위성통신 시큐리티 (Security)의 구조적 개관

김 동 규/아주대학교 컴퓨터공학과 교수

□차 례□

Ⅰ. 서 언

위성 통신 시스템이 광범위한 용도를 지니고 있고 관련 응용 서비스의 유형도 확대되고 있음은 주지의 사실이다. 국산 위성 시스템 개발이 활발히 진척되고 있고 그에 따라 위성 서비스의 사용 측면에서 부각되는 중요한 문제들을 인지하고 그 해결책에 관련되는 기술개발이 관건화 되고 있다.

본 기고에서는 위성 통신 환경에서 상대적으로 취약한 사항으로 인식되고 있는 시큐리티 관련 문제에 대하여 논의 하여 봄으로써 전반적인 이해를 높이고 기술개발 방향에 기여할 수 있기를 바란다.

Ⅱ. 시큐리티 관련 위성 통신 시스템의 구성요소

위성 통신망이 시큐리티 측면에서 지상망보다 훨씬 취약한 요소를 많이 지니고 있다는 것은 포착가능한 이동하는 위성 실체가 있다는 점 외에는 일반적인 무선 통신망과 유사하다. 즉, 통신 채널이 물리적으로는 열려 있어 누구나 접근이 용이하다. 그러므로 지상망과는 다른 기준과 방법에서 시큐리티 기능이 제공되어야 한다.

모든 통신망이 그렇듯이 위성망은 물리적인 구성 실체들과 논리적인(소프트 웨어)구성 실체들의 결합이다. 먼저 물리적인 구성 요소들은 :

- 위성망 관제 본부
- 위성망 관제국 (TTC 사이트 : Telemetry, Tracking, Commanding)
- 사용자 망 본부 : 개별 사용자(회사 등 조직)는 물리적으로 위성채널을 대여 받아 자신 전용의 위성 VAN(Value-Added Network)을 구축할 수 있다. 이렇게 구축된 사용자 VAN 네트워크의 본부를 말한다.
- 허브/지구국 (Hub/Earth station)
- 소형 지구국(VSAT)
- 단말기
- 위성

이들 시스템 구성 요소들은 다양한 토플로지로 결합될 수 있다. 시스템 구성도는 위성과 구성 요소간에는 상향빔, 하향빔 무선 링크로 연결되고, 위성이 아닌 구성요소들 간에는 지상 회선 링크나 아니면 위성을 경유하는 무선 링크(1 hob 혹은 2 hob 링크)로 연결될 수 있다.

위성 시스템 토플로지 구성의 전형적인 특성으로는 망형(Mesh형)구성이 용이하고 경제적이어서 허브를 중심으로 하는 점-대-점 성형 구성과 함께 융통성 있게 시스템 설계에 반영할수 있는 점이다.

그림 1의 위성망 구성 요소 각각에 필요한 시큐리티 기능이 탑재 되어야 한다. 어떤 기능이 어느 위치에 배치될 것인가는 특정 시큐리티 요구사항에 따라 결정 되어야 한다.

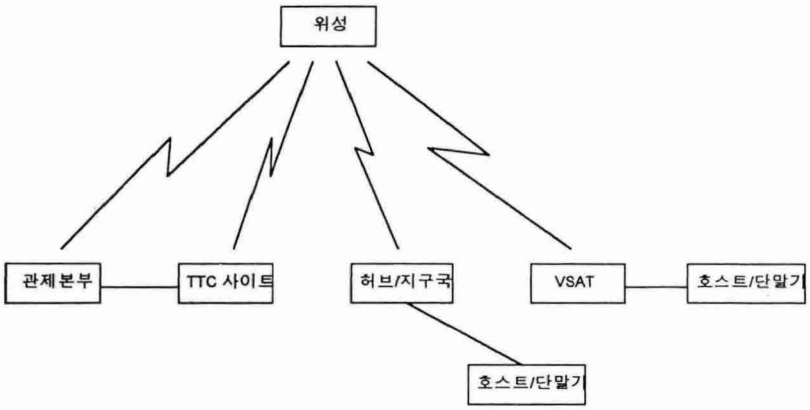

그림 1. 위성망 구성요소

Ⅲ. 위성통신 시큐리티 접근 전략

위성 통신망에서 요구되는 시큐리티 서비스의 유형은 다양하다. 이를 개별적으로 접근하는 것은 비효율적이며 기능 중복, 필요한 경우의 호환성 등에 문제가 제기 되므로 조직적이고 구조적인 접근이 필요하다. 다음의 서비스 유형별로 분류하여 본다.

- 관제어 신호 보호
- 접근 제어
- 정보통신 서비스 데이타 보호

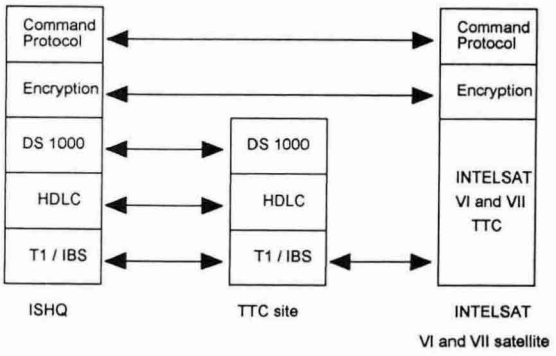

그림 2. INTELSAT VI and VII 관제망의 계층화 구조

Flag	Address	Control	Information	FCS	Flag
8 bits	8 bits	8 bits	Command bits	16 bits	8 bits

그림 3. HDLC Frame 구조

1. 관제망 신호 보호

INTELSAT의 관제망에서 사용하고 있는 접근 방식[1]이 전형적인 것이다. 관제망 신호 보호는 위성 통신망의 안전한 운용을 위하여 제 1 차적인 중요성을 갖는다. 관제 센타와 위성간에 고의적인 혹은 비고의적인 공격에 의하여 잘 못된 명령이 실행되는 것을 막는다. 이를 전제로 각종 서비스 데이타의 보호기능이 제공된다.

그림 2에서 보는 바와 같이 관제본부와 위성간에 양단간(end-to-end) 프로토콜에 따라 관제 신호가 암호화되어 전달되고 이상 없음이 확인된 명령이 실행 된다. 여기서 암호화는 관제 명령의 정당성과 무결성을 입증하기 위한 수단이다. 본부와 TTC 사이트 간에는 HDLC 프로토콜이 사용되어 (그림 3) HDLC정보 필드에 암호화된 관제 명령이 인코딩 되어 전달되고 헤드가 벗겨진 명령은 위성의 TTC모듈에 직접 전달된후 복호화되고 실행된다.

채용되는 알고리즘은 NSA KI-23으로 단일 비밀키가 암호화와 복호화에 사용되고 특정 키관리 방식에 따라 키의 운용이 관리된다.[1] 다양한 시큐리티 위배 유형을 검출하고 바로잡기 위한 적정한 신호 보호체계가 설계되고 구현 되어야 한다. 적정한 시큐리티 모델이라 함은 시큐리티 요구 사항을 충족 시키는 보호강도를 갖고 또한 반응 시간 한계를 충족시킬수 있도록 충분히 빠른 실행이 보장되는 것을 말한다.

관제망 신호 보호 서비스 기능은 기본적으로 그림 1의 구성요소 가운데 관제 본부, TTC 사이트, 위성의 세가지가 관련되고 따라서 이들에 기능이 탑제 된다(그림 2)

2. 접근 제어

위성 채널을 사용하는 직접위성 방송의 제한 수신 시스템처럼 송신기에서 스크램블된 신호를 수신측의 수신인가를 받은 가입자만이 디스크램블하여 프로그램을 시청하거나 이용할 수있도록 하는 시스템들은 전형적인 접근제어 서비스가 된다.

그림 4에 개괄적인 시스템의 기능 구조가 주어져 있다. 수신자격여부 점검 메세지 (ECM : Entitlement Checking Message)와 수신자 관리 메세지 (EMM : Entitlement Management Message)는 영

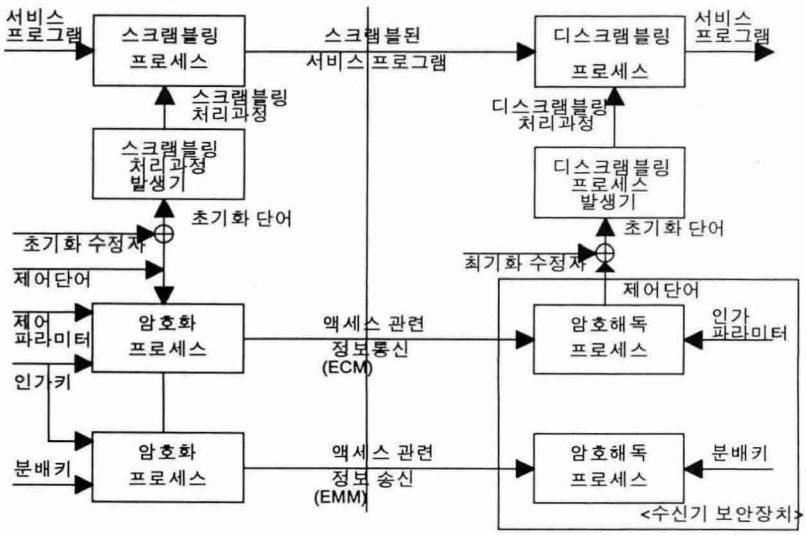

그림 4. 제한수신 시스템의 기능도

상, 음성, 데이타 신호와함께 채널 다중화기에 입력되어 수신측으로 전송되며 수신기의 디코더에서 다시 추출되고 해석되어 수신신호를 디스크램블하는 제어신호로 사용된다.

제한 수신 시스템의 여러가지 고려 사항들이 충족될 수 있도록 시스템의 설계가 이루어져야 한다. 접근제어 시스템에서는 효율적인 가입자 관리체계(SMS : Subscriber Management System)의 설계가 큰 비중을 갖는 관건이 된다. 이 관리체계는 몇가지 기능 모듈로 구성되며 암호화된 제어 단어를 가입자 관리 시스템에서 생성하여 제공하며, 키 분배및 회수, 분실키의 재교부등의 방법을 통해 수신 허가 관리 기능을 수행하여 과금 처리와 신규 가입 및 허가 만료처리, 단일 프로그램의 수신허가 및 과금등의 기능을 한다. 관리 시스템은 가입자의 사용이력을 데이타베이스에 저장하여 장기간 관리하여 스크램블링/디스크램블링에 관한 제어단어의 생성과 수신 허가 점검 메세지와 수신 허가 관리 메세지를 생성 및 전송, 관리할 수 있는 기능을 수행하고 과금을 처리할 수 있는 기능을 갖는다. 프로그램 수신허가 및 과금은 프로그램 단위로 처리한다[2].

접근 제어 서비스 기능이 탑재되는 위성망 구성요소는 서비스 제공자의 허브/지구국, VSAT, 단말기가 된다. 구조적으로는 Hub/지구국과 VSAT/단말기의 양단간(end-to-end) 프로토콜의 실행으로 서비스가 제공된다.(그림 5)

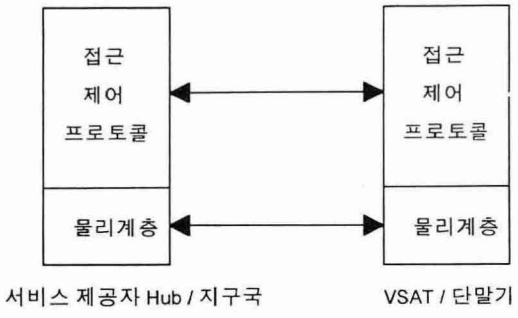

그림 5. 접근 제어 서비스 구조

3 정보 통신 서비스 데이타 보호

위성망을 통하여 연결되는 호스트, 단말기, 각종 정보통신 자원들 간에 교환되는 다양한 정보통신 서비스 관련 데이타의 보호는 본질적으로 위성망이 아닌 다른 지상 설비망의 경우와 유사하다. 다만 위성망에서 위성은 데이타 링크계층 이하의 역활만을 수행하는 것으로 볼수있고 따라서 데이타 링크 레벨이하 에서의 시큐리티가 관련되는 경우만 위성 링크가 시큐리티에 관여한다. 그러나 이경우에도 엄밀히 따지면, 관제망 신호 보호의 경우와는 구조적 차이가 있다. 위성 자체는 데이터 링크 상에서 리피터(Repeater)기능을 수행하는 요소가 됨으로 위성 자체에는 아무런 시큐리티 기능을 탑재할 필요가 없다. 따라서, 일반 정보 통신 서비스 데이타 보호에 관한한 위성이나 위성관제 센타는 투명한(transparent)요소로 간주할 수 있다. 데이타 보호 서비스는 호스트, 단말기, Hub, VSAT등의 요소간에 양단간 (end-to-end) 형태로 이루어진다.

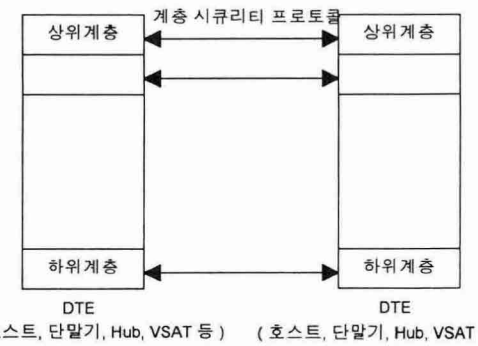

그림 6. 위성망의 일반 정보 통신 서비스 데이타 보호 구조

그러므로 이 경우에는 OSI 혹은 분산 시스템 시큐리티 구조에 관련된 모든 내용들이 적용될수 있다[3,4,5]. 각종 서비스(비밀성, 무결성, 액세스 제어, 신분확인, 부인 방지등), 메카니즘 관리등의 개념과 기법 및 모델등이 고려된다. 시큐리티 기능의 통신망 계층 배치, 서비스와 메카니즘 연

관성 등도 마찬 가지다.

위성 통신망에 연결된 다양한 분산응용 시스템에서의 서비스 데이터보호는 구조적인 모델을 근간으로 하여 필요한 재단 작업(engineering)을 행하는 방식으로 구현되어야 한다. 이러한 모델을 OSI 시큐리티 구조의 확장을 포함하여야 하고 단일 PC, LAN, 소형 혹은 대형 메인프레임으로 부터 가장 일반적인 OSI 및 ODP(Open Distributed Processing)에 이르기까지 어떤 유형의 동작 환경에 대해서도 유연한 구현 적용이 가능하여야 한다. 또한 모든 종류의 사용자, 프로그램, 데이타, 응용에 대해서도 쉽게 적용이 이루어져야 한다.

EU의 CEC COST-11 Ter Project로서 1985부터 1990년 까지 6년간 진행된 연구의 결과로서 도출된 CISS(Comprehensive Integrated Security System) [3] 모델은 위의 요구 사항을 최대한으로 충족시키는 모델로서 다양한 환경에서 실제 구현에 관한 측면에서 많은 진척이 이루어지고 있는 사례이다. 그림 7에 CISS의 개념적 모델이 나타나 있다.

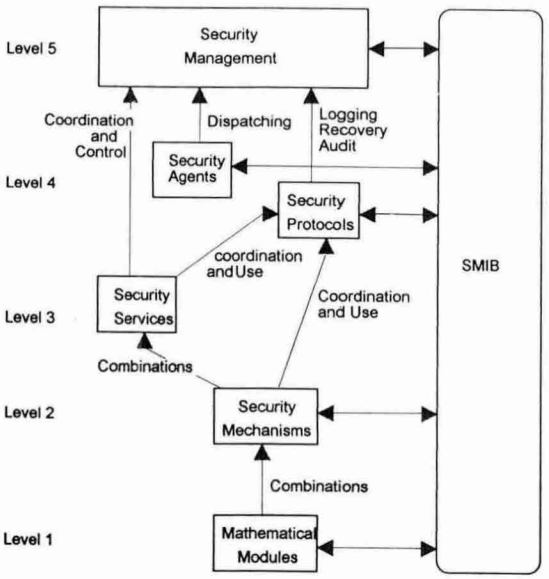

그림 7. CISS의 개념적 모델

Ⅲ. 결 언

이상에서 위성통신 시스템의 시큐리티 문제에 대하여 개괄적으로 고찰하였다. 위성 통신 시큐리티의 전형적인 서비스 유형으로서 관제망 신호 보호, 접근 제어, 정보 통신 서비스 데이타 보호의 세가지를 제시하고 이들 각각에 대한 구조적인 접근책을 논하였다. 이러한 구조적인 접근 방식은 국제 표준 기술 동향을 반영하여 시스템의 호완성, 관련 제품 개발의 시장성과 수명성을 보장할수 있다. 본기고에서 개관한 구조적인 접근책을 통하여 복잡하게 보이는 위성 시스템의 시큐리티의 본질에 대한 정의, 기술 개발의 방향을 제시함으로써 위성 시스템 시큐리티 문제에 대한 혼선을 정리하고 효율적인 기술개발을 추진하는 데에 기여할수 있기를 바란다. 본 기고에서는 위성 시큐리티 구조의 각 구성 요소에 대한 세부적인 기술적 전개는 다루지 않았음을 주지하기 바란다.

참 고 문 헌

1. Raymond L. Pickholtz, et. al "Security Analysis of the INTELSAT VI and VII Command Network," IEEE Journal on Selected Areas in Communications, VOL 11, NO. 5, June 1993.
2. CCIR Document Rep. 1079-1, General characteristics of a Conditional-Access Broadcasting System, 1992.
3. S. Muftic, et. al Security Architecture for Open Distributed Systems, John Willey & Sons, 1993.
4. 김 동규외, 키 서버 기능을 갖는 네트워크 보안 시스템 개발에 관한 연구, 과기처/전자통신연구소 과제 최종 보고서, 1993
5. 김 동규외 OSI 통신망 구조에서의 네트워크 안전체제 연구, 과기처/전자통신 연구소 과제 최종보고서, 1992

筆者紹介

▲김 동 규(金東圭)

- 1947년생
- 서울대 공대 졸(BE)
- 미국 캔자스 주립대 대학원 졸(Ph. D. 전산학 정보 통신 제공)
- 미국 캔자스 주립대 교수
- 과학기술 연구소 연구원
- 한국전자통신연구소 선임연구원
- 1994년 현재 아주대학교 컴퓨터공학과 교수
  한국통신정보 보호학회 부회장
- 연구관심분야 : 정보통신 프로토콜 엔지니어링
  컴퓨터 통신 네트워크
  정보통신 시규리티
  분산 응용통신 서비스