위성관제통신에서 안정성을 위한 인증

박 정 현† · 임 선 배†

요 약

본 논문에서는 위성관제센터와 위성간의 명령어 및 텔레메트리 통신의 안정성을 위해 Shamir의 서명 방식을 변형한 인증 방식을 제안한다. 제안된 방식은 위성 고유 ID를 이용하며 재생 공격에 대한 보호를 위해 시간 함수를 도입한 패스워드 개념의 인증 방식으로 위성의 실체 인증을 위해 사용한다. 또 사용중인 키와 알고리즘 내용을 포함한 명령어 카운터가 메시지 로딩과 명령어 실행시 인증으로 이용되며 이를 기반으로 위성관제통신의 안정성을 위한 인증 모델을 제안 하였다. 그밖에 위성관제센터와 위성간의 비밀 통신에 사용했던 비밀 키 교체와 확인을 위해 Two-way 키교체 방식을 제안 하였다.

Authentication for Security on Satellite Control Communications

Jeong Hyun Park† · Sun Bae Rim†

ABSTRACT

This paper presents an authentication model for security on satellite command & control communications. The proposed authentication scheme is based on the modified Shamir's signature scheme using a satellite ID (Identity) and the model uses time stamp for protection of command replay attack from unauthorized center. The message authentication with command counter that includes an available key and the algorithm is for loading and execution of commands in the model. Two-way scheme for key change and confirmation between satellite control center and satellite is also proposed.

1. 서 론

위성관제통신에서 위성은 권한이 없는 곳으로부터 명령어 신호가 왔을 때는 이를 정확히 인증하여 받아들이지 않고 정당한 위성관제센터에서 온 신호만 받아들여 실행해야 한다. 만약 명령어 신호를 정확히 인증하지 못하면 위성은 악의를 가진 사람에 의해서 사보타지 될 수 있으므로 이를 방지할 수 있는 안전한 인증 프로토콜이 필요하다. 인증(Authentication)은 크게 사용자 인증과 메시지 인증으로 구분되며 사용자 인증은 엔티티 인증(식별:Identification) 형태로 이용되기도 한다. 또 암호 기술을 기본 개념으로 하는 인증은 대칭형 암호 알고리즘을 이용한 인증 방식, 비대칭 암호 알고리즘을 이용한 인증방식, 그밖에 영지식 기반(Zero-Knowledge based protocol)을 둔 인증방식[2]이 있다. 대칭형 암호 알고리즘을 이용한 인증 방식은 DES[13]등의 알고리즘을 이용하여 고속으로 구현될 수 있으나, 큰 비용을 요구하는 키관리 문제를 가지고 있다. 비대칭 암호 알고리즘을 이용한 인증 방식은 복잡한 키관리 문제는 없으나, 커다란 비밀키(Secret Key)의 저장, 공개키 디렉토리의 유지 또는 저장, 공개키 증명서(Certificate)의 인증, 요구되는 계산량(Computation Complexity)의 매우 커서 고속 동작

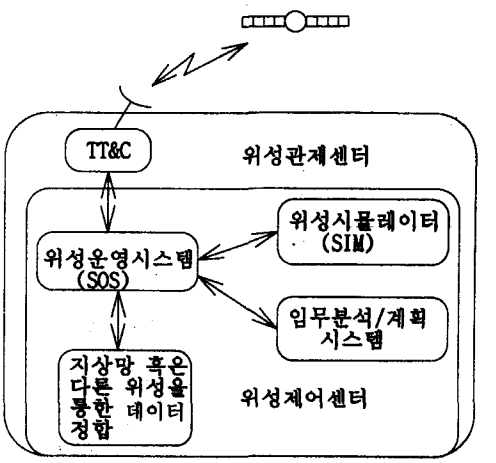
† 정 회 원:한국전자통신연구원 이동관리연구실
논문접수:1997년 1월 21일, 심사완료:1997년 9월 30일

이 불가능 한 것 등의 단점을 갖는다. 영지식 기본 인증 방식은 기본적으로 ID(Identity) 기본 시스템[12]에서의 인증을 위한 키관리 문제가 없고 요구되는 연산수가 비교적 작아 고속 동작이 가능하다. 그러나 사용자 신분 인증과 카드 발행을 위한 집중화된 키 인증센터(KAC:Key Authentication Center)가 요구되고, 인증시 이용되는 비밀키의 양이 비교적 많다. 그러나 영지식 기본 인증 방식은 계산량 및 소요 메모리 측면에서 상기의 인증 방식보다 우수하므로 특히 스마트 카드 분야에 널리 이용될 전망이다. 본 연구에서는 Shamir의 서명 방식[1]을 변형한 인증 방식을 제안한다. 제안된 방식은 위성 고유 ID를 이용하고 시간함수를 도입한 패스워드 개념의 인증 방식으로 위성의 실체 인증을 위해 적용하며 이를 기반으로 위성관제통신의 안전성을 위한 인증 모델을 제시 한다. 이를 위해 먼저 위성관제통신과 안전성을 살펴보았고 특별히, 위성관제통신의 안정성을 위해 인증 모델외 위성관제센터와 위성간의 비밀통신에 사용했던 비밀키 교체 방법과 확인 과정을 제시한다. 제안된 인증 모델과 키 교체 확인 방안은 위성관제통신에서의 안전성을 위한 연구 방향으로 활용 가능하리라 본다.

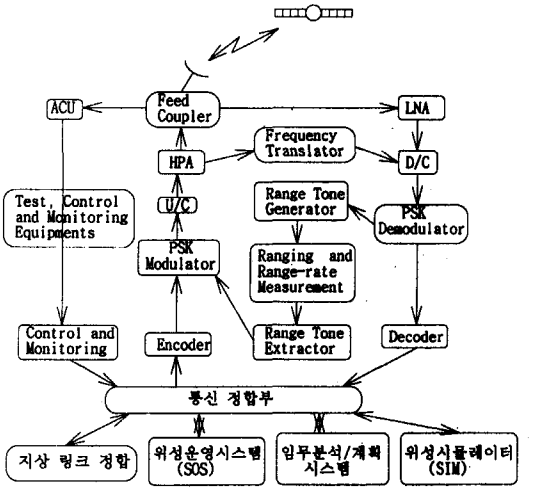
2. 위성관제통신과 안정성

2.1 위성관제통신망 구성

(그림 1)은 TT&C국을 중심으로 한 위성관제센터와 위성간의 시스템 구성이다. 여기서 TT&C국과 위성제어센터는 지상 링크로 직접 연결될 수 있고, 단일 홉(Single hop) 위성 혹은 두번의 위성을 거친 연결을 고려할 수 있으나 지역이 넓은 곳에서나 고려되며 보통은 위성제어센터와 TT&C국이 직접 연결되어 있다((그림 2) 참조).



(그림 1) 위성관제센터와 위성과의 통신 환경
(Fig. 1) Communication environments between command & control center and satellite



HPA: High Power Amplifier, U/C: Upconverter, LNA: Low Noise Amplifier
ACU: Automatic Gain Control Unit, D/C: Downconverter

(그림 2) TT&C국 기능 다이어그램
(Fig. 2) Functional diagram of TT&C system

• TT&C(Telemetry, Tracking and Command)

TT&C는 위성운영시스템에서 온 위성제어신호 및 위성 트래킹 명령어를 받아 전송 프레임 처리를 하고 변조후 S 밴드로 높여 위성으로 보낸다. 이 시스템은 또 실시간 텔레메트리 데이터를 받아 복조후 위성제어시스템으로 보낸다. TT&C는 안테나, RF 장비, IF 장비, 타임 및 주파수 기준 신호 생성부, 텔레메트리/텔레 명령어 처리부, 운영제어 및 관리부 등으로 구성된다. 그밖에 수신단에 LNA, 복조부, 그리고 디코더부 등이 있다.

• 위성 운영 시스템(Satellite Operation System)

위성운영시스템은 위성의 상태를 실시간 모니터링하며 통신을 통해 위성을 제어할 수 있는 원격 명령어를 만든다. 위성운영시스템은 원격 명령어를 보내

고 위성으로부터의 텔레메트리 정보를 수신하고 위성 임무를 분석하기 위해 위성임무분석 및 계획 시스템, 그리고 TT&C 사이에 통신 링크를 가진다. 위성운영 시스템은 TT&C에서 수신한 텔레메트리 데이터로부터 위성운영 헤더 정보를 추출하고 이를 위성 임무 분석 및 계획 시스템으로 보낸다. 위성운영 시스템은 위성과의 비접속 시점에 앞으로의 분석을 위해 실시간과 관련 자료를 저장하며 저장 데이터를 재처리하고 데이터 경향을 분석한다. 위성 운영 시스템은 위성 임무 분석 및 계획 시스템에서 생성한 임무를 처리하기 위해 원격 명령어 절차를 준비한다. 또한 위성운영 시스템은 TT&C를 정기적으로 모니터링 하며 워크스테이션을 포함한 컴퓨터 및 I/O 장비, 그리고 위성과 TT&C를 모니터하고 제어할 수 있는 S/W로 구성된다.

• 위성 시뮬레이터(Satellite Simulator)

수학적 모델을 이용해 위성의 동작을 시뮬레이션하기 위한 S/W이다. 위성 시뮬레이터는 명령어 검증, 운영 훈련, 위성제어절차 검증, 비정상적 상황의 분석 등을 하는데 이용한다. 실제 동작 환경에 대해 제약조건을 갖으면서 가능한 정확하게 위성의 상태를 모형화하는 위성 시뮬레이터 모델은 시뮬레이션 결과로 위성의 상태를 숫자/문자 형태로 궤도나 위치 정보를 나타내 준다. 위성 시뮬레이터는 실시간 동작하며 원격 명령어를 받아 관련 서브 시스템으로 분배하며 이를 텔레메트리 형식으로 위성 운영 시스템으로 보낸다. 위성 시뮬레이터는 여러 경우에 대한 초기 데이터를 데이터베이스화하고 있어 우주상태의 시뮬레이션을 가능케 한다.

• 임무 분석 및 계획 시스템

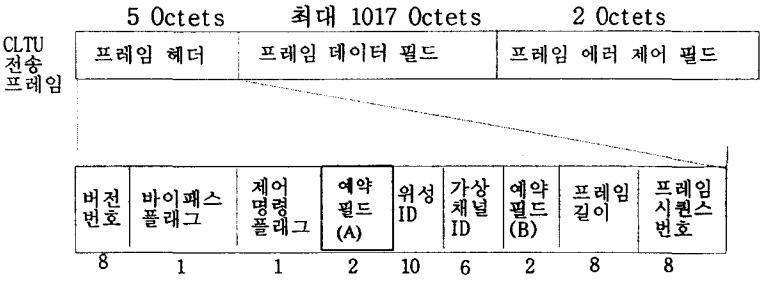
임무 분석 및 계획 시스템은 위성의 궤도 및 위치를 분석하고 예측하여 위성 동작 일정을 만들 수 있도록 해준다. 위성 이용자의 요구로부터 위성 궤도와 위치 정보를 갖고 임무 계획 일정을 발생한다. 위성 트래킹 데이터로부터 궤도 결정, 예측, 그리고 조정 기능을 하고 위성 위치는 특정 지역의 영상 데이터를 모아 이를 이용해 계산하는 위성 시뮬레이터는 임무 일정을 일간, 주간 등 이용자 요구에 따라 발생 가능하다. 이 임무 일정은 위성 운영 시스템으로 보내 명령어를 생성하는데 이용된다. 임무 분석 및 계획 시스템은 워크스테이션에 주변장치 그리고 임무 분석 및 계획 S/W로 구성된다.

2.2 위성 전송 프레임 구조

지상망과 연결된 환경에서는 TT&C국과 위성제어센터간에 특정 프로토콜(HDLC)이 이용되기도 한다. 그러나 이는 위성제어센터와 TT&C국 사이에 존재하며 TT&C국에서 위성, 그리고 위성에서 TT&C국 사이에는 존재하지 않는다. HDLC를 이용할 경우 명령어 생성기에서 발생한 명령어는 명령어 프로토콜에 따라 명령어 프레임에 부쳐지며 이 명령어 프레임은 암호화되어 HDLC 프레임에 넣어지게 된다. TT&C국은 HDLC 오버 헤드를 자르고 암호화된 명령어 메시지를 명령어 신호 발생기로 입력해 위성으로 전송하게 된다. 위성은 이 메시지를 받아 복호화한 후 실행하게 된다. 위성관제센터와 위성간에 주고 받는 전송 프레임의 기본 구조는 (그림 3), (그림 4)와 같다. (그림 3)은 위성으로 보내지는 명령어를 위해 TT&C국에서 만들어지는 기본 전송 프레임 형태이고 (그림 4)는 위성에서 위성관제센터로 보내지는 텔레메트리 신호에 대한 프레임 형태이다. TT&C국에서 위성으로 보내는 Forward Channel 혹은 Uplink 프레임을 CLTU(Command Link Transmission Unit)라 하며 위성에서 위성관제센터로 보내는 Backward Channel 혹은 Downlink 프레임을 CLCW(Command Link Control Word)라 한다. 이들 프레임 구성은 다음과 같다.

• CLTU(Command Link Transmission Unit)

원격 명령 전송 프레임 구조는 5 Octets 프레임 헤더, 최대 1017 Octets의 가변적인 프레임 데이터 필드, 선택적인 2 Octets의 프레임 에러 제어 필드로 구성되며 최대 1022 혹은 1024 Octets의 길이를 갖는다. 또 프레임 헤더는 2 Octets에 걸쳐 버전 번호(2 bits), 바이패스 플래그(1), 제어명령 플래그(1), 예약 필드 A(2), 그리고 위성 ID(10)를 구성하며, 1 Octet내에 가상 채널 ID(6)과 예약필드 B(2)를 가지며 프레임 길이 1 Octet, 프레임 시퀀스 번호 1 Octet 등으로 구성된다. 프레임 데이터 필드는 최대 1017 Octets이고 원격 명령 데이터 혹은 제어 명령 정보가 포함된다. 프레임 에러 제어 필드는 FEC(Frame Error Control) 코



(그림 3) CLTU 기본 전송 프레임
(Fig. 3) Transport frame of CLCU

드로 16 비트 CRC(Cyclic Redundancy Check) 에러 검출 코드를 부가 한다.

• CLCW(Command Link Control Word)

CLCW는 위성내의 원격 명령 모듈에 의해 생성되고 원격 측정 전송 프레임의 운영제어필드(Operational Control Field) 혹은 가상채널 데이터 유니트(VCDU: Virtual Channel Data Unit)에 실려지는 4 Octets 제어정보로, 지상에 전송되는 원격명령 전송 상태 정보이다.

CLCW 프레임

(그림 4) CLCW 기본 프레임
(Fig. 4) Transport frame of CLCW

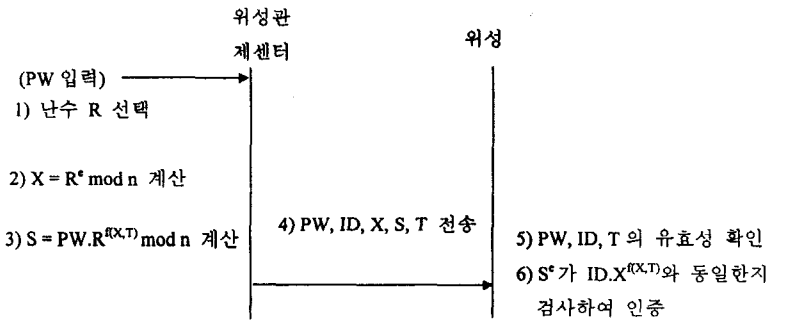
2.3 안전성

TT&C국에서 위성으로 전송하는 명령어는 위성에 의해 진정으로 TT&C국에서 보내온 신호인가를 확인할 수 있어야 한다. 권한이 없는 곳으로부터 명령신호가 왔을 때는 이를 정확히 인증하여 받아들이지 않고, TT&C국에서 온 신호는 받아들여 실행해야 한다. 만약 명령신호를 정확히 인증하지 못하면 위성은 악의를 가진 사람에 의해서 사보타지될 수 있으므로 안전한 인증 프로토콜이 필요하다. 특별히, 위성관제센터와 위성간의 통신에 있어서 안전성 문제는 기본적으로 위성제어 신호 내용을 권한이 없는자가 해독 및 악용하는데 있으며 전송중인 데이터에 불법적인 추가, 삭제, 그리고 변경의 문제, 그리고 과거에 이용되었던 제어신호의 재전송 문제 등으로 고려될 수 있다. 그밖에 다음과 같은 문제가 고려된다.

- 암호모드로 해서 명령어를 암호화하여 보낼 때 비권한자가 평문 모드로 전환 가능성
- 위성에서 보내온 텔레메트리 값이 파괴되었을 때 위성관제센터는 위성으로 리셋 명령을 보낸 후 다시 텔레메트리 정보를 보내도록 한다. 이때 비권한자가 이전 전송과정을 모니터링하여 재생공격 가능성
- 명령어 자체의 변경
- 위성에서 발생한 텔레메트리 메시지의 변경
- 복호기의 on/off 비트의 변경
- 인증 혹은 비인증 비트의 변경
- 위성관제센터의 실체 위장
- 위성관제센터에서 발생한 명령어 변경 전달 등

3. 위성관제통신을 위한 인증 방식

본 소절에서는 공개키 암호 방식에 기반을 두면서 인증서를 필요로 하지 않는 Shamir의 서명 방식에 패스워드(PW) 개념을 도입하여 위성관제센터와 위성간의 실체 인증을 위한 인증 방식을 제시한다. 이를



(그림 5) 위성관제센터와 위성간의 실체 인증 과정
(Fig. 5) Entity authentication procedure between command & control center and satellite

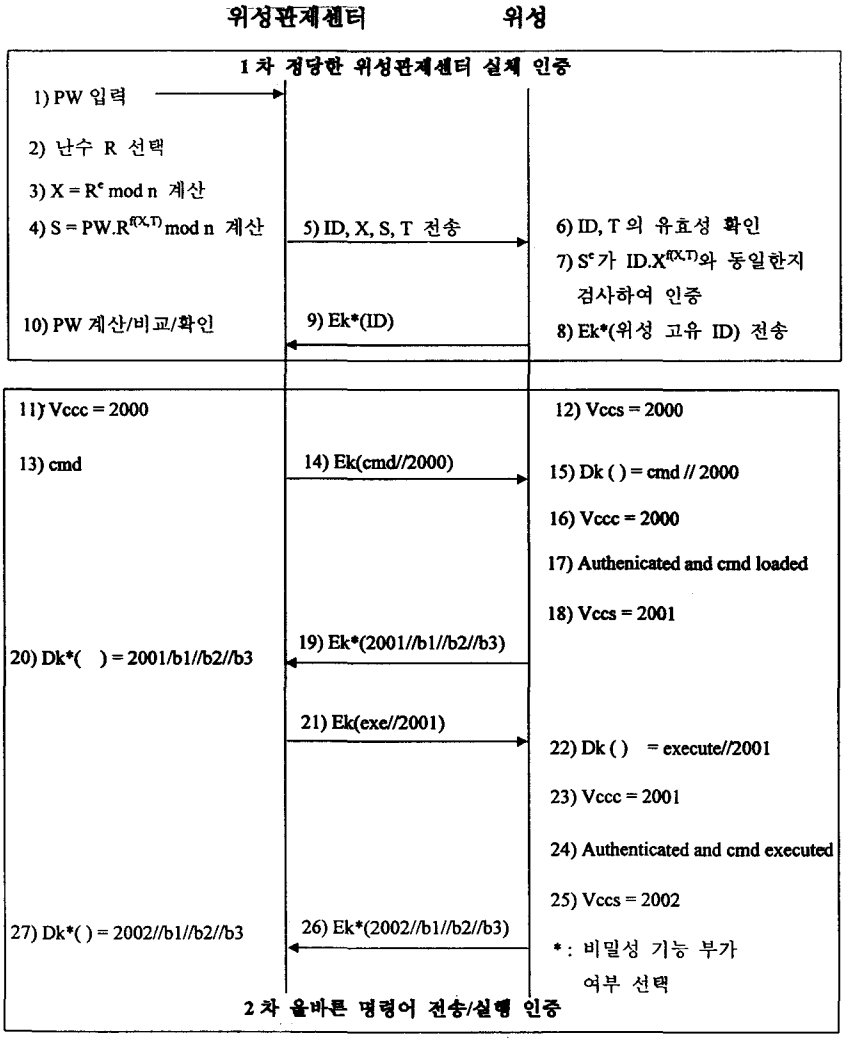
위해 키센터 기능을 갖는 위성관제센터는 RSA 서명 방식[10]의 공개정보(n, e)와 비밀정보(d, p, q), 그리고 일방향 함수 f를 준비 한다. 그리고 위성의 고유 ID로부터 $PW = (ID)^d \bmod n$을 계산한다. 이후 위성 발사시 d, p, q, f 그리고 PW를 저장한다. 여기서 p와 q는 큰 소수이며 n은 p와 q의 곱이다. 이후 위성에 접속하려는 이용자는 PW를 알아야 하며 정확한 PW를 가진 사람만이 위성으로부터 올바른 이용자로 인증을 받게 된다. (그림 5)는 위성관제센터와 위성간의 인증 과정이다.

위 인증 방식은 RSA 방식을 기반으로 합성수에 대한 소인수 분해의 어려움에 안전성을 두고 있기 때문에 계산량이 비교적 높다. 따라서 계산량은 많으나 높은 안전성을 기대하면서 비교적 단순하면서 일방향 인증 환경에 적합한 인증 방식이다. 또한 이 방식은 time stamp(T)를 도입하므로 재생 공격을 방지할 수 있게 했다.

4. 위성관제통신의 안전성을 위한 인증 모델

위성관제센터와 위성간의 통신에 있어 안전성 문제점을 해결하기 위해, 앞에서 제시된 Shamir의 서명 방식에 패드워드 개념을 도입하여 1차 위성의 실체 인증이 가능한 발신처 확인을 위한 인증으로 적용하고 이어서 카운터 값을 이용하여 명령어의 무결성과 보호를 위한 인증이 가능한 위성관제통신 안전성을 위한 인증 모델을 제시 한다. 여기서 1차 위성관제센터와 위성간의 실체 인증을 위한 기반은 RSA 방식에 바탕을 두며 올바른 명령어의 전송 및 실행 여부를 확인하기 위한 2차 인증에서는 인증의 처리 속도가 빠르면서 좀더 간단한 공통키 암호방식에 기반을 둔다. 이 경우 위성관제센터에서 위성으로 보내는 명령어에 비밀성 기능을 부가하는 것보다는 명령어의 무결성과 인증에 더욱 초점을 두는 형태가 바람직하며 이와 같이 1차 인증과 2차 인증을 거치므로 앞에서 언급된 안전성 문제를 해결하게 된다. 이들 인증 과정을 (그림 6), (그림 7), (그림 8), 그리고 (그림 9)에서 각각 제시 했다. 여기서 (그림 6)은 위성관제센터와 위성간에 정상적으로 이루어지는 인증 과정이며 1차 정확한 위성관제센터의 확인을 위한 인증 과정과 2차 올바른 명령어 및 실행 신호의 사용 여부 확인을 위한 인증 과정을 나타냈다. 그리고 (그림 7)은 위성관제센터에서 위성으로 메시지 전송시(Uplink) 에러가 발생했을 경우 인증 과정이며 (그림 8)은 Downlink에서 에러가 발생한 경우이고, (그림 9)는 Uplink와 Downlink에서 에러가 발생한 경우를 각각 보여 준다.

(그림 6)은 1차 실체 인증과 2차 명령어 인증 과정을 보여 주고 있다. 특별히 위성관제통신에서 명령어 보호의 목표는 명령어의 비밀성보다는 인증성과 무결성이다. 이는 위성과 위성관제센터간에 인증 방식을 도입한 암호 모드 동작으로 가능하다. 암호 모드에서 명령어 동작 절차는 평문 모드에서의 절차와 같이 전달되고 실행된다. 한 명령어는 명령어 부가 부분과 실행 부분이 있으며 명령어 인증은 각 부분에서 인증을 적용하므로 가능하다. 인증 방식은 위성과 위성관제센터간에 공통 암호 방식과 비밀키, 그리고 타

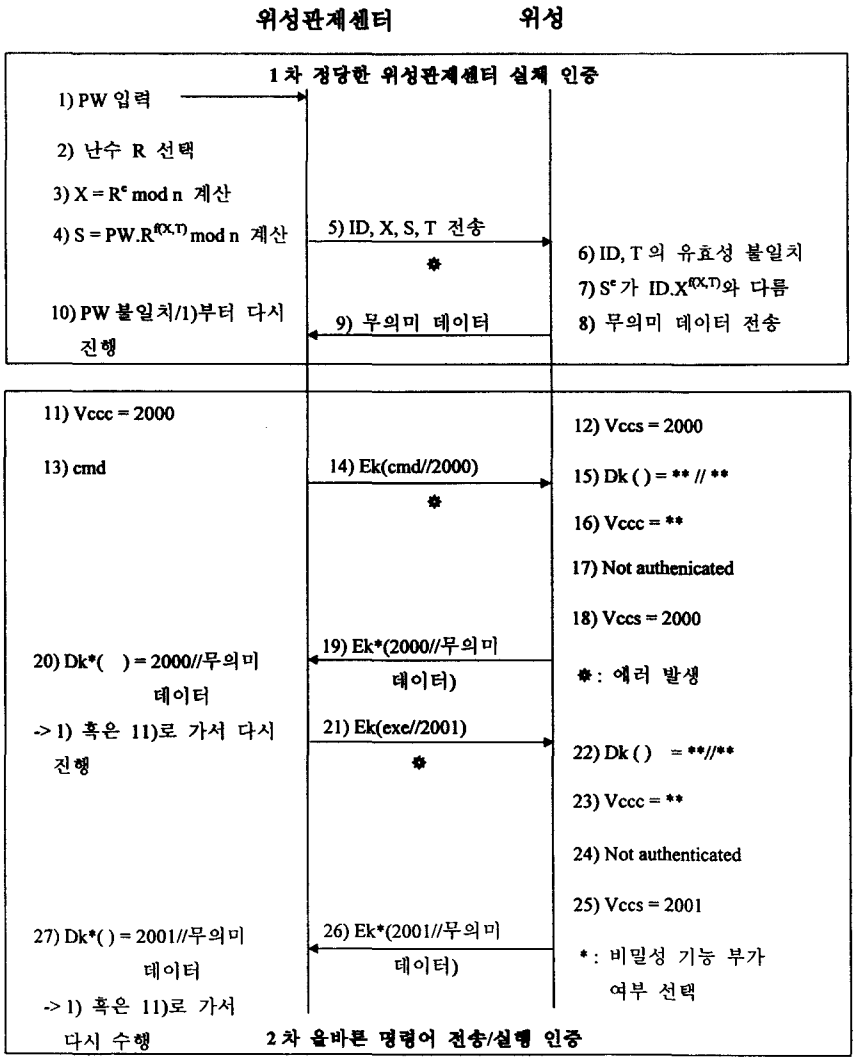


(그림 6) 위성관제통신 인증 모델

(Fig. 6) Authentication model for satellite command & control communications

당한 명령어 번호를 유지하게 하는 카운터를 공유하므로 가능하다.

비밀키는 위성과 위성관제센터에서 각 히 설치된 PROM에 보유하고 있는 키 중 하나를 선택해서 이용한다. 위성관제센터는 타당한 명령어 카운터 값을 (Vccc) 가져야 하며 위성도 타당한 명령어 카운터 값을 가져야 한다. 정상 동작 조건에서 두 카운터 값은 같은 수를 유지해야 하며 위성관제센터에서 위성으로 보내는 메시지 내에 이 카운터 값이 있다. 위성은 수신된 명령어가 위성관제센터에서 발생되었는지를 결정하는데 명령어 속에 내포된 카운터 값을 이용한다. 또한 위성관제센터에서 위성으로 보내지는 메시지 내에는 Vccc 값이 포함되며 각 전송에 대해 고유하다. 그 외 타이밍 정보를 추가하여 비권한자에 의해 행해지는 명령어 재생 공격을 방지할 수 있다. 위성관제센터에서 위성으로 보내는 메시지는 Ek(cmd/Vccc) 형태이며 여기서 Ek(*)는 암호키 k로 암호화한 것을 의미 한다. 또 //는 concatenation을 의미하며 cmd는

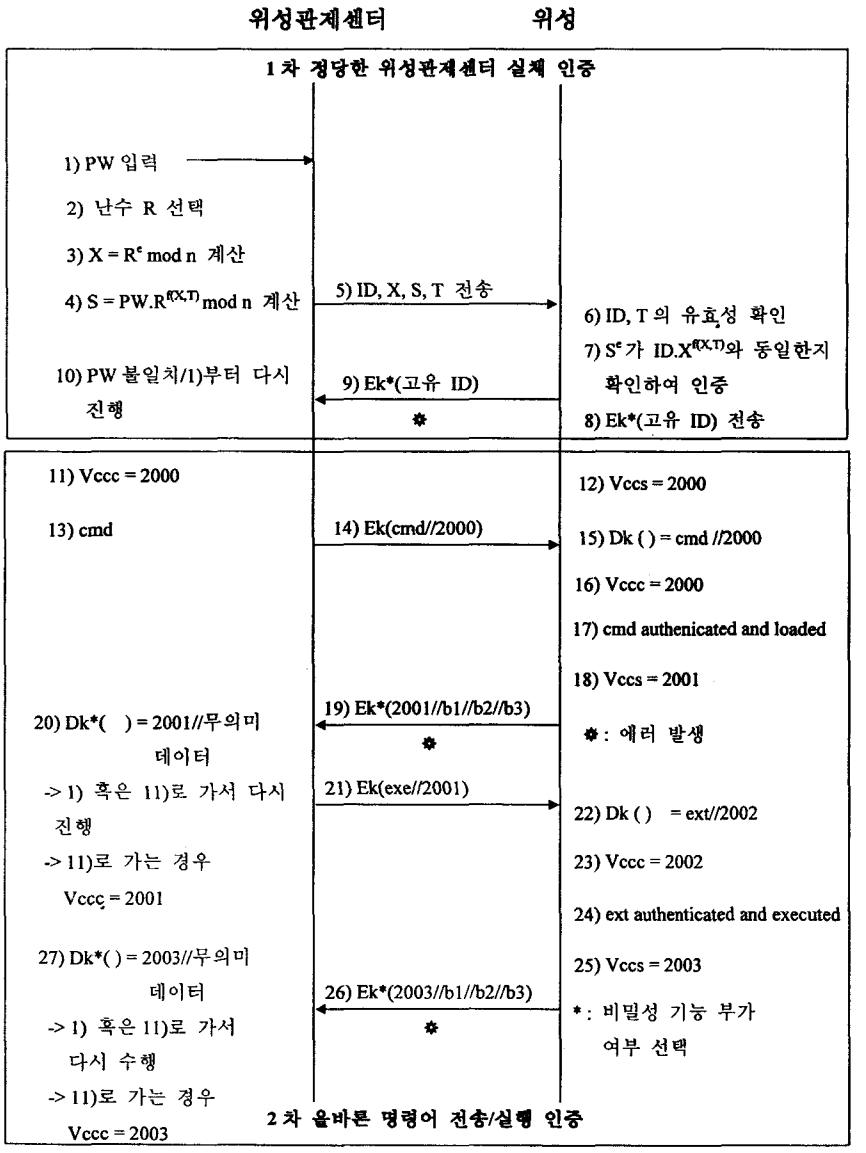


(그림 7) Uplink에서 에러가 발생된 경우
(Fig. 7) Case of error occurrence at up link

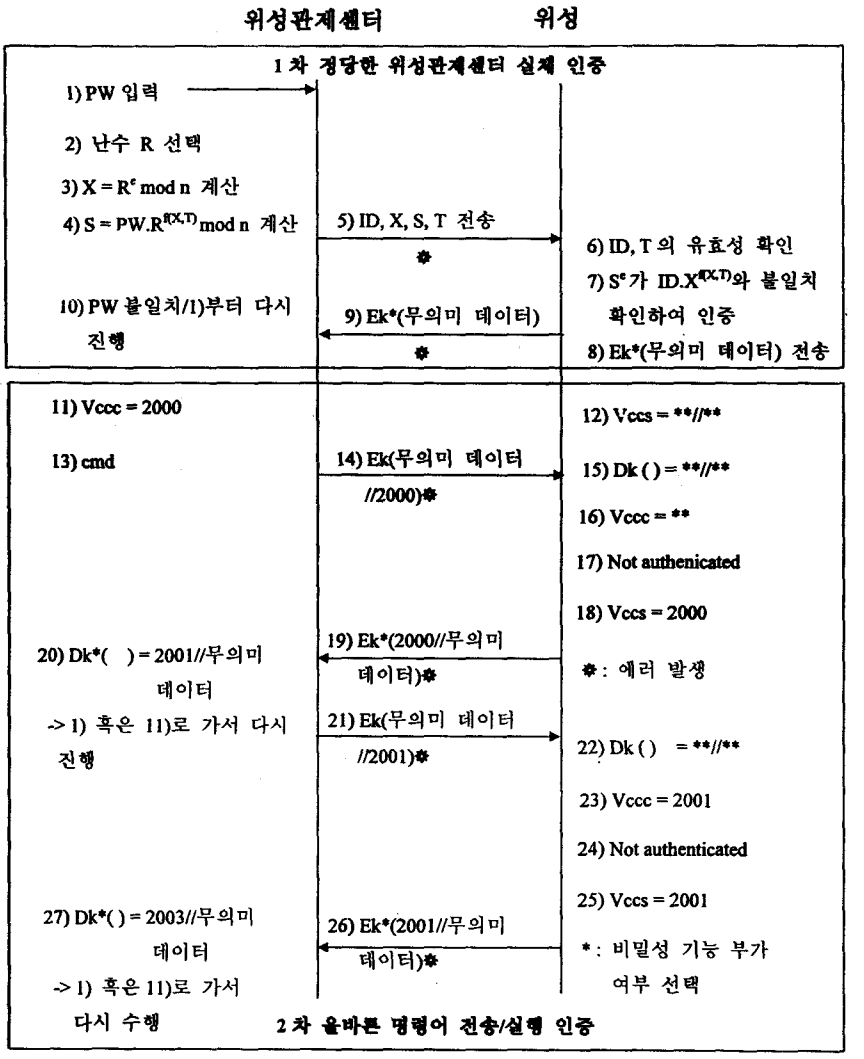
명령어, 그리고 exe는 실행 신호를 의미하고 Vccc는 위성관제센터에서의 카운터 값이다. 위성에서 위성관제센터로 보내는 텔레메트리 메시지는 Vccs//b1//b2//b3 형태를 갖으며 여기서 Vccs는 위성이 갖고 있는 카운터 값이며 b1은 복호기의 *on/off* 비트, b2는 복호기 busy/not busy 비트, b3는 authenticated/not authenticated 비트를 의미 한다. 다음은 위성관제센터와 위성간의 명령어 인증 시나리오이다. 명령어 인증을 위해 위성관제센터는 명령어를 발생하고 Vccc 내용을 추가한다. 이를 암호화하여 위성으로 보내면 위성은 이를 같은 암호 알고리즘을 이용해 복호화하고 Vccs 내용과 복호된 Vccc 내용을 비교한다. 이것이 같으면 위성은 명령어를 인증한 후 인증된 명령어를 명령어 레지스터로 넣는다. 그리고 위성은 Vccs 내용을 증가하고 3개의 평문 상태 비트에 Vccs의 내용을 추가해 위성관제센터로 보낸다. 위성관제센터는 수신한 텔레메트리 Vccs를 이용해 Vccc 값을 조정한다. 그리고 명령어 실행을 위해 명령어 대신 명령어

실행 신호로 바꾼 후 앞의 명령어 인증 과정과 똑같이 수행한다.

(그림 7)의 경우는 위성관제센터에서 위성으로 명령어 전송시 에러가 발생된 경우이며, 에러는 1차 인증시 혹은 2차 인증시 각각 발생 가능하다. 이런 경우 보통은 1차 인증 과정부터 다시 시작하며 전송 프레임 헤더 내의 2 비트 예약 필드를 이용해 선택적으로 처리 가능하다. 즉, 예약 필드 비트 값이 00의 경우는 사용치 않으며 01의 경우는 1차 인증 과정부터, 10의 경우 2차 인증 과정부터, 그리고 11의 경우는 사용 암호키의 교체 기능으로 한다. (그림 8)의 경우는 **위성**에서 위성관제센터로 텔레메트리 전송시 에러가 발생된 경우로 위성관제센터는 카운터 값만을 변경하여 인증 과정을 처음부터 다시 시작한다.



(그림 8) Downlink에서 에러가 발생된 경우
(Fig. 8) Case of error occurrence at down link



(그림 9) Uplink와 Downlink에서 에러가 발생된 경우
(Fig. 9) Case of error occurrence at up & down link

(그림 9)는 Uplink 혹은 Downlink 상에서 명령어 혹은 텔레메트리 전송시 에러가 발생된 경우로 위성관제센터는 카운터 값만을 변경하여 처음부터 인증 과정을 다시 시작한다.

5. 안전성을 위한 키교체 및 확인

위성과 위성관제센터간에 이용되는 암호키는 두개의 tamper-resistant module에 저장하여 하나는 위성을 쏘아 올릴 때 탑재하고 다른 하나는 위성관제센터에서 이용한다. 위성의 주기를 10년으로 본다면 예를 들어 하루에 한번씩 암호키를 교체한다고 가정할 때 3650개의 암호키가 필요하다. 하나의 키 바이트가 8바이트(64 비트)라면 전체 암호키를 저장할 때 필요한 메모리는 29.2 Kbytes 정도이다. 암호키 교체는 일정 시간이 지나거나 전송된 메세지의 양이 일정 한도를 넘을 때 자동으로 키교체 프로토콜을 수행하도록 한다. 특히 키의 전체 주기가 완료되기 전에 키를 교

체해야 하며 키 교체는 주로 위성관제센터에서 요구하여 행하는 것이 바람직하다. 또 암호키를 교체 할 때 송신과 수신측이 동시에 이루어져야 하므로 암호키의 교체에 있어 동기화 문제가 발생한다. 이 동기화 문제를 해결하기 위한 방법은 여러 가지 고려될 수 있으나 그 중 한가지가 지정된 시간에 키를 교체하는 방법이다. 그러나 이 방법은 암호 키 교체를 무사히 진행했는지 확인하기가 어려운 단점을 갖고 있어 추가 사항이 필요하다. 이를 위해 메모리에 저장해 놓은 암호키에 식별 번호를 부여하고 위성관제센터는 통신중에 주기적으로 현재 사용 중인 암호키의 식별 번호를 전송하고 암호키 교체를 할 때는 새로운 식별 번호를 전송하여 처리한다. 암호키 식별 번호는 암호화키 저장 메모리 주소로 생각할 수 있다. 위성에서는 항상 식별 번호를 체크하므로 현재 이용 중인 암호키가 올바른 것인지 확신을 가질 수 있으며 교체하는 도중에 통신이 두절되는 등의 문제를 해결할 수 있다. 그러나 이 방식 또한 통신 중에 식별 번호를 확인해야 하는 오버 헤드가 따르는 문제를 갖고 있다. 이에 위 두 방법의 문제점을 해결하기 위해 두 방법의 장점만을 모아 다음과 같은 방식으로 이용할 수 있다. 암호키 교체 시기를 미리 정해 놓고 그 시기의 전후 일정 시간 동안에 식별 번호를 이용한 키교체를 진행한다. 이렇게 하므로 정해진 시간만 키교체에 신경을 쓰면 될 것이고 키 교체 동기화의 확신을 가질 수 있으며 통신의 오버 헤드 증가나 일시적인 통신 두절 등의 문제를 해결 할 수 있을 것이다. 다른 방법으로는 위성과 위성관제센터간에 암호키 교체가 필요하면 언제든지 상호간의 통신에 의해 암호키를 교체할 수 있게 하는 것으로 가장 융통성 있는 방식이라 생각 된다. 암호키 교체는 다음과 같이 이루어지며 교체 과정은 자동적으로 이루어져야 한다.

과정 1: 위성관제센터는 위성에 키교체를 요구한다.
과정 2: 위성관제센터는 위성으로 다음에 이용할 암호키 식별 번호를 전달한다.
과정 3: 위성은 위성관제센터로 사용할 암호키를 확인한다.

위성과 위성관제센터간에 같은 암호키를 공유했는지 확인하기 위해 다음과 같은 two-way 인증 방식을 적용한다.

과정 1: 먼저 위성관제센터는 랜덤수 R을 만들어 암호화하여 위성으로 보낸다.
과정 2: 위성은 R을 복호화한 후 자신이 선택한 랜덤수 R′을 추가해 Ek(R//R′)하여 위성관제센터로 보낸다.
과정 3: 위성관제센터는 수신한 Ek(R//R′)를 복호화하여 수신한 R이 자신이 보낸 R과 같은지 확인하므로 위성관제센터와 위성간의 키가 공유되었음을 확신한다.
과정 4: 그리고 위성관제센터는 R′을 암호화하여 위성으로 보내며 위성에서는 이를 복호화하여 자신이 보낸 랜덤수 R′인지를 확인하여 같으면 서로간에 암호 키가 공유했음을 믿는다.

만약 확인 과정에서 오류가 발생되었으면 암호키 교체의 과정을 재시도 해야 한다. 기존에 암호키는 파기하여 나중에 읽더라도 알아 볼 수 없도록 해야 하며 파기하는 방법으로는 암호키에 암호키와 같은 크기의 랜덤수를 ex-OR하여 없앨 수 있다.

6. 결 론

위성관제통신에서 안전성은 전송 데이터의 비밀성보다는 인증성이 더욱 크다. 이에 본 연구에서는 기존의 인증 방식들을 분석하여 위성관제통신에 적합한 인증 방식을 제안 했다. 특별히 본 연구에서는 Shamir의 서명 방식을 변형하여 위성관제통신에서의 실체 인증 모델로 제시 했으며 이는 one-way 인증 환경에 적합하며 위성의 고유 ID를 이용해 패스워드 개념을 도입하여 위성을 접속하려는 이용자를 식별토록 했다. 또 제안된 인증 방식은 RSA 방식에 기반을 두면서 합성수의 소인수 분해의 어려움에 바탕을 두고 있어 안전성을 매우 높다고 할 수 있다. 그리고 위성관제통신에서 안전성을 위해 1차 실체 인증에 이어 2차 명령어의 인증이 가능토록 했다. 더욱이 명령어 인증에서는 위성과 위성관제센터간에 사용 중인 알고리즘, 비밀키, 그리고 타당한 명령어 번호를 결합한 카운터 값을 도입하였으며 명령어의 단계적 인증이

가능하도록 했다. 제안된 인증 방식을 기반으로 위성과 위성관제센터간의 정상적인 통신 과정에서의 인증 과정, Uplink에서 에러가 발생된 경우, Downlink에서 에러가 발생된 경우, 그리고 Uplink와 Downlink에서 에러가 발생된 경우에 대해 각각 인증 과정을 제시했다. 그밖에 위성관제센터와 위성간에 사용 중인 비밀키의 교체 및 변경 확인을 위해 two-way 인증 방식을 제안 및 적용해 보였다. 이는 위성관제통신에서의 안전성 문제를 보완할 수 있는 연구로 기대한다.

참 고 문 헌

[1] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. of Crypto'84, 1984.

[2] L.C. Guillou and J.J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors and Minizing Both Transmission and Memory," Eurocrypt'88, Lecture notes in Computer Science, Vol.330, pp.123-128, 1988.

[3] Tri T. Ha, "Digital Satellite Communications," Macmillan Publishing Company, 1986.

[4] M. Fiat and A. Shamir, "How to prove yourself: Practical solution to Identification and Signature Problems," Proc. Crypto'86, Santa Babara, Springer-Verlag, LNCS Vol.263, pp.186-199, 1986.

[5] R.L. Pickholtz, D.B. Newman, Y.Q. Zhang, and M. Tatebayashi, "Security Analysis of the INTELSAT VI and VII Command Network," IEEE Journal on selected areas in comm., Vol.11, No.5, pp.663-672, June 1993.

[6] J.H. Park and S.H. Lee, "A Key Distribution Scheme with Directly Mutual Authentication," Proc. of ICS'96, Taiwan, pp.60-66, December 1996.

[7] A. Shamir, "How to share a secret," Communication of the ACM, Vol.22, No.11, pp.612-613, November 1979.

[8] K. Koyama and K. Ohta, "Identity-Based Conference Key Distribution Systems," Proc. Crypto 87, pp.175-184, 1984.

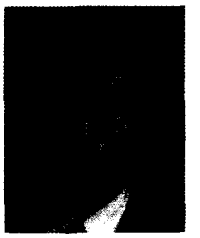
[9] W. Diffie and M. Hellman, "Privacy and Authentication: An Introduction to Cryptography," Proc. IEEE, Vol.67, No.3, pp.397-427, 1979.

[10] R.L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Crytosystems," Communication ACM, Vol.21, No.2, pp.120-126, 1978.

[11] C.P. Schnorr, "Efficient Signature Generation by Smart Cards," Journal of Cryptology, pp.161-174, April 1991.

[12] S. Tsujii, J. Chao, and K. Araki, "A Simple ID-based Scheme for Key Sharing," IEEE Journal on Selected areas in Comm., Vol.11, No.5, pp. 730-734, June 1993.

[13] NBS, "Data Encryption Standard," U.S. FIFP PUB 46, pp.1-18, January 1977.



박 정 현

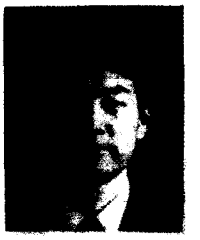
1982년 2월 숭실대학교 전자공학과 졸업(학사)

1985년 2월 숭실대학교 대학원 전자공학과 졸업(공학석사)

1997년 2월 충북대학교 대학원 전자계산학과 졸업(이학박사)

1982년 3월~현재 한국전자통신연구원 이동관리연구실 선임연구원

관심분야: 네트워크 시큐리티, 시큐리티 프로토콜, 이동 및 위성 통신 보안



임 선 배

1978년 2월 고려대학교 전자공학과 졸업(학사)

1989년 2월 한국과학기술원 전산학과 졸업(석사)

1993년 2월 고려대학교 대학원 전자공학과 졸업(공학박사)

1979년~1984년 금성사/금성반도체 선임연구원

1984년 3월~현재 한국전자통신연구원 이동관리연구실장, 책임연구원

1997년 3월~현재 TTA SC7 IMT-2000 망 연구위원회 의장

관심분야: IMT-2000 Network/Security/Protocol/UPT