通信情報保護學會誌
第5卷 第2號, 1995. 6

OSI 참조모델의 네트워크 계층 보호 프로토콜

박 영 호*, 문 상 재*

요 약

본 논문에서는 ISO/IEC의 표준안인 네트워크 계층 보호 프로토콜(NLSP)을 연구 분석한다. NLSP는 네트워크 계층에서 보호서비스를 제공하기 위하여 종단 시스템 및 중간 시스템에서 구현되어질 수 있으며 네트워크 계층의 부계층으로 동작되고 비접속 네트워크 보호 프로토콜(NLSP-CL) 및 접속 네트워크 보호 프로토콜(NLSP-CO)로서 동작 가능하다. 본 논문에서는 NLSP의 보호연관, 기능 및 절차, 그리고 제공되는 위치에 관하여 기술한다.

1. 서 론

정보통신 기술과 전자기술의 발전으로 우리사회는 산업사회로부터 급속히 정보화사회로 이행되고 있으며 컴퓨터통신망을 통한 서비스 이용이 대중화되고 있다. 그러나 컴퓨터통신망에서 가장 큰 장애요소 중 하나로 컴퓨터 범죄를 들 수 있으며 이러한 장애요인은 컴퓨터가 네트워크에 연결되어 있는 상황에서는 더욱 심각하다[1,2]. 따라서 이를 막을 수 있는 대책이 필요하다[3].

컴퓨터통신망의 보호체계를 통한 기술적 방안으로 ISO 7498-2[4]에서는 OSI 참조모델의 보호 구조를 정의하고 있다. 컴퓨터통신망에서 종단간 보호를 위해서는 제 4계층인 트랜스포트 계층과 제 7계층인 응용 계층에서 보호서비스를 제공하는 것이 적합하며 물리적인 보호는 제 1계층인 물리 계층에서 보호서비스를 제공하는 것이 적합하다[5-7]. 또한, 인터네트워크와 같이 중간 시스템을 고려해야 하는 경우에는 제 2계층인 데이타 링크 계층과 제 3계층인 네트워크 계층에 보호서비스를 제공하는 것이 적합하다. 그러나 데이타 링크 계층에서는 비밀보장 서비스만이 제공되는 것에 반해 네트워크 계층에서는 부인봉쇄 서비스를 제외한 대부분의 보호서비스가 제공되므로 네트워크 계층에 보호서비스를 제공하는 것이 유리하다. 네트워크 계층을 위한 보호 프로토콜은 NIST의 SP3(security protocol 3)[8]과 ISO/IEC의 표준안인 NLSP(network layer security protocol)[9]가 있다.

본 논문에서는 ISO/IEC의 표준안인 네트워크 계층 보호 프로토콜을 연구 분석한다. NLSP는 네트워크 계층에서 보호서비스를 제공하기 위하여 종단 시스템 및 중간 시스템에서 구현되어질 수 있으며 네트워크 계층의 부계층으로 동작된다. NLSP는 비접속 네트워크 보호 프로토콜(NLSP-CL) 및 접속 네트워크 보호 프로토콜(NLSP-CO)로서 동작 가능하다. NLSP-CL은 데이타 발신처 확인, 접근제어, 비접속 비밀보장,

* 경북대학교 전자공학과

트래픽 흐름 비밀보장 그리고 비접속 무결성 서비스들을 제공하며 NLSP-CO는 대등 실체 확인, 접근제어, 접속 비밀보장, 트래픽 흐름 비밀보장 그리고 회복기능을 갖는 접속 무결성 서비스들을 제공한다.

2. NLSP의 보호연관

NLSP의 동작은 보호서비스 선택 정보, 보호 알고리듬 식별자 그리고 암호 키와 같은 보호관리 정보에 의해 제어되며 이러한 보호관리 정보들을 보호속성이라 한다. 두 통신 객체간에 보호를 제어하는 보호속성들의 집합이 보호연관이며 통신 객체들은 NLSP의 동작을 위하여 보호연관을 공유해야 한다. 통신 객체 사이에 협상을 통하여 동일한 보호속성 정보를 공유하는 과정을 보호연관 설정이라 한다. 보호연관을 설정하는 방법에는 보호관리에 의해 미리 설정하는 방법과 보호연관 프로토콜을 사용하는 방법이 있다.

그림 1은 NLSP에서 정의하는 보호연관의 속성들이다. 그림 1의 a)에서 g)까지는 NLSP-CO 및 NLSP-CL에서 공통으로 사용되는 보호연관의 속성들이며 h)는 NLSP-CL에서의 보호서비스 보호연관 속성들을 나타낸 것이고 i) 및 j)는 NLSP-CO에서의 보호서비스 보호연관 속성 및 접속형 프로토콜의 보호연관 속성을 나타낸 것이다. NLSP는 SDT PDU 캡슐화를 사용하여 사용자 데이타 및 프로토콜 제어 정보를 보호한다. 캡슐화는 ISN(integrity sequence number), 패딩, ICV(integrity check value), 그리고 암호화에 기초하여 이루어지며 이러한 기능은 보호연관 속성에 의해서 적용된다. 그림 2는 NLSP 통신에서의 SDT(secure data transfer) PDU 캡슐화 과정에서 사용되는 보호 메카니즘들의 보호연관 속성들을 나타낸 것이다.

```
a) SA(security association) identification
   · My_SA-ID    : Integer of range, The local identifier of the SA
   · Your_SA-ID  : Integer of range, The remote identifier of the SA
b) Indicator of whether the NLSPE initiated or responded to the SA
   establishment
   · Initiator   : Boolean
c) UN address of peer NLSP entity
   · Peer_Adr    : Octet string
d) NLSP address of entities served through the remote peer
   · Adr_Served  : Octet string
e) Security services selected for the SA (for NLSP-CL and NLSP-CO )
   · AC          : Integer of range constrained by ASSR
   · TF_Conf     : Integer of range constrained by ASSR
f) Parameter protection
   · Param_Prot  : Boolean
g) Label mechanism attributes
   · Label       : Boolean
   · Label_Set   : Set of
                   {Label_Ref    : Integer
```

```
                    Label_Auth    : Object identifier
                    Label_Content: To format defined by Label_Auth}
h) Security services selected for the SA (for NLSP-CL)
    · DOAuth      : Integer of range constrained by ASSR
    · CLConf      : Integer of range constrained by ASSR
    · CLInt       : Integer of range constrained by ASSR
i) Security services selected for the SA (for NLSP-CO)
    · PE auth     : Integer of range constrained by ASSR
    · CO Conf     : Integer of range constrained by ASSR
    · CO int      : Integer of range constrained by ASSR
j) CO protocol related attributes
    · Retain_On_Disconnect        : Boolean
    · Protect_Connect_Params      : Boolean
    · No_Header                   : Boolean
```

그림 1 NLSP에서의 보호연관 속성등

Fig. 1 SA attributes in NLSP.

```
a) Mechanisms selected for the SA
    · ISN                 : Boolean
    · Padd                : Boolean
    · ICV                 : Boolean
    · Encipher            : Boolean
b) ISN mechanism attributes
    · ISN_Len             : Integer
    · Data_My_ISN         : ISN for last normal data sent
    · Data_Your_ISN       : ISN for last normal data received
    · Exp_My_ISN          : ISN for last expedited data sent
    · Exp_Your_ISN        : ISN for last expedited data received
c) Padding mechanism attributes
    · Traff_Padd          : Form constrained by ASSR
d) ICV mechanism attributes
    · ICV_Alg             : Object identifier
    · ICV_Blk             : Integer
    · ICV_Len             : Integer
    · Data_ICV_Gen_Key    : Form constrained by ASSR
    · Data_ICV_Check_Key  : Form constrained by ASSR
    · Exp_ICV_Gen_Key     : Form constrained by ASSR
```

· Exp_ICV_Check_Key : Form constrained by ASSR

e) Encipherment mechanism attributes

· Enc_Alg : Object identifier
· Enc_Blk : Integer
· Data_Enc_Key : Form constrained by ASSR
· Data_Dec_Key : Form constrained by ASSR
· Exp_Enc_Key : Form constrained by ASSR
· Exp_Dec_Key : Form constrained by ASSR

그림 2 SDT PDU를 캡슐화하기 위한 보호연관 속성들

Fig.2 SA attributes for SDT PDU based encapsulation function.

3. NLSP의 기능 및 절차

NLSP-CO와 NLSP-CL에서의 보호는 모든 서비스 파라미터 보호, NLSP 사용자 데이타 보호, 그리고 비보호가 있다. 모든 NLSP 서비스 파라미터 보호는 주소와 사용자 데이타를 포함하는 모든 파라미터들을 보호하며 보호연관 속성 Param_Protec이 True일 때 선택된다. NLSP 사용자 데이타 보호의 경우 사용자 데이타는 보호하나 다른 NLSP 서비스 파라미터들은 보호하지 않으며 보호연관 속성 Param_Protec이 False 일때 선택된다. 비보호의 경우 모든 NLSP 서비스 파라미터들은 UN(underlying network) 서비스 파라미터들로 복사되며 모든 NLSP 절차들은 수행되지 않는다. NLSP-CO와 NLSP-CL은 SDT PDU를 사용함으로써 NLSP 서비스 파라미터들을 보호할 수 있으며 NLSP-CO는 No-header 형으로써 NLSP 사용자 데이타를 보호할 수도 있다. NLSP에서 사용되는 PDU는 SDT PDU, CSC(connection security control) PDU, 그리고 SA(security association) PDU의 세가지 방식이 있다.

SDT PDU 구조는 그림 3과 같다. SDT PDU는 무결성 서비스를 제공하기 위하여 무결성 검사 값을 첨가하고 비밀보장 서비스를 제공하기 위하여 보호영역을 암호화 한다.

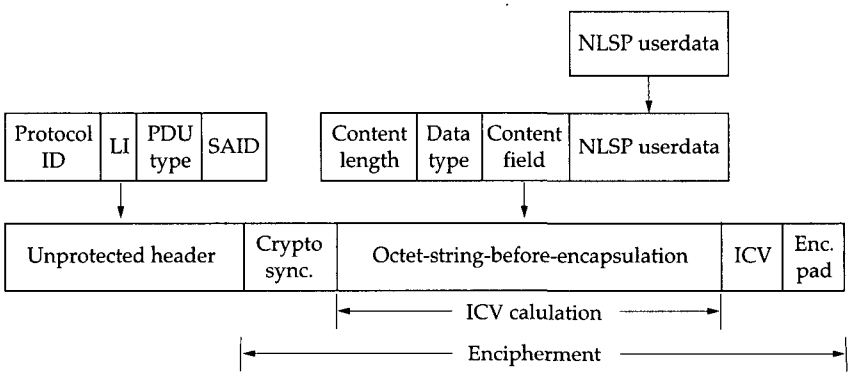


그림 3 SDT PDU의 구조

Fig.3 Structure of SDT PDU.

비보호 헤더 영역은 프로토콜 식별자, 길이, PDU 형태, 그리고 보호연관 식별자 영역으로 구성된다. 프로토콜 식별자 영역은 NLSP 식별자 (1000 1011)를 나타내며 길이 영역은 PDU 형태와 SAID 영역을 합한 길이를 나타낸다. PDU 형태 영역은 SDT PDU임을 나타내기 위하여 0100 1000의 값을 가지며 SAID 영역은 상대 객체 보호연관 식별자를 나타내며 NLSP-CO인 경우에는 사용되지 않는다. 암호 동기 영역은 선택 영역이며 특정 암호화 알고리듬을 위해 사용될 수 있다. 암호화 패딩 영역은 비밀보장 서비스를 위한 블록 암호화 알고리듬을 제공할 목적으로 사용된다. 캡슐화되기 전의 옥테트 스트링의 형태는 그림 4와 같다.

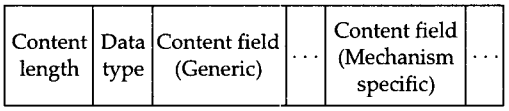


그림 4 캡슐화되기 전 옥테트 스트링의 구조

Fig.4 Structure of octet_string_before_encapsulation.

내용 길이 영역은 모든 내용 영역과 데이타 형태의 길이를 나타내며 데이타 형태 영역은 1 옥테트이다. 데이타 형태 영역의 비트 8은 방향지시 플래그를 나타내며 비트 7은 "Last/Not Last" 플래그를 나타낸다. 표 1은 비트 6에서 비트 1에 대한 데이타 형태를 나타낸 것이며 표 2은 내용 영역을 나타낸 것이다.

보호연관 PDU는 프로토콜 식별자, 길이, PDU 형태, 보호연관 식별자, 보호연관 프로토콜 형태, 그리고 보호연관 PDU 내용영역으로 구성되어 있으며 구조는 그림 5와 같다. 프로토콜 식별자 영역은 NLSP 프로토콜 식별자(0100 0101)를 나타내며 길이 영역은 PDU 형태와 보호연관 식별자 영역의 길이를 나타낸다. PDU 형태 영역은 보호연관 PDU임을 나타내기 위하여 0100 1001의 값을 가지며 보호연관 식별자 영역은 상대 객체의 보호연관 식별자를 나타낸다.

표 1 데이타 형태

Table 1. Data type.

Value	Service primitive
000000	Not related to any NLSP service primitive
000001	NLSP_UNITDATA req/ind
000010	NLSP_CONNECT req/ind
000011	NLSP_CONNECT req/conf
000100	NLSP_DATA req/ind
000101	NLSP_DATA_ACKNOWLEDGE req/ind
000110	NLSP_EXPEdITED DATA req/ind
000111	NLSP_DISCONNECT req/ind
001000	SA protocol
001001-011111	Reserved for future use
100000-111111	Reserved for private use

표 2 내용 영역 형태

Table 2. Content field type.

Value	Content field type
00-5F	Reserved for private use
60-9F	Reserved for future use
A0-BF	Reserved for SA-P use
C0-CF	Reserved for mechanism independent use
D0-FF	Reserved for mechansim dependent use

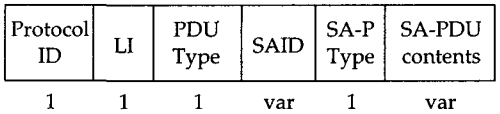


그림 5 보호연관 PDU의 구조

Fig.5 Structure of security association PDU.

보호연관 프로토콜 형태 영역은 보호연관 프로토콜을 제공하는데 사용된 메카니즘을 지시하는 식별자를 나타낸다. 보호연관 내용영역은 교환 식별자, 내용길이, 그리고 내용영역으로 구성되며 그림 6과 같다. 교환 식별자 영역은 PDU가 첫번째 키토큰 교환과 연관되면 0000 0000의 값을 두번째 인증/협상 교환과 연관되면 0000 0001의 값을 포함한다. 또한 SA 해제/중지 요청과 연관되면 1000 000의 값을 해제/중지 확인과 연관되면 1000 0001의 값을 포함한다. 내용길이 영역은 자신의 영역을 제외한 모든 내용영역의 옥테트 길이를 나타낸다. 내용 영역은 형태, 길이와 값으로 구성되며 그 값은 표 3과 같다.

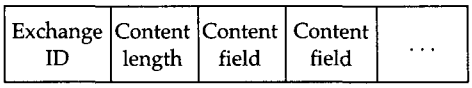


그림 6 보호연관 내용의 구조

Fig.6 Structure of SA content.

표 3 보호연관 내용영역의 형태

Table 3. Type of SA content field.

Value	Service primitive
A0	My SAID
A1	Old your SAID
A2	Key token-1
A3	Key token-2
A4	Authentication digital signature
A5	Authentication certificate
A6	Service selection
A7	SA rejection Reason
A8	SA Abort/Release Reason
A9	Label-def
AA	SA flags
AB	key selection
AC	ASSR
AD-BF	Reserved for future use

접속 보호 제어 PDU는 프로토콜 식별자, 길이, PDU 형태, 보호연관 식별자, 내용 길이와 CSC-PDU 내용 영역으로 구성되며 그림 7과 같다.

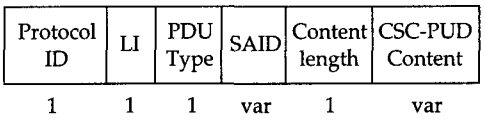


그림 7 접속보호제어 PDU의 구조

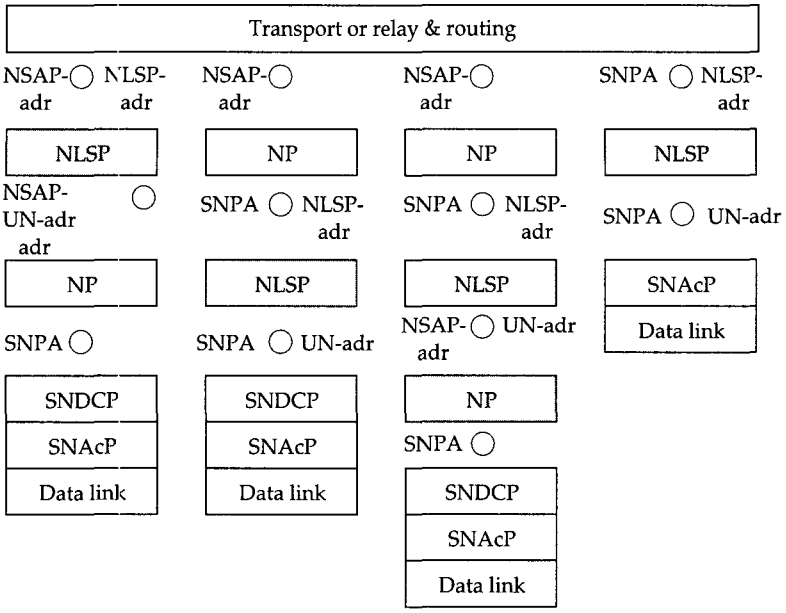
Fig.7 Structure of connection security control PDU.

프로토콜 식별자 영역은

NLSP 프로토콜 식별자(1000 1011)를 나타내며 길이 영역은 PDU 형태와 보호연관 식별자 영역의 길이를 나타낸다. PDU 형태 영역은 CSC PDU를 나타내기 위하여 **111111의 값을 가지며 비트 7은 UNC-UND(UN connect-UN data) 플래그를 비트 8은 보호연관 프로토콜 플래그를 나타낸다. 보호연관 식별자 영역은 상대 객체의 보호연관 식별자를 나타내고 내용 길이 영역은 CSC PDU의 내용영역 길이를 나타낸다. CSC PDU 내용영역의 구조는 제공되는 접속 인증 메카니즘에 의존적이며 암호화 인증 데이타 영역과 키 정보 영역으로 구성된다.

4. NLSP의 위치

NLSP 서비스 인터페이스에는 NLSP 서비스와 UN 서비스가 있다. NLSP 객체는 NLSP 서비스 사용자와 UN 사이에 위치하고 대응 SAP (service access point)는 NLSP-SAP와 UN-SAP이다. 그림 8은 네트워크 계층 내에서 NLSP 객체의 가능한 위치 및 주소를 나타낸 것이다.



NSAP : Network service access point
SNPA : Subnetwork point of attachment
SNAcP : Subnetwork access point
SNDCP : Subnetwork dependent convergence protocol

그림 8 NLSP 부계층을 갖는 네트워크 계층에서의 주소

Fig.8 Addresses in a network layer containing a NLSP sub-layer with one network protocol above/below NLSP.

접속형 NLSP에서 대부분의 복잡도는 접속 설립에 있다. NLSP-CONNECT 파라미터 보호가 요구되면 파라미터들은 SDT PDU에서 캡슐화되고 No-Header 모드인 경우는 전송전에 암호화된다. 접속이 설립되면 사용자 데이타는 SDT PDU에서 캡슐화함으로써 보호된다. No-Header 모드가 선택되면 NLSP는 단지 암호화를 수행함으로써 사용자 데이타를 보호한다. NLSP-CO는 그림 9와 같이 위치할 수 있다. NLSP 하위 인터페이스는 서비스 사용자가 트랜스포트 사용자가 아니라 NLSP 사용자라는 것을 제외하고는 OSI 네트워크 서비스와 일치한다. 그림 10은 신뢰할 수 있는 중간 시스템으로 구성된 네트워크에서의 NLSP-CO의 위치를 나타낸 것이며 그림 11은 신뢰할 수 있는 중간 시스템 및 신뢰할 수 없는 중간 시스템으로 구성된 네트워크에서의 NLSP-CO의 위치를 나타낸 것이다.

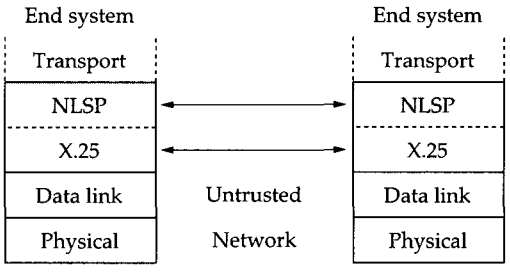


그림 9 종단 시스템에서의 NLSP-CO 위치

Fig.9 Placement of NLSP-CO between end systems.

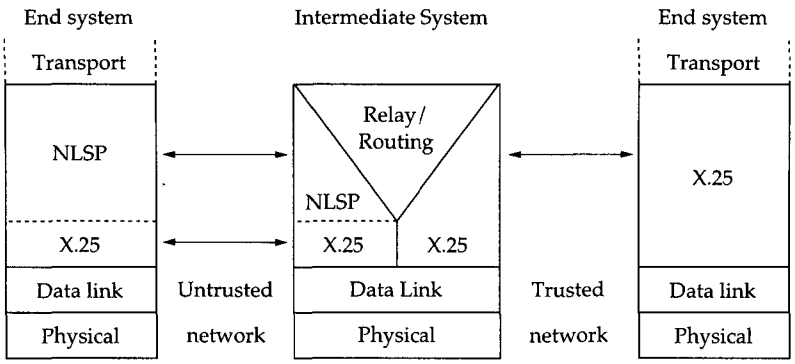


그림 10 신뢰할 수 있는 중간 시스템으로 연결된 NLSP-CO 위치

Fig.10 Placement of NLSP-CO with an trusted intermediate system.

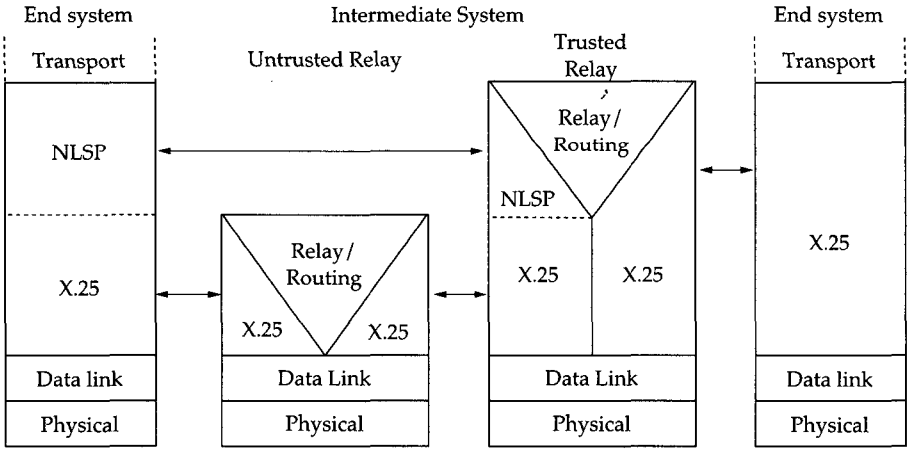


그림 11 신뢰할 수 없는 중간 시스템으로 연결된 NLSP-CO 위치

Fig.11 Placement of NLSP-CO with an untrusted intermediate system.

NLSP-CL을 위한 보호는 SDT PDU에서 사용자 데이타를 캡슐화함으로써 제공된다. NLSP-CL은 그림 12와 같이 위치할 수 있다. 그림 12에서 NLSP는 네트워크 계층 상단에 위치하며 CLNP가 동작하기 전에 SDT PDU의 NSDU들을 캡슐화한다. 이 방식은 단지 종단 시스템간에만 사용될 수 있다. 그림 13에서 NLSP는 비접속 프로토콜 PDU를 캡슐화하는 CLNP 아래에 위치한다. 이 방식은 신뢰할 수 있는 중간 시스템과 연결된 경우나 네트워크 릴레이가 없는 두 통신 시스템 사이에서 사용된다. 그림 14의 방식은 가장 융통성 있으며 어떤 환경에서도 동작할 수 있

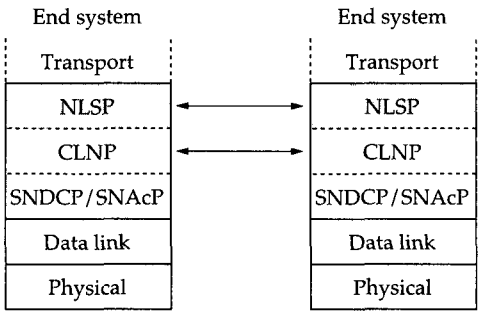


그림 12 종단 시스템에서의 NLSP-CL 위치

Fig.12 Placement of NLSP-CL between end system.

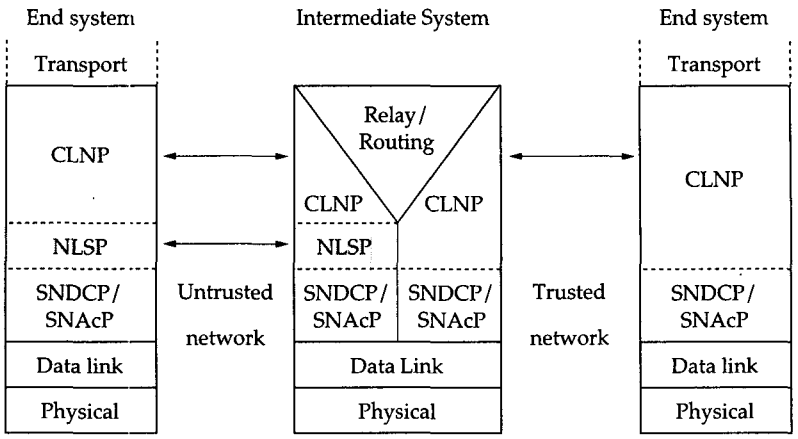


그림 13 신뢰할 수 있는 중간 시스템으로 연결된 NLSP-CL 위치

Fig.13 Placement of NLSP-CL with an trusted intermediate system.

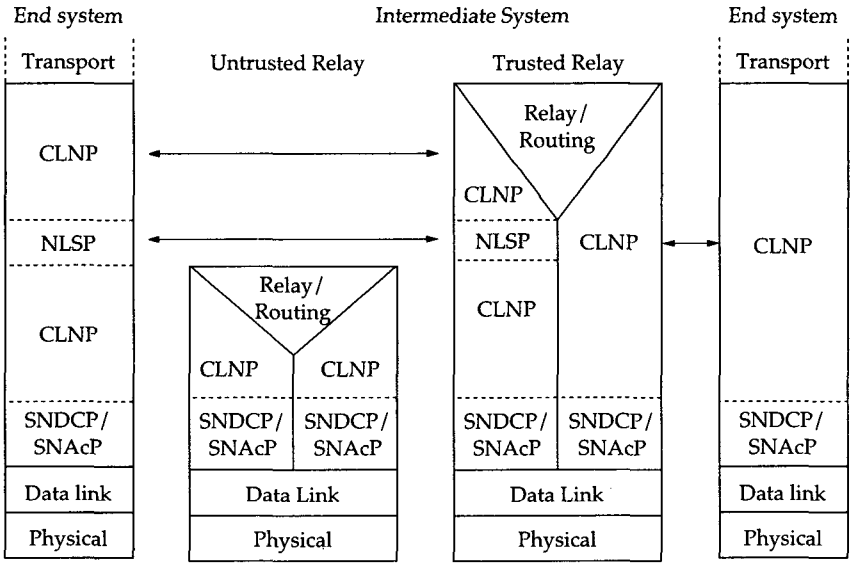


그림 14 신뢰할 수 없는 중간 시스템으로 연결된 NLSP-CL 위치

Fig.14. Placement of NLSP-CL with an untrusted intermediate system.

다. 신뢰할 수 있는 중간 시스템은 NLSP에서 제공된 보호정보를 제거한 후 상위 CLNP 프로토콜로써 중계한다. 신뢰할 수 없는 중간 시스템은 하위 CLNP 프로토콜로써 중계하며 NLSP에서 제공된 보호서비스는 투명하게 통과한다.

5. 결 론

본 논문에서는 ISO/IEC의 표준안인 NLSP의 보호연관, 기능 및 절차, 그리고 제공되는 위치에 관하여 중점적으로 연구 분석하였다. NLSP에서의 보호연관은 크게 보호서비스에 관련된 보호속성과

SDT PDU 캡슐화 과정에서 사용되는 보호 메카니즘들의 보호속성이 있다. NLSP에서의 보호는 모든 서비스 파라미터 보호, NLSP 사용자 데이타 보호와 비보호가 있으며 사용되는 PDU는 SDT PDU, CSC PDU, 그리고 SA PDU의 방식이 있다. NLSP가 제공되는 위치는 접속형인 경우와 비접속형인 경우로 그리고 중간 시스템을 신뢰할 수 있는 경우와 신뢰할 수 없는 경우로 분류된다.

참 고 문 헌

[1] Warwick Ford, Computer Communications Security, Prentice Hall, chap. 1-2, 1994.

[2] D.W. Davies and W.L. Price, Security for Computer Network, Wiley Interscience, chap. 1, 1989.

[3] 박영호, 문상재, 김세헌, 강신각, 임주환 "컴퓨터 범죄 방지를 위한 정보통신망의 보호방안에 관한 연구," 통신정보보호학회지, 제 4권, 제 2호, pp. 47-57, 1994년 6월

[4] ISO , Information Processing - Open System Interconnection - Basic Reference Model - Part 2 : Security Architecture, ISO 7498-2, 1989.

[5] CCITT, Message Hanhering system : EDI Messaging System, Draft Recommendation X.435, Version 6.0, Nov. 1990.

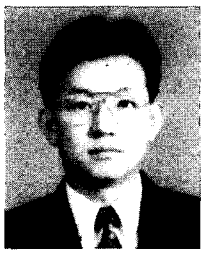
[6] ISO/IEC, Transport Layer Security Protocol, ISO/IEC 10736, Octorber 1993.

[7] ISO, Information Processing - Data Encipherment - Physical Layer Interoperability Requirements, ISO 9160, February 1988.

[8] SDNS Program Office, Security Protocol 3(SP3), SDN.301, Revision 1.5, May 1989.

[9] ITU-T/ISO/IEC, Information Technology - Open Systems Interconnection - Network Layer Security Protocol, International Standard, November 1993.

□ 著者紹介



박 영 호

1989년 2월 경북대학교 전자공학과 (공학사)
1991년 2월 경북대학교 전자공학과 (공학석사)
1991년 3월 ~ 현재 경북대학교 전자공학과 박사과정

문 상 재

통신정보보호학회지 제4권 제2호 참조.