안전한 종합정보통신망을 위한 키 분배 프로토콜과 호 제어

정 현 철[†] · 신 기 수[†] · 이 선 우[††] · 김 봉 한[††] ·
김 점 구[†††] · 이 재 광[††††]

요 약

정보화 시대가 도래하면서 여러 가지 정보(텍스트, 화상, 음성)를 통합, 전송할 수 있도록 개발된 통신망이 종합 디지털 통신망(ISDN : Integrated Services Digital Network)이다. 이러한 ISDN은 모든 정보가 디지털 형태로 전송되고, 통신망 접속이 개방성을 갖기 때문에 중요 정보 자원에 대한 위협 및 침입 등의 보안 문제점이 증가하고 있다.

본 논문에서는 중요 정보 자원을 보호하기 위해, ISDN에 적용할 수 있는 암호화 시스템과 적용방식을 연구하였고, ISDN 시스템 구조와 ITU-T 권고 Q.931 프로토콜을 분석하여 효율적인 정보보호 서비스를 제공하는 암호화 키 분배 프로토콜과 하이브리드 암호화 시스템을 이용한 사용자 정보의 비밀성을 제공하는 호 제어 방법을 제안하였다.

Key Distribution Protocol and Call Control for Secure ISDN

Hyun Cheol Chung[†] · Ki Soo Shin[†] · Sun Woo Lee[††] · Bong Han Kim[††] ·
Jeom Gu Kim[†††] · Jae Kwang Lee[††††]

ABSTRACT

ISDN is network which has been developed to integrate and transfer some information(data, video, voice). In the ISDN, security problem that threat and intrusion about important information resource increase because every information is transferred in the form of digital and access of network has patency.

In this paper, for protect important information resource, studied that apply application method and encryption system to ISDN, and ISDN system structure, ITU-T Q.931 protocol were analyzed, and proposaled encryption key distribution protocol, call control with hybrid encrytion system for user information privacy to provide security service.

1. 서 론

정보화 사회에서 정보는 그 무엇보다도 큰 가치를 가지게 된다. 그러므로 정보의 빠른 유통을 위한 요구가 사회적으로 증대되었고, 이러한 요구를 충족시키기 위하여 컴퓨터의 디지털 기술과 데이터 통신 기술의 결합을 통한 새로운 통신서비스가 개발되어 왔다. 그러나 각 서비스마다 별도의 전송매체와 인터페이스를 사용함으로써 비효율적이고 비용과 운용상의

† 정 회 원 : 한국전자통신연구소 부호기술부
†† 준 회 원 : 한남대학교 전자계산공학과
††† 정 회 원 : 안양전문대 전자통신과 강사
†††† 정 회 원 : 한남대학교 전자계산공학과 조교수
논문접수 : 1996년 9월 13일, 심사완료 : 1996년 10월 29일

많은 문제점을 안고 있었다. 이에 다양한 서비스를 동일한 인터페이스를 통하여 통합적으로 제공하기 위한 새로운 통신망의 개발이 필요하게 되었다. 이 망이 종합 디지털 통신망인 ISDN(Integrated Services Digital Network)이다[1, 2].

미국과 일본을 비롯한 일부 선진국에서는 1980년대 초부터 ISDN 구축을 시작하여 1980년대 후반 이후부터는 ISDN 상용 서비스를 제공하고 있으며, 우리 나라에서도 제 8차 경제사회 5개년 계획이 완료되는 2001년까지 전국적인 규모의 ISDN를 구축한다는 목표 하에 지난 87년초 ISDN 기본계획을 수립하여 계속 추진하고 있다.

ISDN은 다양한 종류의 정보 서비스를 종합적으로 제공할 수 있도록 하나의 회선을 통하여 가입자의 디지털 통신망이 디지털 방식으로 접속된다. ISDN은 음성 및 비음성 서비스를 통합하여 처리할 수 있으며, 회선 교환 및 패킷교환을 동시에 제공한다. 그러나 모든 정보가 디지털 형태로 전송되고 통신망 접속이 개방성을 갖기 때문에 중요 정보 자원에 대한 위협이 날로 증가하는 추세이다. 따라서 기존의 통신망과 연동 또는 통합하여 다양한 정보 서비스를 제공하는 ISDN에서의 사용자 중요 정보 자원의 취약성에 따른 불법적인 침입자로 부터의 우연 또는 의도적인 침입 위협에 대한 대책이 절실히 요구되는 실정이다[12].

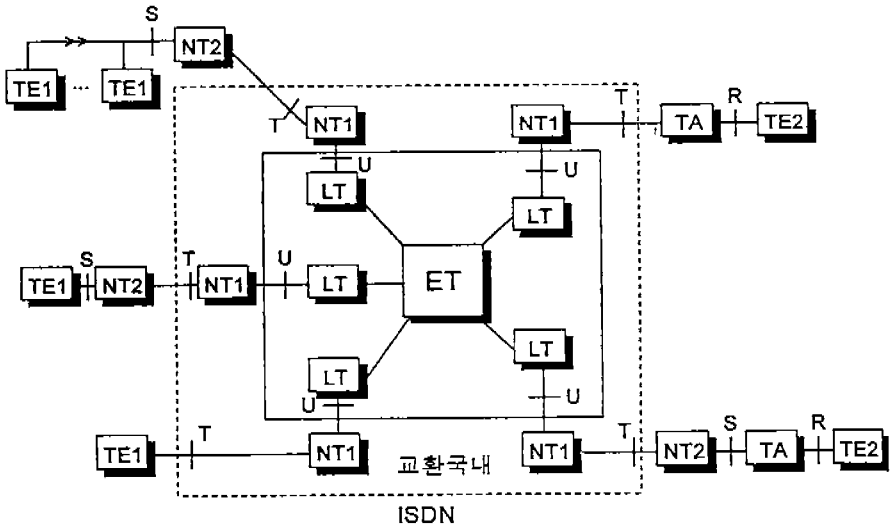
본 논문에서는 ISDN 사용자-망 인터페이스 구조와 ISDN에 적용할 수 있는 암호화 시스템과 적용방식을 연구하였고, Q.931 프로토콜을 분석하여 효율적인 사용자 정보의 비밀성과 사용자에 대한 인증 서비스를 제공하는 암호화 키 분배 프로토콜과 호 제어 방법을 제안하였다.

2. ISDN 사용자-망 인터페이스

ISDN을 구현하는데 가장 중요한 부분은 사용자-망 인터페이스이며 접속 형태의 표준은 세계 여러 나라의 모든 통신망에서 사용자의 단말기들을 접속하여 통신할 수 있도록 하는 것을 목적으로 하고 있다. 사용자-망 인터페이스에서는 먼저 표준화할 규정점(인터페이스)을 명확히 할 필요가 있다[3, 4, 5, 6].

2.1. 인터페이스 점

사용자-망 인터페이스에는 (그림 1)에 나타난 것처



(그림 1) ISDN의 기준점
(Fig. 1) ISDN Reference Points

럼 R, S, T, U 인터페이스 점이 존재한다.

(1) R점

ISDN 비표준 단말기(TE2 : Terminal Equipment2)와 단말 어댑터 장치(TA : Terminal Adapter) 사이에 위치하는 인터페이스 점이다.

(2) S점

ISDN 표준 단말기(TE1)와 망 종단장치2(NT2 : Network Termination2)사이에 위치하는 인터페이스 점이다.

(3) T점

망 종단장치2(NT2)와 망 종단장치(NT1)사이에 위치하는 인터페이스 점이고, ISDN 표준 단말기(TE1)과 망 종단장치1(NT1)사이에 위치하는 인터페이스 점이다.

(4) U점

망 종 단장치1(NT1)과 회선 종단사이에 위치하는 인터페이스 점이다. 사용자 선로의 조건이 각 국의 크기, 인구밀도 등의 차이로 가변성이 크기 때문에 전 세계를 하나의 사용자선 디지털 전송 방식으로 통일한다는 것은 불가능하므로 CCITT는 U 기준점에 대한 표준을 권고하지 않는다.

2.2. 기능 그룹

(1) 망 종단장치1(NT1)

NT1은 거리 및 선로 품질 등의 특성면에서 차이가 있는 여러 종류의 사용자선을 수용하여 사용자측에 표준화된 사용자-망 인터페이스를 제공하는 기능과 동기 기능 등을 구비하고 있다.

(2) 망 종단장치2(NT2)

NT2는 하나 이상의 단말장치들이 동시에 망을 액세스할 수 있도록 하는 기능을 제공한다.

(3) 터미널 어댑터(TA)

기존의 ISDN 비표준 단말장치는 TA를 통하여 ISDN에 접속된다.

(4) ISDN 표준 단말1(TE1)

인터페이스 권고안에 준하는 단말 기능을 나타낸다.

(5) ISDN 비표준 단말2(TE2)

인터페이스 권고안에 준하지 않는 기존 단말의 기능을 나타낸다.

이상의 기능 그룹에 대한 정의는 〈표 1〉에 요약되어 있다[4, 5, 6].

〈표 1〉 기능 그룹의 정의

〈Table 1〉 Definition of Functional Devices

NT1	망 종단장치1 (Network Termination1)	사용자선 종단 계층 1로의 보수 기능 모니터 타이밍, 전력 전송 급전 계층 1로의 다중화 인터페이스 종단 (복수단말의 충돌제어) 기능을 포함
NT2	망 종단장치2 (Network Termination2)	계층 2, 3의 프로토콜 처리 계층 2, 3에서의 다중화 교환, 집선, 보수기능 인터페이스 종단
TE TE1 TE2	Terminal Equipment ISDN 표준 단말 (Terminal Equipment Type 1) ISDN 비표준 단말 (Terminal Equipment Type 2)	프로토콜 처리 보수 기능 인터페이스 기능 다른 장치와의 변환기능
TA	단말 어댑터 장치	인터페이스 변환 기능

2.3. 채널 종류와 접속구조

(1) 채널의 종류

채널 종류는 〈표 2〉와 같이 전송 정보에 따라서 사용자 정보를 위한 정보 채널과 신호 정보를 위한 신호 채널로 나뉘어진다. 정보 채널은 통신 속도에 따라서 나누어지며, 주로 전화 서비스를 위한 64Kbps 채널 속도의 B 채널을 기본 채널로 하고, 고속 데이터 서비스 또는 영상 서비스를 제공하는 고속 H 채널이 규정되어 있다.

〈표 2〉 채널의 종류

〈Table 2〉 Channels

채널 종류		채널 속도	용 도
B		64 Kbps	사용자 정보 전송용 채널 사용자 정보 속도 : 8/16/32/64 Kbps 회선교환/패킷교환/전용선
D		16 Kbps 또는 64 Kbps	회선교환의 신호채널 텔레메터/패킷 정보채널등
H	H_1	384 Kbps	사용자 정보 전송용 채널 회선교환/패킷교환/전용선
	H_{11}	1536 Kbps	
	H_{12}	1920 Kbps	

(2) 액세스 구조

기본 액세스인 경우에는 두개의 B 채널과(각각

64Kbps) 하나의 신호용 D 채널(16Kbps)을 갖고 있는 한 개의 접속 구조로 되어 있다. 일차군 속도 액세스에서는 몇 개의 접속 구조가 정의되어 있으며, B 채널, H_0 채널, H_1 채널과 이들 혼합 접속 구조로 되어 있다.

3. ISDN에 적용 가능한 암호화 시스템과 적용 방식

3.1. 암호화 시스템

암호화 시스템은 크게 비밀 키(대칭:symmetric 또는 conventional) 시스템과 공개 키(비대칭:asymmetric 또는 public) 시스템, 그리고 두 시스템이 갖는 장점을 결합시킨 하이브리드(hybrid) 시스템으로 나눌 수 있다[7, 8, 9, 10].

3.1.1. 비밀 키 암호화 시스템

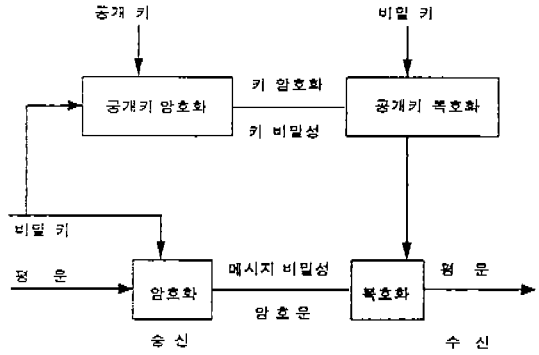
비밀 키 암호화 시스템은 비밀 통신을 원하는 두 사용자가 비밀 키를 공유하여 데이터를 암/복호화하는 것으로서, 현재 가장 널리 알려진 시스템으로는 DES가 있다. DES는 56 비트의 비밀 키를 이용하여 정보를 64 비트 블록 단위로 암호화하는 블록 암호 알고리즘이다.

3.1.2. 공개 키 암호화 시스템

공개 키 암호화 시스템은 각 사용자가 비밀 키와 공개 키를 소유하여 메시지를 수신자의 공개 키로 암호화하여 전송하면 그 공개 키에 대응하는 비밀 키의 소유자만이 암호화된 메시지를 복호화할 수 있다. 공개 키 암호화 시스템은 비밀 키와 공개 키만으로 암/복호화를 할 수 있으므로 암호 키 분배 문제는 발생하지 않지만, 공개 키 관리 센터로부터 공개 키를 얻을 때 상호 인증과 공개 키에 대한 인증이 필요하다. 가장 대표적인 공개 키 암호 알고리즘에는 RSA가 있으며, 하드웨어로 제작되기도 하였으나 암/복호화 과정에 많은 모듈라 곱셈을 포함한 멱승연산이 필요하므로 암호화 속도가 DES보다 훨씬 떨어진다. 이러한 단점이 있으나 신분 인증이나 디지털 서명을 수행할 수 있으므로 인증이나 비밀 키 분배 프로토콜에 이용된다[7].

3.1.3. 하이브리드(hybrid) 암호화 시스템

하이브리드 암호화 시스템은 공개 키 암호화 시스템과 비밀 키 암호화 시스템을 결합한 시스템이다. 하이브리드 암호화 시스템에서는 키 분배는 공개 키 시스템으로 수행하고 정보의 암호화는 비밀 키 시스템으로 수행한다. 하이브리드 암호화 시스템은 (그림 2)와 같다.



(그림 2) 하이브리드 시스템
(Fig. 2) Hybrid System

하이브리드 암호화 시스템은 공개 키 시스템의 키 분배와 인증 수행 기능, 그리고 비밀 키 시스템의 속도의 장점을 결합한 것이다. 따라서 ISDN 정보보호 시스템에 가장 적합한 암호화 시스템이라고 할 수 있다.

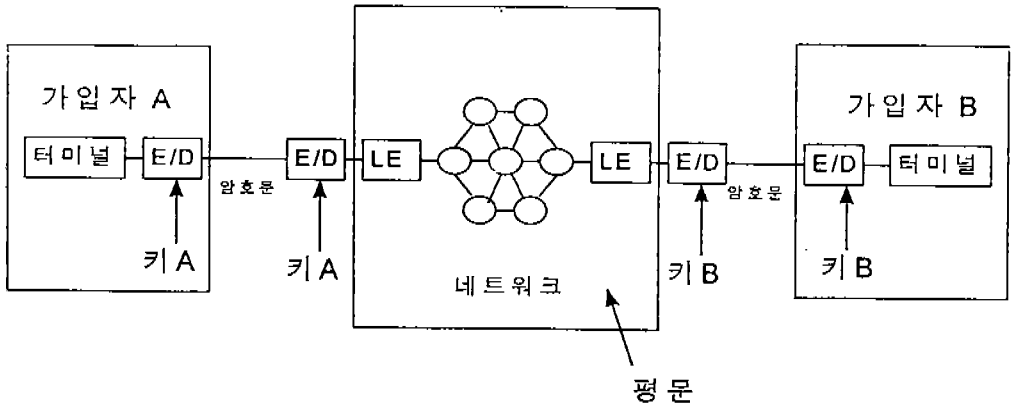
3.2 암호화 시스템 적용

원격 통신 시스템에 암호화 시스템을 적용하는 방법으로서는 (1) link-by-link, (2) node-by-node, (3) end-to-end 암호화 방법이 있다[8].

(1) link-by-link 암호화

이 방법은 투명한 방법으로 구현할 수 있고, 네트워크 프로토콜에 영향을 미치지 않기 때문에 원격 통신 시스템에 암호화를 적용할 수 있는 가장 간단한 방법으로 (그림 3)과 같다.

암호화 장치는 보통 사용자 인터페이스와 로컬 교환기의 사용자 종단 장치(user termination)에 위치한다. 이 방법의 단점은 네트워크의 노드와 로컬 교환기를 지나는 모든 트래픽은 평문이라는 것이다. 그렇지만 가로채기(interception)에 가장 취약한 링크가 있는 사용자 루프를 보호하기 때문에 효율적이라고 할



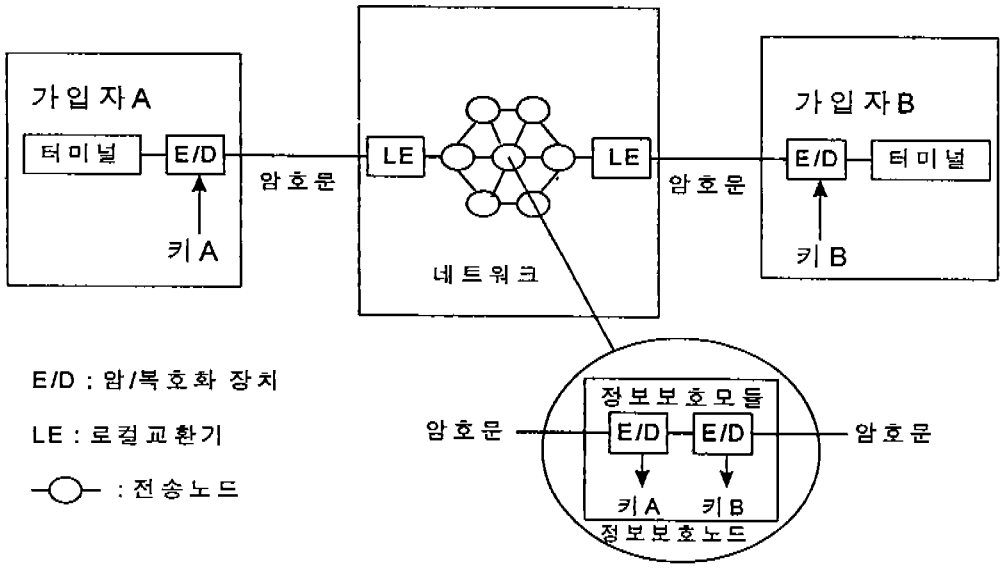
(그림 3) link-by-link 암호화
(Fig. 3) Link-by-link Encryption

수 있으나 이 방법은 네트워크 링크를 부분적으로 보호한다는 문제점을 갖는다.

(2) node-by-node 암호화

이 방법은 link-by-link 암호화를 수정한 것으로서, 네트워크에 있는 어떤 특정 노드들에 대한 정보보호를 제공된다. 암호화에 의해 보호된 각 링크는 자기 자신의 단일(비밀)키를 사용한다. 그러나 하나의 키로부터 다른 키들의 변환은 특정 노드에 위치한 정보보호 모듈 내에서만 할 수 있다. 그러면 네트워크는 암호화된 호(call)를 위한 특별한 라우팅을 제공해야만 하며, node-by-node 암호화는 (그림 4)와 같다.

이 방법은 소, 중규모 네트워크에서는 매우 효과적



(그림 4) node-by-node 암호화
(Fig. 4) Node-by-node Encryption

이다. 사용자의 수가 많아지면 트래픽 흐름의 과도한 혼잡을 피하기 위해, 특정 노드의 수를 늘려야 하기 때문에 많은 노드들의 정보보호를 보장하는 것이 어려운 단점이다. 그리고 link-by-link와 node-by-node 암호화는 두번 또는 그 이상의 암/복호화되는 데이터 흐름을 요구하고, 누적되는 지연은 네트워크 서비스의 질 및 망 성능에 크게 영향을 미칠 수 있다.

(3) end-to-end 암호화

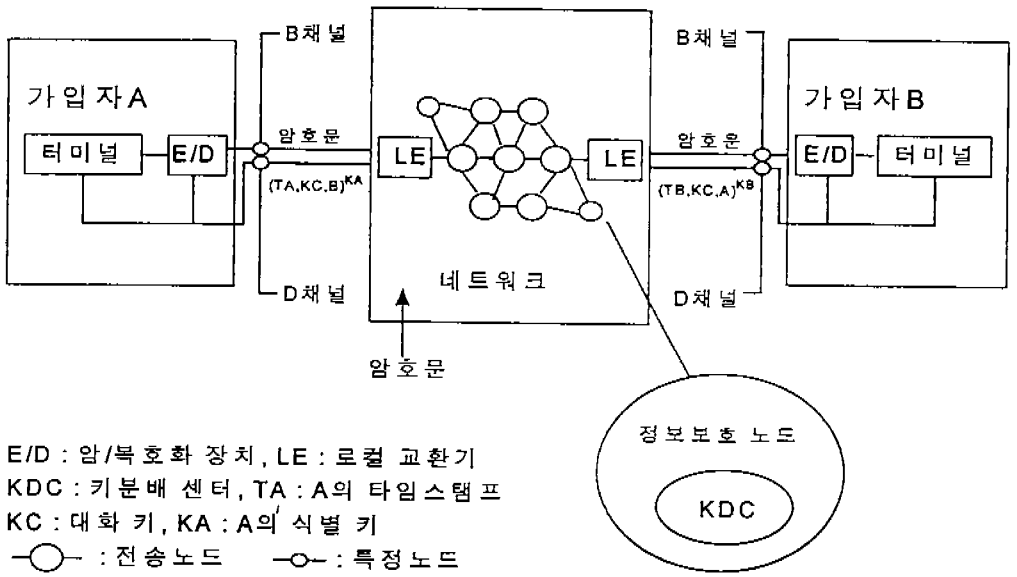
이 방법은 송신자에 의해서만 암호화되고 수신자에 의해서만 복호화된다. 네트워크는 데이터 전송 과정에서 완전한 투명성을 제공한다. ISDN 정보보호 관점에서는 이 방법이 가장 좋은 방법이다. 왜냐하면 네트워크에서의 모든 통신은 암호화를 유지하기 때문이며, end-to-end 암호화는 (그림 5)와 같다.

이 방법을 이용하여 비밀 키 암호 알고리즘을 이용하면 각 사용자 쌍은 비밀 키를 공유해야 한다. 그러면 약 200만 사용자를 갖는 네트워크에서는 거의 20조 사용자 쌍의 비밀 키를 사용하게 된다. 또 신뢰성 때문에 키는 한번만이 아니라 계속해서 만들어지고 분배되어야만 한다. 즉, 시간이 어느 정도 경과하거나 키 누출의 위협이 있을 경우에는 즉시 변경해야 한다. 그리고 만약 공개 키 알고리즘을 이용하면 각 사용자는 자기 자신의 키 쌍을 생성한다. 그리고 복호화 키는 비밀로 하고 암호화 키는 공개 디렉토리에 저장해야 한다. 그러나 사용자 수가 많은 규모가 큰 네트워크는 계속해서 새로운 사용자가 들어오고, 사용자들간의 정보 전송을 위해 키를 교환해야하기 때문에 필요한 정보보호 규칙을 이용해서 처리해야한다. 그러면 네트워크는 공개 키 분배 서비스도 제공할 수 있다.

4. ISDN 암호화 키 분배 프로토콜과 호 제어

4.1. ITU-T Q.931 분석

ITU-T 권고 Q.931은 ISDN 사용자-망 인터페이스에서 호 제어를 위한 망 접속의 설정 유지보수 및 해제를 위한 절차 등을 규정하고 있으며, 이러한 절차들은 기본 및 1차군 속도 인터페이스구조의 D채널을 통해서 교환되는 메시지 항들로 정의된다. 현재 ITU-T 권고 Q.931에서 정의된 절차들은 회선 교환 접속, 사용자-사용자간 신호 접속 및 패킷 교환 접속의 제어에 대한 내용이다[12].

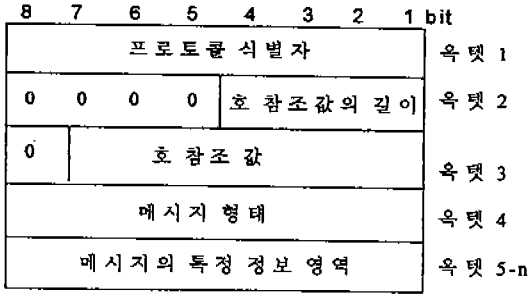


(그림 5) end-to-end 암호화
(Fig. 5) End-to-end Encryption

4.1.1. 제어 메시지 구조

호 제어를 위한 메시지 구조는 (그림 6)과 같으며 이 제어 메시지에서 사용되는 일반 정보 영역와 메시지 형태에 따라 사용되는 특정 정보 영역으로 구성된다. 모든 메시지에서 공통으로 사용되는 일반 정보 영역은 프로토콜 식별자, 호 참조 그리고 메시지 형태로 구성되어 있다. 그리고 호 설정과 호 해제를 위한 메시지의 특정 정보 영역에는 사용자간 정보 전송을 위한 최대 131 바이트(최소 2 바이트)의 정보를 포함할 수 있는 가변 길이의 정보 표현 영역이 존재하며, 이들 사용자 정보들은 통신망에 투명성있게 전달된다.

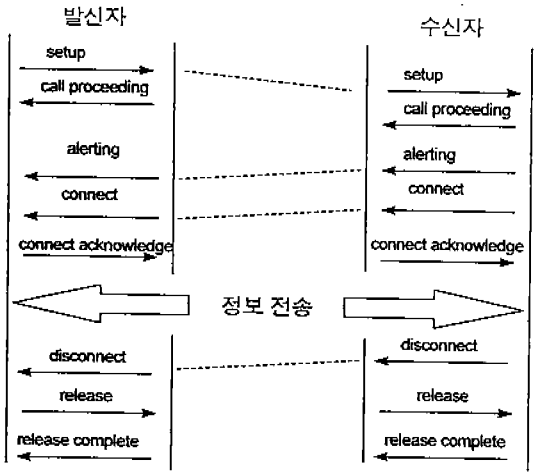
프로토콜 식별자는 ITU-T 권고 Q.931에 대해서만 "00001000" 값으로 정의 되어 있다. 호 참조는 발생된 특정 호를 구분하기 위하여 호 참조 플래그와 호 참조값으로 구성된다. 호 참조 플래그는 발신측에 대해 "0", 그리고 수신측에 대해서는 "1"로 표시되며, 호 참조 값은 발신측에 의하여 호가 시작될 때 할당되어 호 진행동안 고정값을 가지며 종료시 다른 호에 재 할당할 수 있다. 메시지 형태는 전송되는 메시지의 기능 및 종류를 구분하기 위하여 사용된다.



(그림 6) 제어 메시지 구조
(Fig. 6) Control Message Format

4.1.1. 회선 교환의 호 제어 절차

회선교환에서의 호 제어 절차는 (그림 7)과 같이 구현된다. 호 접속 해제는 발신측이나 수신측 어느측에서도 먼저 시작할 수 있다. 회선 교환의 호 제어를 위해 사용되는 메시지는 호 설정 메시지(SETUP 메시지, CALL PROCEEDING 메시지, ALERTING 메시지, CONNECT 메시지, CONNECT ACKNOWLEDGE 메시지), 정보 전달 단계 메시지 그리고 호 해제 메시지(DISCONNECT 메시지 RELEASE 메시지, RELEASE COMPLETE 메시지)로 나누어진다.



(그림 7) 회선 교환의 호 제어 절차
(Fig. 7) Call Control Procedure of Circuit-switched

4.2. 비밀 키 암호화 시스템을 이용한 키 분배 및 호 제어

사용자간에 비밀 키 암호 시스템을 사용하여 정보보호 서비스를 이용한 통신을 하고자 할 때는 먼저 통신에 사용하는 대화 키(conversation key)인 공통 키(common key)를 공유해야 한다. 이를 위해서 ISDN에서는 end-to-end 암호화 기술을 적용하여 키 분배 서비스는 제어 정보를 전송하는 D 채널을 이용한 공통 채널 신호방식 네트워크을 사용한다[7].

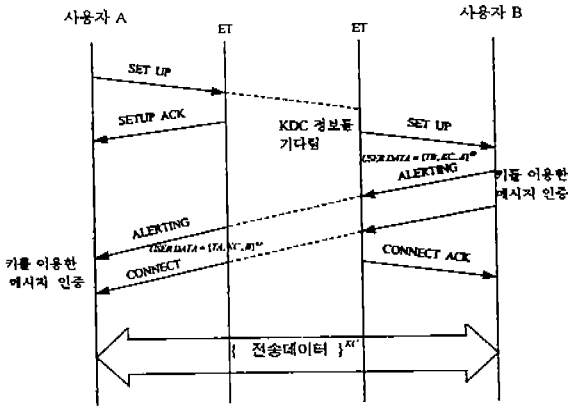
정보보호 서비스를 이용하고자 하는 사용자는 네트워크를 통하여 키 분배 센터(KDC)로부터 식별 키(Identification Key)에 대한 관리를 제공받는데 이 식별 키는 사용자와 키 분배 센터만 알고있다. 이 센터들은 특정 노드에 위치하여 공통 채널 신호방식 네트워크로 연결되어 있다. 사용자는 네트워크에 있는 센터들 가운데 하나의 선택를 자신의 키 분배 센터로 선택하게 된다. 따라서 각각의 로컬 교환기(local exchange)는 각 사용자에 대하여 정보보호 서비스를 엑세스할 수 있는 권한에 대한 정보인 KDC의 주소들을 기록, 관리해야 한다.

키 분배 절차를 위해서 별도의 채널을 따로 제공할 필요는 없고 ISDN 프로토콜의 회선-교환 연결 확립

절차에 키 분배 절차를 집적화 할 수 있다. 비밀 키를 이용한 암호화 키 분배 절차를 수행하는 프로토콜은 회선 교환 연결 절차를 수행하는 D채널에서 이루어진다.

여기서 프로시져의 계층 3은 CCITT 권고안 Q.930 초안 3에 기초로 하며, 계층 1과 계층 2는 Q.910과 Q.920 권고안을 기초로 한다. 회선 교환에서의 암호화 키 분배를 위한 호 제어 절차는 (그림 8)과 같다.

이 분배 절차에서 키를 이용한 메시지 M의 암호화는 $\{M\}^K$로 표시한다. 사용자 A는 네트워크 사용자 인터페이스를 통하여 SETUP 메시지를 전송함으로서 호(call)을 초기화한다. SETUP 메시지에는 네트워크에서 호 처리에 필요한 정보가 들어있다. 따라서 사용자 메시지 전송시 정보보호 서비스를 제공받기 위해서는 SETUP 메시지에 암호화 호 지시자(Crypt Call Indicator)를 추가하여 보낸다.



KDC : 키 분배 센터, TA : A의 타임 스탬프, KC : 대화 키
KA : A의 식별 키, ET : Exchange Terminal

(그림 8) 암호화 키 분배를 위한 회선 교환 호 제어 절차
(Fig. 8) Circuit-switched Call Control Procedure for Encryption Key Distribution

그러면 네트워크는 사용자 A의 터미널에 SETUP 메시지의 acknowledge를 위한 SETUP ACKNOWLEDGE 메시지를 보낸 후에 요구에 따라 호를 설정할 것인지를 결정한다. 그리고 요구된 정보보호 서비스에 대한 액세스가 호출하는 사용자 A와 호출된 B가 정당한지를 점검해야 한다. 만약 A와 B가 같은 교환기를 사용하고, 둘 다 정보보호 서비스 사용자이면, 호출된 주소를 갖는 B 채널은 idle하게된다. 그리고 공통 채널 신호방식 네트워크를 이용하여 교환기 LE는 다음 메시지를 사용자 B의 키 분배 센터(KDC_B)에게 보낸다.

순서 1) $LE \rightarrow KDC_B : B, A, KDC_A$

여기서, KDC_A는 A의 키 분배 센터의 주소이다. 이 메시지를 받은 B는 대화 키인 KC를 생성한다. 그리고 다음 메시지를 준비한다.

$MB = \{TB, KC, A\}^{KB}$

여기서, MB는 B에서 전송되는 메시지를 나타내고, KB는 B의 식별 키고, TB는 KDC_B와 B의 로컬 시간이다. 그러면, KDC_B는 KDC_A와 연결을 한 다음에 준비된 메시지를 보낸다.

순서 2) $KDC_B \rightarrow KDC_A : \{A, KC, B\}^{KD}$

여기서, KD는 KDC_B와 KDC_A에 의해 공유된 암호화 키다. 그러면 KDC_A는 다음 응답을 보낸다.

순서 3) $KDC_A \rightarrow KDC_B : MA = \{TA, KC, B\}^{KA}$

여기서, MA는 A에서 전송되는 메시지를 나타내고, KA는 A의 식별 키고, TA는 KDC_A와 A의 로컬 시간이다. 그러면, KDC_B는 호출한 교환기에게 다음 메시지를 보낸다.

순서 4) $KDC_B \rightarrow LE : B, MB, A, MA$

이 메시지를 받은 교환기는 호출된 사용자의 인터페이스에 따라 사용자 B의 터미널에 SETUP 메시지를 전송한다. 이 SETUP 메시지에는 원래의 정보에 암호화 호 지시자와 함께 사용자 데이터 필드에는 MB를 추가한다. SETUP 메시지에 따라 요구사항을 이행하는 터미널 B는 ALTERING 메시지를 이용하여 응답할 때, 교환기는 사용자 데이터 필드에 MA가 포함된 ALTERING 메시지를 호출하는 사용자 인터페이스에 따라 사용자 A의 터미널에 전송한다.

터미널 A와 B는 각각 MA와 MB를 받으면 사용자에 의해 키 KA와 KB를 이용하여 이 메시지를 복호화하여 인증한다. KDCA에 의해 만들어진 메시지 MA에는 Time stamp TA가 들어있다. 복호화시에 터미널은 TA로 점검하는데 자체 로컬 시간과 비교하여 허용 범위에 맞는지를 확인한다. 만약 점검 결과가 만족하게 되면 사용자 A는 수신된 메시지가 불법적인 응답이 아니라는 것을 확인한다. 즉, 이전의 전송을 침입자가 기록해 두었다가 재 전송한 것이 아니라는 것을 확인한다.

호출된 사용자의 주소를 메시지의 내용에 포함시키는 것은 정보보호 프로토콜에 매우 중요하다. 만약 B의 주소가 남아 있어서 침입자가 이것을 X로 변경해 버리면, A는 SETUP 메시지를 통하여 X와 통신하는 것을 모르고 B하고 통신하는 것으로 믿게 하는 결과가 된다. 만약 두 점검 결과에서 하나가 만족스럽지 못하면 터미널 A와 B는 메시지에 호출 클리어를 요구하는 DISCONNECT 메시지를 보낸다.

터미널 B의 점검 결과가 만족하면 네트워크에 CONNECT 메시지를 보낸다. 그러면 교환기는 이 메시지를 받음에 따라 연결 확립을 위해 호출하는 사용자 인터페이스에 CONNECT 메시지를 보낸다. 그러면 이제부터는 사용자 A와 B간의 전송은 키 KC를 이용하여 암/복호화를 수행하여 안전한 통신을 수행하게 된다.

만약에 사용자 A와 B가 같은 교환기를 사용하지 않으면 A의 교환기는 자신의 사용자가 관리 기간 내에는 요구에 따라 호출 확립을 결정한 후에, 교환기간에 전송되는 정보에 사용자 A의 키 분배 센터의 주소와 암호화 지시자를 네트워크에 보내서 적절한 상호-교환 신호방식과 교환 절차를 시작한다. 그러면 사용자 B의 교환기는 네트워크로부터 호출에 대한 정보를 받은 후에 사용자 B가 연결되어 있으면 호를 연결할 것인지를 결정한다. 그러면 B의 키 분배 센터와 연결하게 되어 위의 절차를 계속하게 된다. 메시지 MA는 end-to-end 신호방식으로 공통 채널 신호방식 시스템의 USER DATA 필드를 이용하여 사용자 A에게 네트워크를 통하여 보내지게 된다.

4.3. 하이브리드 암호화 시스템을 이용한 키 분배 및 인증과 호 제어

비밀 키 암호화 시스템에서는 A와 B간의 안전한 통신 링크를 확립하기 위하여 먼저 암호화 키인 비밀키를 교환해야 한다. RSA 알고리즘같은 공개 키 방법에서는 A와 B간의 안전한 통신을 위해 공개 키를 교환해야 한다. 그리고 이 두 시스템은 키값의 교환을 증명해야 한다. 즉 A는 수신된 키가 반드시 B로부터 온 것임을 보증해야하고 그 반대도 보증되어야 한다[10].

본 논문에서는 비밀키 암호화 시스템과 공개키 암호화 시스템을 결합한 하이브리드 암호화 시스템을 이용하여 사용자 정보의 비밀성과 인증을 확립하고자 한다. 따라서 A와 B간의 안전한 통신을 위해서는 먼저 상호간의 키 보증을 확립할 수 있는 키 인증 센터를 두어야 한다.

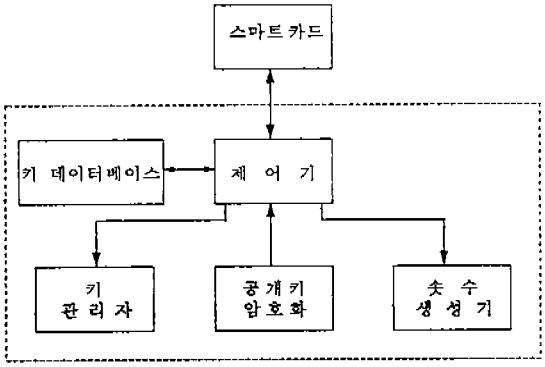
4.3.1. 키 인증 센터

규모가 큰 네트워크 시스템에서 안전한 통신 링크를 확립하고자 하는 사용자들에 대하여 모든 사용자의 공개 키를 보증하는 키 인증 센터를 확립해야 한다. 즉 네트워크의 각 사용자는 공개 키를 생성하게 되고, 키 인증 센터에 의해 증명되어야 한다. 사용자는 한번의 공개 키에 대한 인증을 받으면 자신의 공개 키를 다른 사용자에게 보내야 한다. 그리고 네트워크의 모든 사용자는 자신의 공개 키와 비밀 키를 생성하여 KCC(Key Certification Center)에 공개 키를 등록하고, 또 KCC도 자신의 공개 키와 비밀 키를 생성하여 사용자에게 알려줌으로서 모든 사용자는 인증 센터의 공개 키를 알고 있어야 한다.

사용자의 키 쌍은 KCC에 의해 또는 자기 스스로 생성할 수 있지만 KCC가 생성하는 것으로 한다. 그러면 KCC는 사용자의 공개 키와 자기 자신의 비밀 키를 이용한 식별 번호(identification number)를 암호화하여 스마트카드에 A의 비밀 키와 자신의 공개 키를 기억시킨다. 데이터는 A의 개인 식별 번호(PIN: Personal Identification Number)를 이용하여 스마트카드에서 암호화되며, KCC의 구성은 (그림 9)와 같다.

스마트 카드에는 인증서도 포함되는데, 이 인증서의 사용가능한 기간은 처음과 마지막 날짜 값을 이용하여 확인한다. 그래서 A는 네트워크에서 다른 사용자와 안전한 통신 링크를 원하면 자신의 인증 된 키를 보내야한다. A의 인증된 공개 키를 받은 모든 사

용자는 KCC의 공개 키를 이용하여 이를 복호화하여 식별 번호와 공개 키를 얻어서 이것이 정말로 A의 공개 키임을 안다. 그러면 A에게 자신의 인증서를 보낸다. 그러면 A는 같은 방법으로 이것이 B의 공개 키인지 아닌지를 확인한다. 따라서 공개 키는 메시지에 대한 비밀 키 암호화 시스템을 이용하기 위한 키를 교환하는데 이용된다. 이 프로시져는 재생(playback) 공격에 대해 보호되어야 한다. 이 공격에 대하여 보호하는 유일한 방법은 인증서에 인증 토큰을 포함하는 것이다. 이 방법은 CCITT와 ISO에서 제안된 디렉토리 인증 골격의 세방향 강한 인증과 매우 유사하다.



(그림 9) 키 인증 센터
(Fig. 9) Key Certification Center

4.3.2. 키 등록 절차

먼저 (그림 10)과 같은 키의 등록절차가 필요하다.

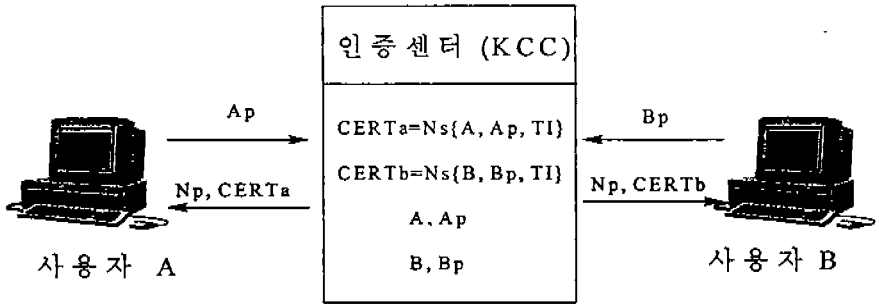
1)사용자 A와 사용자 B는 자신의 공개키와 비밀키를 발생시켜 자신의 공개키인 Ap와 Bp를 키 인증 센터에 등록한다.

2)키 인증 센터는 자신의 공개키와 비밀키를 발생시켜 자신의 비밀키로 사용자 A, 사용자 A의 비밀키, 인증서의 타당성 주기를 암호화하여 인증서 CERTa를 만든다. 또 자신의 비밀키로 사용자 B, 사용자 B의 비밀키, 인증서의 타당성 주기를 암호화하여 인증서 CERTb를 만든다.

3)키 인증 센터는 공개키 Np와 CERTa를 사용자 A에게 전달하고, 공개키 Np와 CERTb는 사용자 B에게 전달한다.

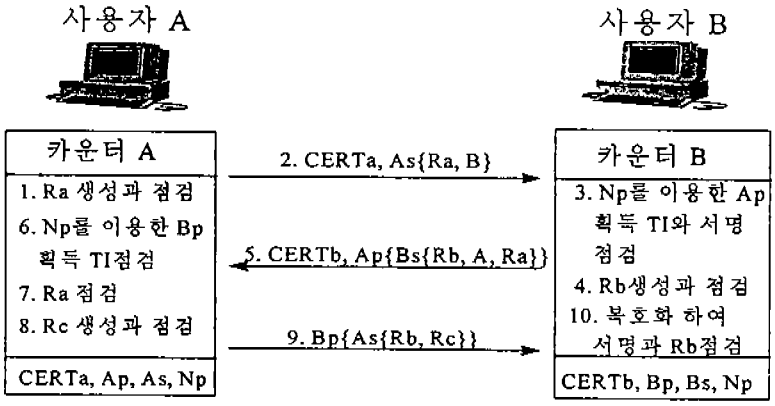
키 인증 센터에 의해 키 등록절차가 확립되면 사용자 상호 인증을 위해 (그림 11)과 같은 통신 절차를 따른다.

여기서 키 Ap를 이용한 메시지 M의 암호화는 Ap{M}로 표현한다. 그리고 A:사용자 A를, Ap:사용자 A의 공개 키를, As:사용자 A의 비밀 키를 나타내고, Bp:사용자 B의 공개 키를, Bs:사용자 B의 비밀 키를, Np:인증 센터의 공개 키를 나타내며, Ns:인증 센터의 비밀 키를, CERTa:사용자 A의 인증서를, TI:인증서의 타당성 주기를, Ra, Rb, Rc:카운터에 의한 순서부분을 이용한 난수를 나타낸다.



CERTa : 사용자 A의 인증서, CERTb : 사용자 B의 인증서,
Ap : 사용자 A의 공개 키, Bp : 사용자 B의 공개 키,
Ns : 인증센터의 비밀 키, Np : 인증센터의 공개 키,
TI : 인증서의 타당성 주기, A : 사용자 A, B : 사용자 B

(그림 10) 키 인증 센터 확립 절차
(Fig. 10) Key Certification Center Establishment Procedure



CERTa : 사용자 A의 인증서, CERTb : 사용자 B의 인증서,
Ap : 사용자 A의 공개 키, Bp : 사용자 B의 공개 키, As : 사용자 A의 비밀 키
Bs : 사용자 B의 비밀 키, Np : 인증 센터의 공개 키, A : 사용자 A, B : 사용자 B
Ra, Rb, Rc : 카운터에 의한 순서부분을 이용한 난수

(그림 11) 인증과 키 비밀성을 위한 통신 절차
(Fig. 11) Communication Procedure for Authentication and Key Secrecy

4.3.3. 사용자 상호 인증과 통신 절차

사용자 상호간의 인증과 키 비밀성을 위한 통신 프로시져는 다음과 같다.

1)A는 위조를 예방하고 재생 공격을 알아내기 위해 사용하는 난수 Ra를 만들어낸다. Ra는 카운터 A에 의해 생성된 순서부분에 포함되어있고, 모든 세션에서 매번 유일성에 대해 점검된다. Ra는 토큰의 한 부분이지만 암호화되지 않는 부분이기 때문에 비밀키 암호에 대한 메시지 키로서만 사용되고 이 암호에 대한 비밀 키로는 사용되지 않는다.

2)그러면 A는 다음 메시지를 B에게 보낸다.

CERTa, As{Ra, B}

3)그러면 B는 다음 과정을 실행한다.

①Np를 이용 복호화하여 CERTa로 부터 Ap를 얻는다. 그리고 A의 인증이 만료되지 않았는지 점검 한다.

②서명을 검증하고 서명된 정보의 무결성을 점검한다.

4)B는 Ra와 같은 목적으로 사용하기 위해 난수 Rb를 생성한다. 순서번호에 없는 이 숫자는 토큰의 서명이 되고 암호화된 토큰의 한 부분을 형성하기 때문에 비밀 키 부분을 형성하는데 이용될 수 있다.

5)B는 A에게 다음 메시지를 보낸다.

CERTb, Ap{Bs(Rb, A, Ra)}

6)A는 다음 과정을 실행한다.

①Np를 이용하여 복호화하여 CERTb로부터 Bp를 얻는다. 그리고 B의 인증서가 기간이 만료되지 않았는지 점검한다.

②인증 토큰을 복호화한 다음 서명을 검증한다. 그리고 서명된 정보의 무결성을 점검한다.

7)A는 수신된 난수 Ra가 보낸 Ra와 동일한 지를 점검한다.

8)그러면 A는 난수 Rc를 생성하고 점검한다. Rc는 비밀 키 암호 시스템에서 비밀 키를 위하여 Rb와 결합할 목적으로 생성하는 또 다른 난수이다. 일단 세션이 끝나면 이 생성된 세개의 난수는 모두 없어지게 되고 단지 순서부분만 참조를 위해 기억시켜 둔다.

9)A는 다음 인증 토큰을 B에게 보낸다.

Bp{As(Rb, Rc)}

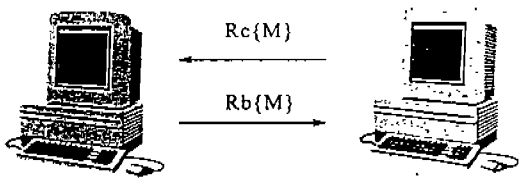
10)B는 다음 과정을 실행한다.

①인증 토큰을 복호화하고 서명을 점검하고 서명된 정보의 무결성을 점검한다.

②수신된 Rb가 보낸 Rb와 동일한 것인지 점검한다.

상호 인증이 확립된 후 (그림 12)와 같이 사용자 A는 Rb를 이용하여 메시지를 암호화한 후 사용자 B에게 전송하면, 사용자 B는 자신이 알고 있는 Rb를 이

용하여 복호화를 한 후 메시지를 받아 볼 수 있다. 반대로 사용자 B는 Rc를 이용하여 메시지를 암호화한 후 사용자 A에게 전송하면, 사용자 A는 자신이 알고 있는 Rc를 이용하여 복호화한후 메시지를 받아 볼 수 있다.



Rb, Rc : 카운터에 의한 순서 부분을 이용한 난수

(그림 12) 메시지 비밀성을 위한 통신 절차
(Fig. 12) Communication Procedure for Message Secrecy

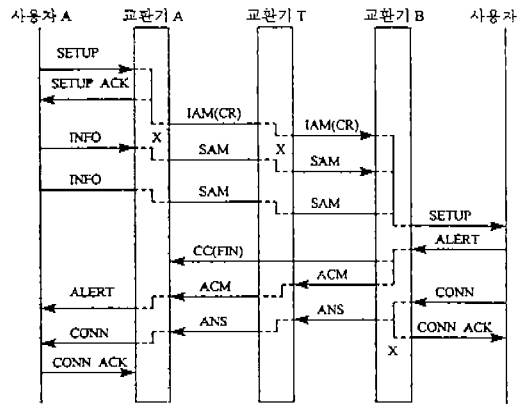
이 시스템의 장점은 사용자는 네트워크에서 상대방에 대한 공개 키를 인증할 때에 KCC를 한번만 액세스하면 된다. 그래서 긴 디렉토리를 분배할 필요도 없고, 통신을 원할 때 on-line 키 분배 센터로부터 새로운 세션 키를 얻어야하는 결점(bottleneck)도 없다. 또 다른 장점은 사용자 자신들이 직접 비밀 키와 공개 키를 생성할 수 있고, KCC가 할 수도 있다. 또 이 하이브리드 암호화 시스템을 이용하면 디지털 서명과 인증의 부가적인 장점을 갖는다.

이 하이브리드 암호화 시스템은 점-대-점, 패킷 교환 통신, 전자우편 시스템과 같은 여러 가지 통신 시스템의 응용에 맞출 수 있다.

4.3.4. ISDN에서의 구현

ISDN 구조와 프로토콜은 하이브리드 암호화 시스템에서의 키 분배 기능은 D채널을 이용한 회선 교환 연결 확립 절차에 집적화할 수 있다. 권고안 Q.910과 Q.920이 계층 1과 2에 Q.930이 계층3에 적합하며, 이 절차는 (그림 13)과 같다[2].

사용자 A의 터미널은 사용자-망 인터페이스에 따라 SETUP 메시지를 전송하므로서 호를 초기화한다. 메시지의 사용자 데이터 필드에는 안전한 통신 절차에 따른 호를 처리하기 위해 필요한 사용자 A의 인증서와 인증 토큰 등이 포함되어 있다. 네트워크는 SETUP



X : 사용자 정보 채널 연결
IAM : Initial Address Message
ACM : Address Complete Message
ANS : Answer Message

(그림 13) ISDN에서의 안전한 통신 절차의 집적화
(Fig. 13) Integration into ISDN of Secure Procedure

메시지를 알리기 위해 터미널에 SETUP ACKNOWLEDGE 메시지를 보낸 후에 호를 요구에 따라 확립할 것인지를 결정한다. 그러면 교환기 A는 지시에 따라 교환기 B를 이용하여 사용자 정보 채널을 확립하기 위하여 공통 채널 신호방식 네트워크를 이용한다. 그러면 B의 교환기는 호출된 사용자의 인터페이스에 따라 SETUP 메시지를 전송하므로서 프로시져를 계속한다. 메시지에는 USER DATA 필드에 A의 인증서와 인증 토큰이 들어있다. 그러면 사용자 B는 A의 인증서와 토큰의 인증성을 확인한다. 만약 만족하면 지시에 따라 USER DATA 필드에 자신의 인증서와 토큰을 포함한 ALERT 메시지로 응답한다. 그러면 교환기가 호출하는 사용자 인터페이스에 따라 전송한다. 그러면 A는 B의 인증서와 토큰을 인증한다. 만약 만족하지 못하면 터미널은 네트워크에 호 클리어 요구 메시지인 DISCONNECT메시지를 네트워크에 보낸다. B 터미널도 이와 같이 동작한다. 만약 만족하면 네트워크에 CONNECT 메시지를 보낸다. 그러면 교환기 A는 사용자 인터페이스에 따라 CONNECT 메시지를 보낸다.

A의 토큰으로 구성된 세방향 인증의 세 번째 메시지는 공통 신호방식 시스템을 통하여 사용자-대-사용자 신호방식을 이용하여 B에게 전송된다. 만약 B가 인증된 토큰을 받은 후에 이를 만족하면, 이 후의 A와 B간의 전송은 난수 Rb와 Rc의 조합인 키를 이용

하여 암호화된다. 그렇지만 B가 A의 인증이 만족하지 않으면 연결 해제를 할 수 있다.

그러면 이제 B 채널을 통하여 암호화된 메시지가 전송되게 된다. 이때 비밀 키 암호화 시스템의 비밀키는 B 채널에서 수행되는 통신에 대한 인터럽트 없이 D 채널을 통하여 사용자-대-사용자 신호방식을 이용하여 변경할 수 있다. 또 ISDN D 채널 신호방식은 네트워크 상에서 호출하는 상대방을 식별을 할 수 있기 때문에, 이것은 여러 레벨에 정보보호를 적용할 수 있다.

5. 결 론

현재 선진국에서는 미래의 정보화 사회를 위한 종합 정보 통신망 구축과 활용을 위한 노력으로 팩시밀리, 텔레텍스, 비디오텍스 등을 통합하기 위해 필요한 사용자 인터페이스, 대중화 등 관련 기술 개발에 노력을 계속하고 있으며, 80년대 초에 ISDN 시범 서비스를 완료하고 현재는 사용 서비스의 초기 단계에 진입한 실정이다. 국내에서도 1985년 ISDN 기술의 연구 개발을 단계적으로 추진하여 3단계인 1997년부터는 전국적으로 서비스를 확대할 예정으로 추진 중에 있다.

ISDN은 사용자가 필요로 하는 음성, 화상, 데이터 등 다양한 종류의 서비스를 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 프로토콜이 개발되어야 한다.

ISDN에서 정보보호 서비스를 제공하기 위해서는 가장 효율적인 암호화 시스템을 정합한 최적의 정보보호 프로토콜이 개발되어야 한다. 따라서 본 논문에서는 ISDN의 사용자-망 인터페이스의 구성과 ISDN에서 적용 가능한 암호화 시스템과 적용방식과 Q.931 프로토콜을 분석하여 호 제어 절차를 제안하였다. 또한 비밀 키 시스템을 이용해 ISDN에서의 사용자 사이의 정보에 대한 비밀성과 인증 시스템을 제안하였다. 본 논문에서 연구한 하이브리드 암호화 시스템의 키 인증 센터의 확립 절차와 인증과 키 비밀성 그리고 메시지 비밀성을 ISDN의 통신절차에 직접 적용하면 사용자 정보에 대한 비밀성과 인증 서비스를 제공할 수 있다.

앞으로의 연구에서는 종합적인 ISDN 정보보호 서비스를 제공하는 방안에 대해서 진행하여, 이를 ISDN 시스템 구조와 프로토콜에 효율적으로 정합하는 방안에 대해서 좀 더 연구가 진행되어야 하겠다.

참 고 문 헌

[1] ITU-T Recommendation I.310 ISDN-Network Functional Principles, 1993.

[2] ITU-T Recommendation Q.920 Digital Subscriber Signalling System No.1 (DSS1)-ISDN, 1993.

[3] ITU-T Recommendation I.430 Basic User-Network Interface-Layer 1 Specification, 1993.

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

[5] Umberto De Julio, Giorgio Pellegrini, "Layer 1 ISDN Recommendations," IEEE Journal on SAC, Vol. SAC-4, No. 3, May 1986.

[6] Sadahiko Kano, "Layer 2 and 3 ISDN Recommendations," IEEE Journal on SAC, Vol. SAC-4, No. 3, May 1986.

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

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

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

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

[11] 김봉한, 이선우, 이재광, "ISDN 정보보호 프로토

콜 적용에 관한 연구," 한국정보과학회 충청지부 추계학술논문발표집, 제7권, 제1호, 1995.
[12] 박응기, 정기현, 정현철, 손기욱, 신기수, "ISDN에서의 인증 방법," 한국정보과학회 충청지부 추계학 술논문발표집, 제7권, 제1호, 1995.
[13] 권태경, 강명호, 송주석, 정기현, 신기수, "ISDN 사용자 정보의 비밀보장에 관한 연구," 한국정보과학회 추계학술논문집, 제 21권, 2호, 1994.

정 현 철

1989년 계명대학교 전자계산학과 졸업(공학사)
1991년 경북대학교 대학원 컴퓨터공학과 졸업(공학석사)
1991년~현재 한국전자통신연구소 연구원
관심분야:통신정보보호, 계산이론

신 기 수

1975년 서강대학교 전자공학과 졸업(공학사)
1989년 충북대학교 컴퓨터공학과 졸업(공학석사)
1975년~1977년 육군 전략통신사령부 근무
1977년~1978년 삼성전기 근무
1978년~1980년 원효전자 근무
1980년~현재 한국전자통신연구소 책임연구원
관심분야:컴퓨터 네트워크, 통신정보보호

이 선 우

1995년 한남대학교 공과대학 전자계산공학과(공학사)
1995년~현재 한남대학교 대학원 전자계산공학과 석사과정
관심분야:컴퓨터 네트워크, 컴퓨터통신 정보호

김 봉 한

1994년 청주대학교 이공대학 전자계산학과(공학사)
1996년 한남대학교 대학원 전자계산공학과(공학석사)
1996년~현재 한남대학교 대학원 전자계산공학과 박사과정
관심분야:컴퓨터 네트워크, 컴퓨터통신 정보호

김 점 구

1990년 광운대학교 이과대학 전자계산학과(이학사)
1994년 광운대학교 전산대학원 전자계산학과(이학석사)
1991년~1993년 (주)제성프로젝트 정보통신전자기술연구소
1995년~현재 안양전문대 전자통신과 시간강사

이 재 광

1984년 광운대학교 이과대학 전자계산학과(이학사)
1986년 광운대학교 대학원 전자계산학과(이학석사)
1993년 광운대학교 대학원 전자계산학과(이학박사)
1986년~1993년 군산전문대학 전자계산학과 부교수
1993년~현재 한남대학교 전자계산공학과 조교수
1994년~현재 한국정보처리학회 학회지 편집위원
1995년~현재 한국통신정보보호학회 학회지 편집위원
관심분야:컴퓨터 네트워크, 컴퓨터통신 정보보호, 네트워크 관리