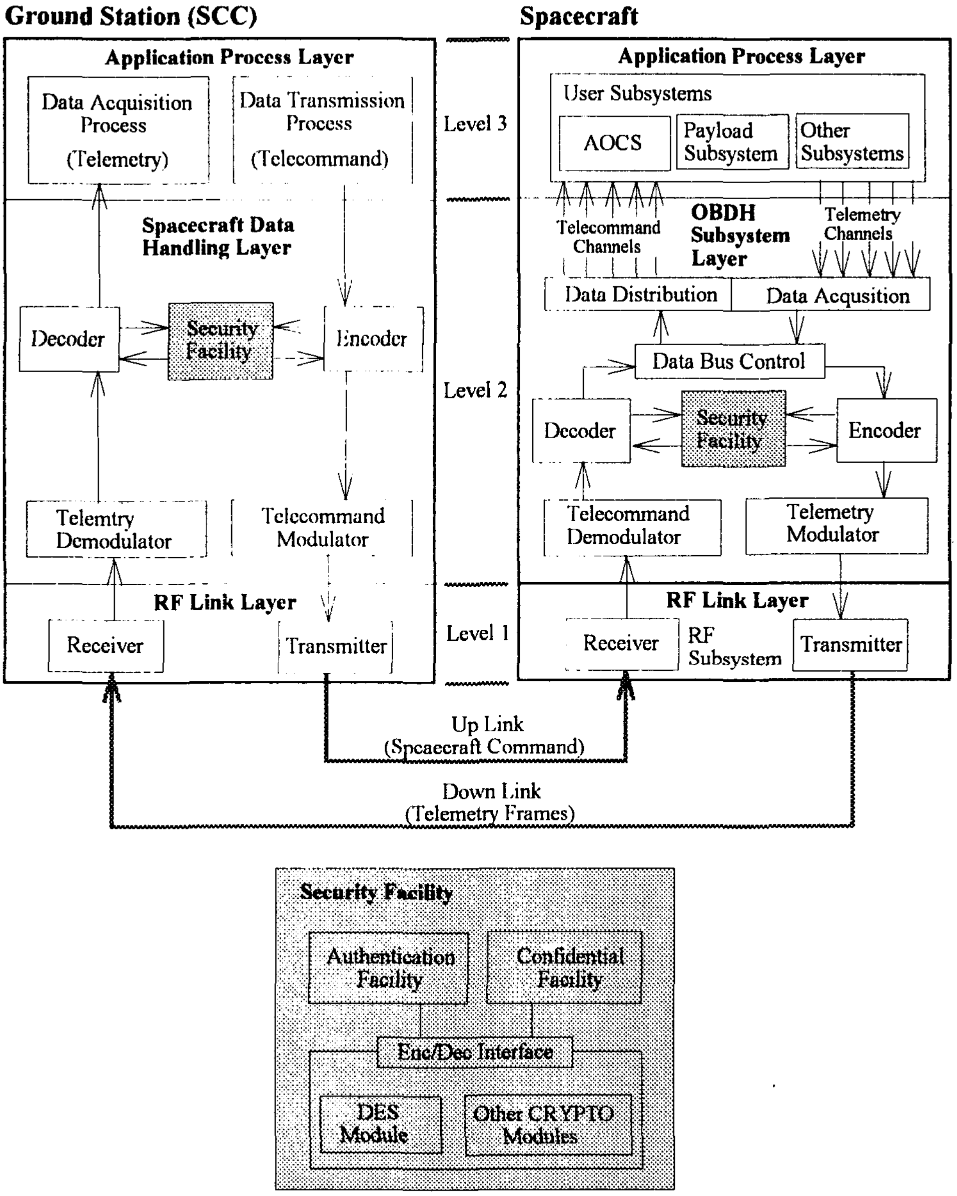
Step 1. A	: Generate a telecommand TC;
Step 2. A	: Calculate authenticator $MAC_A = E_{WK_A}[\{TC, SEQ_A\}]$;
Step 3. A	: Encode a spacecraft command SCMD = $\{SYNC, TC, MAC_A\}$;
Step 4. A ---> SAT	: Send the SCMD;
Step 5. SAT	: Receive and decode a SCMD = $\{SYNC, TC, MAC_A\}$;
Step 6. SAT	: Calculate authenticator MAC_{SAT}; $MAC_{SAT} = E_{WK_A}[\{TC, SEQ_A\}]$
Step 7. SAT	: Compare MAC_A and MAC_{SAT}; If both MACs are matched correctly, then set authentication status ASTAT to the success; If successful comparison, then increment SEQ_A by one; Otherwise, set authentication failure to ASTAT;
Step 8. SAT	: Encode telemetry TM;

TM = {SYNC, TC, MAC_A, ASTAT, other items}
Step 9. SAT ---> A : Send the TM;
Step 10. A : Receive the TM and decode it;
TM = {SYNC, TC, MAC_A, ASTAT, other items}
Step 11. A : If ASTAT is authentication success, then increment SEQ_A by one;

In the designed authentication protocol, sequence number is adopted to prevent any copied spacecraft command from being used for replay attack by hackers. The working key is used to calculate the MAC for some period temporarily, and should be changed when the valid period expires. Communication satellite, should have a capability of real time processing, can employ fast DES implementation using current hardware technologies for the authentication. SCC can use DES cipher using not only hardware implementation but also software implementations due to high performance of computer system.

4. Layered Architecture of the Security Enhanced Satellite System

For exploiting the proposed authentication mechanism, we present a layered architecture for the security management, from the general aspects of the design, as shown in figure-3. There are three level layers for communication and mission processing on both SCC and spacecraft [1,2,10,15]. In the second level of three layers, security facility is interfaced with the encoder and decoder that are used for preprocessing of modulator or post processing of demodulator. The SCC consists of application process layer, spacecraft data handling layer, and RF link layer. On the SCC side, data transmission process issues a telecommand for control of communication satellite. The issued telecommand is passed to encoder of spacecraft data handling layer for generating a spacecraft command. The spacecraft command encoder can use security facility to get a MAC or enciphered telecommand, and fill them into the spacecraft command structure. The spacecraft command will be sent to the communication satellite by RF transmitter after modulation. The spacecraft consists of application process layer including AOCS and payload subsystem, OBDH(On Board Data Handling) subsystem layer, and RF link layer. On the spacecraft, demodulated telecommand should be authenticated or deciphered by decoder whenever the spacecraft command is received by RF receiver. The authenticated telecommand could be routed to the related internal subsystem through telecommand channels connected to data bus control mechanism. The security facility has the authentication and confidentiality mechanisms, and can be flexibly reconfigured with extended security capabilities. These security facilities are connected to the cryptographic modules to have encryption and decryption capabilities through common interface.



<Figure-3> Layered Architecture : Security Enhanced Mànagement

5. Conclusion

After launching the communication satellite, secure control issue is an important task to maintain attitude, orbit, and resources of the satellite. SCC(Satellite Control Center), TT&C(Telemetry, Tracking, and Commanding), and NCC(Network Control Center) should be in charge of monitoring and control of communication satellite network. Especially, the SCC is responsible for issuing the spacecraft command to control the spacecraft directly. Generally, there are many kinds of threats on the RF link between the SCC and the spacecraft. For protecting the satellite communication system against the vulnerabilities, security services and mechanisms are required for secure control of communication satellite.

In this paper, we give the details of a design for security architecture and authentication mechanism. For exploiting security services to be incorporated to the SCC and communication satellite, authentication protocols and encryption schemes are proposed based on the DES cryptosystem. The proposed security architecture can be implemented by employing fast DES-based hardware and software technologies sufficient to achieve the real time processing capability for communication satellite. Performance analysis and the implementation of the proposed mechanism still remain for the future works.

References

1. M. H. Harati, "ZOHREH : The Iranian Domestic Satellite System," Proceedings of '92 UN Workshop on Space Communication for Development, Seoul, Korea, Nov. 24 - 27, 1992, pp. 141 - 154.
2. S. Braithwaite, "Spacecraft Technology : Data Handling," Course Vugraphs, Department of Aeronautics and Astronautics, University of Southampton, UK, Sep. 6 - 19, 1992, pp. 4 - 10 of Chapter 18.
3. Horst Feistel, william A. Notz, and J. Lynn Smith, "Some Cryptographic Techniques for Machine-to-Machine Data Communications," Proceedings of the IEEE, Vol. 63, No. 11, Nov. 1975, pp. 1545 - 1554.
4. Ralph C. Merkle, "Secure Communications Over Insecure Channels," Communications of the ACM, Vol. 21, No. 4, Apr. 1978, pp. 294 - 299
5. Roger M. Needham and Michael D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Communications of the ACM, Vol. 21, No. 12, Dec. 1978, pp. 993 - 999.
6. Gustavus J. Simmons, "Symmetric and Asymmetric Encryption," Computing Surveys, Vol. 11, No. 4, Dec. 1979, pp. 305 - 330.
7. Gerald J. Popek and Charles S. Kline, "Encryption and Secure Communication Networks," Computing Surveys, Vol. 11, No. 4, Dec. 1979, pp. 332 - 356.
8. Victor L. Voydock and Stephen T. Kent, "Security Mechanisms in High-Level Network Protocols," Computing Surveys, Vol. 15, No. 2, Jun. 1983, pp. 135 - 171.
9. Martin E. Hellman, "Commercial Encryption," IEEE Network Magazine, Vol. 1, No. 2, Apr. 1987, pp. 6 - 10.
10. Ki-Yoong, Hong, "Secure Control of Satellite Communication System Using Cryptosystem," Proceedings of the 9th Korea Automatic Control Conference International Session, Taejeon, Korea, Oct. 1994, pp. 218 - 223.
11. Jennifer Seberry and Josef Pieprzyk, "Cryptography: An Introduction to Computer Security," Prentice Hall of Australia Pty Ltd, Edited by Richard P. Brent, 1989, pp. 77 - 89.
12. Han Hwangbo, "Mugunghwa - The First Korean Domestic Satellite for FSS & DBS

Services," Proceedings of '92 UN Workshop on Space Communication for Development, Seoul, Korea, Nov. 24 - 27, 1992, pp. 165 - 174.

13. 강자영, 김재한, "인공위성의 활용과 발전 추세," 통신위성.우주산업연구회지, 제2권 창간호, 1993. 10, pp. 34 - 49.
14. 공남수, "위성통신 감시제어 시스템 기술 소개," 통신위성.우주산업연구회지, 제2권 제1호, 1994. 4, pp. 58 - 65.
15. 김동규, "위성 통신 시큐리티(Security)의 구조적 개관," 통신위성.우주산업연구회지, 제2권 제1호, 1994. 4, pp. 105 - 110.
16. 정선종, "무궁화 위성에 의한 디지틀 위성 방송 서비스 전망," 통신위성.우주산업연구회지, 제2권 제2호, 1994. 8, pp. 8 - 12.