위성망의 보호모델 및 관련 서비스*

°박 영 호, 문 상 재
경북대학교

Security Model and Services for Satellite Communication Networks*

°Young Ho Park, Sang Jae Moon
Kyungpook National University

요 약 문

위성망은 정보의 유출이 쉬운 전송로를 가질뿐만 아니라 다자간에 이루어지는 통신망이므로 정보보호가 요구된다. 본 논문에서는 위성망의 정보 보호모델을 제안하고, 관련된 보호서비스를 제시한다. 본 위성망 보호모델에서는 OSI 참조모델 계층 2에 해당하는 MAC와 LLC 부계층들 사이에 SDE 부계층을 두어 데이타의 안전한 교환이 이루어지도록 하며, SDE 부계층에서 제공하는 보호서비스들로는 데이타 비밀보장, 비접속 데이타 무결성, 데이타 발신처 확인, 그리고 접근제어 서비스이다.

1. 서 론

오늘날 사회가 다양화되고 복잡해짐에 따라 필요한 정보의 양은 급속히 증가하고 있다. 이러한 다양한 정보를 다루기 위하여 세계 각국은 기존의 지상망에 의존한 통신

---

* 본 논문은 체신부:한국전기통신공사의 통신학술단체 육성지원금에 의하여 이루어졌음

및 방송 체계의 단계를 넘어 위성망을 이용하는 새로운 통신 및 방송 체계를 개발 발전시켜 나아가고 있다. 데이타, 영상, 그리고 멀티미디어를 다루는 위성망은 정보의 노출이 쉬운 전송로를 가질뿐만 아니라 다자간에 이루어지는 통신망이므로 정보보호의 요구가 절실하다.

통신망은 불법적인 수정 및 유출로부터의 데이타 보호, 발견되지 않는 상실이나 첨가로부터의 데이타 보호, 그리고 데이타 송·수신자의 확인 등을 위한 보호가 필요하다. 그리고 이러한 보호의 목적으로 사용되는 서비스들로는 신분확인(authentication), 접근제어(access control), 데이타 무결성(data integrity), 비밀보장(confidentiality), 그리고 부인봉쇄(non-reputation) 서비스이다[1].

일반적으로 OSI 참조모델을 위한 SDNS(secure data network system)에서는 SP3(secure protocol 3)과 SP4(secure protocol 4)에 대해서는 비교적 잘 정의되어 있으나, 실제에서 많이 채택할 수 있는 데이타 링크 계층에서의 보호 통신 규약은 아직 정의되어 있지 않으며 현재 연구 중이다[2]. 또한, ISO 7498-2에서는 OSI 참조 모델에서의 보호에 관한 기본모델의 구조에 관하여 명시하고 있으며, 모델로서 패킷 교환망과 광역 통신망을 기준으로한 정보 보호서비스를 계층별로 구분 적용하고 있다[1]. LAN에서의 정보보호을 위하여 IEEE에서는 802.10(security working group)을 구성하여 표준화 작업을 추진하고 있으며, 표준안인 SILS(standard for interoperable LAN security)는 안전한 데이타 교환(SDE:secure data exchange), 키이 관리, 그리고 시스템/시큐리티 관리들로 정의된다[3]. 그러나, 위성망에서의 정보보호에 관해서는 표준안이 아직 없는 상황이고 표준화 활동도 미비한 실정이다.

위성망은 물리적으로 위성과 지구국으로 이루어지며, 각 지구국은 기존의 지상망에 연결하여 사용할 수 있고, 사용자 단말기는 지구국에 직접 연결하거나 혹은 기존의 지상망에 연결하여 사용할 수 있다[4]. 이러한 관점에서 볼때, 위성망은 다른 망과 연결하여 사용할 수 있는 적응성을 가져야하며, OSI 참조모델에 준하여 정보보호 위성망을 구현해야 한다[5].

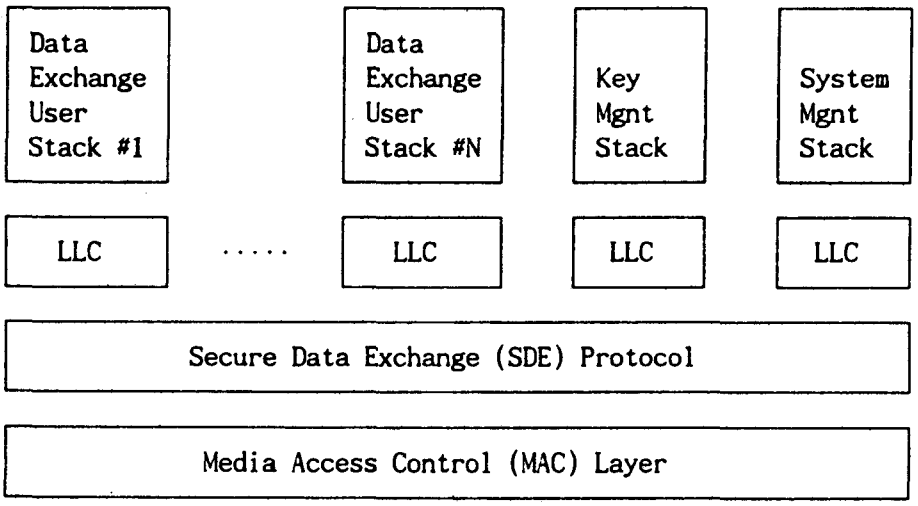
본 논문에서는 ISO 7498-2에서 제안한 OSI 보호모델과 IEEE 802.10에서 채택한 SILS 모델을 결합한 구조를 이용하여 위성망의 안전한 보호모델을 제안하고, 관련된 보호서비스를 제시한다. 본 위성망 보호모델에서는 OSI 참조모델 계층 2에 해당하는 MAC와 LLC 부계층들 사이에 SDE 부계층을 두어 데이타의 안전한 교환이 이루어지도록 하며, SDE 부계층에서 제공하는 보호서비스들로는 데이타 비밀보장, 비접속 데이타 무결성, 데이타 발신처 확인, 그리고 접근제어 서비스이다.

2. IEEE 802.10 SILS의 구성과 프로토콜

LAN에서의 정보보호 필요성이 증가함에 따라 IEEE에서는 802.10(security working group)을 구성하여 LAN 정보보호 표준화 작업을 수행하고 있으며, 표준인 SILS(standard for interoperable LAN security)는 안전한 데이타 교환(SDE:secure data exchange), 키이 관리(key management), 그리고 시스템/시큐리티 관리(system/security management)들로 구성된다[3].

2.1. SILS 모델

IEEE 802.10에서 추진하고 있는 SILS 모델은 다음과 같이 3 분야로 구성된다. SDE 프로토콜은 OSI 기본 모델(ISO 7498)의 계층 2 프로토콜로서 계층 2에서 데이타의 안전한 교환을 제공하며, 키이관리 프로토콜은 계층 7 프로토콜로서 계층 2에서 데이타를 암호하는데 사용할 키이를 관리하고, 시스템/시큐리티 관리 프로토콜은 계층 7 프로토콜로서 보호 프로토콜을 안전하게 관리하는데 사용된다.



LLC : Logical Link Control

Fig. 1. Structure of SILS stack

그림 1은 SILS 모델의 전체적인 구조이다[3]. 여기서 데이타 교환 사용자 스텍은 기존의 네트워크 통신 프로토콜로서 SDE로부터 보호서비스를 제공받으며, 데이타 교환 사용자 스텍에 안전한 보호서비스를 제공하는 SDE 프로토콜은 키이관리와 시스템 관리에 의존한다. 또한 SMIB(Security Management Information Base)는 계층 7의 시스템 관리와 키이 관리에서 SDE 부계층으로의 통신경로를 제공하며, 그 구성은 그림 2와 같다.

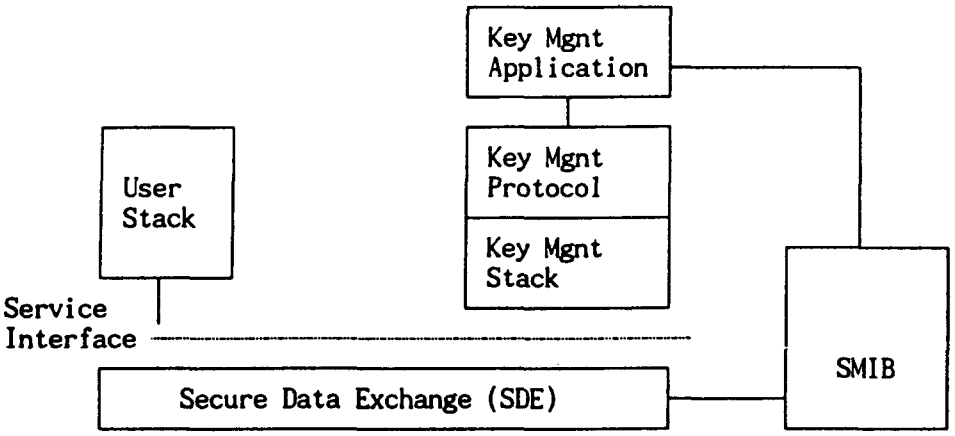


Fig. 2. Use of SMIB

2.2. SDE 프로토콜

SDE 부계층은 IEEE LAN의 LLC 부계층과 MAC 부계층 사이에 위치하며, 이 부계층들은 OSI 기본 참조 모델의 계층 2에 해당한다. ISO 7498-2에서는 계층 2에서 비밀보장과 트래픽 흐름 보호의 서비스만을 제공하고 있으나, IEEE 802.10의 SILS 모델의 SDE 부계층에서는 데이타 비밀보장, 비접속 데이타 무결성, 데이타 발신처 확인, 그리고 접근 제어의 서비스들을 제공하고 있다. SDE 앤티티는 IEEE 802.10 LAN의 MAC 부계층 위에서 부가된 비접속 서비스를 수행하고, 이는 암호 메카니즘을 이용하여 MAC 부계층을 통하여 정보보호를 위한 보호서비스를 투명하게 제공한다.

SDE 프리미티브들은 SDE 부계층과 LLC 부계층 사이에서 공급되는 서비스로써 투명한 보호서비스를 제공하며, 그 구성은 그림 3과 같다.

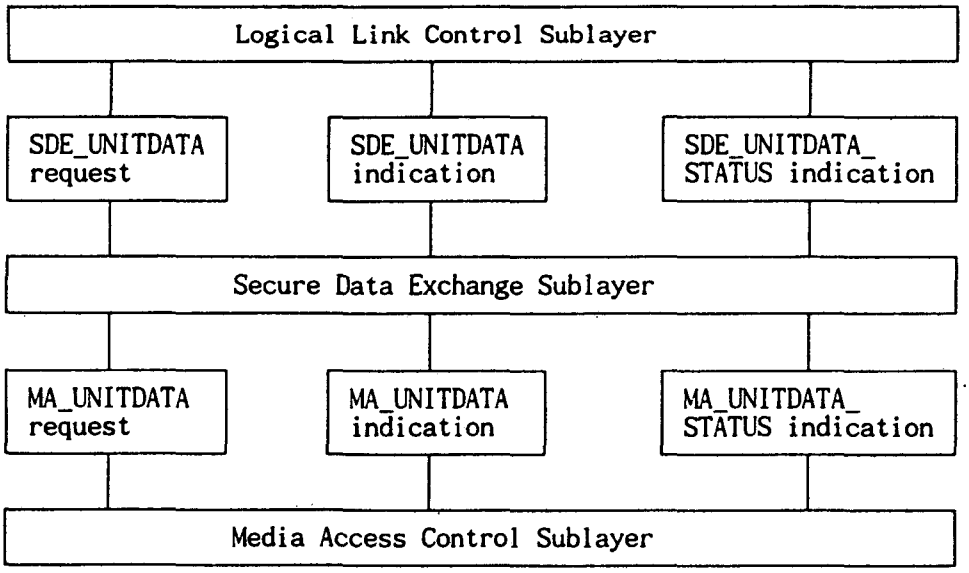


Fig. 3. SDE primitive

SDE 프리미티브들의 파라미터들은 다음과 같다.

SDE_UNITDATA.request	source_address
	destination_address
	data
	priority
	service_class
SDE_UNITDATA.indication	source_address
	destination_address
	data
	reception_status
	priority
	service_class
SDE_UNITDATA_STATUS.indication	source_address
	destination_address
	transmission_status
	provided_priority
	service_class

3. 보호서비스

위성망에서의 정보보호 체계가 제공하는 주요 서비스로는 신분확인, 접근 제어, 비밀보장, 데이타 무결성, 그리고 부인 봉쇄 등이 있다. ISO 7498-2에서는 OSI 참조 모델에서의 구조 및 보호서비스에 관하여 명시하며, 여기서 정의하는 보호서비스와 그 의미는 다음과 같다[1].

1) 신분확인 (Authentication)

수신된 데이타 실체가 요구된 실체라는 것을 확인하는 것을 의미하며 다음과 같이 구분한다.

① 데이타 발신처 확인 (Data orgin athentication)

데이타 발신처의 확증(corroboration) 즉, 데이타 발신처의 확인과 자격유무를 제공하는 서비스를 의미한다.

② 대등실체 확인 (Peer entity authentication)

통신 당사자간의 신분확인과 자격유무의 점검, 그리고 대등 실체간의 신뢰성있는 연결의 확립 또는 데이타 전송의 과정에 적용되는 서비스를 의미한다.

2) 접근 제어 (Access control)

비인가된 동작들의 위협에 대하여 자원을 보호하는 것을 의미한다.

3) 비밀보장 (Confidentiality)

비인가된 개인, 실체, 그리고 처리(process)들에 의해 데이타 내용을 알 수 없도록 하는 것을 의미하며 다음과 같이 구분한다.

① 접속 비밀보장 (Connection confidentiality)

N 접속에서 모든 N 사용자 데이타의 비밀보장을 제공한다.

② 비접속 비밀보장 (Connectionless confidentiality)

비접속 N-SDU에서 모든 N 사용자 데이타의 비밀보장을 제공한다.

③ 선택 영역 비밀보장 (Selective field confidentiality)

N 접속 혹은 비접속 N-SDU에서 N 사용자 데이타내의 선택적 영역의 비밀보장을 제공한다.

④ 트래픽 흐름 비밀보장 (Traffic flow confidentiality)

트래픽 흐름을 관찰함으로서 유추될 수 있는 정보의 보호를 제공한다.

4) 데이타 무결성 (Data integrity)

데이타의 내용 자체가 비인가된 방식으로 변경 혹은 삭제가 되지않는 데이타의 무결성을 의미하며 다음과 같이 구분한다.

① 복구기능을 갖는 접속 무결성 (Connection integrity with recovery)

N 접속에서 모든 N 사용자 데이타의 무결성을 제공하고, 전체 SDU 데이타내의 어떤 데이타의 변경, 삽입, 삭제, 혹은 재사용을 감지하고 복구기능을 갖는다.

② 복구기능이 없는 접속 무결성 (Connection integrity without recovery)

위의 서비스와 같은 기능을 가지나 복구 기능은 없다.

③ 선택영역 접속 무결성 (Selective field connection integrity)

접속상에서 전송된 N-SDU의 N 사용자 데이타내의 선택영역의 무결성을 제공하고 선택된 영역이 변형,삽입,제거, 혹은 재사용 되었는지를 결정하는 형태를 가진다.

④ 비접속 무결성 (Connectionless integrity)

비접속 SDU의 무결성을 제공하고 수신된 SDU가 변형되었는지를 결정하는 형태를 가진다. 또한, 부가적으로 재사용 감지의 제한된 형태가 공급되어질 수도 있다.

⑤ 선택영역 비접속 무결성 (Selective field connectionless integrity)

비접속 SDU내의 선택된 영역의 무결성을 제공하고, 선택된 영역이 변형되었는지를 결정하는 형태를 가진다.

5) 부인 봉쇄 (Non-reputation)

발신자가 발신사실을 혹은 수신자가 수신사실을 부인하는 것을 정보보호의 방법으

로 봉쇄하는 것을 의미하며 다음과 같이 구분한다.

① 발신 부인 봉쇄 (Non-reputation with proof of orgin)

데이타의 수령이 데이타의 발신 부인 봉쇄 서비스와 함께 제공된다. 이것은 발신자가 보낸 데이타 혹은 그 내용을 부인할 수 없도록 한다.

② 수신 부인 봉쇄 (Non-reputation with proof of delivery)

데이타의 발신이 데이타의 수신 부인 봉쇄 서비스와 함께 제공된다. 이것은 수신자가 받은 데이타 혹은 그 내용을 부인할 수 없도록 한다.

4. 위성망의 보호모델 및 관련 서비스

대부분 위성망은 성형 구성방식(star topology)이며, 물리적인 구성형태는 그림 4와 같다.

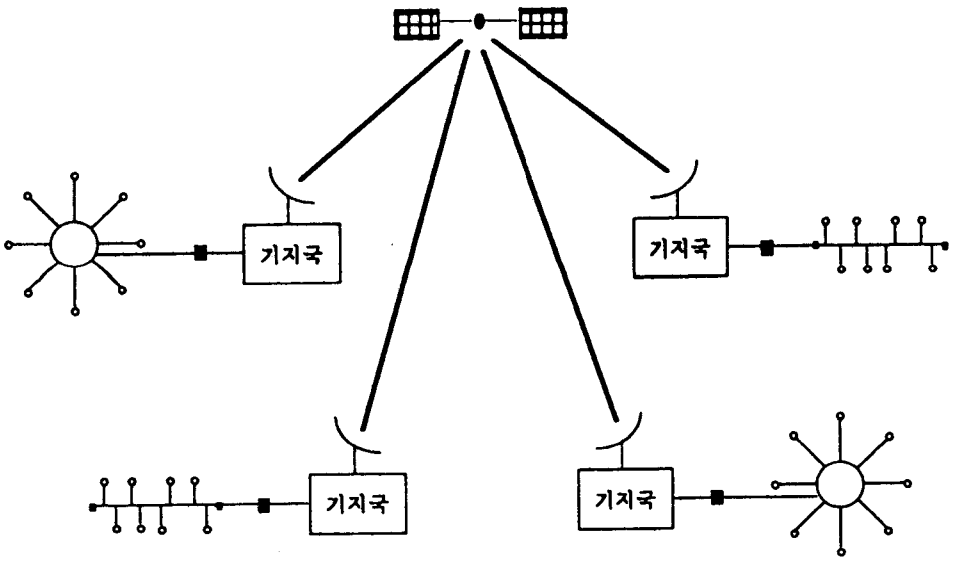


Fig. 4. Physical architecture of a satellite network

위성망의 구성은 위성과 지구국으로 이루어지며, 각 지구국은 규모가 큰 지구국 혹은 규모가 적은 VSAT일 수도 있다. 이러한 지구국에 기존의 지상망을 연결하여 사용할 수 있고, 사용자 단말기를 지구국에 직접 연결하거나 혹은 기존의 지상망에 연결하여 사용할 수 있다. 이러한 관점에서 볼때, 위성망은 서로 다른 망과 연결하여 사용할 수 있는 적응성을 가져야 하며, 정보보호 위성망을 OSI 참조 모델에 준하여 구현해야만 한다. 이러한 정보보호 위성망 모델은 그림 5와 같다.

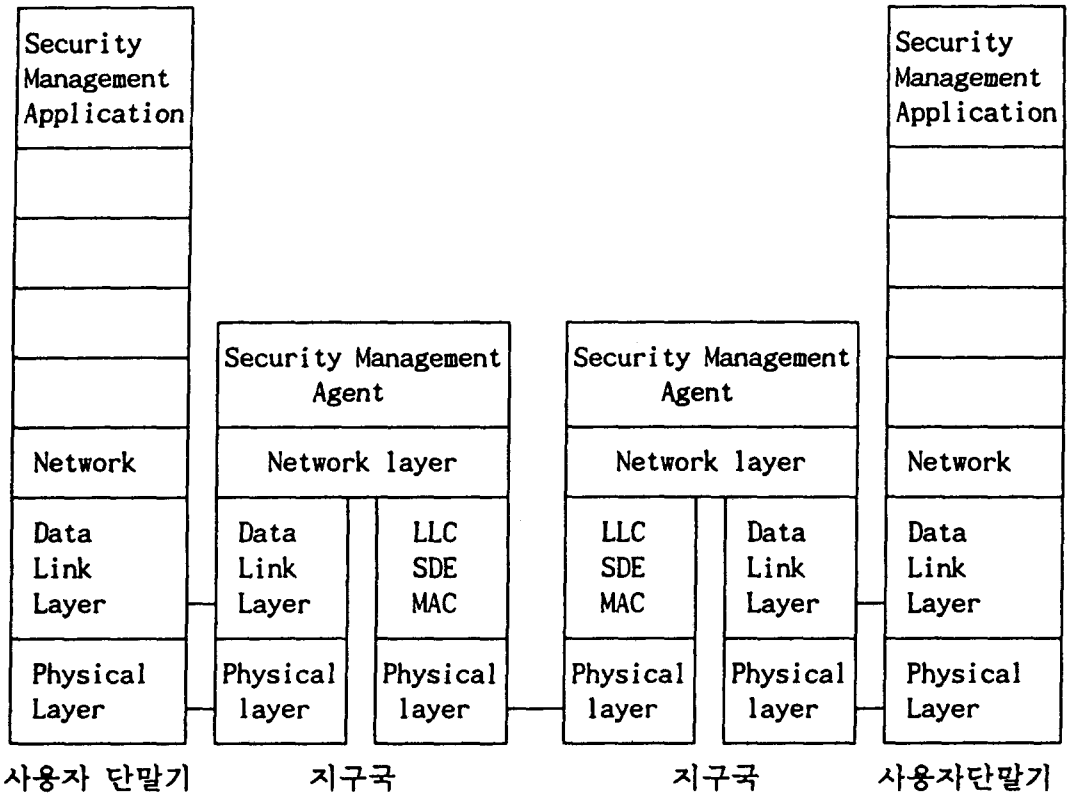


Fig. 5. Protocol layer of a satellite network

그림 5에서 계층 2에 위치하는 MAC 부계층은 위성링크에 대한 다원접속을 제어하고, LLC 부계층은 위성링크에 대한 오류 및 흐름제어의 기능을 가지며, 그리고 SDE 부계층은 데이타의 안전한 교환기능을 제공한다. SDE 부계층은 단일 PDU 형태를 사용하고, SDE PDU의 구성은 그림 6과 같이 clear header, protected header, data, pad, 그리고 ICV(integrity check value) 영역들로 이루어진다.

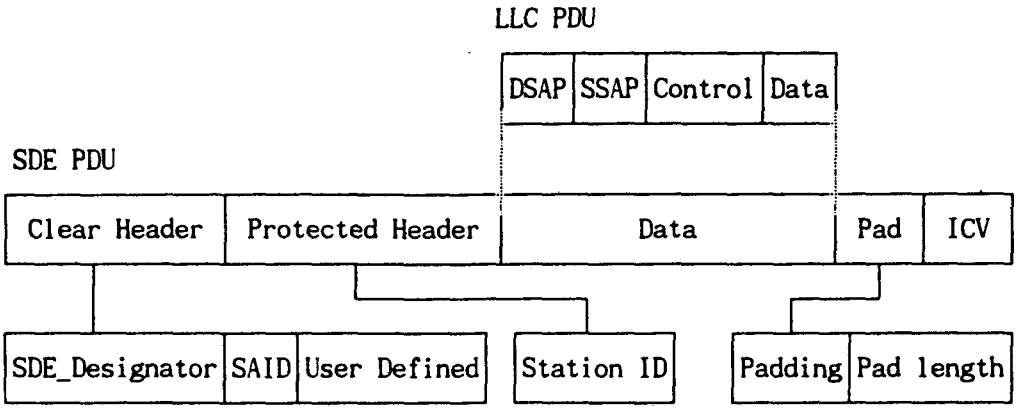


Fig. 6. Structure of a SDE PDU

SDE PDU 구성요소들의 기능은 다음과 같다.

1) clear header

clear 헤드는 SDE_designator, SAID(security association identification), 그리고 사용자 정의 영역으로 구성된다. SDE_designator는 SILS 스테이션이 없는 경우는 SDE 프레임을 받지 못하게 되며, SAID 영역은 목적지 SDE 앤티티와 관련된 보호 관련 식별자가 있고, 사용자 정의 영역은 최대 20 옥테트까지의 가변영역을 가질 수 있다.

2) protected header

보호 헤드는 그림 6과 같이 station ID 영역이며, 전송국을 유일하게 구분한다.

3) data

데이타 영역은 LLC의 PDU에 해당하며 전송하고자 하는 데이타이다.

4) pad

pad 영역은 padding과 pad 길이 영역으로 이루어지며, pad 길이 영역은 실제 padding의 길이이다.

5) ICV

ICV 영역은 SDE PDU의 마지막 부분에 위치하며, ICV 영역의 길이 혹은 ICV 영역의 유무는 시스템 관리에 의해서 결정된다. 또한, 이 영역은 무결성 서비스를 제공한다.

SDE 부계층에서 제공하는 서비스들은 데이타 비밀보장, 비접속 데이타 무결성, 데이타 발신처 확인, 그리고 접근 제어이며 그 기능은 다음과 같다.

1) 데이타 비밀보장 (Data Confidentiality)

LLC PDU 를 암호화함으로서 데이타 비밀보장 서비스를 수행한다. 또한, 다수의 암호화 알고리듬을 사용 가능하며 데이타 암호 키이와 암호 알고리듬을 선택하기 위해서는 외부키이 관리 서비스에 의존한다.

2) 비접속 데이타 무결성 (Connectionless integrity)

무결성 확인값(Integrity Check Value)을 계산하여 SDE PDU에 추가 함으로서 비접속 데이타 무결성 서비스를 수행한다. 또한, integrity 키이와 알고리듬을 선택하기 위해서는 외부키이 관리 서비스에 의존한다.

3) 데이타 발신처 확인 (Data orgin authentication)

키이 관리 활용 혹은 보호 헤드내에 station ID를 둠으로서 데이타 발신처 확인 서비스를 수행한다.

4) 접근 제어 (Access control)

SDE는 SMIB와 연결되어 접근제어 서비스를 제공하며 SDE entity는 보호 협상이 이루어지기 전에는 PDU를 송·수신할 수 없다.

그림 5에서의 관리체계에서는 사용자 단말기에 있는 보호관리 응용은 응용 프로세스로서 동작하고, 각 지구국에 보호관리 agent를 두어 응용 프로세스와의 상호통신에 대응토록 한다. 각 지구국에서는 OSI를 기준으로 하여 둔 7계층 통신 프로토콜에 대해서 모두를 지원할 필요는 없다. 각 지구국을 proxy node로서 동작시키면 OSI 7계층 모

두를 사용했을때 야기되는 구현의 복잡성 및 시스템의 성능저하를 방지할 수가 있기 때문이다. 보호관리 응용프로세스들은 TCP/IP(transmission connection protocol/internetwork protocol)에 기초한 ISODE를 이용한 시스템 관리 환경을 구축하여 기초적인 보호 관리 기능들을 제공한다[7,8]. ISODE에서 네트워크 관리의 manager와 agent들간의 시스템 관리 관련통신을 담당하는 CMIS/CMIP(common management information service/common management information prtocol)의 기능이 제공된다.

5. 결 론

본 논문에서는 ISO 7498-2에서 제안한 OSI 보호모델과 IEEE 802.10에서 채택한 *SILS* 모델을 결합한 구조를 이용하여 위성망의 안전한 보호모델을 제안하고, 관련된 보호서비스를 제시한다. 본 위성망 보호모델에서는 OSI 참조모델 계층 2에 해당하는 MAC와 LLC 부계층들 사이에 SDE 부계층을 두어 데이타의 안전한 교환이 이루어지도록 하며, SDE 부계층에서 제공하는 보호서비스들로는 데이타 비밀보장, 비접속 데이타 무결성, 데이타 발신처 확인, 그리고 접근제어 서비스이다. 앞으로 이러한 위성망에 적합한 키이 관리와 시스템 관리 프로토콜들이 개발되어져야 한다.

참 고 문 헌

[1] ISO 7498-2, *OSI Security Architecture*, 1987.

[2] R. Nelson, "SDNS Archtecture and End-to-End Cryption," CRYPTO 90' pp.347-352, August 1990.

[3] IEEE 802.10, *Standard for Interoperable Local Area Network(LAN) Security (SILS)*, P802.10/D6, September 1989.

[4] K.M.Sundara Murthy and Kenneth G.Golden, "VSAT Networking Concepts and New Applications Development" IEEE Comm. Magazine, pp.43-49, May 1989.

[5] "사설 위성통신망의 정보보호를 위한 망의 설정 및 기본정보보호 방식에 관한 연구," 한국전자통신연구소 최종 연구보고서, 경북대학교, 1991년 10월

[6] ISO 7498, *OSI Basic Reference Model*, 1987.

[7] Uyless Black, *TCP/IP and Related Protocols*, McGraw-Hill, 1992.

[8] R.J.Cypser, *Communications for Cooperating Systems*, Addison Wesley, 1991.