論 文

LLC/MAC 계층 구조에서의 정보 보호 프로토콜에 관한 연구

正會員 柳 煌 彬* 正會員 李 載 廣**

A Study on the Information Security Protocol in LLC/MAC Layer Architecture

Hwang Bin Ryou* Jae Gwang Lee** *Regular Members*

要 約

본 논문에서는 LLC/MAC 계층 구조에서의 정보 보호 프로토콜에 대하여 기술하였다. 근거리 통신망에서의 정보 보호 위협과 취약성, 이의 해결을 위한 요구 서비스, 그리고 IEEE 802 근거리 통신망 구조에서의 정보 보호 프로토콜의 적용 대안을 기술하였다. 정보 보호 서비스를 제공하기 위해 LLC/MAC 서비스 프리미티브를 이용한 정보 보호 프로토콜(SP2 : Security Protocol 2) PDU 구성을 제안하였으며, SP2 프로토콜을 구성하기 위하여 DES 알고리즘의 ECB, CBC 모드와 FIPS의 DAA를 이용하였다. 제안된 SP2 프로토콜은 데이타 발신처 인증, 데이타 비밀유지, 데이타 무결성 서비스를 제공한다.

ABSTRACT

In this paper, an Information Security protocol in LLC/MAC Layer Architecture is discussed. This paper examines the security Vulnerability and threats, the security Service required to protect these threats, and architectural considerations of security protocol in IEEE 802 LAN architecture. To provide an Information security service, an information security protocol(SP2 : Security Protocol 2) PDU construction with LLC/MAC service primitives is suggested. To construct the SP2 protocol, the ECB, CBC mode of DES algorithm and DAA(Data Authentication Algorithm) of FIPS is used. The SP2 protocol suggested in this paper provides data origin authentication, data confidentiality, data integrity service.

I. 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 생성되고 저장되는 정보와 통신망을 통하여 전송되는 중요 자원에 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

*光云大學校 電子計算學科
Dept. of Computer Science, Kwangwoon Univ.
**群山實業專門大學 電子計算科
論文番號 : 92-116(接受1992. 9. 16)

근거리 통신망이 고속 전송과 상호 연결 범위의 확장 등으로 급속히 발달(FDDI, HS LAN, LAN Bridge, LAN Server 설비 등)하여 자원의 이용 범위가 날로 확장되고 있는 추세이다.[15][16] 그러나, 근거리 통신망의 개방형 구성 방식은 중요한 정보 자원에 대한 정보 보호 취약성이 증가하여 중요 정보의 누출, 오용, 불법 변경, 파괴, 개인 프라이버시 침해, 바이러스 등의 위협을 가지게 되어 이에 대한 정보 보호 구조가 절실히 필요한 상태이다. 하지만 근거리 통신망 통신 기술과 정보 보호 메카니즘의 개발이 병행되어 진행되지 않았을 뿐 아니라 정보 보호 메카니즘이 기존 통신망 운용에 장애가 되고 상호 연결에 제한이 될 수 있기 때문에 이의 해결을 위한 근거리 통신망 정보 보호 구조와 정보 보호 프로토콜의 개발이 매우 중요한 과제로 대두되고 있다.[2][14][16]

근거리 통신망에서의 정보 보호 필요성이 증가함에 따라 IEEE에서 '88년에 802.10(Security working Group)을 구성하여 근거리 통신망 정보 보호를 위한 프로토콜 표준화 작성 작업을 시작하여 표준안인 SILS(Standard for Interoperable LAN Security)를 발표하였으며, SILS는 현재 4분야로 구분 진행중인데 분야 A(SILS 모델)와 분야 B(데이타의 안전한 교환을 위한 프로토콜)는 현재 Draft가 나와 있는 상태이고 나머지 분야는 아직 작업 결과가 미진한 상태에 있으므로 전체적으로 예비 규정단계라고 할 수 있다.[6][7]

IEEE 802에서 작성한 근거리 통신망의 표준안에서는 전송 매체의 구성 형태 및 액세스 방식에 따라 MAC 서브계층을 4가지로 구분하여 제공하고 있으며, 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(패킷, 프레임)는 방송 통신 방식으로 수행되므로 어떤 노드이든 PDU를 액세스할 수 있으므로 정보 보호가 취약하다. 그러므로 근거리 통신망에서의 정보 보호는 논리적으로 peer entity간에 오가는 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 있으며, 이러한 공격에 대한 정보 보호를 위해서는 암호화 시스템을 이용한 정보 보호 프로토콜이 필요하다.

본 논문에서는 근거리 통신망에서 사용하는 IEEE 802 규격에 의한 근거리 통신망 프로토콜에 대하여 정보 보호 측면에서 분석하였으며, 분석한 정보 보호 취약성을 해결하기 위한 요구사항을 충족시키고, 제한 사항을 최소화하기 위하여 LLC /MAC 서비스 프리미티브를 이용한 정보 보호 프로토콜(SP2 : Security Protocol 2)을 제안하였다. 제안된 SP2 프로토콜을 구성하기 위해서 DES(Data Encryption Standard), ECB(Electronic Codebook), CBC(Cipher Block Chaining) 모드와 DAA(Data Authentication Algorithm)를 사용하였다. 제안된 SP2 프로토콜은 정보 보호 취약성을 해결하기위한 데이타 발신자 인증, 데이타 비밀유지, 데이타 무결성 서비스를 제공할 수 있다.

Ⅱ. LAN 계층 2 정보 보호 서비스와 구조적 대안

1. IEEE 802 LAN 프로토콜의 정보 보호 취약성과 요구 서비스

ISO 정보 보호 구조 표준안인 ISO 7498-2는[5] 구조적인 모델로서 패킷 교환망(PSN)과 광역 통신망(WAN)을 기준으로 한 정보 보호 서비스들을 계층별로 구분 적용하였다. PSN과 WAN에서의 데이타 링크 계층과 네트워크 계층의 서브 네트워크와 인터네트워크 기능은 IEEE 802 LAN 구조에서의 데이타 링크 계층의 속성과 유사하다. 하지만 근거리 통신망은 특성상 WAN과 PSN과는 다른 속성을 가지기 때문에 근거리 통신망 속성에 적합한 정보 보호 구조가 필요하다. 근거리 통신망 속성에는 데이타 전송 특성, 데이타 수신 특성, 주소 공간, 지리적 분산 등 4가지 특성을 갖는다.

데이타 전송 특성은 WAN에서는 계층 2인 데이타 링크 계층에서 독립적인 링크들간에 점대점(Point-to-point)패킷 교환이 이루어지고 계층 3인 네트워크 계층에서는 중계 기능에 의한 방송(Broadcasting)모드로의 전송 가능성이 있는데 반하여 근거리 통신망에서는 통신망의 구성상 LLC 계층에서 방송 모드로의 전송이 이루어진다. 근거리 통신망에서 데이타 전송의 방송 특성은 두가지의 문제점을 갖는다. 첫째는 근거리 통신망을 구성하는 모든 노드는 자기 노드를 제외한 다른 모든 노드들에게 데이타를 전송할 수 있

으며, 둘째는 데이타 전송의 송신측을 확인하기가 어렵기 때문에 다른 송신측 주소를 이용하여 다른 노드들에게 PDU를 전송할 수 있으므로 정당한 사용자로의 가장이 발생할 수 있다. 또 wiretapping에 취약하여 어떤 노드, 또는 노드들이 단일 tap을 이용하여 위조 또는 자원을 이용할 수 있으므로, 권한을 가지지 않는 자의 자원 이용이 발생할 수 있다.

데이타 수신 특성은 전송 특성과 유사하다. LLC 계층에서의 방송 특성은 모든 노드들이 전송되는 모든 PDU를 액세스할 수 있으므로 두가지 문제점을 갖는다. 첫째는 권한을 가지지 않은 노드가 데이타를 수신할 수 있고, 둘째는 원하는 목적지에서 데이타를 수신하기 전에 PDU에 들어 있는 데이타를 변경할 수 있다. 이 점은 링형 근거리 통신망에서 가장 정보 보호 위협의 노출이 크다. 수신 특성이 갖는 정보 보호 위협은 권한을 가지지 않는 자가 정보 누출과 데이타 수정을 할 수 있다.

주소 공간(Address Space)의 경우, 근거리 통신망은 LLC 계층에서 주소는 노드 인터페이스를 구분하며 단일 주소 공간을 갖는다. 이 주소는 제어 담당국(NIU)에 의해 관리되지만 주소의 타당성 여부를 확인할 수 없다. 즉, 주소의 인증을 명확하게 할 수 없고 주소의 간단한 점검을 통하여 액세스에 대한 제어를 명확하게 할 수 없다. 이와같이 주소 관리를 통한 제어가 명확하지 않기 때문에 정보 보호 취약성으로는 정당한 사용자로의 가장과 권한은 가지지 않는 자의 자원 이용이 발생할 수 있다.

지리적 분산의 경우, 근거리 통신망을 구성하는 기기들이 지리적으로 분산되어 있기 때문에 도청이나 Wiretapping에 취약하다. 따라서 데이타 수정, 권한을 가지지않는 자에게 정보 누출의 위협이 발생한다. 특히 wiretapping과 같은 공격은 특정 노드뿐 아니라 전체 노드들에게 전송되는 모든 데이타를 수신할 수 있다.

지금까지 근거리 통신망 속성에 따른 정보 보호 취약성을 분석하였으며, 이 취약성들은 정보 보호 서비스를 이용하여 해결할 수 있다. 근거리 통신망에서 발생할 수 있는 위협과 이를 막기 위한 정보 보호 서비스와 그 기능은[5]

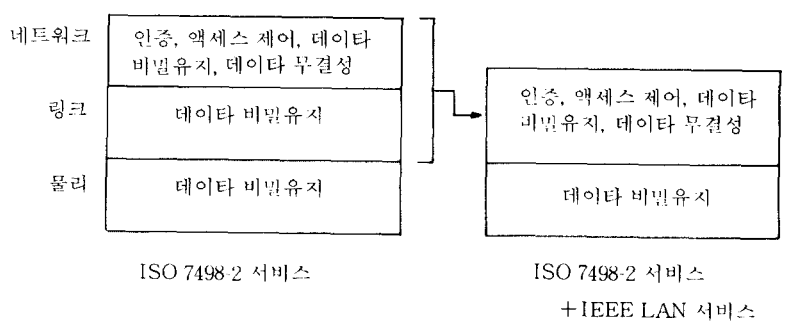
1)데이타 수정-무연결 데이타 무결성(connectionless data integrity) : 단일 무연결 PDU의 데이타가 임으로 변경되거나 파괴되지 않게 하는 성질로서 위장된 데이타 송신, 권한을 가지지 않는 자에 의한 데이타의 수정으로부터 보호한다.

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 예방하는 것으로서 어떤 노드이든 정당한 권한없이 임의로 다른 국에 PDU를 전송하지 못하도록 한다.

4)권한을 가지지 않는 자에게 정보 누출-데이타 비밀유지(data confidentiality) : 정보가 권한을 가지지 않는 개체들, 액티티들, 프로세스들에 의해 이용되거나 노출되지 않도록 하는 성질로서 권한없이 데이타를 액세스하지 못하도록 하며, 도청(엿듣기)

표 1. ISO 7498-2 서비스와 LAN 서비스
Table 1. ISO 7498-2 Service and LAN Service



으로부터 보호한다.

지금까지 분석한 근거리 통신망 속성에 따른 위협을 해결하기 위해 필요한 정보보호 서비스를 제공하는 정보 보호 구조(하위층)는 표 1의 오른쪽에 표시되어 있다.

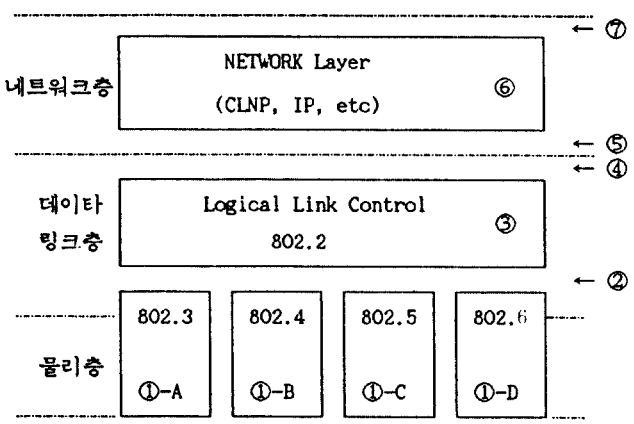
이 정보 보호 서비스들은 단일 메카니즘인 암호화 기술을 이용하여 제공할 수 있다. 데이타 비밀유지 서비스는 간단하고 신뢰성이 높은 방법인 키이를 이용한 암호 알고리즘을 적용하여 송수신되는 데이타(SDU : Service Data Unit)를 암호화함으로서 데이타의 노출을 방지할 수 있다. 무연결 데이타 무결성 서비스는 암호 알고리즘, 키이 관리, 데이타 조합의 검사합(checksum)를 이용하여 MAC(Message Authentication Code)를 생성하여, 이를 SDU에 추가하여 전송한다. 수신인 경우에는 같은 과정을 수행하여 수신된 값과 비교하여 같으면 무결성을 확증한다. 데이타 발신처 인증은 LLC SDU(Service Data Unit)에 Prefix나 Suffix로써 데이타 영역에 송신측 주소의 복사 본을 포함시켜 암호화하여 송신하면, 수신측은 이를 복호화한 후 조소를 확인함으로서 쉽게 제공할 수 있다. 액세스 제어 서비스는 암호화 키이 관계, 즉 암호화 연관(cryptographic association)의 관리와 응용을 통하여 제공 가능하다. 즉, 전송되는 모든 PDU가 암호화 된다면 암호화 메카니즘과 암호화 키이를 알고 있는 노드만이 정보를 교환할 수 있으므로, 이러한 설비가 없는 노드들은 암호화된 정보들을 액세스할 수 없다.

단일 암호화 시스템을 이용하여 제공되는 이 서비스들은 근거리 통신망 인터페이스에 대한 복잡도와 성능에 미치는 영향을 최소화하여 제공되도록 하는 것이 중요하다.

2. 근거리 통신망 프로토콜에서의 정보 보호 프로토콜 적용 대안

OSI 기본 참조 모델을 근거로 한 근거리 통신망 정보 보호 프로토콜의 적용 위치에 대한 대안은 그림 1과 같다. 그림 1에서는 프로토콜 적용 가능성을 크게 두가지로 생각해 볼 수 있다.[6][8] 하나는 계층 사이에 적용시키는 방법(②,④,⑤,⑦)과 다른 하나는 기존 프로토콜에 집적시키는 방법(①,③,⑥)이다. 계층 사이에 정보 보호 프로토콜을 적용시키면 규정된 서비스 프리미티브와 연관된 프로토콜 제어 정보만 액세스하면 되지만, 기존 프로토콜에 정보 보호 프로토콜을 집적시키려면 프로토콜의 모든 정보를 액세스하게 된다. 따라서, 집적화하는 것이 실제적이지만 기존 프로토콜을 전체적으로 수정해야 하는 문제점을 갖는다.

네트워크 계층에 대한 정보 보호 프로토콜은 ANSI



802.3 : CSMA/CD 802.4 : TOKEN BUS 802.5 : TOKEN RING 802.6 : MAN
IP(Internet Protocol) CLNP(Connectionless Network Protocol)

그림 1. LAN 정보 보호 프로토콜 적용 위치 대안
Fig 1. Alternatives for the placement of LAN security protocol

에서 개발한 SDNS SP3 프로토콜[6]이 있는데, 이는 이기종 네트워크간의 통신에서 정보 보호를 제공하기 위해 IP(Internet Protocol)에 설치된다. MAC 계층에 정보 보호 프로토콜을 적용하는 경우에는 기존 프로토콜을 수정해야 하는 어려움이 있을 뿐 아니라 이기종 매체간의 브리지를 이용한 연결에는 적합하지 않다. MAC와 LLC 서브 계층 사이에 적용한 정보 보호 프로토콜(그림 1의 ②)은 세가지의 서비스 프리미티브(MA_DATA.request, MA_DATA.confirm, MA_DATA.indication)만 액세스하면 된다. 그러므로 이 간단성이 정보 보호 프로토콜을 적용시키는데 큰 장점이며, 또 LLC 헤더에 있는 다중 MAC 주소를 이용하여 정보 보호 서비스를 원하는 시스템과 원하지 않는 시스템을 구분 제공할 수 있다. 즉 LSAP(Link Service Access Point)에 있는 DSAP(Destination Service Access Point) 정보를 이용하여 점검 후 바이패스하거나 아니면 키이 관리 트래픽과 정보 보호 서비스 알고리즘을 제공하면 된다. 현재 IEEE 802.10 SILS에서도 이를 이용한 SDE(Secure Data Exchange) 프로토콜을 개발중에 있다. SDE 프로토콜을 이용하여 정보 보호 서비스를 제공하기 위해서는 키이 관리 프로토콜과 시스템/계층 관리가 필요한데 이는 ISO 7498-4를 기본 개념으로 수행한다.

Ⅲ. SP2(Security Protocol 2) 프로토콜

1. SP2 프로토콜 구조

근거리 통신망에서 전송되는 데이타에 대한 정보 보호 서비스(발신처 인증, 액세스 제어, 비밀유지, 무결성)를 제공하기 위해서 LLC와 MAC 계층 사이에 SP2 프로토콜을 위치시킨다. SP2 프로토콜은 암호화 알고리즘을 이용하여 MAC 서브 계층을 경유하여, 정보 보호를 위한 정보 보호 서비스를 end-to-end로 투명하게 제공하도록 한다. 본 연구에서는 SP2 프로토콜을 적용하기 위하여 SP2_DATA.request와 SP2_DATA.indication 프리미티브를 추가하였으며 이에 대한 프리미티브 파라메타는 다음과 같다. 또 기존의 MA_DATA.request와 MA_DATA.indication의 파라메타도 약간 변경시켰으나, 기존의 근거리 통신망과는 호환성을 유지할 수 있다. 서비스 프리미티브 파라메타는

```
MA_DATA.request     (
                      destination_address,
                      m_sdu,
                      requested_service_class
                    )
MA_DATA.indication  (
                      destination_address,
                      source_address,
                      m_sdu,
                      requested_service_class
                    )
SP2_DATA.request    (
                      sp identifier,
                      key identifier,
                      initial vector,
                      station id,
                      m_sdu,
                      padding,
                      message authentication code
                    )
SP2_DATA.indication (
                      sp identifier,
                      key identifier,
                      initial vector,
                      station id,
                      m_sdu,
                      padding,
                      message authentication code
                    )
```

이다. 이 서비스 프리미티브들을 이용한 SP2 프로토콜 구조는 그림 2와 같다. SP2 프로토콜은 전송되는 PDU 중 암호화가 필요한 프레임을 암호화함으로서 end-to-end 통신을 안전하게 보호해 주는 역할을 한다.

2. SP2 프로토콜 PDU 구성

LLC/MAC 사이에 위치하는 SP2 프로토콜은 계층간에 전송되는 앤티티인 PDU의 전송을 투명하게 수행하기 위하여 PDU 단위로 동작되어야 한다. 이는 근거리 통신망 구성노드 가운데 모든 노드들이 정보 보호를 원하는 것은 아니다. 따라서 원하는 노드는 전송되는 PDU들을 암호화하여 전송하지만 원하

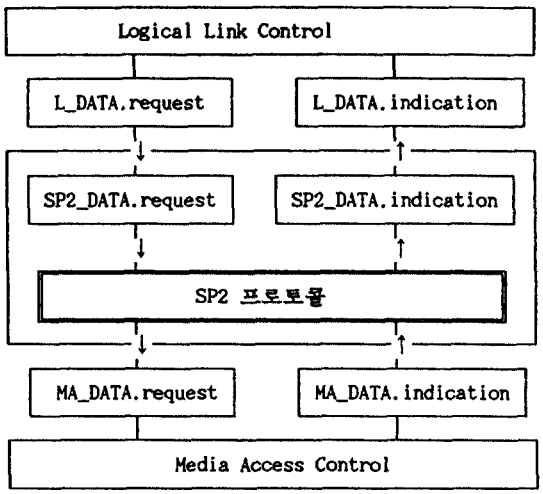


그림 2. SP2 프로토콜 구조
Fig 2. SP2 Protocol Architecture

지 않는 노드들 간에 전송되는 PDU는 SP2 프로토콜을 바이패스하여 기존 근거리 통신망 운용에 장애가 되지 않도록 한다. SP2 프로토콜의 운용 흐름도는 그림 3과 같다.

SP2 프로토콜이 흐름도에 따라 수행되어지는 SP2 PDU 구성은 그림 4.와 같다.

그림 4에 나타난 것 처럼 SP2 PDU는 8개의 필드로 구성되어 있다. 각 필드에 대한 구성 순서는 처리 절차에 기술되어 있다.

3. 무결성과 비밀유지 서비스

3.1 무결성 서비스

송수신되는 데이타가 변경 또는 파괴되지 않았음을 확증해 주는 무결성(integrity) 서비스를 제공하기 위해서 DAA(Data Authentication Algorithm)[13]를 이용하여 MAC 값을 계산한다. DAA는 DES 알고리즘[10]의 CBC(Cipher Block Chaining) 모드[11]를 적용한다.

D를 64 비트 입력 벡터, O를 64 비트 출력 벡터라고 할때 DAA는 다음 식으로 나타낼 수 있다.

$$O = e(D) \tag{1}$$

여기서 무결성을 인증하고자 하는 데이타는 연속적인 64 비트 블럭들($D_1, D_2, \ldots, D_n$)로 나뉘어 DES 알고리즘의 ECB(Electronic Codebook) 모드를 수행한다. 이때 입력되는 데이타 블럭은 반드시 64 비트의 블럭으로 나뉘어지는 것은 아니다. 즉, 맨 마지막 블럭은 64비트가 아닐 수 있으므로, 이때는 0 비트를 추가하여 64 비트를 만들어 DAC(Data Authentication Code)계산에 사용한다. 이 0 비트는 DAC 계산에만 이용되고 전송되지는 않는다. DAC 계산은 다음과 같다.

$$O_1 = e(D_1)$$

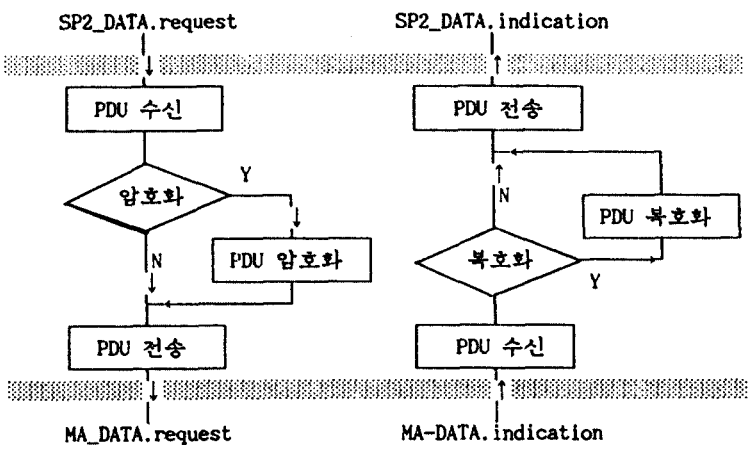
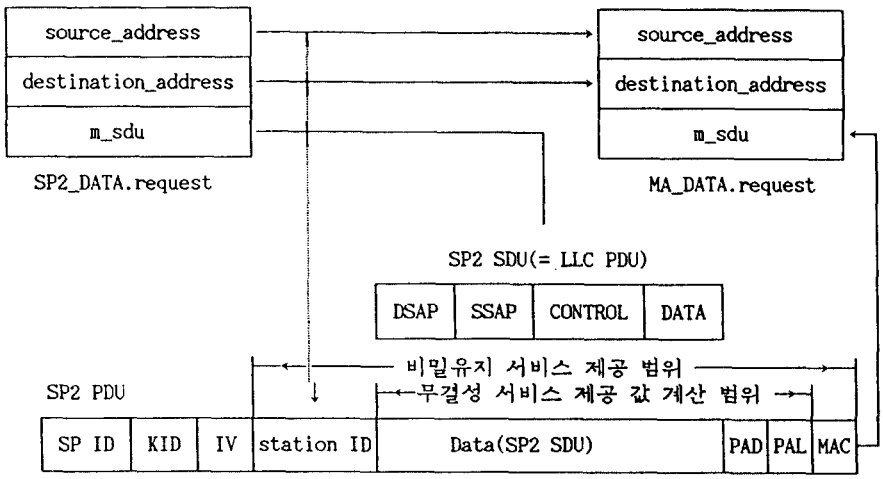


그림 3. SP2 프로토콜 흐름도
Fig 3. Flowchart of the SP2 Protocol



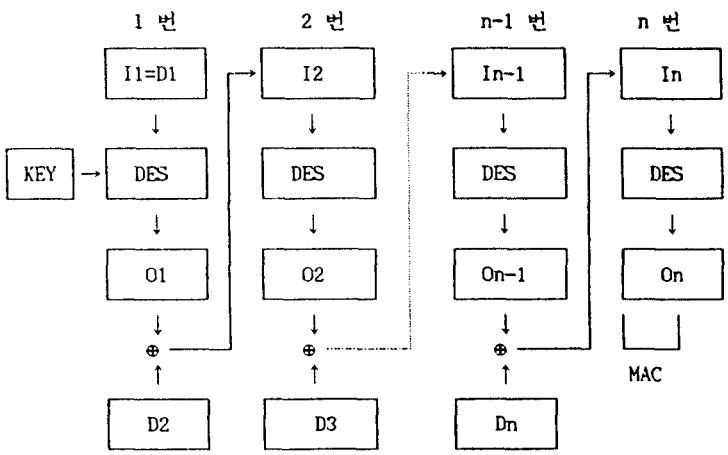
DSAP:Destination Service Access Point; PAL:Padding Length;

SSAP:Source Service Access Point; IV:Initial Vector;PAD:Padding;

SP ID:SP2 Identifier;KID:Key Identifier;

MAC:Message Authentication Code

그림 4. SP2 PDU의 구성
Fig 4. construction of SP2 PDU



D1=IV:Initial Vector, ⊕:Exclusive-OR, I:입력 블럭, KEY:암호화 키이(EK),

O:출력 블럭, DES:Data Encryption Standard, MAC:Message Authentication Code

그림 5. DAA 블럭 다이아그램
Fig 5. Block Diagram of the DAA

$O_2 = e(D_2 \oplus O_1)$
$O_3 = e(D_3 \oplus O_2)$
.
.
$O_n = e(D_n \oplus O_{n-1})$

계산된 O_n 가운데서 상위 32 비트만을 MAC로 사용한다. MAC를 계산하기 위하여 CBC 모드를 적용한 DAA의 블럭 다이아 그램은 그림 5와 같다.

CBC 모드 적용시 IV(Initial Vector)=D1이고 데이타는 D2, D3,...,Dn이 된다. 송신자는 암호화 키이를 이용하여 데이타에 대한 MAC를 계산한후, 이 MAC를 송신 데이타(PDU)의 MAC 필드에 추가하여 송신한다. 수신측은 수신된 데이타에 대하여 송신측과 같은 알고리즘을 이용하여 MAC 계산을 수행한 후 수신된 MAC와 계산된 MAC와 비교하여, 만약 같으면 데이타가 전송중에 변경 또는 파괴되지 않았음을 확증하므로서 무결성 서비스를 제공한다.

3.2 비밀유지 서비스

데이타의 비밀성을 유지하는 비밀유지(Confidentiality) 서비스는 권한을 가지지않은 사용자가 데이타를 이용하지 못하도록 하는데 목적이 있다. 즉, 평문을 암호화 키이를 이용하여 암호문으로 바꾸어 전송되도록 하며, 비밀유지 서비스를 제공하기 위해서 DES의 CBC 모드[11]를 이용한다. 평문을 암호문으로 변경하기 위한 CBC 모드블럭 다이아그램은 그림 6과 같다.

데이타를 전송하기 전에 암호화하고자 하는 데이타에 포함시켜야 할 내용이 있다. 즉, 발신처를 인증하기 위한 송신자의 주소와, 무결성 서비스를 제공하기 위해 계산된 MAC 값이다. 그리고 또 한가지는 DAC를 계산할 때와 마찬가지로 암호화하여 전송하고자 하는 데이타가 반드시 64 비트 블럭 단위가 아닌 경우가 있기 때문에, 64 비트 블럭으로 만들기 위해 0 또는 1로 padding이 필요하다. 근거리 통신망에서 전송되는 데이타 단위는 옥텟(octet)이기 때문에 padding은 옥텟의 정수배가 되며, 이때 수신측이 몇 옥텟이 padding 되었는지는 알 수 있어야 한다. 따라서, 전송되는 데이타에 대해 pad 길이 필드(한 옥텟 길이)를 추가하여 padding 길이 값을 표시하게 한다. padding 길이를 계산하기 위해서는 식(2)를 적용한다.

Padding 길이 = 암호화 입력 블럭 크기 − ((Station−ID + Data(SP2 SDU) + pad 길이 필드 + MAC MOD 암호화 블럭 길이) (2)

공식 (2)를 적용하면 맨 마지막 블럭의 길이에 따라 padding되는 길이는 표 2와 같다.

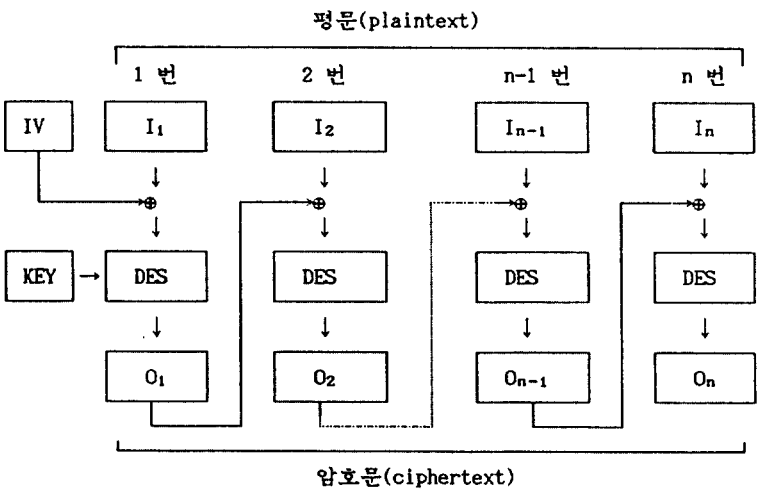


그림 6. DES CBC 모드 블럭 다이아그램
Fig 6. Block Diagram of DES CBC mode

표 2. 맨 마지막 블럭 길이와 Padding 길이
Table 2. The Final Block Length and Padding Length
(단위 : 옥텟)

맨 마지막 블럭 길이	Padding 길이
1	6
2	5
3	4
4	3
5	2
6	1
7	0
8	7

4. SP2 프로토콜 PDU 처리 절차

SP2 프로토콜 PDU를 처리하기 위해서는 송수신을 수행하는 노드들에 대해 먼저 암호화 키이(EK : Encryption Key)를 분배하여야 하며, 본 논문에서는 Time Quantum을 이용한 암호화 키이 분배 방식[11]을 따른다. 이 방식을 수행하면 송수신 노드는 암호화 키이(EK)와 암호화 키이 식별자(KID)를 분배받는다.

SP2 프로토콜 PDU 처리 절차는 SP2_DATA.request를 MA_DATA.request로 변환하는 송신 절차와 MA_DATA.indication를 SP2_DATA.indication로 변환하는 수신 절차로 나눌 수 있다. 전송 절차를 수행하고자 하면 먼저 SP2 DATA.request의 source_address와 destination_address를 점검한다. 이때 양 노드가 정보 보호 서비스를 원하는 노드가 아니면 SP2_DATA.request를 MA_DATA.request로 바이패스되도록 하여 기존 시스템 운용과 같이 수행되도록 하며, 만약 정보 보호 서비스를 원하는 노드이면 SP2 프로토콜 처리 절차를 수행한다. 이때 SP2 프로토콜 PDU의 송수신 절차는 알고리즘 1, 2와 같다.

알고리즘 1. 송신 절차

```
Process Send_to_MAC_Layer( ) ;
Var
  SDU : Service Data Unit ;
  PAD : Padding ;
  PAL : Padding Length ;
  MAC : Message Authentication Code ;
  SP ID : Security Protocol Identifier ;
  KID : Key Identifier ;
  IV : Initial Vector ;
  DAA( ) : Data Authentication Algorithm ;
  DES CBC MODE( ) : Encrypt & Decrypt
                    Algorithm ;
Begin
    Receive from LLC layer ;
    PAL := 8 - reminder of [SDU length /8] ;
    length of PAD := PAL
    append PAD, PAL to new SDU ;
    MAC := DAA(SDU, PAD, PAL) ;
    append MAC to SDU ;
    STATION  ID := Source Address of
                   SP2_DATA.request ;
    append STATION  ID to SDU ;
    encrypted STATION  ID, SP2 SDU, PAD,
              PAL, MAC := DES CBC MODE
              (STATION  ID, SP2 SDU, PAD,
              PAL, MAC) ;
    append SP ID, KID, IV
              to encrypted STATION  ID,
              SP2 SDU, PAD, PAL, MAC ;
    Send to MAC Layer ;
End.
```

알고리즘 2. 수신 절차

```
Process Receive_from_MAC_layer( ) ;
Var
  EK : Encrypt Key
  IV : Initial Vector ;
  PAD : Padding ;
  PAL : Padding Length ;
  MAC : Message Authentication Code ;
  DAA( ) : Data Authentication Algorithm ;
  DES CBC MODE( ) : Encrypt & Decrypt
                    Algorithm ;
Begin
    Receive from MAC layer ;
    EK := ditermine with KID of
          MA_DATA.indication ;
    decrypted STATION  ID, SP2 SDU, PAD,
```

```
                PAL, MAC := DES CBC MODE
                (encrypted STATION  ID,
                SP2 SDU, PAD, PAL, MAC)
                 with EK, received IV ;
    Save STATION  ID for Sender Verify ;
    calculated MAC := DAA(SDU, PAD, PAL) ;
    compare with calculated MAC and received
      MAC ;
    IF not equal each other THEN exception
      handling for error ;
    length of PAD := PAL
    remove PAD, PAL from SDU ;
    Send to LLC layer ;
End.
```

알고리즘 1, 2와 같은 절차는 발신처 인증, 무결성, 비밀 유지 서비스등을 제공한다. 액세스 제어 서비스는 암호화 키이 분배 정책과 방법, 그리고 관리에 따라 제공되어질 수 있다.

Ⅳ. 구현시 고려사항

제안된 SP2 프로토콜을 구현할 때 고려해야 할 사항이 있다.

첫째는 broadcast와 multicast 전송시 정보 보호 서비스를 제공하기 위하여 수신측에 암호화 키이(EK)를 효율적으로 분배할 수 있는 프로토콜을 먼저 고려해야 한다. 이는 같은 트래픽에 대하여 수신측이 같은 EK를 사용하여 복호화해야 하기 때문이다.

둘째는 프레임 길이가 증가한다는 것이다. 최악의 경우에 증가되는 길이는 SPID(1)+KID(2)+IV(8)+Station ID(1)+(PAD+PAL)(8)+MAC(4)=24 octets이다. 이로 인하여 처리할 수 있는 최대 허용치를 초과하는 경우에 에러가 발생한다. 이를 해결하기 위해서는 분할과 조립 과정을 두도록 한다. 즉 SP2 SDU를 두개의 SP2 PDU로 분할하여 송수신이 이루어지도록 한다. 이때 정상적인 PDU와 구분하기 위해서 순서 번호 필드와 분할 플래그 필드를 두어 이를 점검하여 수신시 순서에 맞추어 조립한다.

세째는 정보 보호 서비스의 안정성을 높이기 위하여 알고리즘을 다양하게 제공하는 것이다. 이때 SP ID 필드를 이용하는데 SP ID 필드의 각 비트를 플래그로 사용하는 것이다. 즉, 송신자가 선택한 암호 알고리즘에 따라 플래그를 지정하여 송신하면 수신측에서는 이 필드를 해석하여 복호화시에 사용될 알고리즘을 결정하도록 한다.

네째는 SP2 프로토콜 처리로 인한 overhead를 최소한으로 하는 것이다. 이는 기존 통신망의 성능과 속도의 고속성이 중요한 요인이지만, 정보 보호에서는 안전성이 가장 중요한 요인이다. 따라서 성능과 안전성의 trade-off를 고려하여 정보 보호 서비스 제공이 시스템 전체의 성능에 커다란 장애 요인이 되지 않게 한다.

Ⅴ. 결 론

근거리 통신망 환경에서의 정보 보호 서비스에 대한 요구가 절실히 요구되는 실정이다. 본 논문에서는 IEEE LAN 구조에서의 정보 보호 서비스 제공을 위한 정보 보호 프로토콜 SP2를 제안하였다. 이는 LLC/MAC 서비스 프리미티브를 이용한 SP2 PDU를 구성하여 요구되는 정보 보호 서비스가 제공되도록 하였다. SP2 프로토콜을 구성하기 위하여 DES 알고리즘의 ECB, CBC 모드, 그리고 FIPS pub 113 DAA를 이용하였다.

문제점은 기존 IEEE LAN 프로토콜에 대한 성능 평가에 있어서 트래픽 처리 속도에 대한 분석이 행해지지만 정보 보호는 처리 속도보다는 교환되는 트래픽의 안전성에 대해 분석되어야 한다. 따라서 두가지 분석 요인에 대한 trade-off를 찾아내는 것이다.

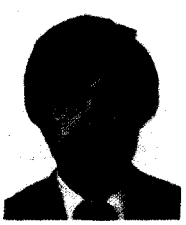
앞으로의 연구 과제는 송신자의 결정에 따라 암호화 알고리즘을 선택할 수 있도록하는 다중 알고리즘을 제공하는 것과 프레임의 분할과 조립 처리 능력을 갖게하는 것이다. 그리고 정보 보호 서비스 제공으로 인한 overhead를 최대한으로 줄여서 네트워크 운용에 장애가 되지 않도록 하는데 있다.

참 고 문 헌

1. 유황빈, 이재광, "Time Quantum을 이용한 LAN에서의 암호화 키이 분배 방식," 한국통신학회논문지, pp629-639, vol.17, no.6, 1992.
2. "정보 통신 보안 표준화 성향 조사 연구," 한국 전산원 최종 보고서, 한국 전산원, 1991.
3. "SDNS Security protocol SP3," SDN.301, Mar 1988.
4. ISO 7498 Information Processing System-Open

System Interconnect Basic Reference Model
5. ISO 7498/2 Information Processing System-Open System Interconnect Security-Architecture
6. "Standard for interoperable Local Area Network (LAN) Security (SILS)," draft p802.10/D5, Jun 1989.
7. KIRKPATRICK, M.E.., "A Security Standard for LANs," Fifth annual computer security applications conference, pp27, Dec 1989.
8. LAMBERT, P.A.., "Architectural considerations for LAN security protocols," proc E.I.S.S. '89, pp5-11, Apr 1989.
9. ANSI X3.92-1981, Data Encryption Algorithm
10. National Bureau of Standards, "The Data Encrytion standards," Federal Information Processing Standards pub 46, Jan 1977.
11. National Bureau of Standards, "DES mode of operation," Federal Information Processing Standards pub 81, Dec 1980.
12. ISO DIS 10039, Information Processing System-Local Area Networks-MAC service Definition.
13. National Bureau of Standards, "Computer Data Authentication," Federal Information Processing Standards pub 113
14. C.P.Pfleeger, "Security in Computing," prentice Hall, 1989.
15. James Matin, K.K.Chapman, "Local Area Networks Architecture and implementations," prentice Hall, 1986.
16. P.J.Fortier, "Handbook of LAN Technology," Mcgraw-Hill, 1989.

≪알 림≫
본 연구는 1992년도 한국 전자통신 연구소의 "91 데이타 보호의 기술기반에 관한 연구"의 연구비 지원에 의한 연구임.



柳 煌 彬(Howang Bin Ryou) 正會員
1949年 8月 15日生
1975年 2月 : 仁荷大學校 電子工學科
1977年 7月 : 延世大學校 産業大學院 電氣電子工學科
1989年 2月 : 慶熙大學校 大學院 電子工學科(工學博士)
1975年～1980年 : 金星半導體(株)
1981年～現在 : 光云大學校 電子計算學科 副教授

李 載 廣(Jae Gwang Lee) 正會員
1956年 3月 12日生
1984年 2月 : 光云大學校 電子計算學科 卒業
1986年 2月 : 光云大學校 大學院 電子計算學科 卒業
1990年 2月 : 光云大學校 大學院 電子計算學科 博士課程 修了
1986年～現在 : 全北 群山實業專門大學 電子計算科 副教授