通信情報保護學會論文誌
第5卷 第1號, 1995. 3

OSI 트랜스포트 계층에서의 보호시스템 개발

박 영 호*, 김 기 현*, 문 상 재*, 강 신 각**

Development of Security System in the OSI Transport Layer

Young-ho Park*, Ki-hyun Kim*,
Sang-jae Moon*, Shin-gak Gang**

요 약

개방형 시스템에서 사용자에게 안전성 및 신뢰성을 보증하기 위하여 정보 보호가 필요하다. 본 논문에서는 트랜스포트 계층에서 보호서비스를 제공하기 위하여 ISO와 IEC에서 표준으로 권고하고 있는 트랜스포트 계층 보호 프로토콜과 보호연관 프로토콜을 분석하고, 표준에서는 정의하지 않았으나 구현상 필요한 세부 사항들을 정의한다. 그리고 구현 모델을 제시하고 이에 기초하여 보호시스템을 개발한다. 개발을 위한 환경으로는 USL의 ONP를 사용한다.

Abstract

The information security is needed to guarantee the safety and the confidence to users in open system. This paper analyzes transport layer security protocol and security association protocol, which are standards proposed by ISO/IEC, to provide a security service in the transport layer and particulars, not in the standard, are defined for development. And this paper suggests a development model and develops security system based upon the suggested model. The ONP of USL is used as the development environment.

1. 서 론

개방형 시스템간의 통신을 보호하기 위하여 ISO 7498-2[1]에서는 OSI 참조모델 내에 보호구조를 정의하고 있다. OSI 참조모델에서 보호서비스 제공을 위한 계층별 적용을 고려해 보면, 응용

* 경북대학교 전자공학과
** 한국전자통신연구소

및 프리젠테이션과 같은 상위 계층에서의 보호는 응용 서비스 요소나 특별한 응용의 활용도에 의존하므로 각 응용별로 구현해야 하는 번거로움이 있다. 반면에 네트워크 레벨에서의 보호는 각 개별 망에 종속적이며 보호 비용이 많이 든다. 트랜스포트 계층에서의 보호는 하위 망의 형태와는 독립적이므로 망의 특성과는 무관하게 사용자에게 보다 유연성 있는 보호서비스를 제공하는 장점이 있으며 부인봉쇄 서비스를 제외한 모든 보호서비스를 제공한다.

트랜스포트 계층에서 보호서비스를 제공하기 위하여 NSA(national security agency), NIST(national institute of standards and technology)와 DCA(defense communication agency)에서는 SDNS(secure data network systems) 프로젝트를 수행하여 SP4(security protocol 4)[2]를 정의하고 있으며, 이를 기초로 하여 ISO와 IEC의 JTC1/SC6에서는 트랜스포트 계층 보호 프로토콜(TLSP, transport layer security protocol)[3]을 표준화 중이다. 또한 두 트랜스포트 객체간에 보호연관 속성을 공유하기 위하여 트랜스포트 계층 보호 프로토콜의 일부분으로써 보호연관 프로토콜(SA-P, security association-protocol)[4]을 권고하고 있다. TLSP는 접속 및 비접속형 TPDU(transport protocol data unit)의 전송에 대한 데이타 보호를 허용하며, 인증, 접근제어, 비밀보장 및 무결성 서비스를 제공한다. SA-P는 두 TLSP 객체간의 상호인증, 보호연관 속성들의 초기화 그리고 무결성 및 비밀보장을 제공하기 위한 초기 정보의 설정 기능을 제공한다.

본 논문에서는 종점간 사용자 데이타의 보호를 위하여 트랜스포트 계층에서 TLSP와 SA-P를 이용하여 보호시스템을 개발한다. 보호시스템 개발을 위하여 먼저 TLSP와 SA-P를 분석하고 표준에서는 권고하지 않았으나 구현상 필요한 세부 사항들을 정의한다. 그리고 구현 모델을 제시하고, 이 모델에 기초하여 보호시스템을 개발한다. 개발을 위한 OSI 트랜스포트 계층 환경으로는 ONP(open network platform)[5-8]를 사용한다. 보호 알고리듬으로는 비밀보장 서비스를 제공하기 위하여 DES(data encryption standard)[9]를 사용하고 무결성 서비스를 제공하기 위하여 SHA(secure hash algorithm)[10]를 사용한다. 그리고 키 토큰 교환을 수행하기 위하여 Diffie-Hellman 키 분배 알고리듬[11]을 사용하고 인증 기능을 지원하기 위하여 DSS(digital signature standard)[12]를 사용한다.

2. 트랜스포트 계층 보호 프로토콜

TLSP는 ISO/IEC 8073[13] 및 ISO 8602[14]의 확장이며, 접속 및 비접속형 TPDU(tansport protocol data unit)의 전송에 대한 데이타 보호 및 비보호를 허용한다. TLSP는 ISO 7498-2에서 명시하는 트랜스포트 계층 보호서비스인 대등실체 확인, 데이타 발신처 확인, 접근제어, 접속 비밀보장, 비접속 비밀보장, 복구기능을 갖는 접속 무결성, 복구기능이 없는 접속 무결성 그리고 비접속 무결성 서비스들을 제공한다. TLSP는 암호화 메카니즘을 사용하여 이 서비스들을 지원하고, 보호 라벨링(labeling)[15], 키 및 식별자와 같은 보호 속성은 보호관리에 의해 미리 설정되거나 보호연관 프로토콜을 사용하여 설정된다. 키의 재설정은 보호연관 프로토콜이나 프로토콜의 외적 수단을 통하여 지원된다.

그림 1과 2는 OSI 참조모델에서의 접속 및 비접속 TLSP의 위치를 나타낸 것이다. 그림에서 트랜스포트 계층은 TPDU를 구성하는 상위부분과 네트워크 계층과 네트워크 계층 서비스를 사용하여 TPDU를 전송하는 하위부분으로 구분되며, TLSP는 상위부분과 하위부분 사이에 위치한다. TLSP는 접속형 트랜스포트 프로토콜과 비접속형 프로토콜이 모두 같은 형태이며 운용은 네트워크 서비스 형태에 독립적이다. 그러나 제공되는 서비스들은 트랜스포트 프로토콜의 형태에 의존한다.

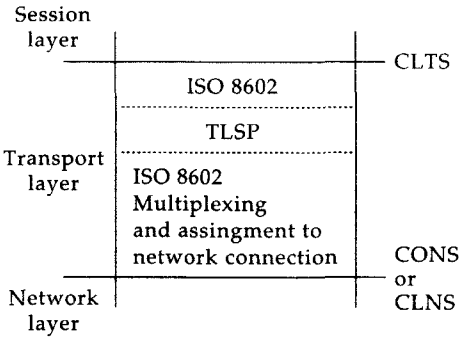


그림 1. ISO 8602에서의 TLSP

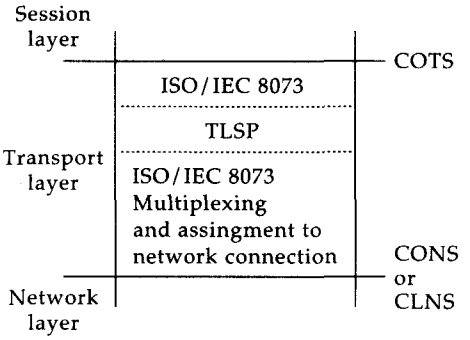


그림 2. ISO/IEC 8073에서의 TLSP

2.1 보호연관 속성

TLSP의 처리는 보호연관에 의하여 결정되며 각 트랜스포트 객체들은 이 연관들을 공유한다고 가정한다. 각 보호연관은 각 종단 시스템에서의 속성 집합에 의하여 정의되며, 보호연관 식별자 SA-ID는 통신을 보호하는데 사용될 수 있는 연관들의 집합을 식별한다. 보호속성들은 상호교환 및 ASSR(agreed set of security rule)[16]을 통하여 설정된다. ASSR은 사용되는 보호 메카니즘을 규정하는 공통된 규칙들의 집합이며, 상호 동의하여 정의할 필요가 있는 모든 파라미터들을 포함한다. 보호 규칙과 식별자는 제 3자에 의해 등록될 수 있다.

TLSP의 보호연관 속성들은 다음과 같다.

- SA(security association) identification
- Indicator
- Address of peer TLSP entity(s)
- Identifier for the agreed set of security rules
- Protection QOS selected for the SA
- Mechanisms selected for the SA
- Label mechanism attributes
- ICV mechanism attributes
- SN(sequence number) mechanism attributes
- EXSN mechanism attributes
- Encipherment mechanism attributes

2.2 트랜스포트 계층 보호 프로토콜의 기능

TLSP는 TPDU를 보호연관 속성에 기초하여 보호하며 SE TPDU(security encapsulation TPDU)로 캡슐화 한다. 캡슐화 기능은 접속/비접속 비밀보장 및 무결성 서비스를 제공하기 위하여 암호화와 무결성 검사 기능을 결합하여 사용한다. 또한 캡슐화 기능은 네트워크 접속의 할당 및 멀티플렉싱을 제외한 트랜스포트 계층의 모든 프로토콜 처리 기능을 수행한 후에 적용된다. 디캡슐화는 디멀티플렉싱 후와 다른 프로토콜 처리 기능을 수행하기 전에 수행된다. TLSP의 기능은 데이타 암호화 기능, 무결성 기능, 보안 라벨 기능, 보호 패딩 기능, 대등 실체 인증 기능 및 보호연관 기능으로 나눌 수 있다. SE TPDU 수신측에서는 보호연관 속성에 의해서 규정된 모든 보호의 존재 여부를 검증한다. 부적당하게 보호된 TPDU는 무시된다.

표 1은 TLSP 기능들이 실제로 구현될 때 트랜스포트 각 등급에서 포함되어지는 관계를 나타낸 것이다.

표 1. 트랜스포트 계층 프로토콜 등급과 TLSP 메카니즘과의 관계

Protocol mechanism	ISO/IEC 8073 class					ISO 8602
	0	1	2	3	4	
Cryptographic confidentiality	m	m	m	m	m	m
ICV processing	m	m	m	m	m	m
Direction indicator processing	*	*	*	*	*	*
Unique sequence Nos.	NA	NA	o	o	o	NA
Peer address check processing	*	*	*	*	*	*
Security labels for cryptographic assoc.	o	o	o	o	o	o
Connection release	o	o	o	o	o	NA
Key replacement	o	o	o	o	o	o

* Procedure always include in class
NA Not applicable
o Negotiable procedure whose implementation in equipment is optional
m Negotiable procedure whose implementation in equipment is mandatory

2.3 SE TPDU의 구조

SE TPDU는 클리어 헤드, 암호화 동기, 보호된 내용 및 ICV 영역으로 구성된다. 그림 3은 SE TPDU의 구조를 나타낸 것이다.

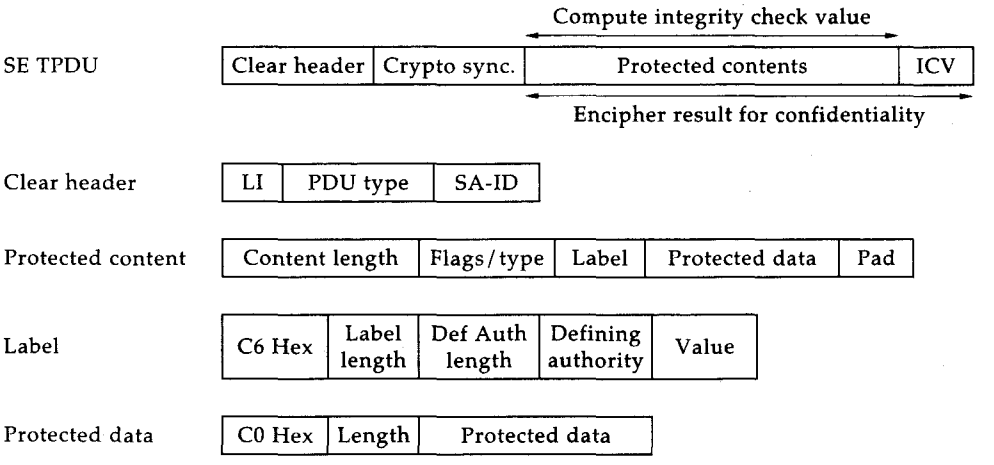


그림 3. SE TPDU의 구조

3. 보호연관 프로토콜

두 통신 객체간에 통신 보호를 제어하는 정보의 집합이 보호연관이며, TLSP의 처리를 위하여 두 트랜스포트 객체는 보호연관 속성을 공유해야 한다. 통신 객체 사이에 협상을 통하여 동일한 보호 속성 정보를 공유하는 과정을 보호연관의 설정이라 한다. 보호연관을 설정하는 방법에는 TLSP를 사용하기 전에 보호 관리에 의해 미리 설정하는 방법과 보호연관 프로토콜을 사용하는 방법이 있다. ISO와 IEC의 JTC1/SC6에서는 트랜스포트 계층 보호 프로토콜의 일부분으로써 보호연관 프로토콜을 권고하고 있으며, 이 보호연관 프로토콜은 보호연관 설정, 유지 및 중지/해제를 수행하기 위하여 비대칭 키 암호화 알고리듬을 사용한다. 보호연관 프로토콜은 TLSP 객체들에게 두 객체간의 상호인증, 보호연관 속성들의 초기화 그리고 무결성 및 비밀보장을 제공하기 위한 초기 정보의 설정 기능을 제공한다.

보호연관을 설정하기 이전에 각 트랜스포트 객체는 지원하는 메카니즘, 각 비대칭 키 암호화 알고리듬에 대한 비대칭 키 쌍, TA(trusted authority)의 확인표, 그리고 TA의 공개키와 이 공개키를 이용하는 비대칭 키 암호화 알고리듬과 같은 정보를 미리 설정해야 하며, 이러한 정보의 사전 설정은 보호정책에 따라 결정된다.

3.1 보호연관 프로토콜의 논리적 기능

보호연관 프로토콜의 논리적 기능은 키 토큰 교환, 상호인증, 보호연관 속성 협상 그리고 보호연관 속성 중지/해제를 수행하는 4가지 기능으로 분류되며 다음과 같다.

첫째, TLSP 객체들은 공유할 비밀값을 생성하기 위하여 키 토큰 교환을 수행한다. TLSP 객체들은 공유 비밀값과 대칭키 암호화 알고리듬을 사용하여 키 토큰 교환 이후의 나머지 SA-P에 대한 비밀보장을 제공하며, 이 공유 비밀값은 보호연관의 키와 ISN(integrity sequence number) 속성 협상시 참조열로 사용된다.

둘째, 보호연관을 설정하는 동안 TLSP 객체는 다른 TLSP 객체를 인증하기 위하여 확인표와 디지탈 서명[17]을 교환한다. 이 기능을 수행하기 위하여 인증 확인표와 공개키 쌍이 필요하다.

세째, 보호연관 속성을 협상하기 위하여 PDU를 교환한다. 보호연관 속성 협상에는 서비스 협상, 라벨 협상, 키와 ISN 선택, 키 대체 그리고 그 밖에 필요한 보호연관 속성 협상이 있다.

네째, 보호연관을 중지 또는 해제를 위하여 PDU를 교환한다.

3.2 보호연관의 설정 및 해제 절차

보호연관 프로토콜의 4가지 논리적 기능은 SA PDU를 교환함으로써 수행된다. 첫번째 교환은 키 토큰 교환이며 암호화를 적용하지 않는다. 두번째 교환은 보호된 보호연관 협상으로 구성되며 인증을 제공한다. 마지막으로 보호연관의 중지 및 해제를 위하여 교환기능이 제공된다.

3.2.1 보호연관 설정

TLSP 객체나 로컬 보호 관리자가 보호연관 설정을 시작할 수 있다. 시작하는 TLSP 객체는 아래 기능들을 수행한 후 다음과 같은 정보를 포함하는 SA PDU를 수신 TLSP 객체로 전송한다.

a) 선택한 보호연관 식별자
b) 키 토큰 1
c) 두번째 SA-P 교환을 보호하기 위해 사용되는 비밀보장 및 무결성 메카니즘

보호연관 요청 PDU 수신시, 수신 TLSP 객체는 개시자가 제안한 보호 메카니즘에 대해 수용 가능한 메카니즘을 선택한다. 이때 수용 가능한 메카니즘이 한 가지도 없는 경우 보호연관의 거절 및 이유를 알리기 위한 SA PDU를 보낸다. 적절한 메카니즘을 선택하였으면 자신의 보호연관에 대한 식별자를 선택하고 키 토큰을 수행한 후 다음과 같은 정보를 포함하는 SA PDU를 개시자에게 보낸다.

a) 선택한 보호연관 식별자
b) 키 토큰 2
c) 선택한 비밀보장 및 무결성 메카니즘

보호연관 요청에 대한 첫번째 응답 PDU 수신시, 시작하는 TLSP 객체는 인증 및 보호연관 속성을 협상하기 위한 두번째 SA PDU를 전송한다. 이때 SA PDU에는 다음과 같은 정보가 포함된다.

a) 상대의 보호연관 식별자(보호연관 헤더부분에 포함)
b) 확인표
c) 보호서비스들의 목록
d) 보호 라벨 집합
e) 키 및 ISN 포인터 집합
f) 그 밖의 보호연관 속성들

위에서 상대의 보호연관 식별자를 제외한 나머지 정보는 SA PDU의 내용 영역에 들어가며 이 정보에 대하여 개시자의 비밀키로 디지탈 서명을 하고 첫번째 교환에서 생성된 세션키로 내용 영역을 암호화하여 전송한다.

개시자로부터 두번째 SA PDU를 수신한 응답자는 첫번째 교환에서 생성된 세션키로 내용영역을 복호화한 후 수신한 확인표와 디지탈 서명을 검증하고 제안된 보호서비스, 보호라벨, 키/ISN 및 그 밖의 보호 속성에 대하여 그 수용 여부를 검사한다. 이중 한 항목이라도 검사에 실패하면 보호연관 설정에 대한 거절과 그 이유를 포함한 SA PDU를 개시자에게 전송한다. 모든 검사를 통과한 경우, 응답자는 제안된 보호서비스, 보호 라벨, 키/ISN 및 그 밖의 보호 속성에 대하여 적절한 것을 선택한 후 다음과 같은 항목을 포함하는 SA PDU를 개시자에게 전송한다.

a) 상대의 보호연관 식별자(보호연관 헤더에 포함)
b) 확인표
c) 선택된 보호서비스
d) 보호 라벨 집합 중에서 선택된 부집합
e) 키와 ISN

위에서 상대의 보호연관 식별자를 제외한 나머지 정보는 SA PDU의 내용 영역에 들어가며 이 정보에 대하여 개시자의 비밀키로 디지탈 서명을 하고 내용 영역을 암호화하여 전송한다.

3.2.2 보호연관 해제/중지

TLSP 객체 또는 로컬 보호 관리자가 보호연관 해제/중지를 시작한다. 보호연관 해제/중지하는 개시자는 보호연관 수립의 개시자가 될 필요는 없다. 보호연관 해제/중지 요구 및 응답을 위한 SA PDU는 확인표와 보호연관 해제/중지 이유 영역을 내용 영역으로 구성하고, 이 내용 영역에 대하여 디지탈 서명과 암호화를 수행한 후 전송한다.

3.3 SA PDU의 구조

SA PDU는 프로토콜 식별자, PDU 길이, PDU 형태, SA-ID, SA-P 형태 및 SA PDU 내용영역으로 구성되어 있다. 그림 4는 SA PDU 구조를 나타낸 것이다. 키 토큰 교환과 디지탈 서명 메카니즘을 사용하는 SA-P에서 보호연관 내용 영역은 교환 ID, 내용 길이 및 내용 영역으로 구성된다.

SA PDU

LI	PDU type	SA-ID	SA-P type	SA PDU content

SA PDU content

Exchange ID	Content length	Content field	Content field	.....

그림 4. SA PDU의 구조

4. 트랜스포트 계층의 보호시스템 개발

트랜스포트 계층 보호시스템을 개발하기 위하여 본 논문에서는 그림 5와 같이 개발 모델을 설정하였다. 트랜스포트 객체가 트랜스포트 계층 사용자로부터 서비스를 요청받으면, 트랜스포트 객체는 그 서비스를 지원해 준다. 만약 보호서비스가 요구된다면 트랜스포트 객체는 TLSP 객체에게 보호서비스를 요청하며 TLSP 객체는 TLSP와 SA-P를 이용하여 트랜스포트 객체에게 보호서비스를 제공해 준다.

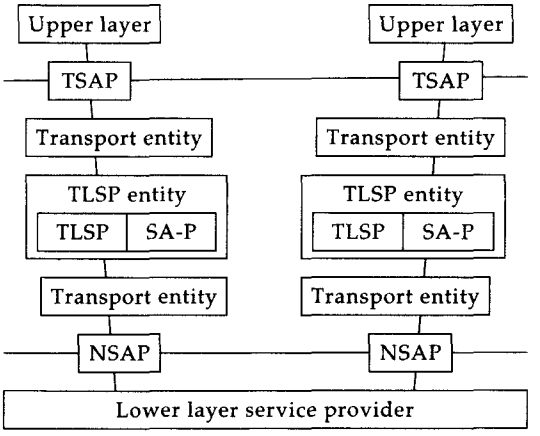


그림 5. TLSP 구현 모델

이 개발 모델에 기초하여 트랜스포트 계층 보호시스템을 개발하고 UNIX 환경에서 동작하는 ONP LAN 트랜스포트 상에서 실험하기 위하여 다음 사항을 가정한다.

첫째, ASSR과 보호연관 협상 이전에 필요한 보호 관리 정보들은 통신 이전에 미리 공유하고 있다고 가정한다. 단, 이 정보들은 본 논문에서 정의한다.

둘째, 트랜스포트 계층을 제외한 타 계층의 보호서비스는 고려하지 않는다.

세째, TLSP와 SA-P를 ONP LAN 트랜스포트에 이식 실험하기 위하여 TP4에서 요구하는 프로토콜 메카니즘만을 구현한다.

4.1 보호 관리 정보의 구성

두 통신 객체간에 TLSP를 통하여 보호서비스를 제공받기 위해 두 통신 객체는 암호 알고리듬, 암복호 키, 인증 기법 및 보호 라벨과 같은 보호 관리 정보를 공유해야 한다. 이 보호 관리 정보들을 SMIB(security management information base)로 구축하기 위하여 본 논문에서는 ASSR, SA-P 정보, 및 TLSP 정보로 구분하여 SMIB로 구성하였다.

먼저 ASSR은 통신 당사자간 동의된 보호 규칙의 집합으로 상호 동의하여 정의할 필요가 있는 모든 파라미터들을 포함한다. ASSR은 유일한 식별자를 가지며 보호연관 설립 과정에서 개시자는 여러개의 ASSR 식별자를 전송하고 응답자는 하나를 선택하게 된다. 본 논문에서는 두 통신자간에 ASSR을 미리 공유하고 있다고 가정하였으며, 한개의 ASSR 식별자만을 이용하였다. 본 논문에서는 ASSR을 그림 6과 같이 구성하였다. 그림 6에서 보호 알고리듬, 디지탈 서명 및 키 정보의 발생은 SA-P 통신을 보호하기 위하여 동적으로 설정할 수 있는 정보로써 본 논문에서는 이들 정보에 대하여 SA PDU 교환 과정을 통하여 협상하도록 설계하였다.

a) ASSR-ID : 1.0014.13.5.111
b) Selected definition module
(PE or DO) Auth: none, low, high
AC : none, low, high
Confid : none, low, high
Integ : none, low, high
c) Security Label
- Sensitivity level
{Unclass, Integrity, Confidentiality, Secret}
• Label ->sensitivity = Unclass
implies
Auth = none, AC = none, Confid = none, Integ = none
• Label ->sensitivity = Integrity
implies
Auth = none, AC = none, Confid = none, Integ = high
• Label ->sensitivity = Confidentiality
implies
Auth = none, AC = none, Confid = high, Integ = none
• Label ->sensitivity = Secret
implies
Auth = high, AC = high, Confid = high, Integ = high
d) Mechanism module - security labels for access control
for security service selected: AC = high or Conf = high
Label_Def_Auth : XYZ
Explicit indication : Yes
e) Protection of all service parameters
for security service selected: Integ = high or Conf = high
f) Mechanism module - Integrity Check Value
for security service selected: Integ 〉 none or Auth = high
or Mechanism security label(Confid = high)
ICV_Alg_ID : XYZ
ICV_Blk_size : x octets
Rekey after : 10,000 PDUs
Key distribution mechanism: asymmetric
g) Mechanism module - Integrity sequence number
for security service selected: Integ = high or Auth = high
ISN_Len : 4 octets
h) Mechanism module - Encipherment
for security service selected: Conf 〉 low
Enc_Alg_ID : XYZ
Enc_Blk_size : x octets
Rekey after : 10,000 PDUs
Key distribution mechanism: asymmetric
i) Mechanism module - Connection authentication
for security service selected: AC 〉 low or PE Auth 〉 low
Enc_Alg_ID : XYZ
Enc_Blk_size : x octets
Key distribution mechanism: asymmetric
j) Mechanism module - Asymmetric key distribution
for mechanism encipher or integrity check value
PKC_Alg_ID : XYZ

그림 6. ASSR

SA-P 정보는 SA-P를 수행하기 위하여 두 통신자간에 공유되어야 할 정보를 포함한다. SA-P 정보는 지원하는 메카니즘, 확인표, TA의 공개키, 그리고 TA의 공개키를 이용하는 비대칭 키 암호화 알고리듬 등을 포함하고 있다. 보호시스템을 개발하기 위하여 이러한 SA-P 정보는 다음과 같이 가정하였다.

a) 지원하는 메카니즘은 ASSR에서 정의한 e)에서 j)까지의 메카니즘 모듈을 그대로 사용한다.

b) 각 보호 알고리듬의 특성은 두 통신자 간에 미리 공유하고 있다고 가정하고 구현시 그 식별자만을 교환하므로써 보호 알고리듬에 대해 동의하게 된다.

c) 키 분배와 인증을 지원하기 위하여 모든 사용자들이 신뢰할 수 있는 센타인 TA(trusted authority)가 존재하며, TA에 대한 전적인 신뢰가 보증된다고 가정한다.

마지막으로 TLSP 정보는 ASSR과 함께 TLSP를 지원하기 위한 정보로써 SA PDU 교환을 통하여 협상된 보호연관 속성들을 포함한다.

그림 7은 위에서 분류한 보호 관리 정보, SA-P와 TLSP의 동작관계를 나타낸 것이다.

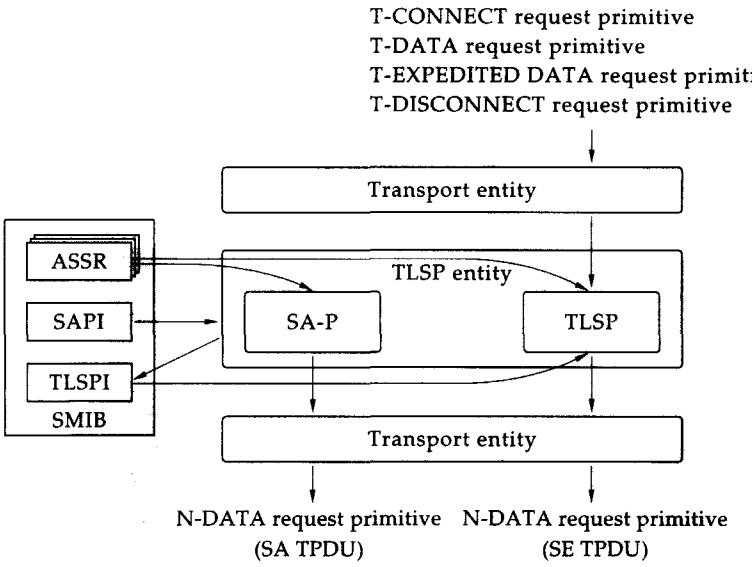


그림 7. 보호 관리 정보(SMIB), SA-P와 TLSP의 동작

4.2 PDU의 구성

보호연관 프로토콜에서 SA PDU의 구조를 정의하고 있으나 개발을 위해서는 SA PDU의 교환 형태별 내용 영역에 대한 보다 세부적인 정의가 필요하다. 이는 보호 관리 정보의 사전 공유 정도에 따라 표준에서 권고하고 있는 기본적인 협상 내용에 부가될 보호연관 속성들이 달라지기 때문이다. SA PDU의 내용 영역에 대한 세부적인 사항을 정의하기 위하여 본 논문에서는 보호 관리 정보에 대한 정의를 하였으며 그림 8과 같이 SA PDU를 구성하였다.

SE TPDU의 구조는 표준에서 권고하고 있는 형태를 따르고 있다.

1st exchange PDU (Initiator)

LI	PDU type	SA-P type	Exchange - ID	Content length	My SAID	Key token 1	Service selection	ASSR	Integ. alg.	Conf. alg.	Auth. mech.

1st exchange PDU (Recipient)

LI	PDU type	SAID	SA-P type	Exchange - ID	Content length	My SAID	Key token 2	Service selection	ASSR	Integ. alg.	Conf. alg.	Auth. mech.

2nd exchange PDU

LI	PDU type	SAID	SA-P type	Exchange - ID	Content length	Certificate	Service selection	Label Def.	Key selection	SA flag	ASSR	Initiator	Integ. alg.	Conf. alg.	Auth. mech.	Digital signature

2nd exchange PDU (Rekey PDU)

LI	PDU type	SAID	SA-P type	Exchange - ID	Content length	Certificate	Old Your SAID	Label Def.	Key selection	SA flag	Digital signature

SA release/abort PDU

LI	PDU type	SAID	SA-P type	Exchange - ID	Content length	Certificate	SA release/abort reason	Digital signature

그림 8. SA PDU의 구조

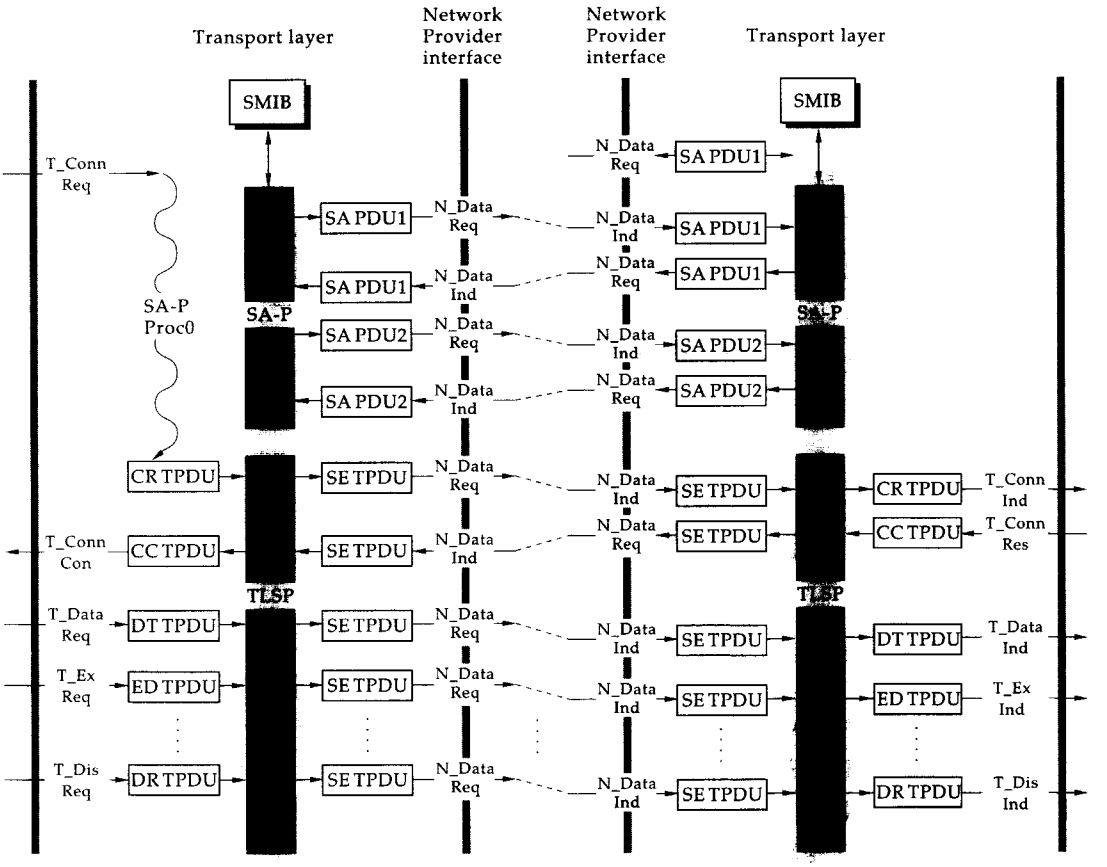


그림 9. 접속형 TLSP 흐름도

4.3 보호 연관 프로토콜과 트랜스포트 계층 보호 프로토콜의 구성

본 논문에서는 SA-P와 TLSP를 ONP LAN 트랜스포트상에서 실험하기 위하여 접속형 TLSP만을 고려하였다. 그림 9는 접속형에서의 순서제어를 나타낸 것이다. TLSP 객체가 트랜스포트 객체로부터 접속 요구를 받으면, TLSP 객체는 SA-P를 이용하여 보호 연관을 설정하고 이를 SMIB에 저장한다. 그리고, TLSP 객체는 보호연관 속성에 기초하여 트랜스포트 객체로부터의 모든 TPDU를 보호한다.

그림 10은 TLSP 보호시스템에서 데이타 송/수신시의 처리절차를 나타내고 있다. 먼저, 송신 절차는 그림 10(a)과 같으며, TLSP 요구 프리미티브를 처리하는 과정이다. TLSP 객체가 TLSP 요구 프리미티브를 받으면, 보호 연관 속성이 저장되어 있는 SMIB에 접근한다. 그리고, TLSP 객체는 발신처 및 수신처 주소와 NSAP를 이용하여 보호연관 속성들을 찾는다. 만약 보호 연관 속성이 존재하지 않을 경우, SA-P를 이용하여 보호 연관을 설정한다. 보호 연관이 SMIB 내에 존재할 경우, 보호 헤드, 무결성을 위한 ICV, 비밀보장을 위한 암호화를 한 후 비보호 헤드를 붙여 SE TPDU로 캡슐화 한다. 그 후에 TLSP 객체는 발신처와 수신처 주소, SE TPDU 및 QOS로 구성된 UN(underlying network) 서비스 요구 프리미티브를 형성하여 하위 계층으로 전달한다. 수신 절차는 그림 10(b)와 같으며 UN 지시 프리미티브를 처리하는 과정이다. TLSP 객체가 하위 계층으로부터 지시 프리미티브를 받으면 PDU의 형태를 검사한다. SA TPDU일 경우 SA-P을 이용하여 보호연관을 설정하거나 해제한다. SE TPDU일 경우, 프리미티브의 인자인 주소와 SAID를 이용하여 SMIB 내의 보호 연관을 찾아 PDU에 적절한 메카니즘을 적용한다. 먼저 비보호 헤드 영역을 제거하고, PDU를 복호화하고 ICV를 검사한다. 그리고 보호 내용 영역을 검사한 후, TLSP 지시 프리미티브를 형성하여 지정된 스택으로 가게 된다. 송수신 과정 중 SN이 Data_local_SN이나 Data_peer_SN을 초과할 경우, TLSP 객체는 SA-P의 키 대체 과정을 수행한다.

4.4 보호 알고리듬

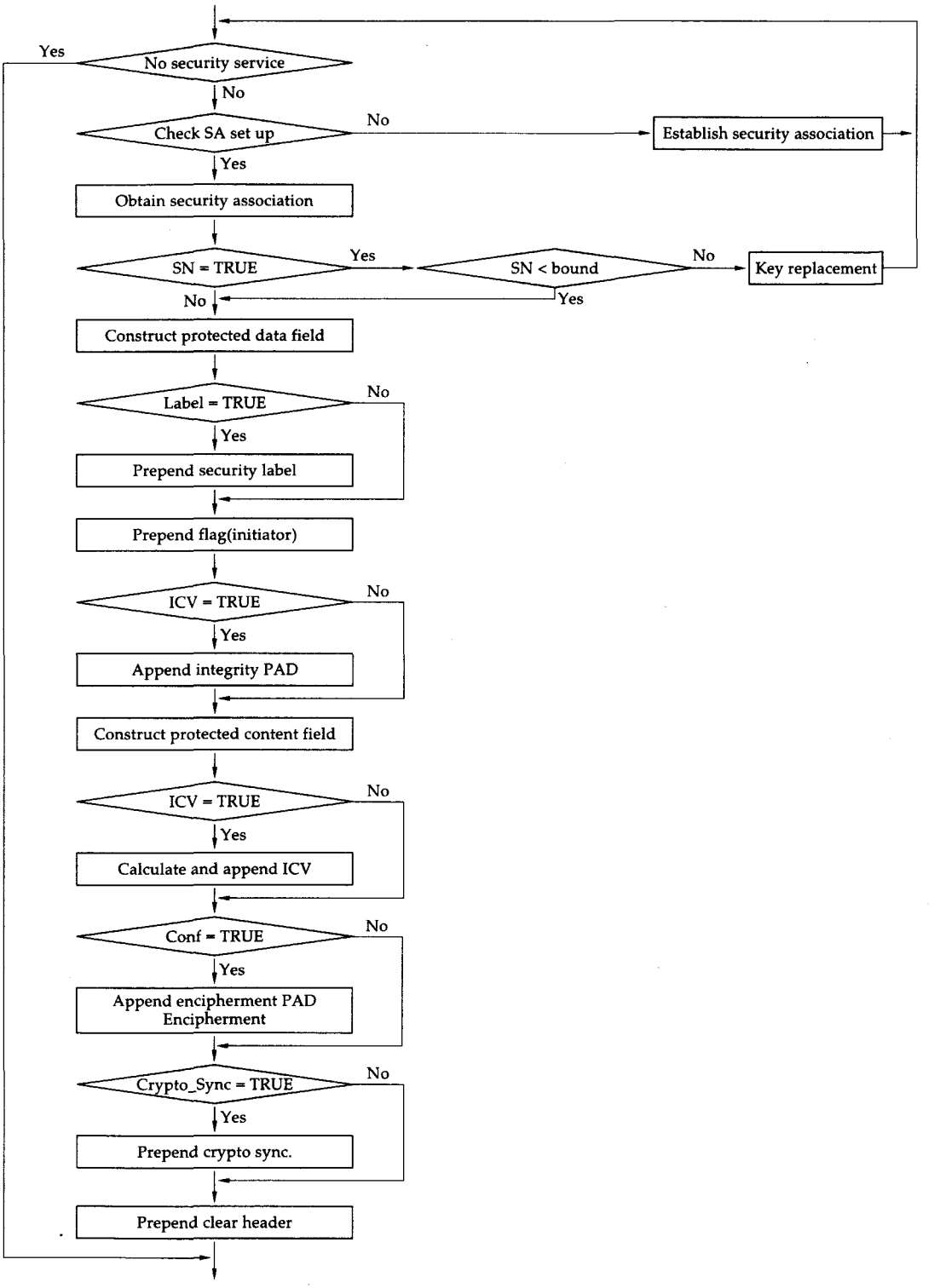
보호 알고리듬으로는 비밀보장 서비스를 제공하기 위하여 DES를 사용하고 무결성 서비스를 제공하기 위하여 SHA를 사용하였다. 그리고 키 토큰 교환을 수행하기 위하여 Diffie-Hellman 키 분배 알고리듬을 사용하고 SA-P 인증 기능의 디지탈 서명을 지원하기 위하여 DSS를 사용하였다.

4.5 보호시스템 개발

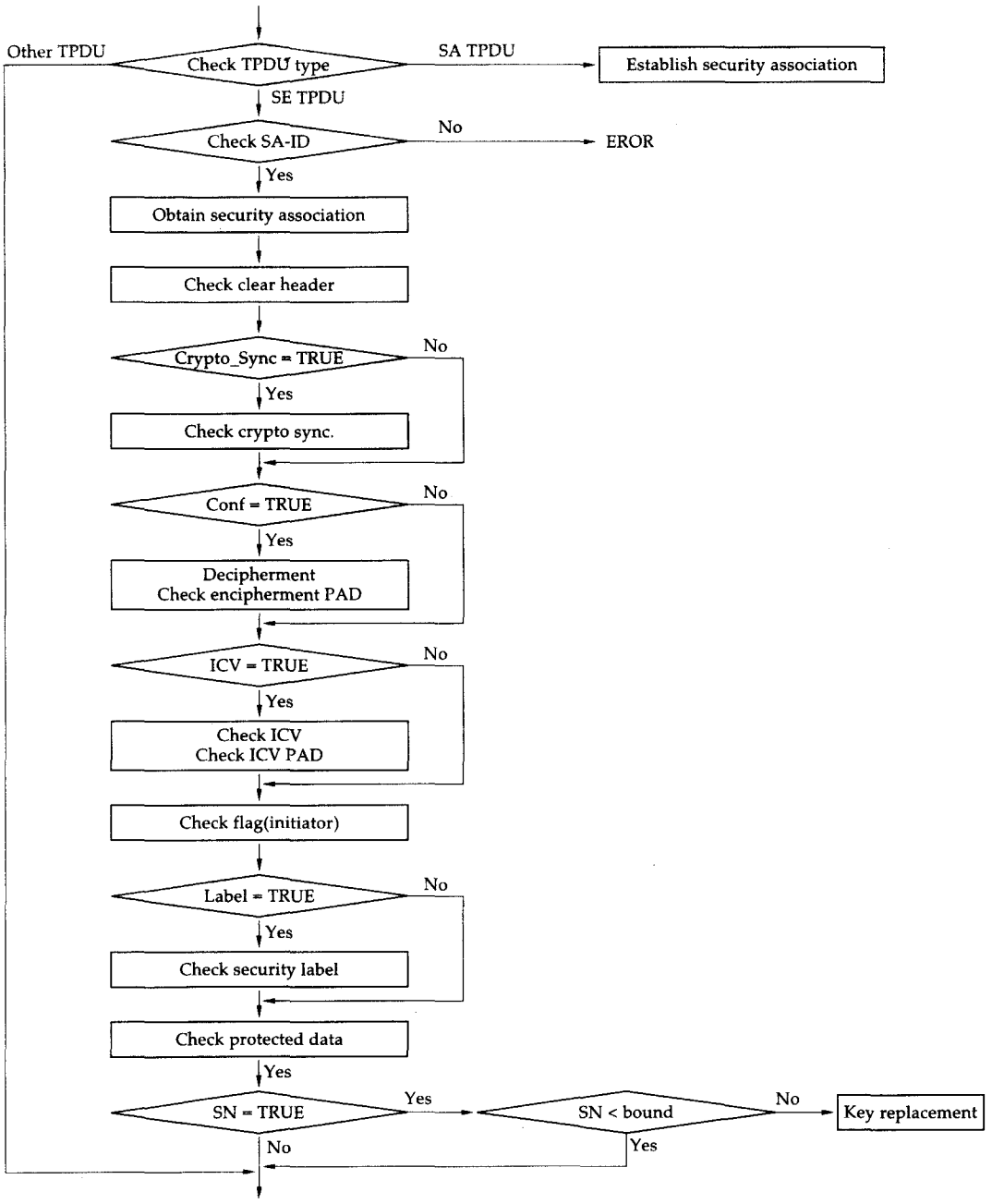
OSI 참조모델에 기초한 개방 시스템의 환경 구축과 이에 따른 실험을 돕기 위하여 UNIX의 등록사인 USL(UNIX system laboratory)의 ONP(open network platform)을 사용하였다. ONP는 UNIX system V용으로 설계된 네트워킹 프로그램, 도구 및 응용의 집합으로서 개방 시스템 응용의 설계, 개발 그리고 실험을 위한 실험적 환경을 제공한다. ONP가 UNIX system V용으로 개발된 이유는 장기적으로 볼 때 OSI 환경의 운용체계에 알맞으며, 이식과 기능 향상이 용이하고 표준 응용 서비스를 제공하기 때문이다. ONP의 하드웨어/소프트웨어 요소들은 크게 다음과 같이 구분된다.

- 응용 서비스 라이브러리
- 기본 스택 프로토콜
- 서브네트워크 프로토콜

ONP WAN/LAN 트랜스포트 패키지 구조 중 그림 11과 같이 ONP LAN 트랜스포트를 구성하고 커널상에 존재하는 프로토콜 스택에 TLSP 및 SA-P를 이식시켜 보호시스템을 개발하였다.


No security service
Yes
No
Check SA set up
No
Establish security association
Yes
Obtain security association
SN = TRUE
Yes
SN < bound
No
Key replacement
No
Yes
Construct protected data field
Label = TRUE
No
Yes
Prepend security label
Prepend flag(initiator)
ICV = TRUE
No
Yes
Append integrity PAD
Construct protected content field
ICV = TRUE
No
Yes
Calculate and append ICV
Conf = TRUE
No
Yes
Append encipherment PAD
Encipherment
Crypto_Sync = TRUE
No
Yes
Prepend crypto sync.
Prepend clear header

(a) 송신



(b) 수신

그림 10. TLSP 보호시스템에서 데이타 송/수신시의 흐름도

ONP LAN 트랜스포트는 CLNP 상에 TP4로 구성되어 있으며 멀티플렉싱과 디멀티플렉싱을 제외한 등급 4의 모든 기능을 제공한다. 보호시스템을 개발하기 위한 접근 방식으로서 TLSP와 SA-P를 트랜스포트 계층의 부계층으로 구성하고 TLSP 객체가 트랜스포트 객체로부터의 모든 TPDU를 보호 캡슐

화하는 방법을 채택한다. 그림 11의 ONP LAN 트랜스포트의 특성 상 멀티플렉싱과 디멀티플렉싱 기능이 없으므로 트랜스포트 계층의 하위 부분은 네트워크 계층 서비스를 사용하여 TPDU를 전송하는 기능만으로 구성된다. 이 기능을 수행하는 함수가 tp4_sendtpdu()와 N_DATAindication() 함수이며 SA-P와 TLSP로 구성된 부계층은 이 두 함수 내에 TLSP_sendtpdu()와 TLSP_DATAindication() 루틴을 추가함으로써 인터페이스된다. 그림 12은 실제 개발된 프로그램 중 인터페이스 부분을 나타낸 것이다.

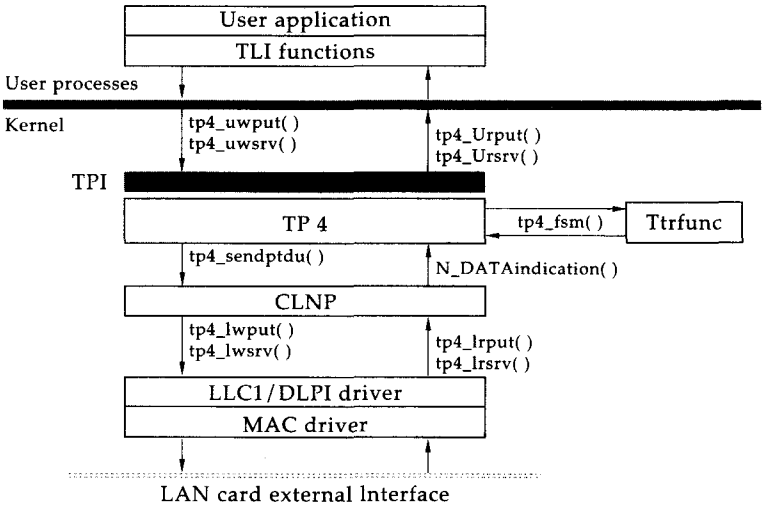


그림 11. 개발된 ONP LAN 트랜스포트의 구성

```
#include "includes.h"
#include "/sap/TLSPProvider.c"

N_DATAindication(rem_nsap_addr, loc_nsap_addr, data, ce, inlp, mp)
nsap_address *rem_nsap_addr;
nsap_address *loc_nsap_addr;
buf_type data;
int ce, inlp;
mblk_t *mp;
{
        register struct Tmachine *machp;
        short check;

        check = TLSP_DATAindication(rem_nsap_addr, data);
        if(check == 0) return;

        tp4.TPDU.tpdu = data;
        tp4.TPDU.released = 0;
        tp4.TPDU.use_inactive = inlp;
        tp4.TPDU.from_naddr = rem_nsap_addr;
        tp4.TPDU.to_naddr = loc_nsap_addr;
```

```
        while ((machp = tp4_inpdu()) != (struct Tmachine *) NULL) {
                if (ce)
                        machp->ncong += 1;
                machp->ntotal += 1;
                if (tp4_fsm(machp, NDATIND, mp) < 0) {
                        if (tp4.TPDU.data != null)
                                BuffFree(tp4.TPDU.data);
                        }
                        mp = (mblk_t *) NULL;
                }
                if (mp != (mblk_t *) NULL)
                        freeb(mp);
        }

        tp4_sendtpdu(mp, bp)
        struct Tmachine *mp;
        buf_type bp;
        {
                short check;

                check = TLSP_sendtpdu(&mp->rem_nsap_addr, bp, 0);
                if(check == 0) return;

                if (bp != null) {
                        if (mp->use_inactive)
                                INLPrequest(TP_SAP, &mp->rem_nsap_addr, bp);
                        else
                                N_DATArequest(TP_SAP, &mp->rem_nsap_addr, bp);
                        tp4.TPDUsent++;
                }
        }
```

그림 12. ONP에서의 TLSP 인터페이스 영역 프로그램

5. 실험 및 고찰

본 논문에서는 트랜스포트 계층 보호시스템을 개발하고 이를 실험하기 위하여 키 토큰 교환 실험, 보호연관 속성 협상 및 해제 실험, 그리고 보호데이타 전송 실험으로 구분하여 실험하였다. 실험의 첫번째 과정은 키 토큰 교환이며 이때 분배된 키는 보호연관 속성 협상 과정에서 키 참조열로 사용된다. 두번째 과정은 보호연관 속성 협상 및 해제 실험이며, 여기서 협상된 보호연관 속성들은 TLSP를 지원하기 위하여 SMIB에 저장된다. 마지막 과정은 보호데이타 전송 실험으로 보호연관 속성에 기초하여 트랜스포트 계층으로부터의 모든 TPDU를 SE TPDU로 캡슐화하여 보호데이타 전송이 이루어진다.

5.1 키 토큰 교환 실험

보호연관 설정을 위한 첫번째 SA PDU 교환인 키 토큰 교환에서는 D-H 키 분배 알고리듬이 사용되었다. 여기서 모든 가입자에게 공통으로 알려진 공개인수는 GF(p)에서의 원시원 a와 법 p이다. 첫번째 PDU 교환에서 사용되는 원시원 a와 법 p의 값은 다음과 같다. 이 값들은 16진수로 표기되어 있다.

원시원 a :

c5de854fdacf6bac6994b878620779c26a
507047e4ecf98873e8be47113458e3
ea8a1486dfdeb1b8bbfd68043c7d99a240
47a87581b7bc4a7e2a0e3b21b354eb

법 p :

83daf2fa40ee2b131452534203d91d34e9
e2ae21183875a2b877e82ae7428af3
9c5b90dc638bf64aed21c1bab03f8f32c75
0d246b03e3c0392faaf777b43e58c

키 토큰 교환 실험에서, 두 통신 객체가 위의 원시원 a와 법 p를 이용하여 비밀 공유 키 열을 생성하는 과정은 다음과 같다.

통신자 A는 비밀 불규칙 정수 X_A, $a < X_A < p-1$,를 발생하고 키 토큰 1 값인 $Y_A = a^{X_A} \bmod p$ 를 계산한다. X_A와 Y_A의 값은 다음과 같다.

비밀 불규칙 정수(X_A) :

551db5c916101f1a9db3e1df1c48090d22
e1d2f417e2982075e0be987888c505
8dd5921d051d9433f79eb0a8bd7d28b9c
1f0188892f7f4257fe4d968356a65c7

키 토큰 1(Y_A) :

fc711867bd65400cd12eaf96093ac1a8a9
d0bc5cd304b636744462666edc1f80
b4ac4b30374635fb5b9fd0f039b7b1bd9b
2b4232d9b9f9342b77e165ae60b090

통신자 B도 비밀 불규칙 정수 X_B, $a < X_B < p-1$,를 발생하고 키 토큰 2 값인 $Y_B = a^{X_B} \bmod p$ 를 계산한다. X_B와 Y_B의 값은 다음과 같다.

비밀 불규칙 정수(X_B) :

9c8852b19e7dc58928092118010e4434cf
aea0b476f40aaacab27848ff95ccd0
8a9f8a7c0383db8abcd91bee3564ede69d
2067f20dbd4f3e3afbdfe3fc84c28b

키 토큰 2(Y_B) :

42f1dfaaf80bff79353905ff4b19fef4509e9
fe060483dfca0a4d7ab1710ab99
8d75a9d2f15943db52eecd785519ea9b6
7073c49bdf9caaa2873272b5d254cca

첫번째 SA PDU 교환을 통하여 교환된 키 토큰 1과 2를 이용하여 두 통신자는 각각 동일한 키 Z_A와 Z_B를 얻는다. 여기서, Z_A와 Z_B는 다음과 같다.

$$Z_A = (a^{X_B})^{X_A} \bmod p = Z_B = (a^{X_A})^{X_B} \bmod p = a^{X_A X_B} \bmod p$$

Z_A = 1266c9590e39680cd977871ce78df4
c10aa7227a0b851132b678d3d1ef81 4f26
4492f35ed8d779c96c22066741a70
2db1ae524c8c83536534a282abf3e047f54

Z_B = 1266c9590e39680cd977871ce78df4
c10aa7227a0b851132b678d3d1ef814f26
4492f35ed8d779c96c22066741a702
db1ae524c8c83536534a282abf3e047f54

위의 실험 결과에서 통신자 A와 B가 동일한 비밀 공유 키열의 생성을 알 수 있다. 여기서 분배된 비밀 공유 키열은 SMIB에 저장되고 보호연관 속성 협상에서 참조된다. 그 밖에 보호연관 설정을 위한 첫번째 SA PDU 교환을 통하여 비밀 보장 알고리듬으로 DES, 무결성 알고리듬으로 SHA, 그리고 디지탈 서명 알고리듬으로 RSA를 설정하였다.

5.2 보호연관 협상 및 해제 실험

시뮬레이션의 첫번째 과정은 키 토큰 교환이며 이때 분배된 키는 다음 PDU 교환의 암복호화 키로 사용된다. 다음은 인증 및 보호연관 속성 협상 과정으로 여기서 협상된 보호연관 속성들은 TLSP를 지원하며 SMIB에 저장된다. 그림 13은 협상된 보호연관 속성들의 예를 나타낸 것이다.

- SA Identification
  Local_SAID : 61616161
  Peer_SAID : 61616162
  SAID_Len : 4
- Initiator : 00
- Peer_Adr : 490001000050cf48b01
- ASSR_ID : 01.14.0014.13.05.111.
- Protection QOS selected for the SA
  QOS_Label : 0 AC : 2
  DOAuth : 0 CLConf : 0
  CLInt : 2 PEAuth : 2
  COConf : 2 COInt : 0
  COIntr : 0
- Mechanisms selected for the SA
  Label : 01 Conf : 01
  ICV : 01 SN : 01
  PEAuth : 0 1 UNPort : 00
- Label mechanism attributes
  Label_Ref : 167
  Label_Def_Auth : 7a
  Label_Content : f400c6050302020202
- ICV mechanism attributes
  ICV_Alg : 25
  ICV_Len : 160
  ICV_Blk : 0
  ICV_Kg : 0
  ICV_Gen_Key :
  ICV_Check_Key :
- SN mechanism attributes
  Data_Local_SN : f34a182a
  Data_Peer_SN : e8691a5f
- EXSN mechanism attributes
  Data_Local_EXSN : 63fc058b
  Data_Peer_EXSN : e883a149
- Encipherment mechanism attributes
  Enc_Alg : 1e
  Enc_Blk : 64
  Enc_Kg : 0
  Enc_Key : 69b24dcea4a00ac9
  Dec_Key : 93822a24dbe5a45e
- User define
  Local_SN : f349f11a
  Peer_SN : e868f34f
  Local_EXSN : 63fbde7b
  Peer_EXSN : e8837a39
  EX_ICV_Gen_Key :
  EX_ICV_Check_Key :
  EX_Enc_Key : f266150ca5f9a591
  EX_Dec_Key : 28cd2f8d34f48276
  Auth_Mch : 13
  Auth_Gen_Key : 93822a24dbe5a45e
  Auth_Check_Key : 6c97937a79b30a86

그림 13. 협상된 보호연관 속성

분배된 키와 SMIB 내의 저장된 속성들에 따라 보호서비스가 제공되어 데이타 전송이 일어난다. 데이타 전송이 끝나고 보호연관 중지/해제 요구를 받으면, TLSP 객체는 SA-P를 이용하여 보호연관 중지 및 해제를 한다. 보호연관 중지일 경우 TLSP 객체는 보호서비스를 중단하고 보호연관 속성들을 SMIB에 저장한다. 보호연관 해제일 경우 TLSP 객체는 보호서비스를 중단하고 보호연관 속성들을 SMIB에 저장하지 않고 버린다.

5.3 보호데이타 전송 실험

TLSP 객체는 SA-P를 이용하여 초기화된 보호연관 속성에 기초하여 보호서비스를 지원한다. 데이타 전송 시뮬레이션을 위하여 사용되는 메세지는 "This program supports the development of OSI transport security protocol and application."이다.

단계 1 : UNPort를 검사한다. 만약 UNPort가 TRUE이면 TLSP를 처리하지 않는다.
단계 2 : SA-P에서 협상된 보호연관 속성값들을 읽어들인다.
단계 3 : SN = TRUE이면 순서번호를 검사한다.
단계 4 : 보호데이타 영역을 구성한다. 이 영역의 값은 다음과 같다.

c0db546869732070726f6772616d207
37570706f72747320746865206465576

656c6f706d656e7420
6f66204f5349207472616e73706f7274
207365637572697479207072f746f6
36f6c20616e642061
70706c69636174696f6e2e0d0a

단계 5 : Label = TRUE이면 라벨 영역을 구성한다. 이 영역의 값은 다음과 같다.

c68b817af400c6050302020202

단계 6 : 플래그 영역을 구성한다. 이 영역의 값은 00이다.

단계 7 : ICV = TRUE이면, ICV 페드 영역을 구성한다. SMIB의 ICV_Blk = 0이므로 이 영역의 값은 없다.

단계 8 : 보호데이타, 라벨, 플래그 및 ICV 페드 영역을 포함하는 보호 내용 영역을 구성한다. 이 영역의 값은 다음과 같다.

eb00c68b817af400c6050302020202c0
db5468697320707261772616d20737
570706f7274732074
686520646576656c6f706d656e74206
f66204f5349207472616e73706f72742
07365637572697479
2070726f746f636f6c20616e64206170
706c69636174696f6e2e0d0a

단계 9 : ICV = TRUE이면, ICV 영역을 구성한다. 여기서 사용된 무결성 알고리듬은 SHA이며, ICV 영역 값은 다음과 같다.

e42fd28efd60cba89451cecf8b7c74a3f
391be92

단계 10 : Conf = TRUE이면 보호내용 영역과 ICV 영역을 암호화 한다. 여기서 사용된 비밀보장 알고리듬은 DES이며 필요하다면 암호화 페디 영역을 구성한다. 암호화된 영역 값은 다음과 같다.

1ef739482b90c4cef517418d763c3280
f8308ac09022a395e89e01ac0370838c
5804d14f22f34bff
56f98c3c19f8e95095b4825ecd9e584b
6230fa76410bd678cd4d3805f2f1588a
4ef3c2dbb4e52c73
c1772ddaa6b380287ff8ddec16e60794
7d80135235f2da3c4d166d20173345f
40fac67faf8ca06a7
52f26bc2e50dea44c8f4da7396a929f7

단계 11 : 만약 요구된다면 암호화 동기 영역을 구성한다. 이 영역의 값은 1e1e1e1e이다.

단계 12 : 클리어 헤더 영역을 구성한다. 이 영역의 값은 054861616162이다.

단계 13 : 클리어 헤더, 암호화 동기, 보호 내용, 및 ICV 영역을 포함하는 SE TPDU를 구성한다. 구성된 SE TPDU는 다음과 같다.

0548616161621e1e1e1e1ef739482b9
0c4cef517418d763c3280f8308ac0902
2a395e89e01ac0370
838c5804d14f22f34bff56f98c3c19f8e
95095b4825ecd9e584b6230fa76410b
d678cd4d3805f2f1
588a4ef3c2dbb4e52c73c1772ddaa6b3
80287ff8ddec16e607947d80135235f2
da3c4d166d201733
45f40fac67faf8ca06a752f26bc2e50de
a44c8f4da7396a929f7

TLSP 객체가 SE TPDU를 수신하여 송신 과정의 역과정을 수행한 후에 같은 전송 메세지를 얻을 수 있었다.

보호 서비스들에 대한 검증은 다음과 같다. 대등 실체 인증은 접속 식별자를 가지고 있는 접속 설정 PDU의 교환을 보호하므로써 이루어 진다. 대등 실체 인증은 접속형 TLSP에서만 제공된다. 무결성 서비스는 전송 PDU의 보호 헤드 영역에서 PAD 영역까지를 해쉬함수를 취하여 ICV 영역에 넣어서 전송하므로써 제공할 수 있었다. 이때, 알고리듬은 SHA를 사용하였다. 이를 통해 불법적인 방법에 의한 전송 PDU의 손상 유무를 확인할 수 있었다. 비밀 보장 서비스는 전송 PDU의

보호 헤드 영역에서 ICV 영역까지를 암호화하여 전송하므로 제공할 수 있었다. 이때 암호화 알고리듬은 DES 방식을 사용하였다. DES 알고리듬의 암복호 키는 분배된 세션키를 사용하였다. 그러므로 매번 세션 키를 분배하므로써 불법적인 제삼자에게 노출없이 전송이 가능하였다. 접근 제어 서비스는 SE TPDU의 라벨 영역에 의해서 제공할 수 있으며 시스템 관리에 의존적이다.

6. 결 론

본 논문에서는 트랜스포트 계층에서 종점간 사용자 데이타의 보호를 위하여 TLSP와 SA-P를 이용하여 보호시스템을 개발하였다. 보호시스템의 개발을 위하여 TLSP와 SA-P를 분석하고, 표준에서는 권고하지 않았으나 구현에 필요한 세부 사항들을 정의하였다. 그리고 구현 모델을 제시하고 이 모델에 기초하여 보호시스템을 개발하였다.

개발된 보호시스템은 SA-P를 이용한 보호연관 설정 과정과 TLSP를 이용한 보호데이타 교환과정으로 구성되어 있다. 먼저, SA-P를 통하여 TLSP 객체간의 상호인증, 보호연관 속성들의 초기화 그리고 무결성 및 비밀보장을 제공하기 위한 초기 정보의 설정 기능을 제공하였다. 보호연관 설정 과정이 끝난 후 TLSP를 이용하여 대등 실체 인증, 비밀보장, 무결성과 접근제어 서비스를 제공하였다.

개발된 보호시스템이 제공하는 보호서비스와 기능을 실험하기 위하여 UNIX 환경에서 동작하는 ONP LAN 트랜스포트에 TLSP와 SA-P를 이식하여 실험하였다. 키 토큰 교환 실험, 보호연관 설정 및 해제 실험 그리고 보호데이타 전송 실험을 통하여 개발된 보호시스템이 표준에서 권고한 기능들을 제공함을 확인하였다.

참 고 문 헌

[1] ISO/IEC 7498-2, *Information Processing Systems - OSI Basic Reference Model - Part 2 Security Architecture*, 1989.

[2] *Formal Description of the SDNS Security Protocol at Layer 4(SP4)*, NIST, 1992. 3.

[3] ISO/IEC 10736, *Transport Layer Security Protocol*, 1993. 10.

[4] ISO/IEC 10736/AM1, *Transport Layer Security Protocol - Amendment 1: Security Association Establishment*, 1993. 10.

[5] *Open Network Platform(ONP) OSI LAN Transport Release 2.0 Programmer's Guide*, 1991.

[6] *Open Network Platform(ONP) OSI LAN Transport Release 2.0 Administrator's Guide*, 1991.

[7] *Open Network Platform(ONP) OSI Lower Layer Services for: LAN Transport Release 2.1, WAN Transport Release 1.2 Programmer's Guide(Version 0)*, 1993.

[8] *Open Network Platform(ONP) Lower Layer Provider Interface (Version 0)*, 1993.

[9] National Bureau of Standard, *Data Encryption Standard*, U.S. FIPS PUB 46, pp. 254-264, 1977.

[10] National Institutes Standard Technology, *Specification for a Secure Hash Standard(SHS)*, FIPS YY Draft, January 1992.

[11] W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Trans. on Inform. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

[12] National Institute Standard Technology, *Specification for a Digital Signature Standard(DSS)*, FIPS XX Draft, August 1991.

[13] ISO/IEC 8073, *Protocol for providing the Connection-mode Transport Service*, 1993.

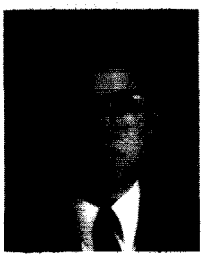
[14] ISO/IEC 8072, *Transport service definition for Open System Interconnection*, 1993.

[15] *NISTIR 4614 Standard Security Label for GOSIP*, An Invitational Workshop.

[16] ITU-T Q2317 X.802, *Lower Layer Security Model*, 1993. 10.

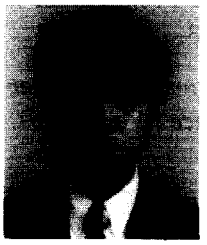
[17] ISO/IEC 9594-8, *Authentication Framework*, 1990. 12.

□ 著者紹介



박 영 호 (정회원)

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



김 기 현

1993년 2월 경북대학교 전자공학과 (공학사)
1993년 3월 ~ 현재 경북대학교 전자공학과 석사과정

문 상 재 (종신회원)

통신정보보호학회논문지 제3권 제2호 참조.

강 신 각 (정회원)

1984년 2월 충남대학교 전자공학과 (공학사)
1987년 8월 충남대학교 전자공학과 (공학석사)
1984년 3월 ~ 현재 한국전자통신연구소 정보통신표준연구센터 선임연구원