조 사 분 석

LAN에서의 정보 보호 모델 분석

강신각* 진병문**

목 차

* 표준연구2실 연구원
** 표준연구2실 실장

Ⅰ. 개 요

정보통신 기술의 발전으로 각종 정보통신 기기 및 컴퓨터통신망의 보급이 급격히 확산되어 본격적인 정보화 사회가 도래하게 되었다. 이에 따라 각종 정보를 대용량 정보매체에 저장하여 통신망을 통한 정보 검색 서비스를 가능하게 하는 등 각종 부가통신 서비스가 출현하게 되고, 원격지 정보 시스템들이 통신망을 통하여 상호 연결되어 정보를 송수신하게 되었다. 이와 같이 각종 정보가 컴퓨터 통신망을 통하여 송수신되게 됨에 따라, 비인가된 자의 정보에 대한 공격이나 컴퓨터 바이러스와 같은 위협으로 부터 정보 보호에 대한 요구가 증대되게 되었다.

컴퓨터통신망중 현재 수많은 이용자에 의해 사용되고 있는 LAN 환경에서도 이러한 정보 보호 필요성이 증가함에 따라 이를 논의하기 위해 1988년 봄에 개최되었던 예비 회의에서 표준화 작업을

의한 정보자원 액세스, 비인가자에의 데이터 노출 등이 있다. 이러한 공격이나 위협중 데이터 변조를 막기 위해서는 데이터의 무결성 서비스가 필요하고, 정당한 사용자로 가장하는 것을 막기 위해서는 데이터 발신처에 대한 신분확인 서비스가 필요하다. 또한 비인가자에 의한 정보자원 사용을 막기 위해서 액세스 제어 서비스가 요구되고, 데이터의 노출과 도청등을 막기 위해서는 데이터에 대한 비밀보장 서비스가 필요하다. 〈표 1〉은 LAN의 특성에 따른 정보보호 취약성과 공격 형태,, 그리고 이를 막기 위해 요구되는 서비스를 보여주고 있다.

〈표 1〉 LAN의 보호 취약성과 서비스

LAN의 특성	취 약 성	위 협	요구 서비스
데이터전송	임의의 Station은 임의의 주소를 사용하여 다른 Sta - tion에 정보전송 가능	-정당한 통신 상대로 가장 -비인가자의 자원사용	-데이터발신처 신분확인 -액세스 제어
데이터수신	모든 Station이 송신되는 데이터 액세스 가능	-데이터 변경 -비인가자에 정보누출	-데이터 무결성 -데이터 비밀보장
주소 공간	주소관리를 통한 분명한 제어 불가능	-정당한 통신상대로 가장 -비인가자의 자원사용	-데이터발신처 신분확인 -액세스 제어
지리적분산	도청 가능성이 큼	-데이터 변경 -비인가자에 정보누출	-데이터 무결성 -데이터 비밀보장

상기의 보호 서비스들 모두는 정보보호 메카니즘 중 암호화 기술에 의해 제공 가능하다. 즉, 비밀보장 서비스를 제공하기 위한 여러 기술중 가장 간단하고 신뢰성 있는 방법은 암호화 메카니즘을 이용하는 것으로 송수신되는 정보를 암호화 함으로써 데이터의 노출을 방지할 수 있다. 무결성 서비스는 비밀보장을 위한 암호화 결과로써 대부분 실현되며, 데이터 영역을 포함하는 암호화 검사합 (Cryptographic Checksum)에 의해 무결성 서비스가 제공 가능하다. 발신처 신분확인 서비스는 송신자 주소의 복사본을 계층2 SDU(Service Data Unit)의 Prefix 또는 Suffix로서 암호화된 데이터영역에 포함시킴으로서 제공될 수 있다.

액세스 제어 서비스는 암호키 관계등과 같은 암호화 연계(Cryptographic Association)의 관리 및 응용을 통해 제공 가능하다.

즉, 모든 PDU가 암호화 된다면 암호화 메카니즘 및 암호 키를 알고 있는 station만이 통신할 수 있고, 이러한 기능이 없는 station은 보호되는 자원들을 액세스할 수 없게 된다.

ISO 7498-2의 보호 구조는 이러한 LAN의 속성을 충분히 고려하지 않고 계층2 보호 서비스로서 비밀보장 기능만을 명시하고 있으므로, IEEE 802.10에서는 LAN에서 요구되는 정보 보호 서비스를 제공하기 위해 보호 모델을 제시하고 이에 따른 표준 규약 개발을 수행하고 있다.

추진키로 하였다. 그리고 "IEEE 802 Technical Committee"와 "IEEE Technical Committee on Security and Privacy"의 후원하에 802.10 (Security Working Group)을 구성하여 LAN에서의 정보 보호를 위한 규약 작성 작업을 시작하게 되었다.

IEEE 802.10에서 작성되고 있는 표준인 SILS (Standard for Interoperable LAN Security)는 LAN에서의 정보 보호를 위한 규약으로서 SILS 모델, 데이터의 안전한 교환을 위한 규약, 키 관리, 시스팀/보호 관리에 대해 명시하고 있다. 본 고에서는 LAN 환경에서의 정보 보호 배경과 필요성, SILS 구조 및 규약체계에 대해 기술한다.

Ⅱ. LAN에서의 정보 보호 서비스 필요성

1. LAN 통신규약의 특성과 보호 취약성

ISO 7498-2에 명시된 OSI 참조모델의 보호 구조는 광역통신망(WAN : Wide Area Network) 구조에 근거하여 작성되었다. 데이터연결 계층 규약의 경우 WAN과 LAN은 유사한 서비스를 제공하고 있으나, LAN에서는 그 특성상 WAN과 다른 속성을 가지고 있다. 이러한 LAN의 속성으로는 데이터 전송특성과 수신특성, 주소공간 특성, 지리적 분산특성이 있으며, LAN의 데이터연결 계층 규약은 WAN의 망 계층 규약과 유사한 특성을 갖는다.

WAN의 경우 데이터연결 계층에서는 독립적인 링크들 사이에 점 대 점(point-to-point) 패킷교환이 이루어지고 데이터의 방송(Broadcasting) 기능은 망 계층에서 이루어지는 반면, LAN에서는 데이터연결 계층에서 방송이 일어나는 특성을 가지고 있다. 즉, LAN에서는 어떤 한 Station에서 임의의 주소를 사용하여 다른 Station으로 PDUs을 전송할 수 있으므로, 비인가자의 자원 사용이나 정당한 사용자로의 위장등의 보호 위협이 발생하게 된다. 그리고, 어떤 한 Station은 임의의 Station에서 전송되는 모든 데이터를 액세스하는 것이 가능하므로, 비인가자에 의한 데이터의 변조등의 위협이 발생한다.

주소공간의 경우 WAN에서는 데이터연결 계층의 주소는 국부적으로 지정 및 관리가 가능하나, LAN에서는 계층2에서 유일한 주소를 가져야 하고 이 주소가 정당한 지 여부를 구별하기가 어려우므로 비인가자의 자원 사용이나 정당한 사용자로의 위장 등의 보호 위협이 발생하게 된다.

또한 WAN과 LAN 모두는 지리적으로 분산되어 있으므로 도청이나 Wiretap등에 취약하고, 그 결과 비인가자에 의한 데이터 변조등의 위협이 발생한다. 이러한 Wiretap과 같은 공격이 있을 경우 WAN에서는 특정 통신 실체에 대한 위협만이 발생하나, LAN에서는 망의 구성상 전체 Station에 위협이 미치게 된다.

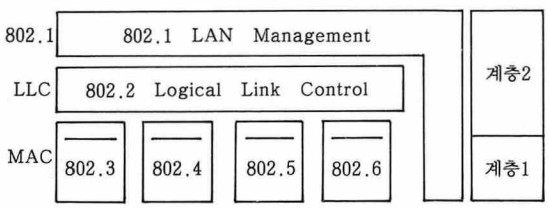
2. LAN에서의 정보보호 방안

LAN의 데이터연결 계층 규약은 앞서 기술한 바와 같이 WAN의 망계층 규약과 유사한 속성을 가지고 있으므로, LAN에서 정보 보호 서비스를 제공하기 위해서는 LAN의 속성을 만족시켜 줄 수 있는 보호 규약이 필요하다.

LAN에서 일어날 수 있는 정보 위협의 형태에는 데이터 변조, 정당한 사용자로의 가장, 비인가자에 의한 정보자원 액세스, 비인가자에의 데이터 노출

Ⅲ. IEEE 802 LAN 규약 구조와 SILS

IEEE 802에서 작성된 LAN 표준에는 MAC(Media Access Control) 규약으로 802.3(CSMA/CD), 802.4(Token-Bus), 802.5(Token-Ring), 802.6(MAN)등이 있으며, 데이터 연결 규약인 802.2(LLC : Logical Link Control)와, 관리 규약인 802.1(LAN Management)가 있다. 이러한 규약은 OSI 기본 참조모델의 제1계층 및 제2계층에 해당되는 것으로 규약 구조는 (그림 1)에 표시된 바와 같다.



(그림 1) IEEE 802 LAN 구조

IEEE 802.10 보호작업그룹에서는 기존의 LAN 모델에 정보 보호 서비스를 제공하기 위한 규약인 SILS를 작성하고 있다. SILS는 4개의 표준으로 이루어지며, 각각은 다음과 같다.

IEEE 802.10A : SILS Model

IEEE 802.10B : SILS SDE(Secure Data Exchange) Protocol

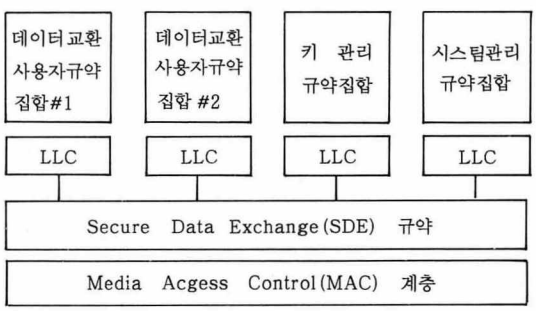
IEEE 802.10C : SILS Key Management Protocol

IEEE 802.10D : SILS System/Security Management Protocol

802.10A는 LAN에서 정보 보호 기능을 제공하기 위한 모델 및 규약의 구조적 체계를 기술하며, 실제 보호 기능을 제공하기 위한 LAN 보호 규약들의 범위 및 사용에 대해 기술하고 있다. 802.10B는 MAC과 LLC 사이에 존재하여 안전한 데이터 교환 기능을 제공하는 규약이고, 802.10C는 SDE 계층에서 사용될 암호 키 관리를 위한 규약이며, 802.10D는 전체 시스팀 관리를 위한 규약이다.

위 규약중 SDE는 완료되어 JTC1/SC6에 표준화 항목으로 제안된 상태이고, 키 관리와 시스팀/보호 관리 규약은 현재 작성되고 있는 중이다. SILS에서 정의되고 있는 세 규약은 각각 상호 독립적으로 구현가능하다. 즉, 한 보호 규약의 사용이 다른 규약의 사용을 강제하지 않도록 규약을 작성하고 있다. 또한 각 규약은 SILS를 구현하고 있지 않은 기존 기기와의 통신에 영향을 끼치지 않고 사용될 수 있는 투명(Transparent) 모드를 함께 지원하고 있다.

SILS 규약집합에는 데이터 교환 사용자 규약집합(Data Exchange User Stack)과 키관리 규약집합, 그리고 시스팀/보호 관리 규약집합이 있으며 그 구조는 (그림 2)와 같다.



(그림 2) SILS 규약집합 구조

여기서 데이터 교환 사용자 규약집합은 SILS가 구현되기 전에 사용되던 기존의 통신규약을 의미하며 SDE의 보호 서비스를 지원받아 보호 기능이 제공될 수 있다.

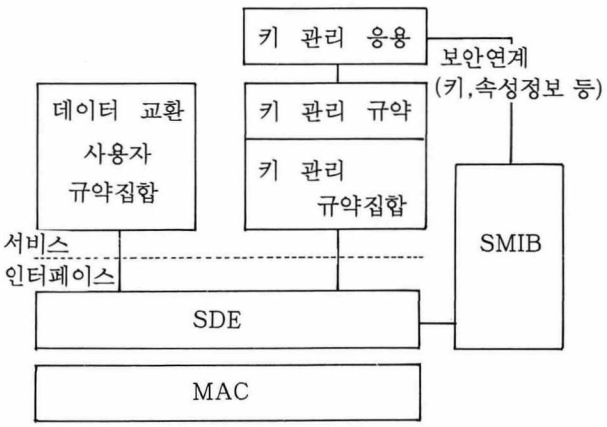
이때 SDE 규약은 키 관리 및 시스팀/보호 관리 규약집합으로부터 데이터 암호화 키와 같은 정보를 지원받아 사용자 규약집합에 보호 서비스를 제공한다. SDE 규약은 투명한 MAC 인터페이스를 제공하므로 기존의 MAC 위에서 동작하는 모든 데이터 교환 규약집합이 SDE와 관계없이 사용될 수 있다.

OSI 환경에서의 관리 모델을 명시하고 있는 IS 7498-4에서는 시스팀 관리(System Management)와 계층 관리(Layer Management)를 정의하고 있으며, SILS는 기본적으로 이러한 개념을 따라 규약을 작성하고 있다. 시스팀 관리는 전체 망과 관련되어 관리 기능을 수행하지만 계층 관리는 어느 특정 계층에 대한 관리 기능을 제공한다. 그러므로 어느 한 계층에서 계층 관리 기능을 수행하는 계층 관리자(LM : Layer Manager)는 자신이 관리하는 계층에서 발생하는 사건에 대한 정보밖에 알지 못하므로 타 계층이 필요로 하는 적절한 처리를 할 수 없다. 따라서 계층7에서 동작하는 시스팀 관리 응용 프로세스가 각 계층 관리자로부터 정보를 받아 전체 시스팀 관리를 수행한다.

이러한 계층 및 시스팀 관리를 위해 각 규약에서 타이머, 버퍼크기, 원도우 크기등과 같은 관리될 객체(Object) 정보를 정의해야 하며, 정의된 객체 정보는 관리정보 베이스(MIB : Management Information Base)에 저장되어 사용된다.

특히 정보 보호 기능을 제공하기 위해 사용되는 객체는 비인가자에게 노출되지 않도록 별도로 관리될 필요가 있으므로 보호 관리정보 베이스(SMIB : Security MIB)를 정의하여 사용하고 있다. 여기서 SMIB의 구조는 구현자에 의해 적절히 실현될 수 있으나, 객체 구조는 IS 10165-2(SMI : Structure of Management Information)으로 표준화되고 있다.

SMIB는 계층7의 시스팀 관리 및 키 관리 응용 프로세스와 SDE 부계층 사이의 통신 경로를 제공한다. 즉, (그림 3)에 표시된 바와 같이 키 관리 응용은 SMIB를 통해 보호 관련 정보를 SDE 규약에 제공하며, 이 정보에 의해 사용자 규약집합에 제공되는 보호 서비스가 영향받을 수 있다.

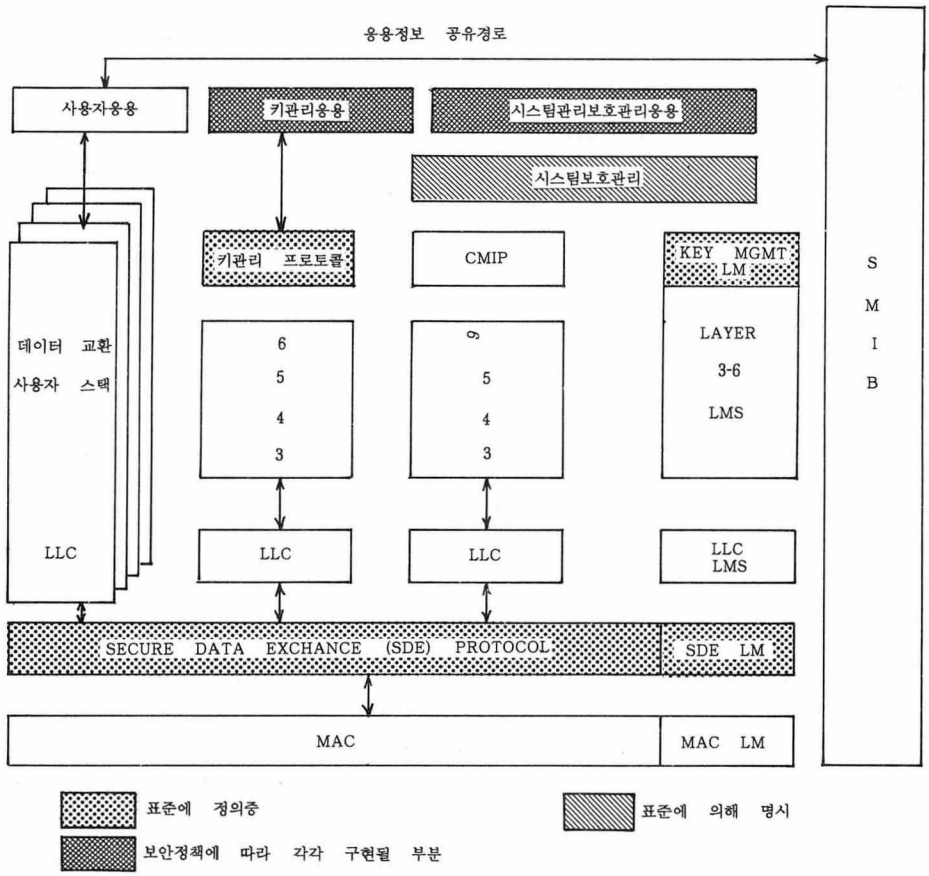


(그림 3) SMIB의 사용

Ⅳ. LAN의 정보 보호 모델

IS 7498에서 정의하고 있는 OSI 기본 참조모델을 따른 OSI 환경에서 ISO SILS 모델과 IEEE 802 SILS 모델은 각각 (그림 4), (그림 5)와 같다. 그림에 표시된 바와 같이 ISO SILS 모델에서는 시스팀 관리를 위해 CMIP를 사용하며, 802 SILS 모델에서는 LLC 위에서 동작하는 802.1 관리체계를 사용한다. SILS는 ISO의 계층7 규약인 공통관리규약(CMIP : Common Management Information Protocol)와 LLC 바로 위에서 동작하는 IEEE 802.1의 관리체계 모두를 지원해야 한다. 그러나 2개의 관리규약이 존재한다고 해서 서로 다른 키 관리 규약을 명시할 필요는 없으므로,

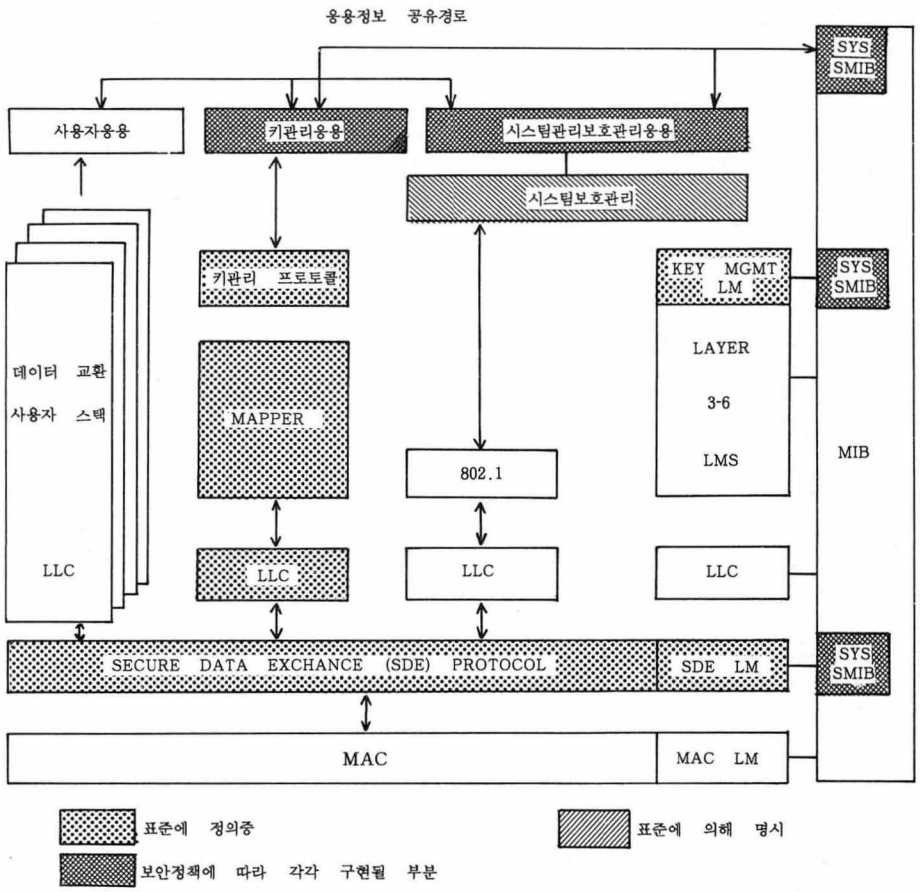
SILS에서는 두 관리 환경에서 하나의 키 관리 규약을 사용할 수 있도록 하는 Mapper를 명시한다. 따라서, 만일 키 관리 규약이 LLC에 의해 제공되지 않고 OSI 상위계층 규약에 의해 제공되는 서비스를 요구할 경우, Mapper가 이러한 기능을 키 관리 규약에 제공하는 기능을 수행한다.



(그림 4) ISO SILS 모델

이러한 ISO SILS 모델과 802 SILS 모델이 결합된 SILS 서비스와 규약의 전체 모델은 (그림 6)과 같다. 그림에서 키 관리 규약과 SDE 규약, 그리고 각각의 계층관리 규약과 Mapper는 SILS에서 정의되고 있다. 관리실체(Management Entity)들로는 계층관리자(LM), 관리정보베이스(MIB), 보호 관리정보 베이스(SMIB), 그리고 시스템/보호 관리가 있다. 이중 시스템/보호 관리는 현재 정의되어 있지 않지만, 시스템/보호 관리 응용이 필요로 하나 CMIP나 IEEE 802.1이 제공하고 있지 않은 보호 특성들을 제공하도록 정의될 것이다. 또한 키 관리 응용과 시스템/보호 관리 응용, 그리고 SMIB 기능은 구현자가 실현하기에 달려있다. 한 예로서 키 관리 규약이 키 교환 기능을 수행하지만

언제 키 교환을 해야할 지 여부는 시스템 구현 정책에 따라 키 관리 응용만이 알 수 있다. 이러한 시스템 전체의 관리를 위해 키 관리 응용과 시스템/보호 관리 응용, SMIB 사이에 통신을 통해 관리정보를 주고받게 된다.

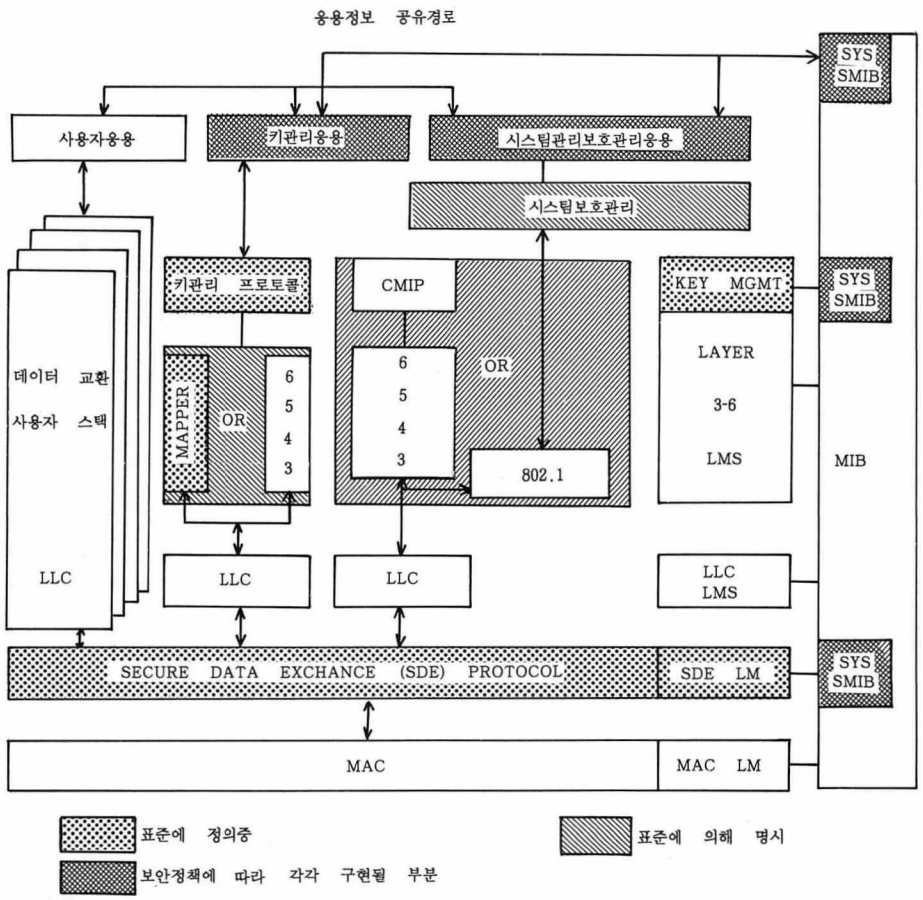


(그림 5) 802 SILS 모델

1. 안전한 데이터 교환 규약 (SDE Protocol)

OSI 기본 참조모델의 제2계층에 해당되는 통신규약으로 데이터 연결계층에서 데이터의 안전한 교환 기능을 제공한다. IS 7498-2에서는 계층2의 정보보호 서비스로 데이터 비밀보장(Confidentiality) 기능만을 정의하고 있지만, SDE에서는 비밀보장 서비스뿐만 아니라 무결성(Integrity), 데이터발신처 신분확인(Authentication), 액세스 제어(Access Control) 서비스를 제공한다.

SDE는 기존의 MAC/LLC 인터페이스를 그대로 유지하고 있으며, 단일 MAC station이나 복수의 station을 지원하는 MAC 브리지에 사용될 수 있다.



(그림 6) 완전한 SILS 모델

2. 키 관리 규약 (Key Management Protocol)

OSI 기본 참조모델의 제7계층에 해당되는 프로토콜로, SDE 계층에서 데이터를 보호하기 위해 사용되는 암호키 관리 서비스를 제공하며, 키의 적절한 발신처 및 목적지를 확인하기 위해 신분확인 메카니즘이 키 관리에 포함된다. 그리고 키 관리 응용은 SILS에 의해 정의되는 키 관리 규약이 제공하는 서비스를 사용한다.

사용자의 다양한 필요를 만족시키고 키 관리규약의 사용에 있어 제한사항을 줄이기 위해 IEEE 802.10은 암호와 및 키 관리 알고리즘과 독립적으로 동작될 수 있는 규약을 개발하고 있다. 이는 사용자가 다양한 알고리즘을 선택하여 사용할 수 있도록 하는 것으로, 이를 위해서는 여러 알고리즘을 쉽게 식별할 수 있는 메카니즘이 요구된다. 현재 ISO에서는 암호 알고리즘의 등록절차를 규정한 표준을 개발하고 있으므로 곧 암호 알고리즘 등록 서비스가 제공될 전망이나, 키 관리 알고리즘

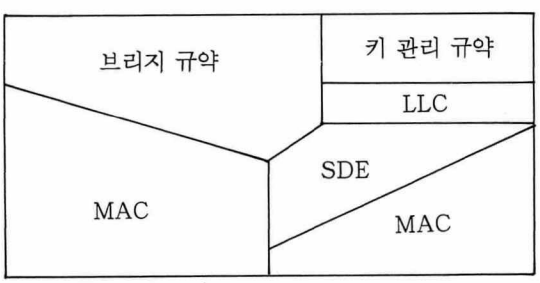
에 대해서는 아직까지 구체적인 활동이 없는 상태이다.

3. 시스템/보호 관리 규약 (System/Security Management Protocol)

전체 시스템의 관리와 보호 기능을 제공하는 규약의 관리를 위해 사용되는 서비스 집합으로, SDE와 키 관리 규약 각각은 시스템 관리에 의해 관리될 필요가 있는 객체를 식별하여 정의하여야 한다. 그리고 계층관리는 해당 계층의 관리될 객체에 대한 부호화와 규약상태에 미치는 영향을 정의한다. 또한 시스템 관리 응용 프로세스는 시스템/보호 관리를 위해 CMIP나 IEEE 802.1을 이용하여 다른 종단 시스템과 통신한다.

4. 브리지 모델 (Bridge Model)

SDE 규약은 MAC 경계에 있으므로 SDE가 브리지에서 구현될 경우 전체 LAN을 보호할 수 있다. 즉, SDE는 브리지 규약이나, 트래픽 발신처 및 해당 LAN에 대한 트래픽을 보호할 수 있으며, SILS 브리지 모델은 (그림 7)과 같다.



(그림 7) SILS 브리지 모델

그러나 LAN의 특성상 LAN에서의 트래픽 보호 기능에 대해 어떤 제한이 있을 수 있다. 즉, 복수의 MAC 브리지가 단일 LAN을 지원할 수 있으므로, 두 브리지가 동일 LAN station에 대한 트래픽 처리를 하려는 경우가 발생할 때 각 브리지는 해당 station에 대해 암호화 정보와 같은 보호연계 (Security Association) 속성을 공유해야 한다. 또한 PDUs 사이에 Cryptographic Chaining을 지원하기가 어려운 문제가 있다.

V. 결 론

LAN은 현재 정보통신망의 기본 구성 요소로서 일반 사용자에 널리 퍼져있고, 그 사용자의 수효 또한 대단하다. 이 에따라 LAN에서의 안전한 정보 교환 및 데이터의 비밀보장 등 정보 보호 서비스에 대한 사용자의 요구가 급증하고 있다. 그러나 OSI 기본 참조모델에서의 정보보호 구조를 명시하고 있는 IS 7498-2에 LAN의 특성에 따른 요구사항이 충분히 고려되지 못하였기 때문에 IEEE 802.10 정보보호 작업그룹은 LAN에서의 정보보호 규약을 작성하게 되었다. IEEE 802.10에서 제정되고 있는 SILS는 이러한 관점에서 충분한 보호 기능을 사용자들에게 제공할 수 있는 해결책으로 여겨지며, 향후 이를 구현한 제품이 널리 공급될 것으로 예상된다.

본 고에서는 LAN의 특성에 따른 정보 보호 서비스의 필요성과, 현재 작성되고 있는 보호 모델 및 규약체계에 대해 살펴보았다. SDE 규약은 이미 완료되어 JTC/SC6에 표준화 항목으로 제안되어 있는 상태이고, 키 관리 규약과 시스템/보호 관리 규약이 제정되고 있는 중이므로 국내에서도 이에 대한 연구가 시급한 실정이다.

참 고 문 헌

1. LAN Security Working Group, Rationale for

Layer 2 Security Services for Local Area Networks, IEEE 802.10, 1989.
2. R.L Parker, Layer 2 Security Services for LANs, The MITRE Corporation, 1989.
3. IEEE 802.10, SILS : Part A…The Model, P802.10A/D1, Dec. 1989.
4. IEEE 802.10, SILS : Part B…Secure Data Exchange, P802.10B/D6, Nov. 1990.
5. IEEE 802.10, SILS, P802.10/D6, Sep. 1989.
6. International Standard, OSI-Basic Reference Model - Part 2 : Security Architecture, ISO/IEC JTC1 IS 7498-2, 1988.
7. USA, US Contribution on Interoperable LAN Security Standard, JTC1/SC6 N6596, 1991.