論文98-35S-4-1

인터네트워크에서의 전송데이타 보호시스템 개발

(A Development of Security System for Transmission Data in the Internetwork)

朴 暎 昊 *, 李 國 熙 **, 文 相 在 **

(Young-Ho Park, Kuk-Heui Lee, and Sang-Jae Moon)

요 약

본 논문에서는 인터네트워크에서 보호서비스를 제공하기 위한 새로운 보호시스템을 개발한다. 본 시스템에 사용한 보호모델은 인터네트워크의 중간 시스템에서 인증 및 무결성 서비스를 제공하며 비밀보장 서비스는 제공하지 않는다. 따라서, 본 모델은 인터네트워크의 중간 시스템에서 전송 데이타의 인증 및 무결성을 알 수 있으며 구현이 간단하고 안전하다. 또한, 본 논문에서는 개방형시스템 환경을 제공하는 USL(UNIX system laboratory)의 ONP(open network platform)를 사용하여 인터네트워크 전송데이타 보호시스템을 개발한다.

Abstract

This paper developments a security system for transmission data in the internetwork. Intermediate system of our model does not fulfill security service of confidentiality but authentication and integrity. Thus this model knows whether the transmission data on the intermediate system is authentic and integral or not, and it is practical and easy to be developmented. This system is developmented using a ONP of USL which prvides environments of the open system.

I. 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 인터네트워크에 연결되어 있는 상황에서는 더욱 심각하다[1]. 따라서 이를 막을 수 있는 대책이 필요하다.

인터네트워크에서 안전한 통신을 위한 보호 프로토콜로는 IP(internet protocol)에서의 보호 및 OSI 구조에 기초한 보호 프로토콜[2,3]이 있다. IP는 1995년 RFC(IPv6, internet protocol version 6)[4,5]가 발표되었으며 데이타를 보호하기 위하여 선택영역을 이용하고 있다. OSI 구조에 기초한 인터네트워크 보호 프로토콜은 네트워크 계층 레벨에서 보호가 이루어지고 있으며 NIST의 SP3(security protocol 3)[6]과 ISO/IEC의 표준안인 NLSP(network layer security protocol)[3]가 있다. 이러한 보호 프로토콜들에서는 인터네트워크에서 보호서비스를 제공하기 위하여 종단 시스템에서만 보호서비스를 설정하는 방식과 종단 및 중간 시스템에 동일한 보호서비스를 설정하는 방식이 있으나 인터네트워크 환경을 고려한 보다 효율적인 보

* 正會員, 尙州産業大學校 電子電氣工學科
(Dept. of Electronics and Electrical Eng., Sangju National Polytechnic Univ.)
** 正會員, 慶北大學校 電子電氣工學部
(School of Electronics and Electrical Eng., Kyungpook National Univ.)
※ 본 연구는 '96 과학재단 핵심전문(KOSEF 961-0905-030-2)의 지원에 의해 이루어 졌슴
接受日字: 1997年4月10日, 수정완료일: 1998年3月30日

호체계가 요구된다.

본 논문에서는 인터네트워크에서 보호서비스를 제공하기 위하여 종단 시스템간에는 비밀성이 유지되며 종단 시스템과 중간 시스템간 그리고 중간 시스템들 간에 인증 및 무결성이 제공될 수 있는 보호시스템을 개발한다. 본 시스템에서 사용한 보호모델[7,8]은 인터네트워크의 중간 시스템에서 단편화 과정을 효율적으로 처리할 수 있고 비밀보장 서비스가 종단 시스템간에 제공되며 중간 시스템에서는 제공되지 않으므로 구현이 비교적 간단하고 안전하다. 본 논문에서는 D-H형[9,10] 키 분배 프로토콜을 이용하여 인터네트워크 보호모델에 적합한 키 분배 프로토콜을 제시한다[8]. 제시한 키 분배 프로토콜은 인터네트워크 보호모델에 적합하며 식별자를 사용하여 인증기능을 갖는다. 또한, 본 논문에서는 UNIX system V 용으로 개방형 시스템 환경을 제공하는 USL(UNIX system laboratory)의 ONP(open network platform)[11-13]를 사용하여 인터네트워크 보호시스템을 개발한다.

Ⅱ. 인터네트워크 보호영역 모델

인터네트워크에서 안전한 통신을 위한 보호 프로토콜로는 IP 보호 프로토콜 및 OSI 구조에 기초한 보호 프로토콜이 있다. 인터네트 프로토콜은 1995년 RFC가 발표되었으며 선택영역을 이용하여 보호를 제공하고 있다. OSI 구조에 기초한 인터네트워크 보호 프로토콜은 네트워크 계층 레벨에서 보호가 이루어지고 있으며 NIST의 SP3과 ISO/IEC의 표준안인 NLSP가 있다.

NLSP와 SP3은 비밀보장, 무결성 그리고 인증 서비스를 제공하며 보호영역은 그림 1과 같다. 그림 1(a)는 신뢰할 수 없는 중간(intermediate) 시스템으로 접속된 경우의 인터네트워크 보호영역을 나타낸 것이다. 이 경우는 네트워크 제공자 및 침입자(intruder)로부터 종단 시스템을 보호하는 방식이다. 중간 시스템에서 보호서비스가 제공되지 않으므로 구현은 비교적 간단하나 네트워크 상에서 전송 데이타의 인증 및 무결성 여부를 알 수 없는 단점이 있다. 그림 1(b)는 신뢰할 수 있는 중간 시스템으로 접속된 경우의 인터네트워크 보호영역을 나타낸 것이다[7,8]. 이 경우는 침입자로부터 종단 시스템 및 중간 시스템을 보호하는 방식이다. 모든 중간 시스템에서는 종단 시스템과 동등한 보호서비스가 제공되므로 전송 데이타의 인증, 무결성 그리고 기밀성 여부를 알 수 있으나 한 중간 시스템이 침입자로부터 노출될 경우 전송 데이타의 모든 내용이 노출되는 단점이 있다. 따라서 모든 중간 시스템에서는 인증, 무결성 그리고 비밀보장 서비스에 관련된 모든 정보들을 안전하게 관리해야 하는 구현상 어려움이 발생한다. SP3과 NLSP에서 전송되는 데이타의 PDU(protocol data unit) 구조는 그림 2와 같다. 그림 2의 PDU에서 ICV(integrity check value) 영역은 무결성 검사를 위한 영역이며 암호화 영역은 비밀성을 제공하는 영역이다.

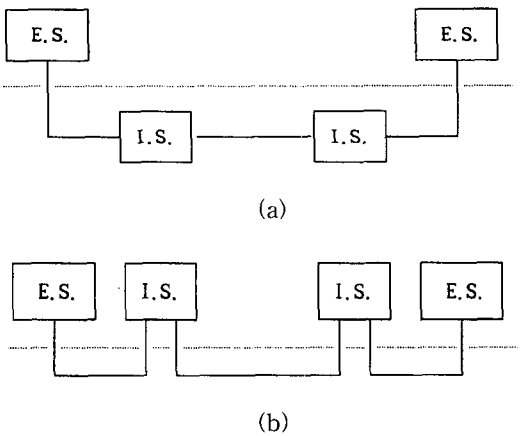


그림 1. SP3과 NLSP에서의 인터네트워크 보호 영역 (a) 신뢰할 수 없는 중간 시스템으로 접속된 경우의 인터네트워크 보호영역 (b) 신뢰할 수 있는 중간 시스템으로 접속된 경우의 인터네트워크 보호영역

Fig. 1. The protection boundary of internetwork in SP3 and NLSP. (a) The protection boundary with untrusted intermediate system. (b) The protection boundary with trusted intermediate system.

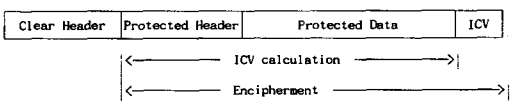


그림 2. SP3과 NLSP에서의 PDU 구조

Fig. 2. The PDU structure in NLSP and SP3.

본 논문에서는 인터네트워크의 특성을 고려하여 그림 3과 같이 2중화 보호영역을 제시한다. 그림 3에서 보호영역 α는 통신자간의 비밀성을 제공하는 영역이다. 인터네트워크의 중간 시스템에서는 전송데이타의

내용을 노출시킬 필요가 없으므로 비밀보장 서비스를 제공하지 않아도 된다.

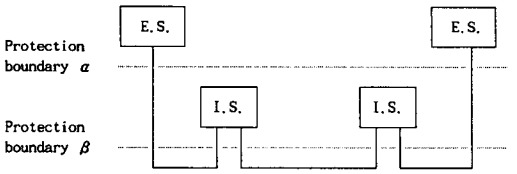


그림 3. 제안한 인터네트워크 보호영역
Fig. 3. The proposed protection boundary in internetwork..

그림 3에서 보호영역 β는 네트워크상에서 인증 및 무결성을 제공하는 영역이다. 인터네트워크에서는 각 네트워크에서 전송할 수 있는 데이타의 최대 전송크기(MTU,maximun transmission unit)를 다르게 규정하므로 단편화 과정이 이루어지고 중간 시스템에서는 전송 단편들의 인증 및 무결화 과정이 필요하다.

이러한 중간 시스템에서의 인증 및 무결성 서비스는 각 네트워크에서 전송 데이타의 투명성을 제공하므로 네트워크 상에서 트래픽 양을 감소시킬 수 있다.

제안된 보호영역 모델에서 그림 2의 NLSP PDU를 사용할 경우 네트워크상에서 단편화 과정이 발생하면 중간 시스템에서는 암호화 영역을 복호할 수 없으므로 수신된 PDU의 ICV 영역을 검사할 수 없으며 전송할 단편들의 무결성 검사를 위해 ICV 영역을 재 설정해야 하는 문제가 발생한다. 따라서 제안한 보호체계에 적합한 PDU를 그림 4와 같이 제시한다.

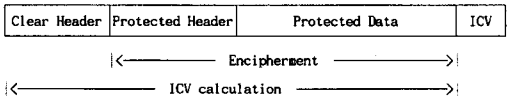
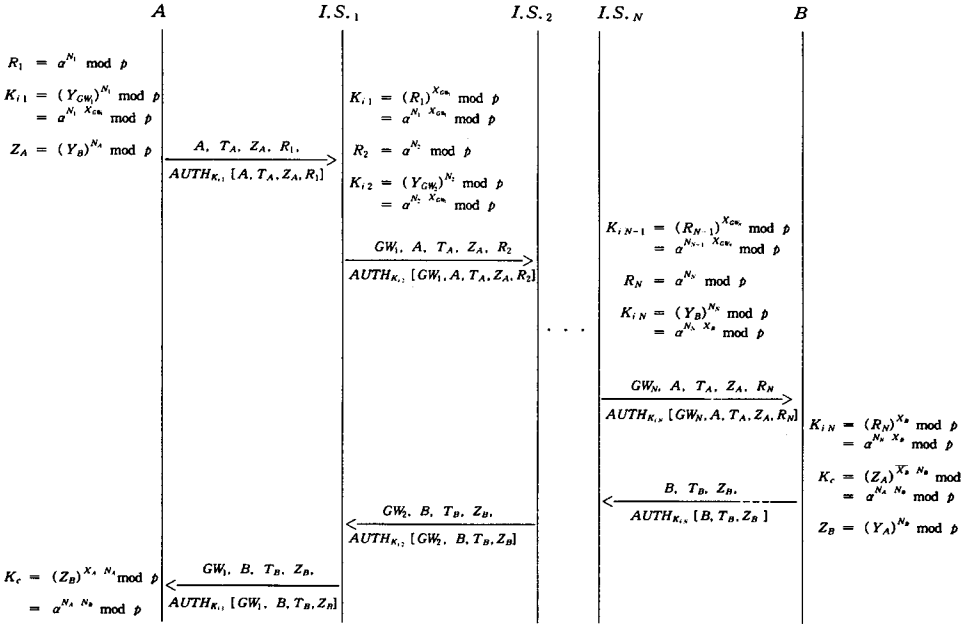


그림 4. 제안한 인터네트워크 보호 시스템을 위한 PDU 구조
Fig. 4. The PDU structure for the proposed security system in internetwork.



where, A,B : User, K_c : Confidentiality key,
GW : Gateway, $K_{i1}, K_{i2}, \cdots K_{iN}$: Integrity key,
T_A, T_B : Time stamp,
$N_A, N_B, N_1, N_2, \cdots N_N$: Random number,
$AUTH_{K_{i1}}[A, T_A, V_A, R_1] = E_{K_{i1}}[FHASH(A, T_A, V_A, R_1)]$

그림 5. 인터네트워크에서 인증 기능을 갖는 키 분배 프로토콜
Fig. 5. The key distribution protocol with an authentication function in internetwork.

그림 4에서 PDU는 보호영역을 먼저 암호화 한후 전체 PDU에 대해 무결성 검사를 하여 ICV 영역을 발생한다. 제안한 보호영역에서 종단 시스템간에는 비밀보장 서비스를 제공하며 중간 시스템에는 비밀보장 서비스를 제공하지 않으므로 중간 시스템에서 전송 데이타의 내용을 알 수 없다. 무결성 서비스는 중간 시스템에서도 제공할 수 있으므로 네트워크 상에서 단편화 과정이 일어날 경우에도 무결성 서비스를 제공할 수 있다.

Ⅲ. 키 분배 프로토콜

암호화 방법에는 크게 대칭 키 암호화 방법 및 비대칭 키 암호화 방법이 있다. 대칭 키 암호화 방법은 처리속도가 빠르고 구현이 간단하나 키 관리가 문제된다. 비대칭 키 암호화 방법은 처리속도가 상대적으로 느리지만 키 관리 및 인증의 기능을 효과적으로 수행할 수 있다. 따라서 일반적으로 정보보호를 위한 암호화 시스템의 구현에서 키 분배에는 비대칭 암호화 방법을 이용하고 이 분배된 암호화 키를 사용하여 전송 데이타의 암복호에는 대칭 키 암호화 방법을 이용한다.

본 논문에서는 무결성 키 분배를 위하여 ElGamal 방식[9]을 비밀보장 키 분배를 위하여 Matsumoto-Imai 방식[10]을 이용하여 본 논문에서 제안한 인터네트워크 보호영역 모델에 적합한 인증 기능을 갖는 키 분배 프로토콜을 그림 5와 같이 제안한다[8]. 본 키 분배 프로토콜은 중간 시스템을 N개라 고려하여 구성하였으며 보호연관 설정시 이루어진다.

Ⅳ. 인터네트워크 보호시스템 개발

본 논문에서는 제안한 인터네트워크 보호시스템을 개발하기 위하여 USL의 ONP를 사용한다. ONP는 UNIX system V용으로 설계된 네트워킹 프로그램, 도구(tool) 및 응용의 집합으로써 개방 시스템 응용의 설계, 개발 그리고 실험을 위한 실험적 환경을 제공한다. ONP가 UNIX system V 용으로 개발된 이유는 장기적으로 볼 때 OSI 환경의 운용체계에 알맞으며, 이식과 기능 향상(upgradable)이 용이하고 표준 응용 서비스를 제공하기 때문이다.

본 논문에서는 그림 6의 ONP WAN/LAN 트랜스포트 패키지 구조 중 ONP LAN 트랜스포트를 구성하고 커널(kernel)상에 존재하는 프로토콜 스택에 개발한 프로토콜을 이식시켜 보호시스템을 개발하였다.

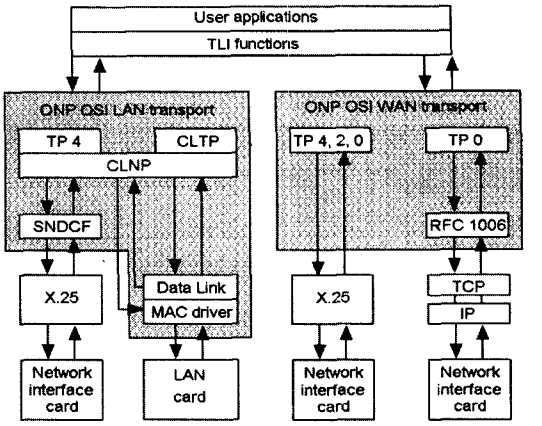


그림 6. ONP LAN/WAN 트랜스포트
Fig. 6. LAN/WAN transport in ONP.

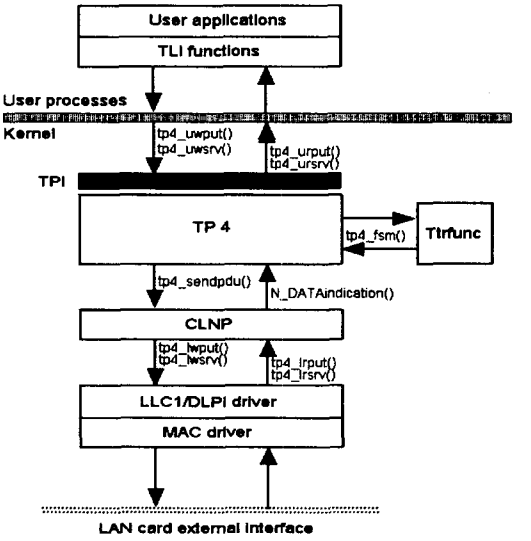


그림 7. ONP LAN 트랜스포트의 구성
Fig. 7. The construction of LAN transport in ONP.

그림 7은 ONP LAN 트랜스포트의 구성을 나타낸 것이다. ONP LAN 트랜스포트는 사용자 처리, 커널과 LAN card로 구성되며 커널은 TPI(transport provider interface), TP4, CLNP, LLC/DLPI(logical link control/data link provider interface) driver 그리고 MAC(medium access control) driver로 이루어져 있다. 본 논문에서는 인터

네트워크 보호시스템을 USL의 ONP상에서 구현하여 실험하기 위하여 비접속 네트워크 계층 프로토콜 상단에 보호를 위한 부계층을 첨가하였다. 이 부계층은 NLSP_sendtpdu()와 NLSP_DATAindication() 루틴을 tp4_sendtpdu()와N_DATAindication() 함수에 추가함으로써 인터페이스 된다. 그림 8은 개발된 프로그램 중 인터페이스 영역을 나타낸 것이다.

보호시스템에 필요한 보호관리 정보인 SMIB는 미리 공유하고 있다고 가정하였으며 DES[14] 및 MD5[15]의 보호 알고리듬을 구현하여 사용하였다. 이러한 보호 알고리듬들은 486 PC(50 MHz)상에서 수행시간이 수 ms에서 수십 ms 정도 소요되므로 실시간 구현이 가능하였다.

```
#include "includes.h"
#include "/int-s/NLSPProvider.c"

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

        check = NLSP_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++;
        }
}

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 = NLSP_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);
}
```

그림 8. ONP 상에서의 인터페이스 프로그램
Fig. 8. The interface program in ONP.

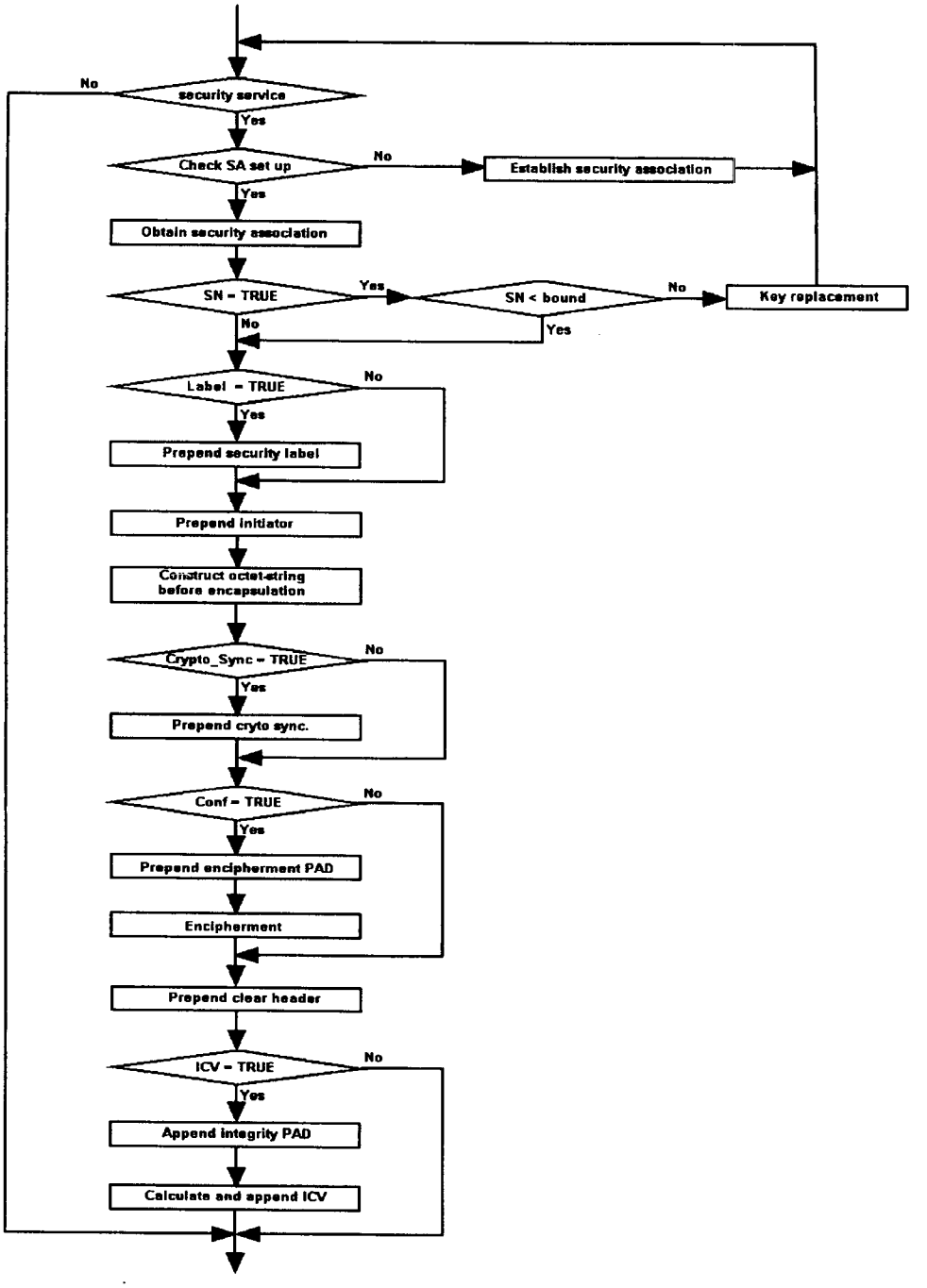


그림 9. 송신 흐름도
Fig. 9. The flowchart of transmission.

본 논문에서 구현한 보호시스템의 송·수신 절차는 다음과 같다. 그림 9는 종단 시스템의 송신절차를 나타낸 것이다. 송신 객체가 보호요구 프리미티브를 받으면, 보호연관 속성이 저장되어 있는 SMIB에 접근한다. 객체는 발신처 및 수신처 주소를 이용하여 보호연관 속성들을 찾는다. 만약 보호연관 속성이 존재하지 않을 경우, 보호연관을 설정한다. 보호연관이 SMIB 내에 존재할 경우, 보호 헤드, 비밀보장을 위한 암호화, 비보호 헤드 그리고 무결성을 위한 ICV를 계산하여 SE PDU로 캡슐화 한다. 그 후에 송신 객체

는 발신처와 수신처 주소, SE PDU 및 QOS로 구성된 UN 서비스 요구 프리미티브를 형성하여 하위 계층으로 전달한다.

그림 10은 종단 시스템의 수신절차를 나타낸 것이다. 수신 객체는 하위 계층으로부터 지시 프리미티브를 받으면 PDU의 형태를 검사한다. SE PDU일 경우, 프리미티브의 인자인 주소와 SAID를 이용하여 SMIB 내의 보호연관을 찾아 PDU에 적절한 메카니즘을 적용한다. 먼저 ICV를 검사하고 비보호 헤드 영역을 검사한 후 PDU를 복호한다. 그리고 보호 내용

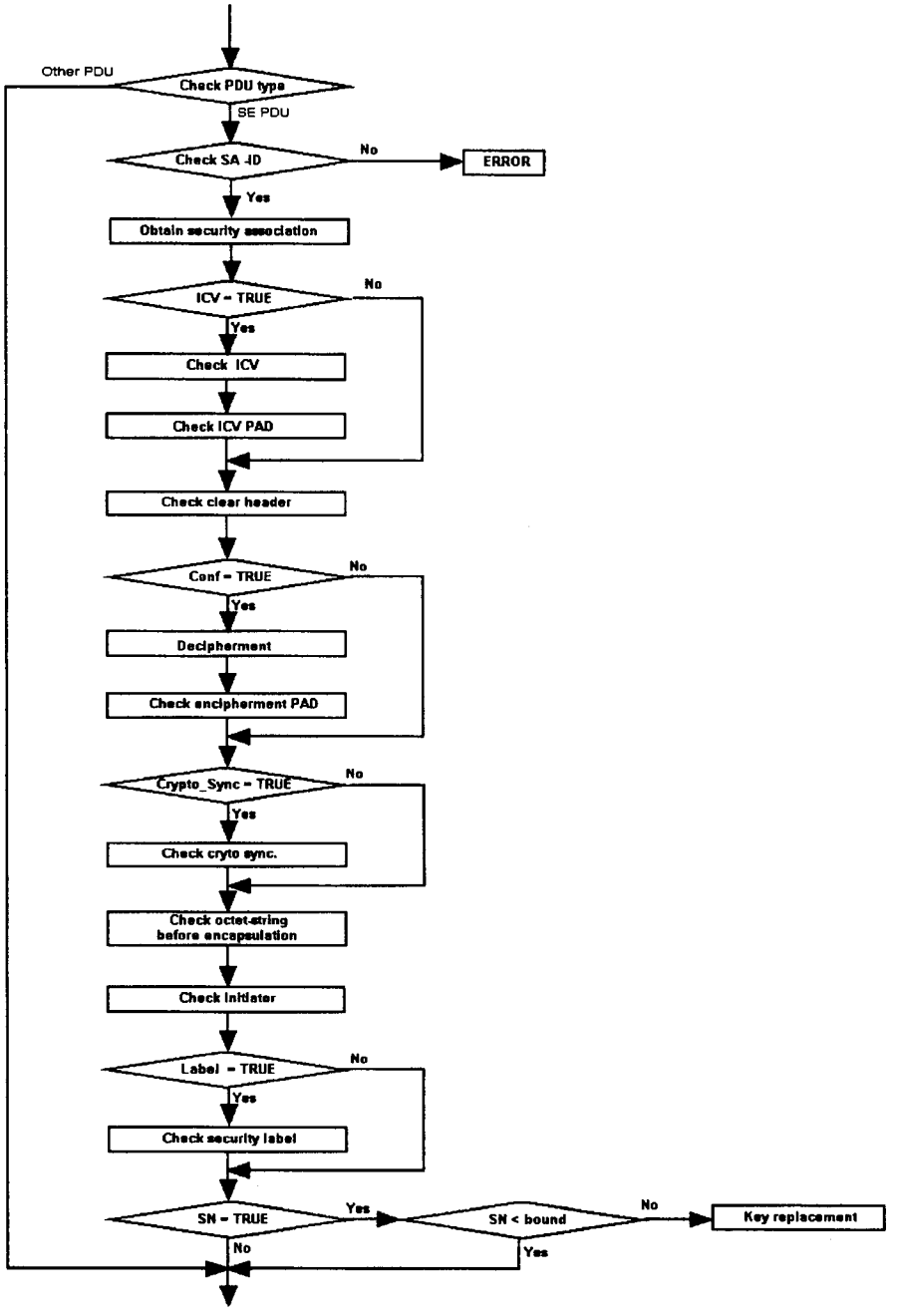


그림 10. 수신 흐름도
Fig. 10. The flowchart of reception.

영역을 검사한 후, 지시 프리미티브를 형성하여 지정된 스택으로 가게 된다. 송·수신 과정 중 SN (sequence number)이 보호연관에 설정된 Data_local_SN이나 Data_peer_SN 값을 초과할 경우, 키 대체 과정을 수행한다. 여기서 Data_local_SN는 송신한 데이터의 순서번호이며 Data_peer_SN는 수신한 데이터의 순서번호이다.

중간 시스템에서의 송·수신 절차는 종단 시스템에서의 송·수신 절차 중 라벨과 시작자를 포함하는 캡슐화 전 옥테트 스트링을 구성하는 과정, 암호 동기 과정 그리고 암호화 과정이 제외되며 나머지 절차는 동일하다.

V. 결 론

본 논문에서 개발한 인터네트워트 보호시스템은 종단 시스템간에는 비밀성이 유지되며 종단 시스템과 중간 시스템간 그리고 중간 시스템들간에 인증 및 무결성이 제공된다. 따라서 본 시스템은 인터네트워크의 중간 시스템에서 비밀보장 서비스가 제공되지 않으므로 구현이 비교적 간단하고 중간 시스템이 노출될 경우에도 비밀보장 키는 노출되지 않으므로 안전하다. 본 키 분배 프로토콜에서는 무결성을 위한 키를 분배하기 위하여 일방 간접 인증 기능을 갖는 one-pass 메카니즘인 ElGamal 방식을 이용하며 비밀보장을 위한 키를 분배하기 위하여 D-H형 방식을 이용하였다. 개발한 인터네트워크 보호시스템은 UNIX system V용으로 개방형 시스템 환경을 제공하는 USL의 ONP를 486 PC에 설치하여 사용하였으며 비접속 네트워크 계층 프로토콜에 제안한 방식들을 이식하여 개발하였다. 보호시스템에 필요한 보호관리 정보인 SMIB는 미리 공유하고 있다고 가정하였으며 DES 및 MD5의 보호 알고리듬을 구현하여 사용하였다. 이러한 보호 알고리듬들은 486 PC(50 MHz)상에서 수행시간이 수 ms에서 수십 ms 정도 소요되므로 실시간 구현이 가능하였다.

참 고 문 헌

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

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

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

[4] Network Working Group, *Internet Protocol Version6 (IPv6) Specification*, RFC 1883, Dec. 1995.

[5] Network Working Group, *Security Architecture for the internet Protocol*, RFC 1825, Aug. 1995.

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

[7] Young-Ho Park and Sang-Jae Moon "Protection boundary for internetwork security," *IEE Electronics Letters*, vol.31, no.10, pp.776-778, May 1995.

[8] Young-Ho Park and Sang-Jae Moon "Protection Boundary and Protocol for Internetwork Security," *KITE Journal of Electronics Engineering*, vol.7, no.2, pp.1-6, June 1996.

[9] T. El-Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. on inform. Theory*, vol. IT-31, July 1985.

[10] T. Matsumoto, Y. Takashima, and H. Imai "On Seeking Smart Public-Key-Distribution Systems," *IEICE Trans.*, vol. E69, no. 2, February 1986.

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

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

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

[14] NBS, *Data Encryption Standard*, U.S. FIFP PUB 46, pp.1-18, January 1977.

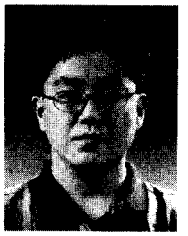
[15] R.Rivest, *The MD5 Message Digest algorithm*, Requests for Comments (RFC) 1321, 1992.

저 자 소 개

朴 暎 昊(正會員)

1966년 10월 17일생. 1989년 2월 경북대학교 전자공학과 졸업(공학사). 1991년 2월 경북대학교 대학원 전자공학과 졸업(공학석사). 1995년 8월 경북대학교 대학원 전자공학과 졸업(공학박사). 1996년 3월 - 현재 상주산업대학교 전자전기공학과 조교수. 주관심분야는 정보보호이론 및 컴퓨터통신 등임

文 相 在(正會員) 第 31卷 A編 第 9號 參照
현재 경북대학교 전자전기공학부 교수



李 國 熙(正會員)

1969년 8월 7일생. 1993년 2월 경북대학교 전자공학과 졸업(공학사). 1995년 2월 경북대학교 대학원 전자공학과 졸업(공학석사). 1995년 3월 - 현재 경북대학교 대학원 전자공학과 박사과정. 주관심분야는 정보보호이론 및 이동통신 등임