通信情報保護學會論文誌
第 8 卷 第 1 號, 1998. 3

ISDN에서의 안전한 패킷교환 서비스를 위한 키 분배 프로토콜과 호 제어

김 봉 한*, 이 재 광**

Key Distribution Protocol and Call Control for Secure Packet-Switched Service in ISDN

Bong-Han Kim, Jae-Kwang Lee

요 약

ISDN에서는 모든 정보가 디지털 형태로 전송되고 통신망 접속이 개방성을 갖기 때문에 중요 정보 자원에 대한 정보보호 문제점이 날로 증가하게 되었다. 따라서 이러한 불법적인 침입자에 의하여 우연 또는 의도적인 침입 위협에 대한 정보보호의 필요성이 절실히 요구되는 실정이다. 그러므로 본 논문에서는 ISDN 패킷교환방식의 가상회선 서비스에서, 비밀키 암호화 시스템과, 비밀키와 공개키 암호화 시스템을 결합한 하이브리드 암호화 시스템을 이용하여 사용자 상호간의 안전한 인증 절차를 제안하였다. 또한 네트워크 내부에 인증센터를 설치하지 않고 네트워크 외부에 인증센터를 설치하여 호 설정 과정 중에 사용자 상호 인증이 이루어짐으로, 보다 신속하고 안전하게 사용자의 중요 정보를 전달할 수 있는 키 분배 프로토콜과 호 제어 방식을 제안하였다.

Abstract

In the ISDN, security problems that threat and intrusion about important information resource increase because every information is transferred in the form of digital access of network has patency. We have need of security which protect important information from illegal intruder. In this paper, propose a secure authentication procedure between users using a secret key cryptosystem and a hybrid cryptosystem in virtual call service of packet-switched ISDN. And propose a key distribution protocol and call control. while call establishment procedure, It can securely transfer important information using a certification authority which is configured not within but outside of the network. It has no effect on the call establishment procedure, and can implement authentication and digital signature for users

* 한남대학교 컴퓨터공학과 박사과정
** 한남대학교 컴퓨터공학과 부교수

1. 서 론

ISDN은 다양한 종류의 정보 서비스를 종합적으로 제공할 수 있도록 하나의 회선을 통하여 가입자의 통신망을 디지털 방식으로 접속한다. ISDN은 음성 및 비음성 서비스를 통합하여 처리할 수 있으며, 회선교환 및 패킷교환을 동시에 제공한다. 그러나 모든 정보가 디지털 형태로 전송되고 통신망 접속이 개방성을 갖기 때문에 중요 정보 자원에 대한 위협이 날로 증가하게 되었다. 따라서 기존의 통신망과 연동 또는 통합하여 다양한 정보 서비스를 제공하는 ISDN에서의 사용자 중요 정보 자원의 취약성에 따른 불법적인 침입자에 의해 우연 또는 의도적인 침입 위협에 대한 대책이 절실히 요구되는 실정이다. 또한 ISDN에 대한 통신 기술과 병행하여 정보보호 메커니즘이 개발 진행되지 않았으며 정보보호 메커니즘이 통신망 운용에 장애가 되고 상호 연동과 통합에 제한이 될 수 있기 때문에 이를 해결하기 위한 ISDN 정보보호 구조와 정보보호를 위한 키 체계의 개발이 매우 중요한 연구과제로 대두되고 있다.

ISDN에서는 초기 ISDN 음성-중심 네트워크와 현재의 ISDN에서 필요한 정보보호 서비스에 대한 연구가 계속되어 왔다. 그러나 ISDN에서의 사용자 통신 정보에 대한 비밀유지를 보호하기 위한 체계적인 방법이 아직 없을 뿐만 아니라 침입자의 가로채기, 내용 알아내기, 통신 내용 변경이나 위조 등이 비교적 쉽게 발생하고 있다. 더구나 네트워크 사용자의 인증을 위한 효과적인 방법인 표준안도 아직 없는 실정이다. 그러므로 ISDN에서의 정보보호 서비스에 대한 필요성은 더욱 더 커지고 있다[9]. 또한 ITU-T 권고 Q.931의 호 설정 절차를 그대로 유지하고 호 설정의 성능을 저하시키지 않으면서 키를 안전하고 빠르게 분배하고 인증을 할 수 있는 암호화 방법에 대한 연구가 필요하게 되었다.

따라서 본 논문에서는 패킷교환 시스템의 구조를 분석하고, 비밀 키 암호화 시스템과 비밀 키 암호화와 공개 키 암호화 시스템을 결합한 하이브리드 암호화 시스템을 이용하여, ISDN의 패킷교환 서비스의 호 설정 과정 중에서 신속하고 안전하게 중요 정보를 전달할 수 있는 키 분배 프로토콜과 호 제어 방식을 제안하였다.

2. PHS(Packet Handler Subsystem) 구조

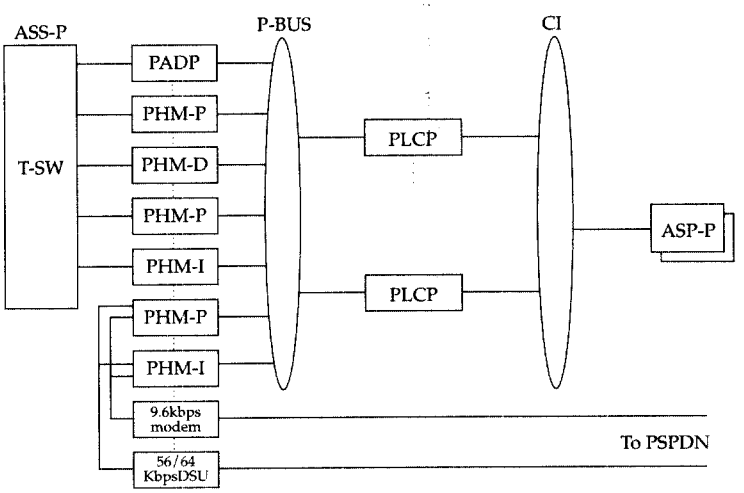
ISDN 교환기인 TDX-10에서 패킷교환 기능은 CCITT 권고안 X.31의 Case B 방식에 따라 구현되고 있다. 패킷교환기의 역할을 하는 TDX-10 패킷 처리 서브시스템(PHS : Packet Handler Subsystem)은 모든 패킷 트래픽이 집중되는 집중형 구조로서, 패킷의 실시간 처리를 요구하는 기능을 수행하는 부분은 적은 전송 지연을 갖고 많은 패킷을 처리할 수 있도록 하였다.

패킷 처리는 PHS에서 수행된다. 타임 스위치의 Nail-Up 경로를 거친 패킷은 해당 패킷 처리 모듈 (PHM : Packet Handler Module)에서 처리된다. Layer 2가 처리된 후 패킷 포맷으로 정리되고, Layer 3에서 데이터 전달도 PHM에서 처리된다. B 채널교환은 D 채널을 통한 사용자-망 간 신호방식에 의하여 B 채널이 PHS에 64Kbps의 회선으로 연결된 후 X.25 프로토콜에 의해 교환이 이루어진다. D 채널 패킷교환은 ISDN 사용자 정합 서브시스템 내에서 통계적으로 다중화된 후 PHS에 64Kbps의 고정 경로를 통해 연결되어 서비스된다.

PHS는 그림 1과 같이 TDX-10 시스템 특성의 하나인 분산제어구조 개념을 적용한 실시간 처리 특성과 용량 증대에 유연하게 대처할 수 있도록 설계되었으며, PLCP(Packet Level

Control Processor)에서는 패킷 호 설정 및 해제 등을 제어하고, PHM은 그 기능에 따라 B 채널 패킷 호를 처리하는 PHM-B, D 채널 호를 처리하는 PHM-D, TDX-10 ISDN간의 연동을 위한 PHM-1, PSPDN과 망 연동을 위한 X.75를 처리하는 PHM-P로 구분된다. PLCP 및 PHM으로부터 메시지를 상호 교환하는 PBUS가 구성된다. PLCP는 비 실시간 처리기능을 수행하는데 PHM(Packet Handling Module)이 DTE 혹은 망으로부터 호 요구 패킷을 수신한 후 가상 호 설정을 위해 라우팅 데이터를 요구하면 착신주소를 번역하고 라우팅 데이터 베이스를 액세스하여 PHM에 라우팅 정보를 제공하는 패킷 호 제어 및 라우팅 정보 처리 기능 등의 일을 수행한다. PHM은 X.25 링크 레벨 기능, 패킷 레벨 기능 및 패킷 시스템 내부 프로토콜 처리 기능 등을 수행한다. 링크 레벨 기능은 X.25/X.75 LAPB 프로토콜을 처리하며, 패킷 레벨 기능은 상위 프로세서인 PLCP의 제어를 받아 가상 호 설정 및 해제 기능을 수행한다. 패킷 시스템 내부 프로토콜 PIP(Packet System Internal Protocol)는 전송 지연을 적게 하기 위하여 수행되는 착, 발신 노드간의 end-to-end 프로토콜로서 패킷 흐름 제어, 패킷 전송 순서 제어, 패킷 재전송 등의 기능을 수행한다.

PBUS(Packet Bus)는 독립된 2개의 10Mbps 고속버스로서의 기능을 갖는데 PHM 상호간 패킷 데이터 전달 및 PLCP 호 제어 관련 메시지의 통신을 담당한다. PBUS는 2단계의 분배 절차를 거쳐 PLCP와 PHM이 차례대로 패킷을 전송할 수 있도록 한다. PADP(Packet Assembly Disassembly Processor)는 PSTN(Public Switched Telephone Network)의 C-DTE에 대한 패킷교환 서비스를 제공하기 위해 CCITT X.3, X.28, X.29 기능을 수행하며, C-DTE로부터 들어오는 데이터를 패킷으로 바꾸거나(Packet Assembly), 그 역의 기능(Disassembly) 등을 담당한다. PADP는 PBUS와 고속의 내부 데이터 링크로 연결되어 PHM과 패킷을 상호 교환한다[15].



PHM : Packet Handling Module
ASP-P : Access Switching Processor for Packet
ASS-P : Access Switching Subsystem for Packet
CI : Control Interworking
PLCP:Packet Layer Control Processor
P-BUS : Packet BUS
T-SW : Time Switch

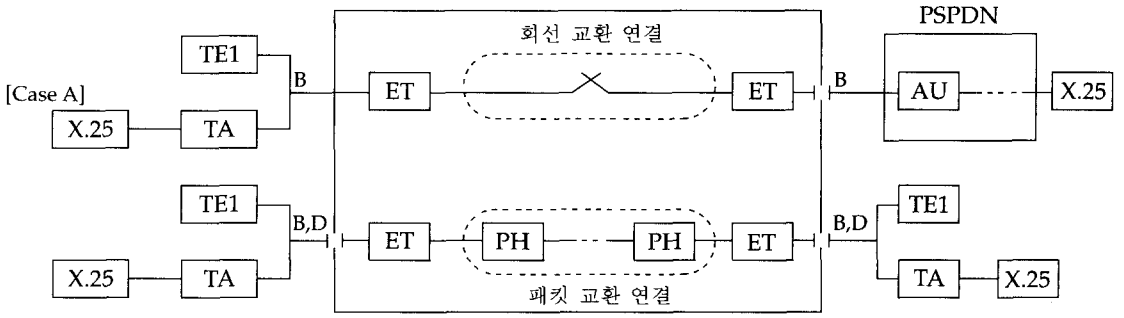
그림 1. Packet Handler Subsystem 구조

3. ISDN에서의 패킷교환 서비스

ISDN에서 패킷교환 서비스를 제공하는 ISDN 패킷 권고안 X.31에 의한 접근은 패킷 데이터 망을 위해 기존에 개발된 패킷 프로토콜인 X.25와 X.25에 기반을 둔 기존의 패킷 데이터 망을 최대한 사용한다. X.31에 의한 접근에서, 연결은 일반 ISDN 절차에 따라서 먼저 ISDN 패킷모드 터미널에서 X.25 패킷-핸들링 기능까지 확립한다. 그리고 이 둘 사이에서의 패킷통신은 일반 X.25 절차에 따라서 연결을 확립한다.

ISDN에서 중요한 패킷교환 서비스의 두 가지 경우는 그림 2와 같다.

a) A 경우 : 패킷교환 공중 데이터 망(PSPDN)에 대해 회선모드 연결을 이용한 패킷교환 서비스
b) B 경우 : ISDN내의 패킷교환 서비스



TE1 : ISDN terminal(packet mode)
TA : Terminal adaptor
X.25 : X.25 terminal
ET : Exchange terminal
PH : Packet handler
AU : Access unit
PSPDN : Packet-switched public data network

그림 2. ISDN에서 두 가지 경우의 패킷교환 서비스

3.1 X.31 A 경우

권고안 X.31 A 경우는 PSPDN 서비스로의 접속을 기술한다. 이 경우에서 ISDN이 패킷모드 서비스를 제공할 수 없으나 패킷처리기에 회선모드의 접속을 제공할 수 있다. 패킷교환 호는 X.25 DTE에 의해 시작되고, TA를 투명하게 통과한다. 그리고 패킷교환 호는 ISDN 회선모드 전송서비스를 요구하고 Q.931 프로시저를 사용하는 AU의 주소를 제공한다. 원래 DTE는 ISDN을 사용하여 PSPDN의 X.25 DCE에 회선교환 연결을 설정한다. 다른 DTE에는 X.25 가상 호 프로시저를 사용하는 PSPDN을 통해서 접속한다. 그래서, ISDN은 멀리 떨어진 AU에 접속시키기 위해서 두 ET 사이에 교환 연결을 한다. 또는 ET는 지역

AU에 직접 연결되기도 한다.

D 채널은 주로 DSS 1 프레임(LAPD)과 메시지(Q.931)를 전송하기 위해 ISDN에서 사용된다. D 채널은 본래 패킷교환 채널이다. 그러나 D 채널과 DSS 1 프로시저는 LE에서 끝난다. LE에 도달한 LAPD 프레임과 Q.931 신호 메시지는 ISDN이나 네트워크를 통해 전달되지는 않는다. X.31 A 경우에 있는 LE가 패킷을 교환할 수는 없고 D 채널이 회선모드 트래픽을 전송할 수 없기 때문에 D 채널은 단지 사용자-망 사이의 신호화를 위해 예비용으로 사용되고 패킷모드 서비스로는 사용될 수 없다. 사용자는 B 채널로만 패킷모드 전송을 할 수 있다[13].

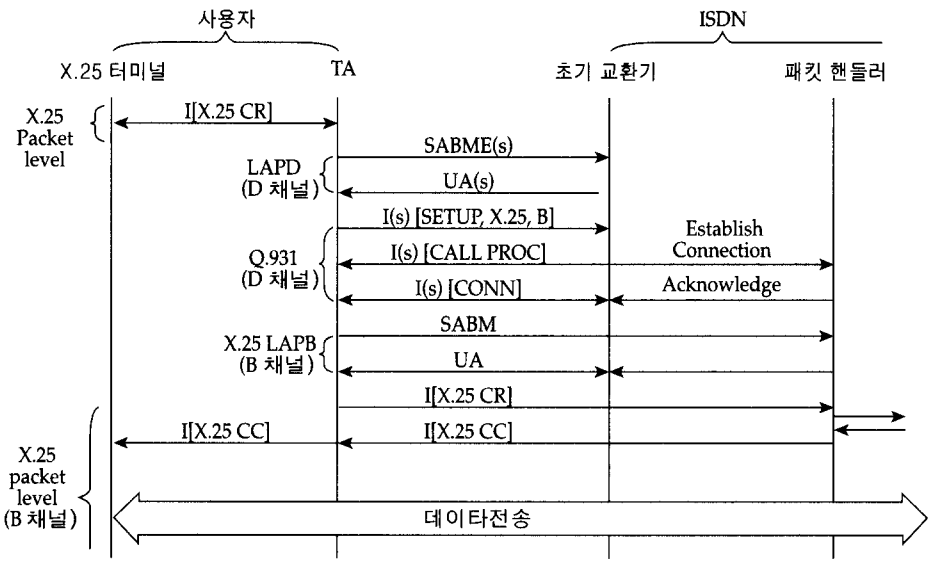
3.2 X.31 B 경우

권고안 X.31 B인 경우, ISDN을 제공할 수 있는 모든 패킷교환 서비스를 가진다. 패킷 호출은 B 채널 또는 D 채널 상에 설치된다. 그리고 이것은 X.25 호의 완전한 프로세싱을 수행하는 ISDN에서 패킷 핸들러(PH)에게 경로를 따라 전달된다. PH는 ISDN내(로컬교환, 원격교환, 또는 패킷교환 모듈 등)의 어느 곳에도 설치할 수 있다. PH에 대한 패킷 호의 라우팅은 요구된 베어러 능력(전송모드=패킷모드)을 기초로 해서 수행된다. 그러므로 사용자는 Q.931 Setup 메시지에서 호출 당사자 넘버를 제공하지 않는다. 호출된 터미널의 주소는 X.25 Call Request 패킷 내에 포함된다. B 경우에서, 초기 시점에서 사용된 채널을 별도로 하여 B 채널 또는 D 채널을 사용할 수 있게 선택할 수 있는 종단면을 표시하는 것이 중요하다.

권고 X.31 B 경우, 패킷모드 서비스(CCITT 권고 X.31) PSPDN은 여전히 분리된 네트워크이지만 패킷 처리(PH)기능은 ISDN의 일부분이다. 그래서 LE가 사용자(X.25 DTE)에게는 네트워크 노드(X.25 DCE)로 보인다. 내부적으로 CCITT 권고 X.25나 다른 어떤 인터네트워킹 프로토콜은 ISDN 패킷 처리기를 PSPDN이나 다른 ISDN PH에 연결하기 위해 사용될 수도 있다. 두개의 DTE는 ISDN을 통해서 X.25 VC 서비스를 받는다.

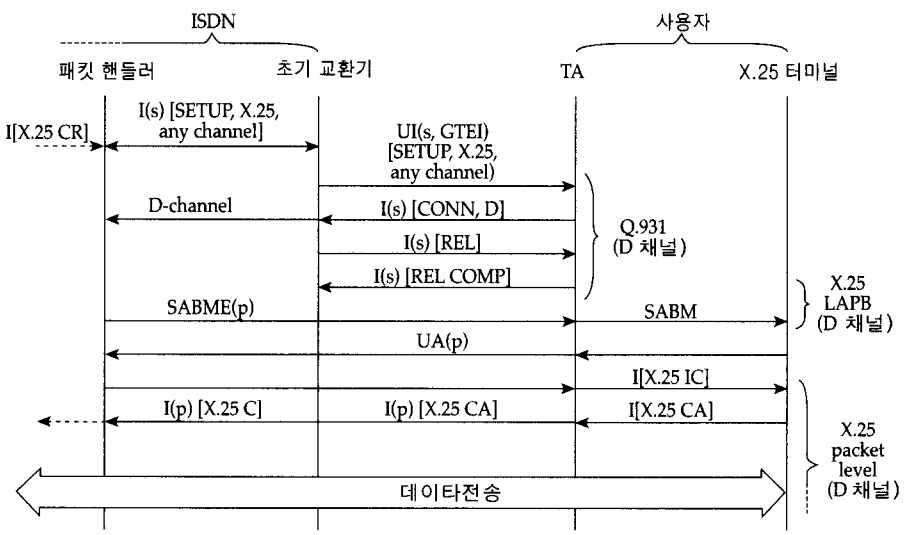
이 모델에서, LE는 PH 기능을 가지거나 패킷교환으로 직접 접속할 수 있다. 어느 경우에서도, LE는 X.25 패킷을 그것이 도달하는 채널에 상관없이 사용하는 방법을 가지고 있다. 그래서 패킷 서비스는 B 채널이나 D 채널에서 제공될 수 있다. 권고 X.31 프로시저는 B 채널에서의 완전한 X.25 LAPB와 PLP의 지원을 규정하고 D 채널에서의 LAPD 프레임에 있는 X.25 PLP 패킷의 전송을 규정한다. 북미의 ISDN 서비스는 B 경우를 기초로 한다.

그림 3은 B 채널 연결을 하는 패킷통신에서 호를 위한 패킷 호 설정 절차를 보여준다. 그림 3에서, 패킷 호는 터미널 어댑터(TA)를 통해 ISDN에 연결되는 X.25 터미널에 의해 발생된다. 터미널은 TA에게 I [X.25(CR)]로 표현된 X.25 호 요구 패킷을 포함한 정보(I) 프레임을 전달한다. 그림 4는 D 채널을 이용해 호를 위한 전입 패킷 호 제공 절차를 보여준다. 이 예는 두 가지 측면에서 이전 것과는 다르다. 첫 번째로 초기 시점에서 호 설정 절차 대신에 종단교환에서 전입 호 절차를 표현한다. 두 번째는 B 채널 대신에, 패킷통신을 위해 D 채널이 사용된다.



LAPD:Link Access Procedures on D-channel, CR : Call Request, CC : Call Connect,
UA : Unnum bered Acknowledgement, SABM : Set Asynchronous Balanced Mode
SABME : Set Asynchronous Balanced Mode Extended

그림 3. 패킷 호 설정 절차(B 채널을 이용한 예)



LAPD:Link Access Procedures on D-channel, CR : Call Request, CC : Call Connect, CA : Call Accept
IC : Income Call, UA : Unnum bered Acknowledgement, TA : Terminal Adaptoer, GTEI : Group TEI in LAPD
TEI : Terminal Endpoint Identifier, SABM : Set Asynchronous Balanced Mode
SABME : Set Asynchronous Balanced Mode Extended

그림 4. 전입 패킷 호 제공 절차(D 채널을 이용한 예)

4. ISDN 패킷교환에서의 키 분배 프로토콜

ISDN에서 암호화 키를 분배하기 위해서는 ISDN이 공중망으로 갖는 특성을 잘 고려해야 한다. 특히, 키와 사용자에 대한 인증을 위해서는 공증 센터를 어디에 어떻게 구축할 것인가를 신중히 검토하여야 한다. 인증 센터 기능을 망 내부에 즉, 교환 시설에 포함 할 경우에는 무엇보다 SS7 신호 프로토콜에 의존하게 되므로 인증 처리 속도는 비교적 빠르게 되겠지만 신호 처리에 많은 부담이 필요하게 된다. 반면에 인증 센터를 일반 사용자 단말기와 같이 ISDN의 망 외부에 구축하였을 경우에는 인증을 위해서 추가적인 호 설정을 더할 필요가 있으므로 호 설정을 위한 시간의 추가적인 부담이 필요하게 된다. 그러나 후자의 경우 이미 구축되어 있는 SS7의 신호 체계에 영향을 주지 않고 정보보호를 위한 키의 생성 및 사용자의 인증이 가능하게 되므로 호 제어 절차 측면에서 더 유리하다.

본 논문에서는 이와 같은 관점에서, 인증 센터를 ISDN의 망 외부에 구축하여 비밀키 암호방식에 대해서는 키의 생성 및 인증을 책임지는 키 생성 센터의 기능을 수행하고 하이브리드 암호화 방식에서는 사용자의 공개키 등록과 인증서 발행을 위한 CA 기능을 수행하도록 한다.

4.1 비밀 키 암호화 방식을 이용한 키 분배 프로토콜

비밀 키 암호화 방식을 이용한 키 분배 프로토콜은 그림 5와 같다.

① 먼저 호 설정을 요구하는 호 발신자 A는 자신의 비밀키 As 즉, 단말기 일련번호 또는 스마트카드 일련 번호로 B의 식별 번호를 암호화한다.

② 암호화된 As[B]를 CR(Call Request) 패킷의 사용자 영역에 첨가한 후 CR(As[B]) 패킷을 통신망에 전송한다.

③ 망은 호출 수신측인 사용자 B 주소를 키로 하여 호출 수신 단말이 포함된 교환기까지 CR(As[B]) 패킷을 전송한다.

④ 수신측 교환기는 IC(Incoming Call) 패킷을 호출 수신측 사용자 B에게 전송한다.

⑤ 수신측 사용자 B는 수신측 교환기로부터 전송된 IC(As[B]) 패킷을 수신하고 수신한 IC 패킷에서 추출된 As[B]와 A의 식별 번호를 자신의 비밀키 Bs로 암호화해서 키 관리 센터 KMC(Key Management Center)에게 호 요청을 하고, CR 패킷에 포함하여 전송한다.

⑥ 키 관리 센터 KMC는 사용자 B로부터 전송된 정보를 순서대로 복호화하고, 사용자 A와 사용자 B의 관계를 확인 한 후 사용자 A와 사용자 B간에 사용될 대화키 KC를 생성한다.

⑦ 키 관리 센터 KMC는 사용자 A의 식별 번호와 사용자 B의 식별 번호를 XOR 연산한 후 결과 값 A⊕B를 대화 키 KC와 함께 사용자 B의 비밀키와 사용자 A의 비밀키로 암호화한다. 암호화된 Bs{A⊕B, KC, As[A⊕B, KC]} 정보를 CLR(Clear Request) 패킷의 사용자 영역에 포함하여 사용자 B에게 전송한다.

⑧ 망은 호출 수신측 사용자 B 주소를 키로 하여 호출 착신 단말이 포함된 교환기까지 CLR(Bs{A⊕B, KC, As[A⊕B, KC]}) 패킷을 전송한다.

⑨ 수신측 교환기는 CLI(Clear Indication) 패킷을 호출 수신측 사용자 B에게 전송한다.

⑩ 사용자 B는 키 관리 센터 KMC로부터 전송된 CLI(Bs{A B, KC, As[A B, KC]}) 패킷을 수신한다. 그리고 수신된 CLI 패킷에서 암호화된 Bs{A B, KC, As[A B, KC]} 정보를 추출하고, 키 관리 센터 KMC에게 CLC(Clear Confirmation) 패킷을 전송한다.

⑪ 사용자 B는 전송된 Bs{A B, KC, As[A B, KC]} 정보를 자신의 비밀키로 복호화한 후 A B가 맞으면 대화 키 KC를 획득한다.

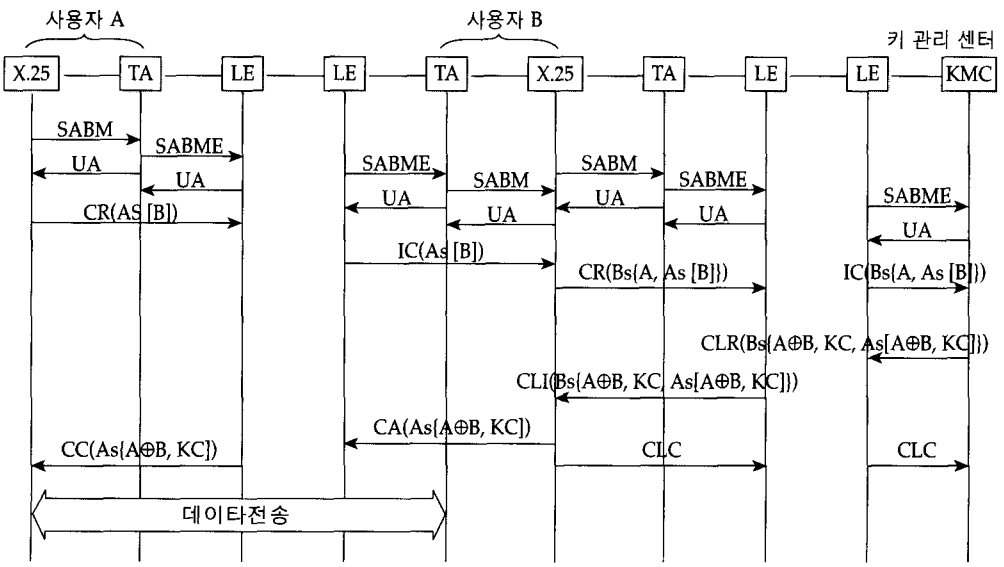
⑫ 사용자 B는 나머지 As[A B, KC] 정보를 발신측 사용자 A에게 CA(Call Accepted) 패킷의 사용자 정보 영역에 첨가한 후, CA(As[A B, KC]) 패킷을 발신측 사용자 A에게 전송한다.

⑬ 발신측 사용자 A는 전송된 CC(Call Connect) 패킷을 수신하고, 수신된 CC(As[A B, KC]) 패킷에서 암호화된 정보를 자신의 비밀키로 복호화한 후 A B가 맞으면 대화 키 KC를 얻는다.

⑭ 정보전송단계

ⓐ 정보보호 대상을 선택하고 이 정보를 대화 키 KC를 이용하여 암호화/복호화한다.

ⓑ 암호화된 정보를 전송하고 이 정보를 복호화하는 과정을 정보 전송이 완료될 때까지 계속 수행한다.



CR : Call Request, CC : Call Connect, IC : Income Call, CA : Call Accept, UA : Unnum bered Acknowledgement, CLR : Clear request, CLI : Clear Indication, ClC : Clear confirmation, SABME : Set Asynchronous Balanced Mode, SABME : Set Asynchronous Balanced Mode Extended, A : 사용자 A, B : 사용자 B, As : 사용자 A의 비밀 키, Bs : 사용자 B의 비밀 키, KC : 대화키

그림 5. 비밀 키 암호화 방식을 이용한 ISDN 가상 회선 서비스

4.2 하이브리드 암호화 방식을 이용한 키 분배 프로토콜

하이브리드 암호화 시스템은 공개 키 암호화 시스템과 비밀 키 암호화 시스템을 결합한 시스템으로, 키 분배는 공개 키 시스템으로 수행하고 정보의 암호화는 비밀 키 시스템으로 수행한다. 하이브리드 암호화 시스템은 공개 키 시스템의 키 분배와 인증 수행 기능, 그리고 비밀 키 시스템 속도의 장점을 결합한 것이다. 따라서 ISDN 정보보호 시스템에 가장 적합한 암호화 시스템이라고 할 수 있다. 사용자 상호간의 안전한 통신을 위해서는 먼저 상호간의 키 보증을 확립할 수 있는 키인증 센터(KCC: Key Certification Center)를 두어야 한다.

4.2.1 키 등록 절차

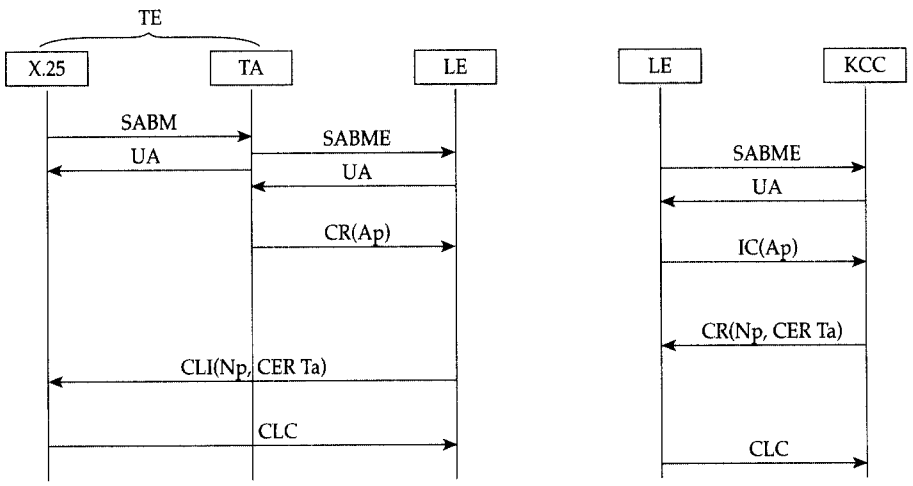
먼저 그림 6과 같은 공개키를 등록하기 위한 호 제어 절차가 필요하다.

① 사용자 A는 자신의 공개키인 Ap를 CR 패킷의 사용자 영역에 포함하여 CR(Ap)패킷을 키인증 센터에 등록한다. 사용자 B도 자신의 공개키인 Bp를 이용해 사용자 A와 같은 과정을 거친다.

② 키인증 센터는 자신의 공개키 Np와 개인키 Ns를 발생시켜 자신의 개인키인 Ns로 사용자 A, 사용자 A의 공개키, 인증서의 타당성 주기를 암호화하여 인증서 CERTa를 만든다. 또 자신의 개인키로 사용자 B, 사용자 B의 공개키, 인증서의 타당성 주기를 암호화하여 인증서 CERTb를 만든다.

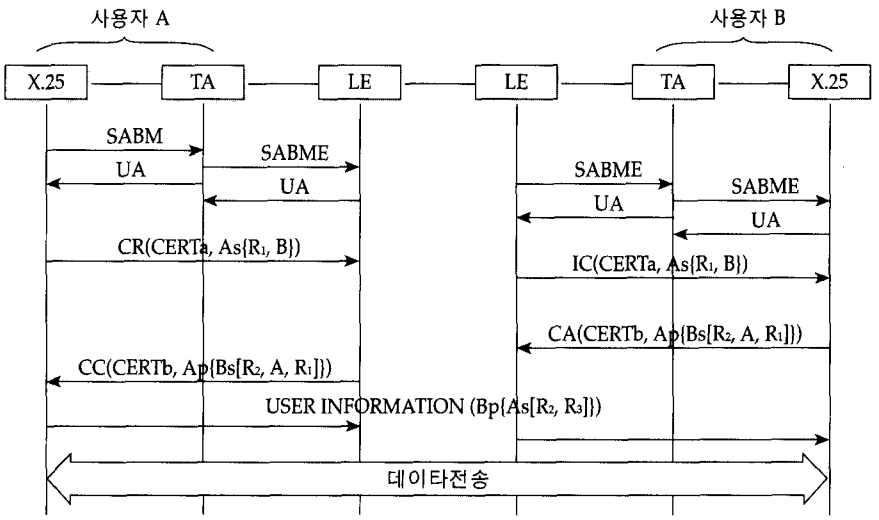
③ 키인증 센터는 CLR 패킷의 사용자 영역에 공개키 Np와 CERTa를 포함하여 CLR 패킷을 사용자 A에게 전달하고, 사용자 B에 대한 절차에서도 공개키 Np와 CERTb를 사용자 A의 절차와 같이 사용자 B에게 전달한다.

④ 사용자 A는 CLI(Np, CERTa) 패킷을



CR : Call Request, IC : Income Call, UA : Unnum bered Acknowledgement, CLR : Clear request,
CLI : Clear Indication, ClC : Clear confirmation, SABME : Set Asynchronous Balanced Mode
SABME : Set Asynchronous Balanced Mode Extended, Ap : 사용자 A의 공개 키, Np : 키 인증 센터의 공개 키,
CERTa : 사용자 A의 인증서

그림 6. 키인증 센터 확립 절차



CR : Call Request, CC : Call Connect, IC : Income Call, CA : Call Accept, UA : Unnum bered Acknowledgement, SABME : Set Asynchronous Balanced Mode, SABME : Set Asynchronous Balanced Mode Extended, A : 사용자 A, B : 사용자 B, CERTa : 사용자 A의 인증서, CERTb : 사용자 B의 인증서, Ap : 사용자 A의 공개 키, As : 사용자 A의 개인 키, Bp : 사용자 B의 공개 키, Bs : 사용자 B의 개인 키, R1, R2, R3 : 난수

그림 7. 하이브리드 암호화 방식을 이용한 상호 인증 절차

수신하고 키인증 센터에게 CLC 패킷을 전송하여 호를 해제한다. 사용자 B도 사용자 A와 같은 절차를 따른다.

4.2.2 사용자 상호 인증과 키 분배 호 제어 절차

키인증 센터에 의해 키 등록절차가 확립되면 사용자 상호 인증을 위해 그림 7과 같은 상호 인증 호 제어 절차를 따른다.

① 사용자 A는 CR 패킷의 사용자 영역에 CERTa, As{ Ra, B }를 포함하여 사용자 B에게 전송한다.

② 사용자 B는 Np를 이용, 복호화하여 CERTa로부터 Ap를 얻는다. 그리고 A의 인증이 만료되지 않았는지 점검하고 서명을 검증하고 서명된 정보의 무결성을 점검한다.

③ 사용자 B는 R1과 같은 목적으로 사용하기 위해 난수 R2를 생성한다.

④ 사용자 B는 CA 패킷의 사용자 영역에 CERTb, Ap{Bs[Rb, A, Ra]}를 포함하여 사용자 A에게 전송한다.

⑤ 사용자 A는 Np를 이용, 복호화하여 CERTb로부터 Bp를 얻는다. 그리고 B의 인증서가 기간이 만료되지 않았는지 점검하고, 인증 토큰을 복호화한 다음 서명을 검증한다. 그리고 서명된 정보의 무결성을 점검한다.

⑥ 사용자 A는 수신된 난수 R1이 보낸 R1과 동일한 지를 점검한다. 그리고 난수 R3을 생성한다.

⑦ 사용자 A는 USER INFORMATION 메시지에 Bp{As[R2, R3]를 포함하여 사용자 B에게 전송한다.

⑧ 사용자 B는 인증 토큰을 복호화하고 서

명을 점검하고 서명된 정보의 무결성을 점검한다. 그리고 수신된 R2가 보낸 R2와 동일한 것인지 점검한다.

4.2.3 메시지 비밀성을 위한 전송 절차

① 정보전송단계

ⓐ 정보보호 대상을 선택한다.

ⓑ 사용자 A가 R2를 이용하여 메시지를 암호화한 후 사용자 B에게 전송하면, 사용자 B는 자신이 알고 있는 R2를 이용하여 복호화를 한 후 메시지를 받아 볼 수 있다. 반대로 사용자 B가 R3을 이용하여 메시지를 암호화한 후 사용자 A에게 전송하면, 사용자 A는 자신이 알고 있는 R3을 이용하여 복호화한 후 메시지를 받아 볼 수 있다.

ⓒ 암호화된 정보를 전송하고 전송된 정보를 복호화하는 과정을 정보 전송이 완료될 때까지 계속 수행한다.

이와 같은 하이브리드 암호화 시스템의 호 제어 절차를 이용하면 사용자는 네트워크에서 상대방에 대한 공개키를 인증할 때에 KCC를 한번만 액세스하면 된다 그래서 긴 디렉토리를 분배할 필요도 없고 통신을 원할 때 키 분배 센터로부터 새로운 세션 키를 얻어야 하는 결점도 없다. 또한 이 하이브리드 암호화 시스템은 패킷교환 통신뿐만 아니라 점-대-점 방식, 전자우편 시스템과 같은 다른 여러 통신 시스템의 응용에도 사용할 수 있다.

5. 결 론

ISDN은 사용자가 필요로 하는 다양한 종류의 서비스(음성, 화상, 데이터 등)를 통합하여 효율적으로 서비스를 제공하기 위하여 디지털 전송과 디지털 교환을 기초로 발전되었다. 따라서 ISDN에서는 통신망 전역에 걸쳐 디지털 전송이 이루어지므로 사용자의 중요 정보 자원에 대한 정보보호 구조 및 프로토콜의 개발이 절실히 요구되는 실정이다. ISDN에서 정보보호 서비스를 제공하기 위해서는 가장 효율적인 암호화 시스템을 정합한 최적의 정보보호 프로토콜 개발과 각 계층별, 서비스별, 채널별 키 관리 체계에 대한 연구의 필요성이 대두되게 되었다.

그러므로 본 논문에서는 PHS 구조와 ISDN에서의 두 가지 경우의 패킷교환 서비스를 분석하였고, 패킷교환 방식에서의 가상 회선 서비스에 대한 호 제어 절차와 비밀 키 암호화 방식과 하이브리드 암호화 방식을 이용한 암호화 키 관리 체계를 제안하였다. 또한 본 논문에서 제안한 키 분배 프로토콜처럼, 네트워크 내부에 인증센터를 설치하지 않고 네트워크 외부에 인증센터를 설치함으로써 호 설정 과정동안에 사용자 상호간의 인증 및 디지털 서명을 구현할 수 있는 호 제어 절차를 제안하였다.

앞으로의 연구에서는 각 채널에 대한 패킷교환 방식에서의 좀 더 안전하고 종합적인 ISDN 정보보호 서비스를 제공할 수 있는 키 관리 방안에 대해 연구를 진행하여, 이를 ISDN 시스템 구조와 프로토콜에 좀 더 효율적으로 정합할 수 있는 정보보호 프로토콜의 키 관리 체계에 대한 연구가 진행되어야 하겠다.

참 고 문 헌

[1] ITU-T Recommendation I.310 ISDN - Network Functional Principles

[2] ITU-T Recommendation I.320 - ISDN Protocol Reference Model

[3] ITU-T Recommendation I.430 Basic User-Network Interface - Layer 1 Specification

[4] ITU-T Recommendation I.324 ISDN Network Architecture

[5] ITU-T Recommendation Q.931 - 기본 호 제어에 대한 ISDN의 사용자-망 인터페이스 계층 3 규격

[6] Warren S. Gifford, "ISDN User-Network Interfaces," IEEE Journal on SAC, Vol. SAC-4, No. 3, May 1986

[7] Diwakar Gan, "Defense Switched Network(DSN) Unique Features in ISDN," ISDN'91, 1991

[8] Simmons, G. J. "Symmetric and Asymmetric Encryption," ACM Computing Surveys, Vol.11, No.4, 1979.

[9] William E. Burr, "Security in ISDN," NIST, 1991

[10] S. Improta, "Privacy and Authentication in ISDN:The Key Distribution Problem," Note Recens(Italy) Vol.33, No.1-2, 1984.

[11] Kare Presttun, " Integrating Cryptography in ISDN," Advances in Cryptology-CRYPTO'87, pp. 9-18, 1987.

[12] G. J. Claassen, G. J. Kuhn, "Secure Communication Procedure for ISDN," COMSIG88, pp. 165-170, 1988

[13] Gary. C. Kessler, "ISDN Concepts, Facilities, and Services," McGraw-Hill Pub, 1995

[14] Kiyoto Tanaka, Ikuro Oyaizu, "A Confidentiality System for ISDN inter-PC High-Speed File Transfer," IEEE, pp 1290-1277, 1994

[15] 한인탁, 전경표, 한기철, "TDX-10에서 D 채널을 통한 패킷교환 기능의 구현," JCCI-92, Vol 2, 1992

□ 著者紹介

김 봉 한

1994년 청주대학교 전자계산학과 학사
1996년 한남대학교 대학원 컴퓨터공학과 석사
현재 한남대학교 대학원 컴퓨터공학과 박사과정

※ 주관심분야: 컴퓨터 네트워크, 정보통신 정보보호

이 재 광

1984년 광운대학교 전자계산과 학사
1996년 광운대학교 대학원 전자계산과 석사
1993년 광운대학교 대학원 전자계산과 박사
1986년 3월 - 1993년 8월 군산전문대학 전자계산학과 부교수
1993년 8월 - 현재 한남대학교 컴퓨터공학과 부교수

※ 주관심분야: 컴퓨터 네트워크, 정보통신 정보보호