通信情報保護學會誌
第2卷, 第2號, 1992. 6

VSAT 위성통신망의 Inbound/Outbound 링크 보호시스템

Security System for the Inbound/Outbound Links of VSAT Satellite Networks

문상재* · 박종태* · 조유제*

요 약

본 논문은 VSAT 위성통신의 기본 보호망 구성과 Inbound/Outbound 링크 보호시스템의 구조, 기능 및 키분배에 대해 논하였다. 그 구성 및 보호관리는 OSI 모델에 준하며, SDNS의 서비스도 수용될 수 있다. 링크 보호서비스는 Inbound/Outbound 링크보호모듈에 의해 수행되나, 보호관리는 HUB host의 응용계층에 있는 보호관리응용에 의해 전적으로 이루워진다.

1. 서 론

VSAT(very small aperture terminal) 위성통신망의 Inbound/Outbound (VSAT에서 중앙국인 HUB로 연결되는 경로를 Inbound, 그 역방향 경로를 Outound) 링크 보호시스템은 본 링크상에서 안전한 데이타통신 서비스를 제공한다. 주요 서비스로 링크상의 정보보호, VSAT와 HUB간의 인증 서비스, 그리고 키이관리를 들 수 있다.

VSAT 위성링크 보호시스템은 SDNS(secure digital network system)[1, 2]의 서비스를 수용할 수 있으면서, 위성 링크에 대해서도 독립적으로 서비스를 수행할 수 있는 것이 바람직하다. SDNS 프로젝트는 그림 1과 같이 OSI 7-계층 구조에 준하는 보호구조를 발전시켜 왔으며, SDNS 보호서비스는 보호 프로토콜 SP(SP3, SP4, 또는 SDNS 링크암호화)들에 의해서 제공된다[2]. VSAT 위성링크의 보호 프로토콜은 네트워크 계층이 아니라, 링크 계층에 위치하므로 SDNS의 SP를 수용할 수 있다.

본 논문에서는 VSAT 위성통신을 위한 기본 보호망 구성과 Inbound/Outbound 링크보호시스템의 구조, 암호화기능, 및 키분배에 대해 논한다. 세션키 교환에는 D-H(Diffie-Hellman) 형 키분배 방식을, 데이타 보호에는 대칭 암호방식을 채택하였다. 본 논문에서 제안된 링크보호 시스템은 보호 위성통신망에 필수적인 무선채널을 보호하는 기본적인 서비스만을 제공하여, 비교적 간단하고 경제적이므로 신용카드 조회로 부터 공공기관의 VSAT 위성통신망등에 널리 활용될 수 있으리라 본다. 또한, 본 VSAT 링크 보호서비스와 SDNS의 보호서비스와 결합하면 VSAT 위성통신망은 각각 단독인 경우에 비해 더 안전하다.

* 경북대학교 공과대학 전자공학과

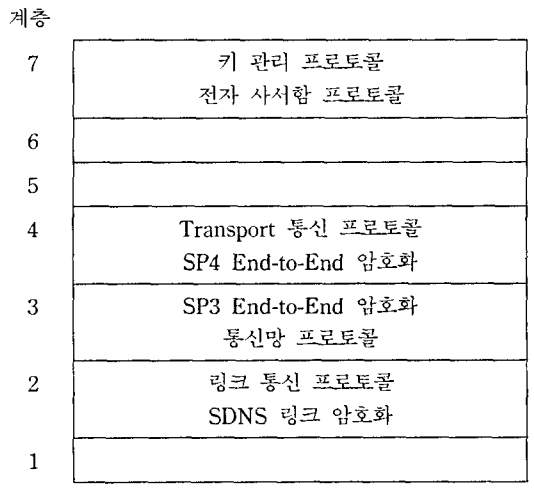


Fig. 1. Placement of SDNS protocols

2. VSAT 위성통신망의 보호구조

VSAT 위성망은 성형구성(star topology)을 채택하여 VSAT 국들이 중앙 HUB 국에 연결되어진다[3]. 가입자 단말기는 VSAT에 직접 연결하거나 기존 지상망을 통하여 연결될 수 있다. 본 연구에서는 VSAT망을 통한 통신 형태는 VSAT와 HUB의 통신, 그리고 VSAT와 VSAT 사이의 통신은 HUB의 중계에 의한 간접 통신만으로 이루워진다고 가정한다.

그림 2는 보호체계를 위한 VSAT 위성망의 프로토콜 계층화이다. 위성링크 암호 프로토콜은 데이타 링크 계층에서 수행되며, 각 VSAT와 HUB의 LCC(logical link control)위에 위치한다. 그리고 SDNS 프로토콜들은 VSAT의 단말기와 HUB의 호스트 계층들에 있어서 결합되어질 수 있다.

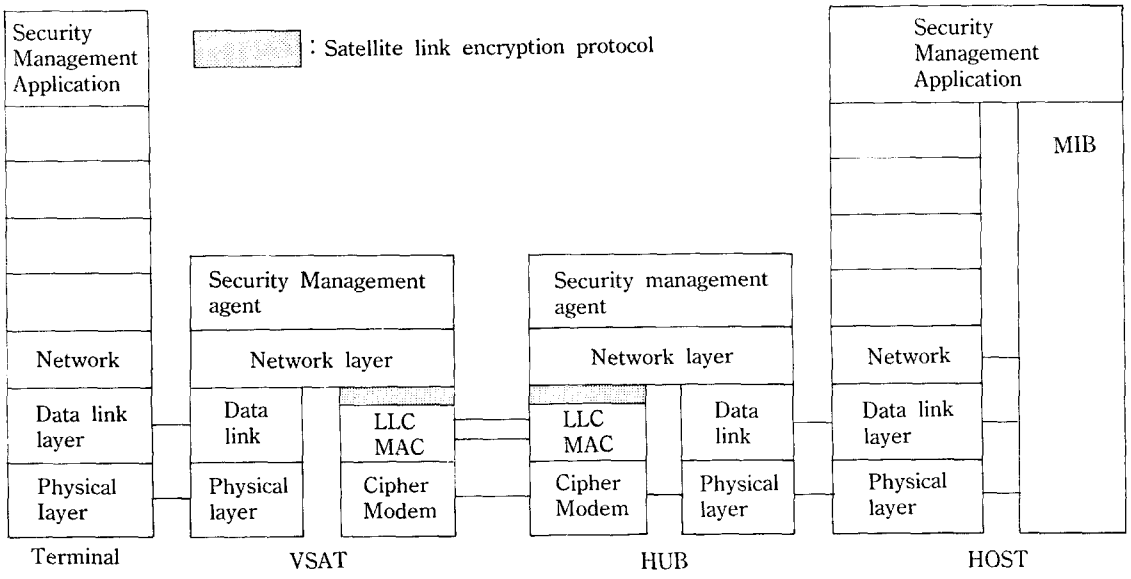


Fig. 2. Protocol layer of a secure VSAT satellite network

VSAT 위성통신망은 기존 단말기 혹은 기존 통신 프로토콜을 수정없이 기존의 지상망과 연동할 수 있어야 하기 때문에 사용자 관점에서 보면 transparent한 서비스를 제공하여야 한다. X.25와 같은 기존의 프로토콜을 사용하는 망이나 단말기를 VSAT에 접속하기 위해서는 HUB와 VSAT은 각기 프로토콜 변환 기능을 가져야 한다. 기존의 지상 프로토콜의 물리계층 및 링크계층은 대응하는 위성 프로토콜로 변환되어야 하고, 반대편에서는 그 역과정이 수행되어야 한다. 따라서, 위성망은 기본적으로 링크 계층 보다 높은 계층에서는 transparent하다고 볼 수 있다.

VSAT 위성통신망의 링크 계층은 MAC(medium

access control) 및 LLC의 두 계층으로 나눌 수 있다. MAC 계층은 위성 링크에 대한 다원접속을 제어하고 LLC 계층은 위성 링크에 대한 오류 및 흐름제어를 담당한다. 일반적으로, Inbound 링크에 대한 다원 접속은 TDMA 방식을 채택하며 Outbound 링크를 통한 데이타 전송은 TDM 방식을 사용한다. 따라서 본 연구에서도 이러한 방식을 채택한다고 가정한다.

Inbound/Outbound 보호시스템은 HUB 보호관리 응용에 의해 전적으로 관리된다. 이 보호관리 응용은 HUB의 응용계층에 있으며 각 VSAT는 VSAT 응용계층에 보호 관리 agent를 가진다.

MIB(managemant information base)는 VSAT망에 저장된 모든 관리정보의 개념적인 저장소이며 관리구성은 OSI 관리구성의 정의에 개략적으로 따른다[4]. 일반적으로 네트워크 관리시스템에서 제공하는 기능은 장애관리(fault management), 구성관리(configuration management), 보안관리(security management), 회계관리(accounting management), 성능관리(performance management) 등을 포함하며 MIB는 이러한 관리기능에 필요한 정보를 저장한다. 시스템 관리기능들 중에 보안관리와 구성관리는 안전한 VSAT 망관리 준비에 직접적으로 관계된다.

MIB는 관리할 각 개체의 특질, 그리고 개체간의 관계에 관한 정보를 가지는 개념적인 구조로 설명된다. 보호관리 기능들은 망상에서 몇몇 기능들을 수행하기 위하여 MIB을 참조한다. 예를들어 인증은 VSAT 망에서 MIB을 참조함으로서 이루어진다. 이경우 단말기는 MIB에 저장될 수 있는 정보에 대해 망차원의 한 예이다.

3. 위성링크 보호서비스

링크 보호시스템에 의해 공급되는 기본적인 서비스들은 Inbound/Outbound 링크상의 데이타 암호화와 VSAT와 HUB간의 인증이다. 인증문제는 공용키이 방식에 의해서 해결한다[5].

VSAT에서 HUB로 전송되는 데이타 패킷들은 근원지 VSAT에 대한 주소를 가지고 있으며, HUB에서 각 VSAT들로 방송되는 패킷들은 목적지 VSAT에 대한 주소를 가진다. 각 VSAT들은 HUB로부터 수신된 패킷중에서 목적지 주소가 자신의 주소와 부합되는 패킷만 받아들이게 된다. Inbound 패킷형식은 preamble, header, data portion, FCS(frame check sequence), postable로 구성되어 있고, outbound 패킷형식은 HDLC 프레임의 형식과 유사하다.

VSAT 위성링크인 Inbound/Outbound에 대한 정보보호에 사용자 데이타 부분만 암호화하는 방법과 헤드를 포함한 전 프레임에 대한 암호화 방법이 가능하다. 전자의 경우는 도청시 헤더의 주소 정보를 통한 통화량 분석이 가능한 문제점이 생긴다. 후자의 경우는 두 레벨의 암호화가 요구되는데, 헤더는 HUB와 모든 VSAT이 가진 공통의 키이로 암호화하고 사용자 데이타는 각 VSAT이 가진 고유의 키이로 암호화하게 된다. 각 VSAT은 수신된 모든 패킷의 헤더를 복호화하여 주소를 체크한 다음, 자신이 수신국인 패킷만 사용자 데이타 부분을 복호화하게 된다.

4. Inbound/Outbound 링크보호 모듈

각 VAST와 HUB에 물리적으로 암호화기인 SM (secure module)을 두고, 데이타의 암호화, 사용할 키이의 생성 및 저장, 그리고 키이관리에 관련된 명령 내용들이 SM 내에서 수행되도록 한다. SM은 크게 프로세스와 암호/복호기로 구성되도록 하고, 프로세서는 관련 프로그램과 필요한 키이를 가지며, 암호/복호기는 해당 세션키이를 사용하여 지정한 데이타 암호화 알고리듬을 수행하도록 한다. 특히, 프로그램 등을 포함해서 한번 내부에 이식된 정보는 평문형태로 결코 다시 유출될 수 없도록 하는 것이 요구된다.

VAST의 SM은 한개의 master키이와 두개의 세션키이를 가지며, master 키이를 사용하여 세션키이를 생성하고, 두개의 세션키이중 하나는 헤드 내용을 암호/복호하기 위한 키이로, 다른 하나는 각 VAST 사용자 데이타를 암호/복호하기 위하여 사용된다. SM은 데이타 암호칩과 프로서세스 ROM으로 구성된다. 데이타 암호칩은 세션키이로 SM에 들어오는 데이타를 암호 혹은 복호 하며, 데이타 암호를 위해서는 DES와 같은 대칭 암호화법을 사용한다. 프로세서는 세션키이 분배, 불규칙 정수(random number)발생, 그리고 보안관리 기능을 수행한다. 보안

기능은 VAST 보안관리 agent에 의해 수행된다.

그림 3은 개념적인 SM 구조의 블록선도이다. VAST master 키이 S_v는 초기에 설정되어지며, 보안을 위해서 주기적으로 변화되어질 수 있다. 공용키이 P_v와 P_H는 VAST와 HUB에 있으며, 이 공용키이들은 세션키이 발생, 그리고 분배에 사용되어진다.

키이 생성과 분배는 HUB에 있는 키이관리에서 담당한다. HUB는 super master 키이에 의해 암호화된 형태에 있어 필요한 키이를 발생시킬 수 있어야 하며, 이 키이들은 외부 메모리에 저장되어질 수 있다. 또한 HUB의 SM은 암호와된 키이들을 복호화할 수 있어야 하므로 내부에 HUB super master 키이를 가져야 한다.

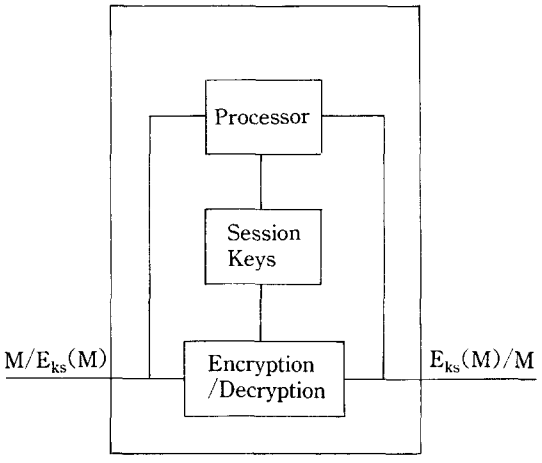


Fig. 3. Structure of the secure module

5. 키이 분배

VAST 링크 보호시스템의 세션키이 분배는 변형된 D-H 알고리듬에 기초한다[7, 8]. 이 프로토콜은 비밀 master 키이 S_V와 S_H가 노출되도 세션키이를 계산하는 것은 보호되므로 안전하다.

세션키이 분배 프로토콜은 다음과 같다. P_V와 P_H가 VAST, V, 그리고 HUB의 공개키이라 하면, $P_i=(e)^{s_i}$이고 이 연산은 GF(q) 상에서 행해진다. q는 소수 혹은 소수승이고 e는 GF(q)의 원시원이며, i=V 혹은 H이다. VAST인 V가 안전한 위성망을 통해서 통신하고자 할때 키이교환에 대한 절차는 다음과 같다.

1. V는 불규칙 정수 R_V를 발생하고 $Z_V=(e)^{R_V}\cdot K_{VH}$를 계산한 후, V의 ID와 함께 HUB로 보낸다. 여기서, $K_{VH}=(P_H)^{S_V}=(P_V)^{S_H}$이다. HUB는 $Z_H=(e)^{R_H}\cdot K_{KH}$를 상호 교환한다. 여기서, R_H는 HUB에서 발생된 불규칙 정수이다.

2. V와 HUB는 세션키이 $K_S=(Z_V\cdot K_{VH}^{-1})R_H=(Z_H\cdot K_{VH}^{-1})^{R_V}=(e)^{R_V R_H}$를 계산한다.

여기서 비밀키이 S_V와 S_H가 노출된다 해도 이산대수문제가 되어 R_V와 R_H를 구할 수 없어 세션키이를 알 수 없다.

키이 분배 시스템은 새로운 세션키이를 VAST들에게 공급하고 이 키이들은 SM의 레지스터로 복사된다. 그리고 과거키이는 바뀌어진다. 이 레지스터는 데이타 암호에 사용될 대칭암호 시스템에 키이를 공급한다.

6. 결 론

본 논문은 VAST 위성통신의 기본 보호망 구성과 Inbound/Outbound 링크 보호시스템의 구조, 기능, 및 키분배에 대해 논하였다. VSAT 링크 보호시스템의 주된 서비스들은 링크를 통해 전송된 데이타의 암호화 그리고 VSAT와 HUB간의 인증이다. 링크 보호서비스들은 링크보호 모듈에 의해 수행되어지나, 관리는 HUB host의 응용계층에 있는 보호관리응용에 의해 전적으로 이루워진다. 링크보호 모듈에서 사용될 세션키이는 D-H형 공용키이 프로토콜에 의해 생성되고, 이 프로토콜은 비밀키이가 노출된 경우에도 세션키이의 계산이 어려워 다른 D-H 변형 방식보다 안전하다. 제안된 링크보호 시스템은 보호 위성통신망에 필수적인 무선채널을 보호하는 기본적인 서비스만을 제공하나, 반면에 간단하고 경제적이므로 신용카드 조회로 부터 공공기관의 VSAT 위성통신망등에 널리 활용될 수 있으리라 본다.

참 고 문 헌

1. ISO DP 7498/2 Information Processing Systems-Open Systems Interconnection-Security Architecture.

2. Ruth Nelson, "SDNS service and Architecture", Crypto '89 Abstract pp.348-352, August, 1989.

3. D. M. Chitre and John S. McCoskey, "VSAT Networks : Architecture, Protocols, and Management," IEEE Comm. Magazine, Vol. 26, pp.28-38, July 1988.

4. ISO/IEC 7498-4, International Standard, Information Processing Systems-Open Systems Interconnection-Basic Reference Model-Parts 4 : Management Framework, 1989.

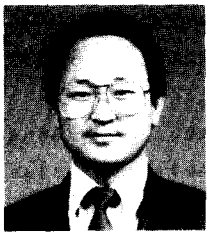
5. W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. on Information Theory, Vol. IT-22, pp.644-654, Nov. 1976.

6. NBS, Data Encryption Standard, US FIFP PUB 46, pp.1-18, 1977.

7. S. J. Moon and P. J. Lee, "A Propose of a Key Distribution Protocol," The Proc. of the Korean Workshop on Information Security and Cryptography, pp.117-124, Sept. 1990.

8. Y. Yacobi and Z. Shmuely, "On Key Distributions," Crypto '89 Abstract, pp.335-346, August 1989.

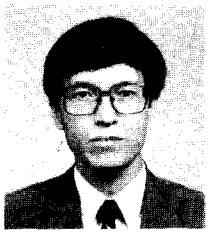
□ 著者紹介



문 상 재(正會員)

1948년 4월 20일생
서울대학교 공업교육과(전자전공 학사)
서울대학교 대학원 전자공학과(석사)
미국 UCLA 공학박사(통신공학 전공)
금성전기주식회사 근무
미국 UCLA 연구조원 근무
미국 Satellite Tech. Management Inc. 근무/미국 UCLA Postdoctor 근무(Dept. of Elec. Eng.)/미국 OMNET 주식회사 Consultant 근무
현재 경북대학교 전자공학과 교수
주관심분야 : 부호기술 및 디지탈통신 등

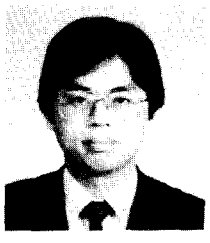
□ 著者紹介



박 종 태(正會員)

1971년~1978년 경북대학교 전자공학과 학사.
1979년~1981년 서울대학교 전자공학과 석사.
1981년~1987년 미국 Michigan 대학 전기전산과 박사.
1985년~1987년 미국 Michigan 대학, Center for information Technology Integration (CITI) 연구원.
1987년~1988년 미국 AT&T Bell 연구소 선임연구원.
1988년 8월~1989년 2월 삼성전자 수석연구원.
1989년 3월~현재 경북대학교 전자공학과 근무.
연구분야 : 데이타베이스, 컴퓨터 네트워크, 인공지능.

□ 著者紹介



趙 有 濟(正會員)

1982년 서울대학교 전자공학과(학사)
1983년 한국과학기술원 전기 및 전자공학과(석사)
1983년 한국과학기술원 전기 및 전자공학과(박사)
1989년~현재 경북대학교 전자공학과 조교수
관심분야 : 컴퓨터 통신망, 광대역 종합정보통신망, 멀티미디어 통신 등