'94 KACC (1994. 10. 17 ~ 20)

# Secure Control of Satellite Communication System using Cryptosystem

**Ki-Yoong Hong**

TT&C Section, Satellite Communications Division, ETRI
Yusong P.O.BOX 106, Taejon, 305-600, Korea
Tel: 82-42-860-5610, Fax: 82-42-860-6430
E-Mail: kyhong@kepler.etri.re.kr

## ABSTRACT

On the satellite communication system, conventional key issues of control have been focused on the attitude and orbit control, monitoring and control of communication payload such as IOT(In-Orbit-Test) and CSM (Communication System Monitoring), TT&C(Telemetry, Tracking, and Commanding) and so on. As the vulnerabilities are being increased on the satellite communication network, security services are required to protect it against security violated attacks. In this paper, a security architecture for satellite communication network is presented in order to provide security services and mechanisms. Authentication protocol and encryption scheme are also proposed for spacecraft command authentication and confidentiality.

**Keywords:** Satellite Communication, Telecommand Security, SCC, TT&C, Authentication, Encryption

## 1. Introduction

Nowadays, communication and information services utilizing satellite communication system are rapidly growing. For communication services of voice/data transmissions and broadcasting, there are a lot of GEO(Geosynchronous Orbit) satellites in space. Currently, constellation frameworks of LEO(Low Earth Orbit) satellites are also considerably required to provide mobile communication and personal communication services in universal. Satellite systems also tend to extend their connectives towards data communication networks, PSTN(Public Switched Telephone Network), and many kinds of ground network systems. The sensitive users and organizations using satellite systems have needs to protect their sensitive or proprietary information because there are unprotected domains in the satellite communication network, especially wireless satellite communication links. It is more important to provide security service for not only sensitive users but also satellite management and control center such as TT&C(Telemetry, Tracking, and Commanding) site, SCC(Satellite Control Center), and NCC(Network Control Center). These centers should have capabilities to access and control satellite system securely against any kind of vulnerabilities because communication satellite or its key component may have unpredictable behavior or unstable state due to any kind of unauthorized or incorrect spacecraft commands. Generally, there are many kinds of threats that are masquerade, data modification, unauthorized resource use, and unauthorized disclosure, and so on [2,3,4,7,8]. Security mechanism for authenticated spacecraft commands is a key element in order to maintain stable and secure state of communication satellite, especially its attitude and orbit, and communication payload status.

In this paper, a security architecture for satellite communication network is presented in order to provide security services and mechanisms. Authentication protocol and encryption scheme are also proposed for spacecraft command authentication and confidentiality.

## 2. Security Services and Mechanisms for Satellite Communication Network

### 2.1 Satellite Communication Network Overview

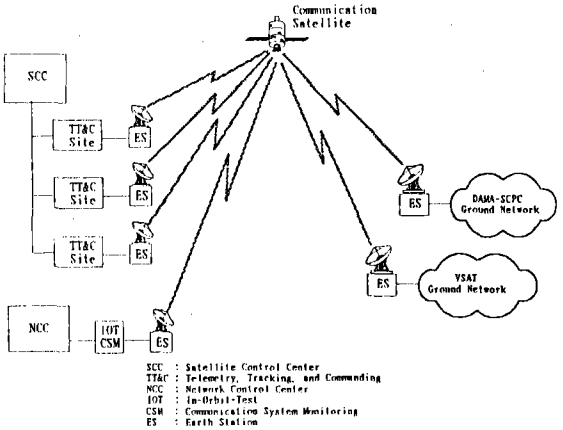
Satellite communication network consists of communication satellite and various kinds of components such as TT&C(Telemetry, Tracking, and Commanding) site, NCC(Network Control Center), terrestrial communication networks based on VSAT(Very Small Aperture Terminal) and DAMA-SCPC(Demand Assignment Multiple Access - Single Channel Per Carrier), etc. An overall configuration of satellite communication network is illustrated on figure-1.

### 2.2 Security Services

In satellite communication network, RF links between communication satellite and ground segment are vulnerable in air interface. There may be also security threats on the centers and other terrestrial network systems such as masquerade, data modification, unauthorized disclosure, illegal attack of spacecraft command, and illegal system access [2,3,4,7,8,14]. For protecting either computer and communication system or satellite communication network against any kind of attacks, the following security services are possibly required.

- Access Control Service

  Access control service provides a capability to prevent unauthorized personnel or communication entity from illegally having an access right on system resources such




<Figure-1> Overall configuration of satellite Communication network

as communication service, payload channel, or capability of the centers. The access control service enables two kinds of services including mandatory access control and discretionary access control services. Mandatory access control service enforces a rule based access control policy that describes access control decision based on the security labeling of resources and user's clearance. Discretionary access control makes an access limitation based on identity based security policy.

- Authentication Service

  Authentication is a security service to prevent unauthorized person or communication entity from illegally impersonating. For the authentication, it is essential to have a capability for validation of the identity of message, node, user, or data origination, etc. The authentication service provides two kinds of authentication schemes such as peer entity authentication and data origin authentication. Communication entities could be secure by means of authentication scheme to verify the identity of the peer entity or party on the logically established communication connection. Data origin authentication enables the recipient to prove the identity of sender as a transmitting source of data unit.

- Confidentiality Service

  Sensitive or proprietary information should be secure against data disclosure in transit on the communication links. Confidentiality service means that unauthorized person or communication entity can not have the message contents or can not analyze traffic flows on the communication network.

- Data Integrity Service

  Communication parties should recognize that unauthorized person or communication entity from illegally modifying or corrupting the information content on the communication link. Data integrity service enables protection capability against an attack of data modification to sensitive information.

- Non-repudiation Service

  Activities among communication entities or parties should be maintained securely against any repudiation of services or activities. Non-repudiation is a security service to prevent person and communication entity or party from illegally repudiating any kind of communication activities.

For the purpose of exploiting security services, we should provide one or any combination of security mechanisms such as access control, encryption, digital signature, data integrity, authentication, key management, traffic padding, routing control, and notarization mechanisms [2,3,7,8,9,19]. Encryption mechanism is suitable for authentication and confidentiality services that are closely related to major issue of this paper.

### 2.3 Encryption mechanism

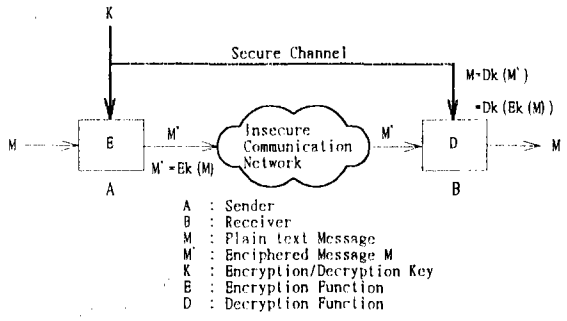
Encryption mechanism enables communication user to protect the sensitive message by converting a plaintext message to the enciphered message. We call this process the encryption. Encryption process requires a key, that is encryption key, to invoke the encryption mechanism for the encipherment of message. When a user wants to have original contents of the message, i.e., plaintext message, from the encrypted message, the user should decrypt the encrypted message by means of a specific key called decryption key. To classify the cryptosystems of encryption and decryption, we can arrange the cryptosystems in symmetric key cryptosystem and asymmetric key cryptosystem [2,3,4,5,6,10]. These cryptosystems have extinguishable characteristics of encryption and decryption process with different key management schemes.

#### 2.3.1 Conventional cryptosystems

Symmetric key cryptosystem has a single key as symmetric for encryption and decryption of the message. In conventional cryptosystems such as symmetric key crytosystem, both encryption and decryption processes require same key in order to encrypt and decrypt the message. This means that keys must be initially transmitted via secure channels so that both parties can have knowledge of them before encrypted message can be sent over insecure channels. Figure-2 shows encryption and decryption functions incorporated with single key. Sender A, who wants to send the message m securely via insecure communication channel, encrypts the message m with encryption key k. After encryption of message M, the encrypted message M', i.e., $E_K(M)$, would be sent to receiver B. Only receiver B with decryption key, that is the same key that was assigned to encryption process, can have original message M after decrypting the received message M', i.e., $D_K(E_K(M))$ is equivalent to M. Secrecy of symmetric cryptosystem is dependent upon how the cryptosystem can privately maintain the key, that is commonly used for both encryption and decryption process, by means of protection scheme such as temper-proof device. DES and FEAL cryptographic algorithms are belong to symmetric key cryptosystem.

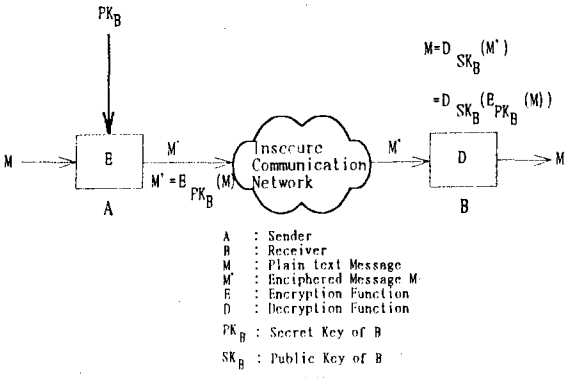
#### 2.3.2 Public key cryptosystems

In public key cryptosystems, there is a pair of two asymmetric keys such as public key and secret key [2,3,4,5,6,10,11,12,13]. A public key can be revealed for encryption process, and a secret key is a decryption key and should not be disclosed. Each key is the functional inverse of the other key, such that using one of the keys on a message produces ciphertext that can be converted back to plaintext by other key. Secure channels are not required to transmit keys on the contrast to the symmetric key cryptosystems, because the intended recipients of a



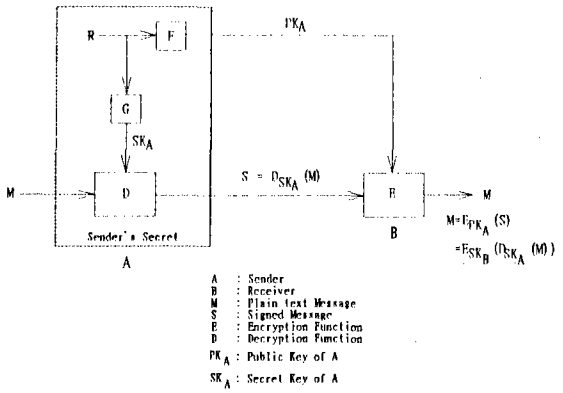

<Figure-2> Mechanism of Symmetric Key Cryptosystem

message have already publicly revealed their encryption keys that can be published in a public key directory or bulletin board. Figure-3 illustrates the encryption and decryption schemes of public key cryptosystems. When user A who wants to send a message M to the recipient B encrypts the message by using the intended recipient B's encryption key $PK_B$, that is already known to the sender A, before sending it. Encrypted message M', that is $E_{PK_B}(M)$, is transmitted to the recipient B via communication network, and can be correctly decrypted only by B with secret key $SK_B$. Any other person only except B, even the sender A, can not decrypt the encrypted message M', that is $E_{PK_B}(M)$, because of lack of knowledge about B's secret key $SK_B$.




<Figure-3> Mechanism of Public Key Cryptosystems

A useful consequence derived from public key cryptosystems is digital signature mechanism. In [2], Diffie and Hellman proposed the use of a digital signature based on public key cryptosystems illustrated on figure-4. The sender A of the message M is in charge of generating a pair of public key $PK_A$ and secret key $SK_A$. As shown in figure-4, these keys are derived from a random seed value R by means of public algorithms F and G in the system. The sender A's public $PK_A$ and secret $SK_A$ keys are normally used for encryption and decryption with public cryptographic algorithm E and D, respectively. Each functional process of cryptographic algorithms E and D is reserved for the other in the digital signature process. For generating a signature, the sender A makes a transformation of message M into a signed message S, i.e., $D_{SK_A}(M)$, by means of employing decryption of M with secret key $SK_A$. The recipient B can obtain the message M by encryption as $E_{PK_A}(S)$ using A's public key $PK_A$. The transformation process of the message M by A's signature is not an encryption process because any other person can recover the message M using A's public key $PK_A$. The effectiveness of a signature lies in the certain knowledge of the public key of the sender. Only the sender A knows secret key $SK_A$, and only A can generate a signature using the $SK_A$. Due to public information $PK_A$ to everyone, anyone can perform a verification process of the signature. A world wide known public key cryptographic algorithm is developed by Rivest, Shamir, and Adleman, and is called the RSA based on the initial capital letter of the name. The RSA algorithm is very popular public key cryptographic algorithm. RSA algorithm can be licensed from RSADSI(RSA Data Security Inc.) in Redwood City, California [3,12,13].




<Figure-4> Principle of Digital Signature

## 3. Authentication and Encryption Control of Communication Satellite

After launching a communication 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 the following section, we propose authentication and encryption schemes that can be employed directly, without third party KMC(Key Management Center), to both SCC and communication satellite for efficient real time processing.

### 3.1 Authentication Control of Communication Satellite

Authentication enables SCC and NCC to make an authenticator 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. Generally, the TC&R(Telemetry, Command, and Ranging) subsystem can be in charge of authentication process in the communication satellite. For

authentication control of communication satellite, we propose two kinds of authentication protocols based on the pre-studied cryptosystems such as DES and RSA without third party KMC(Key Management Center) for real time telecommand and telemetry processing.

● Notations

- $E_K[\,]$ : Encryption Function of Single Key Cryptosystem with Key K
- $D_K[\,]$ : Decryption Function of Single Key Cryptosystem with Key K
- $E_{PK}<>$ : Encryption Function of Public Key Cryptosystem with key PK
- $D_{SK}<>$ : Decryption Function of Public Key Cryptosystem with key SK
- MK : Master Key
- $WK_X$ : Working Key of ID X
- $PK_X$ : Public Key of ID X
- $SK_X$ : Secret Key of ID X
- A : Unique ID of Satellite Control Center
- SAT : Unique ID of 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

● Authentication Only using Single Key Cryptosystem

Let us assume that only one master key MK is kept on the tamper-proof storage of the communication satellite and also maintained on that of the SCC. Initially, the master key should be loaded into the communication 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 authentication signature S. The authentication signature can be a k-bit selected output of final ciphertext, that is called MAC(Message Authentication Code), calculated by means of DES CBC, CFB, or OFB mode. The master key is a key encryption key for the purpose of encrypting a working key. The working key is a data encryption key in order to generate an authentication signature of sensitive telecommand. The followings are authentication protocol based on encryption of single key cryptosystem;

Step 1. A : Generate a telecommand TC;
Step 2. A : Calculate authentication signature $S_A = E_{WK_A}[\{A, TC, SEQ_A\}]$;
Step 3. A : Encode a spacecraft command $SCMD = \{SYNC, A, TC, S_A\}$;
Step 4. A ---> SAT : Send the SCMD;
Step 5. SAT : Receive and decode a $SCMD = \{SYNC, A, TC, S_A\}$;
Step 6. SAT : Calculate authentication signature $S_{SAT}$; $S_{SAT} = E_{WK_A}[\{A, TC, SEQ_A\}]$
Step 7. SAT : Compare $S_A$ and $S_{SAT}$; If both authentication signatures are equivalent, then set authentication success to authentication status ASTAT; If successful comparison, then increment $SEQ_A$ by one; Otherwise, set authentication failure to ASTAT;
Step 8. SAT : Encode telemetry TM; $TM = \{SYNC, SAT, A, TC, S_A, ASTAT, other\ items\}$
Step 9. SAT ---> A : Send the TM;
Step 10. A : Receive and decode a TM; $TM = \{SYNC, SAT, A, TC, S_A, ASTAT, other\ items\}$
Step 11. A : If ASTAT is authentication success, then increment $SEQ_A$ by one;

In the 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 authentication signature for some period temporarily, and should be changed after valid period. A generated new working key can be transmitted securely as an encrypted form by means of master key MK, only known to the SCC and communication satellite. 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.

● Authentication Only using Public Key Cryptosystem

As shown on figure-4, digital signature scheme can be employed to the telecommand authentication between SCC and communication satellite. Let us assume that SCC generates public key $PK_A$ and secret $SK_A$, and send public key to the communication satellite. The following steps are authentication protocol based on the public key cryptosystem.

Step 1. A : Generate a telecommand TC;
Step 2. A : Calculate a signed message $S_A$; $S_A = D_{SK_A}<\{A, TC, SEQ_A\}>$
Step 3. A : Encode a spacecraft command $SCMD = \{SYNC, A, S_A\}$;
Step 4. A ---> SAT : Send the SCMD;
Step 5. SAT : Receive and decode a $SCMD = \{SYNC, A, S_A\}$;
Step 6. SAT : Encrypt $S_A$ with $PK_A$; $\{A, TC, SEQ_A\} = E_{PK_A}<D_{SK_A}<\{A, TC, SEQ_A\}>>$
Step 7. SAT : Compare the received ID A is equal to the decrypted ID A; Compare the recovered $SEQ_A$ is equal to the stored $SEQ_A$; If both comparisons are successful, then set authentication success to authentication status ASTAT; If successful comparison, then increment $SEQ_A$ by one; Otherwise, set authentication failure to ASTAT;
Step 8. SAT : Encode telemetry TM; $TM = \{SYNC, SAT, A, TC, S_A, ASTAT, other\ items\}$
Step 9. SAT ---> A : Send the TM;
Step 10. A : Receive and decode a TM; $TM = \{SYNC, SAT, A, TC, S_A, ASTAT, other\ items\}$
Step 11. A : If ASTAT is authentication success, then increment $SEQ_A$ by one;

### 3.2 Encryption Control of Communication Satellite

For adding an encryption mechanism, we give a formal description of the following protocols based on the upper described authentication protocols in the previous section.

● Authentication and Encryption using Single Key Cryptosystem

The following steps are presented for both authentication and encryption control based on single key cryptosystem.

Step 1. A : Generate a telecommand TC;
Step 2. A : Calculate a authentication signature $S_A = E_{WK_A}[\{A,TC,SEQ_A\}]$; Encrypt a TC, $encTC = E_{WK_A}[TC]$;
Step 3. A : Encode a spacecraft command SCMD, $SCMD = \{SYNC, A, encTC, S_A\}$;
Step 4. A ---> SAT : Send the SCMD;
Step 5. SAT : Receive and decode a SCMD = $\{SYNC, A, encTC, S_A\}$;
Step 6. SAT : Decrypt a encTC, $decTC = D_{WK_A}[E_{WK_A}[TC]]$; Calculate authentication signature $S_{SAT}$; $S_{SAT} = E_{WK_A}[\{A, decTC, SEQ_A\}]$
Step 7. SAT : Compare $S_A$ and $S_{SAT}$; If both authentication signatures are equivalent, then set authentication success to authentication status ASTAT; If successful comparison, then increment $SEQ_A$ by one; Otherwise, set authentication failure to ASTAT;
Step 8. SAT : Encode telemetry TM; TM = {SYNC, SAT, A, encTC, $S_A$, ASTAT, other items}
Step 9. SAT ---> A : Send the TM;
Step 10. A : Receive and decode a TM; TM = {SYNC, SAT, A, encTC, $S_A$, ASTAT, other items}
Step 11. A : If ASTAT is authentication success, then increment $SEQ_A$ by one;

● Authentication and Encryption using Public Key Cryptosystem

The following steps are presented for both authentication and encryption control based on public key cryptosystem.

Step 1. A : Generate a telecommand TC;
Step 2. A : Calculate a signed message $S_A$, $S_A = D_{SK_A}<\{A,TC,SEQ_A\}>$; Encrypt it, $encS_A$, $encS_A = E_{PK_{SAT}}<S_A>$;
Step 3. A : Encode a spacecraft command $SCMD = \{SYNC, A, encS_A\}$;
Step 4. A ---> SAT : Send the SCMD;
Step 5. SAT : Receive and decode a SCMD = $\{SYNC, A, encS_A\}$;
Step 6. SAT : Decrypt $encS_A$ with $SK_{SAT}$, $decS_A = D_{SK_{SAT}}<E_{PK_{SAT}}<S_A>>$; Encrypt a $decS_A$ with $PK_A$, $\{A,TC, SEQ_A\} = E_{PK_A}<D_{SK_A}<\{A,TC,SEQ_A\}>>$;
Step 7. SAT : Compare the received ID A is equal to the recovered ID A; Compare the recovered $SEQ_A$ is equal to the stored $SEQ_A$; If both comparisons are successful, then set authentication success to authentication status ASTAT; If successful comparison, then increment $SEQ_A$ by one; Otherwise, set authentication failure to ASTAT;
Step 8. SAT : Encode telemetry TM; TM = {SYNC, SAT, A, $encS_A$, ASTAT, other items}
Step 9. SAT ---> A : Send the TM;
Step 10. A : Receive and decode a TM; TM = {SYNC, SAT, A, $encS_A$, ASTAT, other items}
Step 11. A : If ASTAT is authentication success, then increment $SEQ_A$ by one;

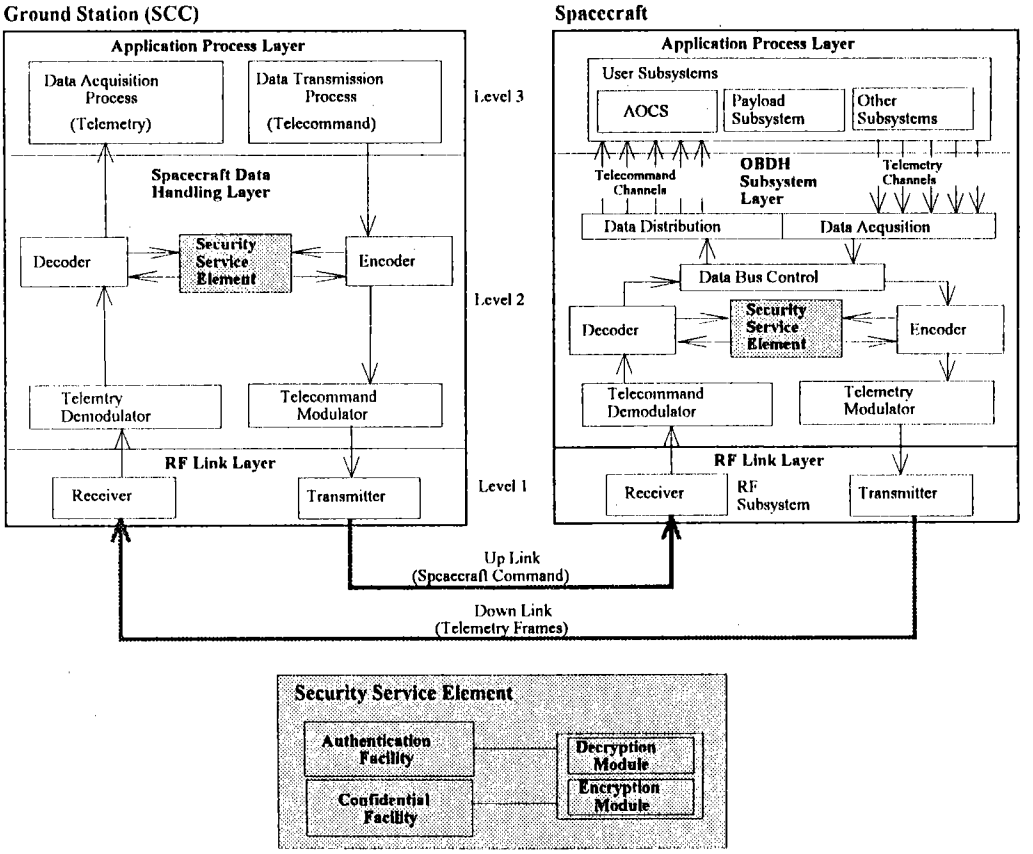
## 4. Security Architecture for Satellite Communication System

For exploiting proposed authentication and encryption services, we propose a conceptual design of security architecture for secure control of communication satellite as shown in figure-5. There are three level layers for communication and mission processing on both SCC and spacecraft. In the second level of three layers, security service element is incorporated to 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 service element to get authentication signature and enciphered telecommand, and fill them into the spacecraft command structure. The spacecraft command is 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 and deciphered by decoder whenever the spacecraft command is received by RF receiver. The authenticated telecommand could be routed to the related internal subsystem via telecommand channels connected to data bus control mechanism. The security service element has facilities of authentication and confidentiality, and can be flexibly reconfigured with extended security capabilities. These security facilities are connected to the cryptographic modules to have encryption and decryption capabilities.

## 5. Conclusion

After launching a 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 telecommand 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 cryptographic features of conventional cryptosystems and public key cryptosystems. For exploiting security services to be incorporated to the SCC and communication satellite, authentication protocols and encryption schemes are proposed based on the conventional cryptosystem and public key cryptosystem, respectively. A proposed security architecture for enforcing these security services is also presented. The security architecture can be implemented by




<Figure-5> Security Architecture for Secure Control of Communication Satellite

employing fast DES-based hardware and software technologies sufficient to achieve the real time processing capability for communication satellite.

## References


1. 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.
2. Whitfield Diffie and Martin E. Hellman, "New Direction in Cryptography," IEEE Transaction on Information Theory, Vol. IT-22, No. 6, Nov. 1976, pp. 644 - 654.
3. R. L. Rivest, A. Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, Feb. 1978, pp. 120 - 126.
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. David B. Newman, Jim K. Omura, and Raymond L. Pickholtz, "Public Key Management for Network Security," IEEE Network Magazine, Vol. 1, No. 2, Apr. 1987, pp. 11 - 16.
11. Robert R. Jueneman, "Electronic Document Authentication," IEEE Network Magazine, Vol. 1, No. 2, Apr. 1987, pp. 17 - 23.
12. Donald W. Davies, "Applying the RSA Digital Signature to Electronic Mail," IEEE Computer, Vol. 16, No. 2, Feb. 1983, pp. 55 - 62.
13. Philip Zimmermann, "A Proposed Standard Format for RSA Cryptosystems," IEEE Computer, Vol. 19, No. 9, Sep. 1986, pp. 21 - 34.
14. 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.
15. 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.