通信情報保護學會誌
第3卷 第1號, 1993.3

# IEEE 802 구조에서의 정보보호 모델 분석

## Analysis of Security Model in IEEE 802 Architecture

유황빈* · 이재광**

## 1. 서 론

고도의 정보화 사회를 구축하기 위한 노력은 컴퓨터 보급의 확산과 정보 통신 기술의 발전에 따라 계속 변화 되어가고 있다. 정보 통신 기술 분야가 일반화되어 감에 따라 컴퓨터에서 생성, 저장, 관리되는 정보 자원과 통신망을 통하여 전송되는 정보자원에 대한 보호는 그 중요성이 점점 더해가고 있다.

인접한 지역내에 산재되어 있는 정보기기를 상호 연결하여 보다 효율적으로 사용할 수 있도록 하는 근거리 통신망 또한 꾸준히 발전해 왔으며, 최근에는 근거리 통신망이 고속 전송과 상호연결 범위의 확장 등으로 급속하게 발달(FDDI, HS LAN, LAN bridge, LAN server 설비 등)로 인하여 자원의 이용 범위가 날로 확장되고 있는 추세이다. 그러나, 근거리 통신망 구성의 개방성은 중요한 정보 자원에 대한 정보보호 취약성이 증가하여 중요 정보의 누출, 오용, 불법 변경, 파괴, 개인 프라이버시 침해, 바이러스 등의 위협을 가지게 되어 이에 대한 정보보호 구조가 절실히 요구되는 상태이다. 또 근거리 통신망에 대한 통신기술과 병행하여 정보보호 메카니즘의 개발이 진행되지 않았으며, 정보보호 메카니즘이 기존 통신망 운용에 장애가 되고 상호연결에 제한이 될 수 있기 때문에 이의 해결을 위한 근거리 통신망 정보보호 구조와 정보보호 프로토콜의 개발이 매우 중요한 과제로 대두되고 있다.

IEEE 표준위원회에서는 근거리 통신망의 정보보호 필요성이 증가함에 따라 '88년 봄에 개최된 예비회의에서 근거리 통신망에 대한 정보보호 프로토콜 표준화를 추진키로 하여 "IEEE 802 technical committee"와 "IEEE technical committee on security and privacy"의 후원하에 802.10(security working group)을 구성하고 근거리 통신망에서의 정보보호 프로토콜 표준안 작성 작업을 시작하였다. IEEE 802.10 표준안인 SILS(Standard for Interoperable LAN Security)는 4분야로 나누어서 작업을 진행하고 있는데 이는,

분야 A : SILS 모델,
분야 B : 안전한 데이타 교환(SDE : Secure Data Exchange) 프로토콜,
분야 C : 키이 관리(Key Management) 프로토콜,
분야 D : 시스템/정보보호 관리(System/Security Management) 프로토콜

이다. 이 가운데 분야 A,B는 draft가 나와있는 상태이고 C,D는 아직 작업 결과없는 상태이므로 전체적으로 예비 규정 단계라고 할 수 있다.

IEEE 802에서 작성한 근거리 통신망 표준안은 전송 매체의 구성 형태 및 액세스 제어 방식에 따라 MAC 서브계층을 4가지로 구분하여 제공하고 있으

* 광운대학교 전자계산학과 교수
** 군산실업전문대학 전자계산과 부교수

며, LLC는 모든 MAC 계층에 공통으로 적용되도록 하고 있다. 따라서 근거리 통신망 구조상 접속된 모든 노드가 네트워크에서 전송되는 모든 데이타 트래픽을 액세스할 수 있다. 즉, LLC에서 전송되는 PDU (Protocol Data Unit : 패킷, 프레임)는 방송 통신 방식으로 수행되므로 모든 노드가 PDU를 액세스할 수 있으므로 정보보호가 취약하다. 그러므로 근거리 통신망 구조에서는 정보보호는 논리적으로 peer entity 간에 송수신되는 PDU에 행해지는 공격(attack)에 대해 필요하다. PDU에 대한 공격에는 PDU를 관찰하여 그 내용을 불법적으로 알아내려는 수동적(passive) 공격과 PDU에 대한 불법적인 처리 (PDU 삭제, PDU 수정, 전송 순서 변경, 가짜 PDU 삽입, 이중 전송 등)를 행하는 능동적(active) 공격이 있는데 이러한 공격에 대한 정보보호를 위해서는 암호화 시스템을 이용한 정보보호 프로토콜이 필요하다.

본 논문에서는 근거리 통신망에서 사용하는 IEEE 802 프로토콜에 대하여 정보보호 취약성과 이의 해결을 위한 요구 서비스, 802.10 SILS 구조 및 프로토콜 체계에 대하여 기술한다.

## 2. IEEE 802 구조에서의 정보보호 서비스

### 2.1. IEEE 802 프로토콜 구조

IEEE 802에서 작성된 근거리 통신망 표준안에는 서브 계층으로서 MAC(Media Access Control) 프로토콜이 있으며, 각각의 액세스별로 802.3(CSMA/CD), 802.4(Token Bus), 802.5(Token Ring), 802.6(MAN) 등이 있다. 또, 데이타 링크 프로토콜인 802.2(LLC : Logical Link Control)와 관리 프로토콜인 802.1(LAN Management)이 있다. 이 프로토콜들은 OSI 기본 참조 모델의 제 1 계층과 제 2 계층에 해당되는 것으로 프로토콜 구조는 그림 1과 같다.

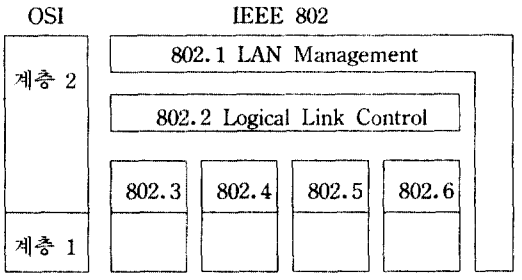


그림 1. IEEE 802 LAN 프로토콜 구조

### 2.2. IEEE 802 프로토콜의 특성과 정보보호 취약성

컴퓨터 통신망의 모델로서 ISO 7498 OSI 기본 참조 모델은 통신 프로세서의 기능을 7계층으로 구분하여, 각 계층은 고유의 통신 서비스를 제공하는 것으로 정의하고 있다. 이 ISO 7498 OSI 기본 참조 모델을 근거로 한 정보보호 구조로서 ISO 7498-2로 작성되었다. 이 구조에서 제공되는 기본 정보보호 서비스로는 액세스 제어(access control), 인증(authentication), 데이타 비밀유지(data confidentiality), 데이타 무결성(data integrity), 부인봉쇄(non-repudiation)등이 있다. 이 표준안은 구조적인 모델로서 패킷 교환망(PSN : Packet Switched Network)과 광역 통신망(WAN : Wide Area Network)을 기준으로 하여 요구되는 정보보호 서비스들을 계층별로 구분 적용하였다.

ISO 7498-2는 계층 2에서 요구되는 정보보호 서비스로서 데이타 비밀유지 서비스만을 제공하는 것으로 되어 있으므로, 이를 그대로 IEEE 802 구조에 적용하기에는 적합하지 않다. 왜냐하면, 데이타 링크층에서 제공하는 서비스는 광역 통신망과 근거리 통신망이 유사하나 근거리 통신망은 그 특성상 다른 속성을 가지고 있다. 즉, 패킷 교환망과 광역 통신망의 데이타 링크 계층과 근거리 통신망의 데이타 링크 계층은 유사한 속성을 가지며, 또 패킷 교환망과 광역 통신망의 네트워크 계층의 서브 네트워크와 인터네트워크 기능도 근거리 통신망 데이타 링크 계층의 속성과 유사하다. 하지만 근거리 통신망은 광역 통신망과 패킷 교환망과는 다른 속성을 가지기 때문에 근거리 통신망 속성에 적합한 정보보호 구조가 필요하다. 근거리 통신망 속성에는 데이타 전송 특성, 데이타 수신 특성, 주소 공간, 지리적 분산

등 4가지 특성을 갖는다.

데이타 전송 특성은 광역 통신망에서는 계층 2인 데이타 링크 계층에서 독립적인 링크들간에 점대점(Point-to-point) 데이타 전송이 이루어지며, 계층 3인 네트워크 계층에서는 서브 네트워크에 대해 방송(Broadcast) 모드의 전송이 수행된다. 그러나 근거리 통신망에서는 통신망의 구성상 LLC 계층에서 서브 네트워크에 대한 방송 모드로의 전송이 이루어진다. 따라서, 근거리 통신망에서 데이타 전송의 방송 특성은 두가지의 문제점을 갖는다. 첫째는 근거리 통신망을 구성하는 모든 노드는 자기 노드를 제외한 다른 모든 노드들에게 데이타를 전송할 수 있으며, 통신망을 구성하는 노드의 액세스에 대한 LLC 계층에서의 제어가 명확하지 않다. 둘째는 데이타 전송의 송신측을 확인하기가 어렵기 때문에 송신측이 다른 노드라고 주장할 수도 있으므로 송신측 노드에 대한 인증이 어렵기때문에, 어떤 노드이든 다른 노드의 주소를 이용하여 다른 노드들에게 데이타를 전송할 수 있으므로 이에 대한 정보보호 위협으로는 정당한 사용자로의 가장이 발생할 수 있다. 또 wiretaping에 취약하여 어떤 노드 또는 노드들이 단일 tap을 이용하여 위조 또는 자원을 이용할 수 있으므로 권한을 가지지 않는 자에 의한 자원 이용이 발생할 수 있다.

데이타 수신 특성은 전송 특성과 유사하다. LLC 계측에서의 방송 특성은 모든 노드들이 전송되는 모든 데이타를 액세스할 수 있으므로 두가지 문제점을 갖는다. 첫째는 권한을 가지지 않는 노드가 데이타를 수신할 수 있고, 둘째는 송신측이 원하는 수신측에서 데이타를 수신하기 전에 다른 노드에서 PDU의 데이타를 변경할 수 있다. 이 점은 특히 링형 근거리 통신망에서 정보보호 위협의 노출이 가장 크다. 따라서 수신 특성이 갖는 근거리 통신망 정보보호 위협은 권한을 가지지 않는 자가 정보를 수신할 수 있고, 데이타를 수정할 수 있다.

주소 공간의 경우, 근거리 통신망은 LLC 계층에서의 주소는 노드 인테페이스를 구분하며 단일 주소 공간을 갖는다. 이 주소는 제어 담당 노드(NIU : Network Interface Unit)에 의해 관리되지만 주소의 타당성 여부를 확인할 수 없다. 즉, 주소의 인증을 명확하게 할 수 없기 때문에 주소의 간단한 점검을 통하여 액세스에 대한 제어를 명확하게 할 수 없다. 이와 같이 주소 관리를 통한 제어가 명확하지 않기 때문에 일어날 수 있는 정보보호 위협으로는 정당한 사용자로의 가장, 권한을 가지지 않는 자의 자원 이용이 발생할 수 있다.

지리적 분산의 경우, 근거리 통신망을 구성하는 노드들은 지리적으로 분산되어 있기 때문에 도청이나 wiretapping에 취약하다. 따라서, 데이타의 수정과 권한을 가지지 않는 자에게 정보 노출의 위협이 발생한다. 특히 wiretapping과 같은 공격은 광역 통신망에서는 특정 통신 실체에 대한 위협만이 발생하나 근거리 통신망에서는 특정 노드뿐만 아니라 전체 노드들에게 위협이 미치게 된다.

## 2.3. IEEE 802 구조에서의 정보보호 대안

2.1절에 기술된 근거리 통신망 속성에 따른 정보보호 위협과 취약점들은 정보보호 서비스를 이용하여 해결할 수 있다. 근거리 통신망에서 발생할 수 있는 위협과 이를 방지하기 위한 서비스 및 그 기능은 다음과 같이 기술할 수 있다.

(1) 데이타 수정-무연결 데이타 무결성(connectionless data integrity) : 단일 무연결 PDU의 데이타가 임의로 변경되거나 파괴되지 않게 하는 성질로서 위장된 데이타 송신, 권한을 가지지 않는 자에 의한 데이타의 수정으로부터 보호한다.

(2) 정당한 사용자로의 가장-데이타 발신처 인증(data origin authentication) : 수신된 데이타의 발신처를 확증하는 성질로서 임의로 발신처 주소를 이용하여 송신하는 노드가 없도록 한다.

(3) 권한을 가지지 않는 자에 의한 자원 이용-액세스 제어(access control) : 임의로 자원을 이용하는 것을 방지하고, 어떤 노드이든 임의로 다른 노드에게 PDU를 전송하지 못하도록 한다.

(4) 권한을 가지지 않는자에게 정보 노출-데이타 비밀 유지(data confidentiality) : 정보가 권한을 가지지 않는 개체들, 앤티티들, 프로세스들에게 이용되거나 노출되지 않도록 하는 성질로서 권한없이 데이타를 액세스하지 못하도록 하며, 도청 (엿듣기)

으로부터 보호한다.

근거리 통신망 구조에서 요구되는 정보보호 서비스들은 근거리 통신망의 기존 특성을 유지하면서 LLC 계층에서 일어날 수 있는 위협들에 대해 모든 사용자와 응용(application)을 위한 정보보호를 제공해야 한다. 근거리 통신망 특성에 따른 정보보호 취약점과 정보보호 위협, 그리고 이를 보호하기 위해 필요한 서비스를 정리하면 표 1과 같다.

표 1. LAN 정보보호 취약성과 요구 서비스

| LAN 속성 | 취 약 점 | 정보보호 위협 | 요구 서비스 |
|---|---|---|---|
| 데이타송신 | 모든 노드가 주소를 이용하여 다른 노드에게 송신 가능 | 정당한 사용자로 가장, 권한을 갖지 않는 자가 자원 이용 | 데이타 발신처 인증, 액세스 제어 |
| 데이타수신 | 전송되는 정보를 모든 노드가 액세스 가능 | 데이타 수정, 권한을 가지지 않는 자에게 정보 노출 | 무연결 데이타, 무결성 데이타 비밀유지 |
| 주 소 공 간 | 주소관리를 이용한 명확한 제어 불가능 | 정당한 사용자로 가장, 권한을 갖지 않는 자가 자원 이용 | 데이타 발신처 인증, 액세서 제어 |
| 지리적분산 | 도청 | 데이타 수정, 권한을 가지지 않는 자에게 정보 노출 | 무연결 데이타 무결성, 데이타 비밀유지 |

표 1에서의 LLC 계층에서 요구되는 정보보호 서비스들은 상호 종속성을 갖는데, 이는 표 2와 같다.

표 2. 정보보호 서비스 종속성

| 정보보호 서비스 종속성 | |
|---|---|
| 서 비 스 | 종 속 성 |
| 비밀유지 | 없 음 |
| 무결성 | 없 음 |
| 인증 | 무결성에 의존 |
| 액세스 제어 | 인증과 무결성에 의존 |

근거리 통신망에서 요구되는 정보보호 서비스들은 암호화 시스템을 이용하여 제공할 수 있다.

데이타 비밀유지 서비스는 이 서비스를 제공하기 위한 여러 기술 중 가장 간단하고 신뢰성이 높은 방법인 키이를 이용한 암호 알고리즘을 적용하여 송수신되는 데이타를 암호화함으로써 데이타의 노출을 방지할 수 있다.

무연결 데이타를 암호화함으로써 데이타의 노출을 방지할 수 있다.

무연결 데이타 무결성 서비스는 암호화를 이용한 데이타 비밀유지 서비스의 자동효과로서 실현되는데 암호 알고리즘, 키이 관리, 그리고 데이타와의 조합으로 생성되는 MAC(message authentication code)를 생성하여, 이를 PDU에 추가하여 전송한다. 그러면 수신측에서는 수신된 PDU를 같은 역의 과정을 수행하여 수신된 값과 비교하여 같으면 무결성을 확증한다.

데이타 발신처 인증 서비스는 LLC 계층의 SDU에 프리픽스(Prefix)나 서픽스(Suffix)로써 암호화된 데이타 영역에 송신측 주소의 복사본을 포함시켜 암호화 시스템을 이용하여 함께 암호화하여 송신하면, 수신측은 이를 복호화한 후 주소를 확인하므로서 쉽게 제공할 수 있다. 즉, 암호화 시스템에서 사용하는 암호화 키이와 암호 알고리즘을 송수신측만이 알고 있기 때문에 송신측만이 자신의 주소를 포함시켜 암호화할 수 있다.

액세스 제어 서비스는 암호화 키이 관계, 즉 크립토그라픽 어쏘시에이션(cryptographic association)의 관리와 응용을 통하여 제공이 가능하다. 만약 모든 PDU가 암호화 된다면 암호화 알고리즘과 암호화 키이를 알고 있는 노드들만이 정보를 수신할 수 있으므로, 이러한 설비가 없는 노드들은 암호화된 정보를 액세스 할 수 없다.

데이타 발신처 인증을 제외한 나머지 서비스들은 데이타 비밀유지를 제공하기 위해 사용하는 암호화 시스템에 의해 제공될 수 있으며 데이타 발신처 인증도 쉽게 제공할 수 있다. 따라서 단일 암호화 시

스템을 이용하여 이 서비스들을 제공하면, 근거리 통신망 인터페이스에 대한 복잡도와 성능에 미치는 영향을 최소화하여 제공할 수 있다.

## 3. IEEE 802.10 SILS의 구성 및 스택

IEEE 802.10에서 작성하고 있는 SILS는 4분야로 구분되어 있으며 그 내용은 다음과 같다.

(1) 분야 A는 SILS 모델로서 근거리 통신망에서 정보보호 서비스를 제공하기 위한 모델과 프로토콜의 구조적인 체계를 규정하며, 또 실제 정보보호 서비스를 제공하기 위한 프로토콜의 범위 및 사용에 대한 프로토콜이다.

(2) 분야 B는 MAC와 LLC 계층 사이에 안전한 데이타 교환을 제공하는 프로토콜이다.

(3) 분야 C는 SDE 프로토콜에서 사용될 암호화 키이 관리 프로토콜이다.

(4) 분야 D는 전체적인 시스템/정보보호 관리 프로토콜이다.

SILS에서의 각 프로토콜은 상호 독립적으로 구현이 가능하도록 하고 있는데 이는 한 프로토콜의 사용이 다른 프로토콜의 사용을 강요하지 않도록 하고 있다. SILS 모델의 구조는 그림 2에 나타나 있다.

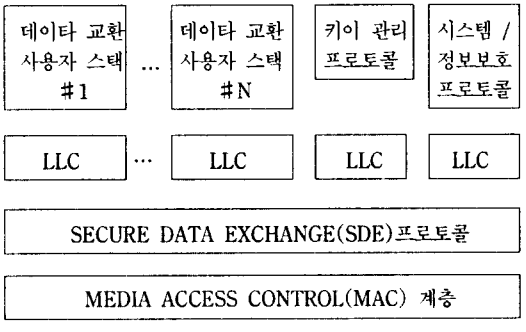


그림 2. SILS 모델의 구조

그림 2에서 데이타 교환 사용자 스택은 SILS를 적용되기 전의 기존 프로토콜이며 SDE 프로토콜을 통하여 전송되는 데이타의 정보보호 서비스를 제공받는다. 이때 SDE 프로토콜은 키이 관리와 시스템/정보보호 관리 프로토콜로부터 암호화 키이 등과 같은 정보를 제공받아 데이타 교환 사용자 스택에 정보보호 서비스를 제공한다. 시스템 관리와 계층 관리는 OSI 환경에서의 관리 모델을 명시하고 있는 ISO 7498-4를 기본 개념으로 프로토콜을 작성하고 있다. 즉, 시스템 관리는 전체 네트워크에 대한 관리 기능을 수행하지만 계층 관리 기능을 수행하는 계층 관리자(LM : Layer Manager)는 자신이 관리하는 계층에서 일어나는 사건에 대한 정보밖에 알지 못하므로 다른 계층이 필요로 하는 적절한 처리를 할 수 없다. 따라서 계층 7에서 동작하는 시스템 관리 응용 프로세스가 각 계층 관리자로부터 정보를 받아 전체 시스템 관리를 수행한다. 계층 관리 및 시스템 관리를 위해서 각 프로토콜에서 타이머, 버퍼크기, 윈도우 크기 등과 같은 관리될 객체를 정의해야 하며, 정의된 객체 정보는 관리 정보 베이스(MIB : Management Information Base)에 저장되어 사용된다. 특히 정보보호 기능을 제공하기 위해 사용되는 객체는 권한을 가지지 않는 자에게 노출되지 않도록 별도로 관리될 필요가 있으므로 정보보호 관리 정보 베이스(SMIB : Security MIB)를 정의하여 사용한다. SMIB의 구조는 구현자에 의해 적절하게 실현될 수 있으나, 객체 구조는 IS 10165-2(SMI : Structure of Management Information)로서 표준화되어 있다. SILS에서는 이 SMIB가 시스템 관리 및 키이 관리 응용 프로세스와 SDE 서브 계층간의 통신 경로를 제공하며 그 구조는 그림 3에 나타나 있다.

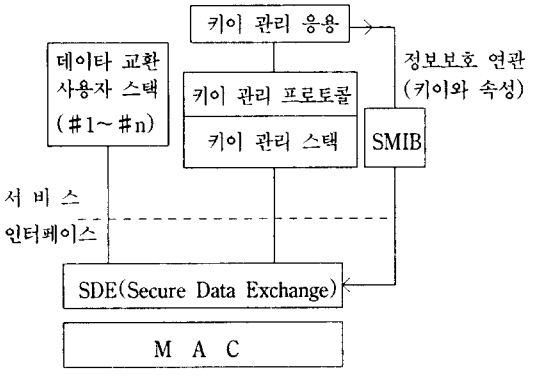


그림 3. SDE와 SMIB 구조

그림 3에 나타난 SMIB와 SDE의 관계는 SDE에서 정보보호 서비스를 제공할 때 키이 관리 응용을 통하여 분배받은 키이를 SMIB가 SDE에게 제공하게 된다. 이 정보에 의해 사용자간의 데이타 교환시에 제공되는 정보보호 서비스가 영향을 받는다.

## 4. SILS 모델

SILS에서는 시스템 관리를 OSI 기본 참조 모델의 ISO와 IEEE 802.1 관리 구조를 지원하도록 하고 있다. IEEE 802.1은 LLC 계층위에서 직접 실행되도록 규정하고 있고 ISO는 계층 7 기능으로서 관리를 규정하고 있다. 시스템 관리를 위해 ISO 모델은 CMIP(Common Management Information Protocol)를 사용하여, IEEE 802.10은 LLC계층 위에서 동작하는 802.1 관리 체계를 모두 지원해야 한다. 하지만 2개의 관리 프로토콜이 존재한다고 해서 서로 다른 키이 관리 프로토콜을 명시할 필요는 없으므로 SILS에서는 두가지 관리 환경에서 하나의 키이 관리 프로토콜을 사용할 수 있도록 Mapper를 이용하도록 규정 중에 있다.

ISO SILS 모델과 IEEE 802 SILS 모델을 결합한 전체적인 SILS 모델은 그림 4와 같다. 현재 키이 관리 프로토콜과 SDE 프로토콜, 이들의 계층 관리자, 그리고 Mapper는 SILS에서 정의 중에 있다. 관리 객체에는 계층 관리자(LM), 관리 정보 베이스(MIB), 정보보호 관리 정보 베이스(SMIB), 그리고 시스템/정보보호 관리는 현재 규정되어 있지 않지만, 시스템/정보보호 관리 응용은 CMIP나 IEEE 802.1이 제공하지 않는 정보보호 특성을 제공하도록 정의할 것이다.

### 4.1. 안전한 데이타 교환 프로토콜

IEEE 802 프로토콜 구조에서의 논리 링크 제어 계층과 매체 액세스 사이에 위치하는 프로토콜로서 데이타의 안전한 교환 기능을 수행한다. ISO 7498-2에서는 데이타 링크 계층에서 필요한 정보보호 서비스로는 데이타 비밀유지 기능만을 정의하고 있지만 SDE 프로토콜에서는 비밀유지 서비스뿐만 아니라 데이타 무결성, 데이타 발신처 인증, 액세스 제어 서비스를 제공한다.

### 4.2. 키이 관리 프로토콜

OSI 기본 참조 모델의 제 7계층에 해당되는 프로토콜로서 SDE 프로토콜에서 데이타의 안전한 교환을 위해 사용되는 암호화 키이 관리 서비스를 제공하며, 키이의 적절한 발신처 및 수신자를 확인하기 위해 신분 확인 메카니즘이 키이 관리에 포함된다.

사용자의 다양한 요구를 만족시키고 키이 관리 프로토콜의 사용에 있어 제한사항을 줄이기 위하여 IEEE 802.10은 데이타의 암호화 수행 알고리즘과 키이 관리 알고리즘이 독립적으로 동작될 수 있도록 개발하고 있다. 이는 사용자가 다양한 알고리즘을 선택하여 사용할 수 있도록 하는 것으로, 이를 위해서는 여러가지 알고리즘을 쉽게 식별할 수 있는 메카니즘이 요구된다. 현재 ISO에서는 암호 알고리즘의 등록 절차를 규정한 표준안을 개발하고 있으나 키이 관리 알고리즘에 대해서는 구체적인 활동이 없는 실정이다.

### 4.3. 시스템/정보보호 관리 프로토콜

전체 시스템의 관리와 정보보호 기능을 제공하는 프로토콜의 관리를 위해 사용되는 서비스의 집합으로 SDE와 키이 관리 규약은 시스템 관리에 의해 관리될 필요가 있는 객체를 식별하여 정의하여야 한다. 그리고 계층 관리는 해당 계층의 관리될 객체에 대한 부호화와 프로토콜의 상태에 미치는 영향을 정의한다. 또한 시스템 관리 응용 프로세스는 시스템/정보보호 관리를 위해 CMIP나 IEEE 802.1을 이용하여 다른 시스템과 통신한다.

### 4.4. 브리지 모델

SDE 프로토콜은 MAC 경계에 있으므로 브리지에서도 구현할 수 있다. 즉, SDE는 브리지 프로토콜이나 트래픽 발신처 및 해당 네트워크 시스템에 대한 트래픽을 보호할 수 있는데 SILS 브리지 모델은

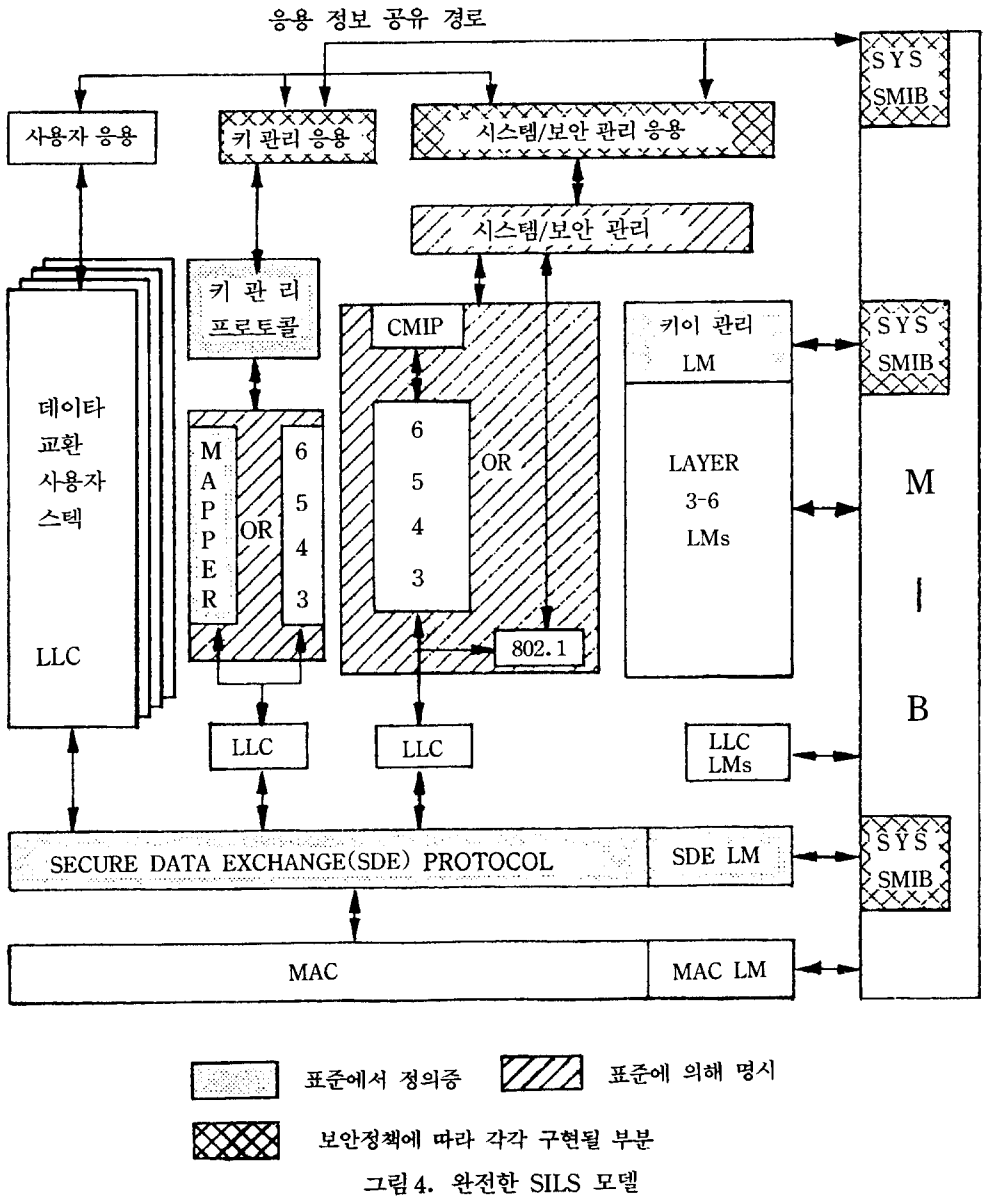


그림 4. 완전한 SILS 모델

그림 5와 같다. 그러나 브리지 모델은 근거리 통신망 특성상 트래픽 보호 기능에 대해 어떤 제한이 있을 수 있다. 즉, 복수의 MAC 브리지가 단일 LAN을 지원할 수 있으므로, 두 브리지가 동일 근거리 통신망에 대한 트래픽을 처리하고자 할 때는 각 브리지는 해당 노드에 대해 암호화 정보와 같은 정보보호 연관(Security Association) 속성을 공유해야 한다. 또한 PDU들간에 Cryptographic chaining을 지원하기가 어려우므로 암호화나 메세지 신분확인에 사용된 알고리즘은 모든 PDU에 대해 동기화될 수 있어야 한다.

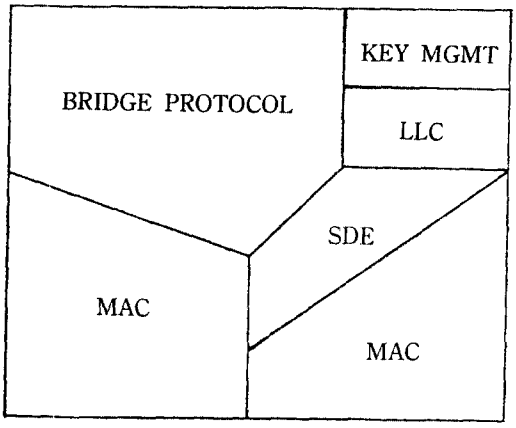


그림 5. SILS 브리지 모델

## 5. 결 론

근거리 통신망의 발달은 속도의 고속성, 상호연결, 크기, 이용범위의 확장등 계속 발전되어 가고 있으나, 정보보호에 대한 기술의 발달은 매우 부진한 실정이다. 현재 국제적으로 IEEE 802 표준위원회에서 추진 중인 표준안인 SILS는 4개의 분야가운데 2개의 분야만이 draft가 나와 있다. 국내에서는 아직 근거리 통신망에서의 정보보호 기술에 대한 기반이 매우 약한 실정이다. 따라서 국내실정에 적합한 정보보호 기술의 개발이 시급한 실정이다. 본 고에서는 draft로 나와있는 IEEE 802.10 SILS에 대한 모델과 구조를 분석하였다. 분석한 내용을 토대로 하여 국내에서의 근거리 통신망 정보보호 프로토콜의 개발이 요구된다.

## 참 고 문 헌

1. ISO 7498 Information Processing System-Open Systems Interconnection-Basic Reference Model.

2. ISO 7498-2 Information Processing System -Open Systems Interconnection-Security-Architecture.

3. ISO DIS 10039 Information Technology-Open Systems Interconnection-Local Area Net-

4. ISO 7498-4 Information Processing System -Open Systems Interconnection-Part 4 Management Framework.

5. "Standard for Interoperable Local Area Network(LAN) Security(SILS) part A-The Model", p.802, 10A/D, Dec. 1989.

6. "Standard for Interoperable Local Area Network(LAN) Security(SILS)" draft p.802, 10B/D 2, Jan. 1990.

7. "Standard for Interoperable Local Area Network(LAN) Security(SILS)", draft p.802, 10/D5, Jun. 1990.

8. "IEEE Standard for Interoperable Local Area Network(LAN) Security(SILS) part B-Secure Data Exchange", draft p.802, 11, May. 1991.

9. Barker, K.E. ; Keenan, T.O., "Local Area Network Security", Canadian Information Processing Society Secsion 84 proceedings, pp.489-499, May. 1984.

10. McKinney, P.C., "How to Make Local Area Networks Secure", CAN. DATASYST. (CANADA) Vol.20, No.4, pp.72-76, Apr. 1988.

11. Townsend, K., "Lock Up Your LANs (Security)", Communicate(UK), pp.42-44, Oct. 1987.

12. Abrams, M.D., Schaen, S.I., "LAN Security a Case Study", Computer Communication Technologies for the 90's. Proceeding of the Ninth Internation Conference, pp.553-557, Nov. 1988.

13. Adams, M.C., "IEEE Safty Standard 802.10 for Local Network", ELEKTRONICA (NETHERLANDS) Vol.39, No.7, pp.20-21,23, 25-27, Apr. 1991.

14. McPartlin, T.O., "Security a LAN's Best Friend", Informationweek(USA) No.318, pp.24 -25, 32, Apr. 1991.

15. Kipkpatrick, M.A., "A Security Standard for LAN's", Fifth Annual Computer Security Applications Conference, pp.27, Dec.1989.

## □ 著者紹介

### 유 황 빈 (정회원)

경희대학교 전자공학과(공학박사)
1974년~1979년 금성전기주식회사
1979년~1981년 금성반도체주식회사
1981년~현재 : 광운대학교 전자계산학과 교수
연구관심분야 : 컴퓨터, 네트워크, 정보통신 Security

### 이 재 광 (정회원)

광운대학교 전자계산학과(이학박사)
1986년~현재 : 군산실업전문대학 전자계산과 부교수
연구관심분야 : 컴퓨터 네트워크, 정보통신 Security