ISDN 사용자 정보의 비밀보장을 위한 키 분배 및 인증 방법

°권태경, 강명호, 송주석

연세대학교 전산과학과

A Method on Key Distribution and Authentication for the Confidentiality of ISDN User Information

°TaeKyoung Kwon, MyeongHo Kang, JooSeok Song

Dept. of Computer Science, Yonsei University

협대역 ISDN은 사용자-망 인터페이스가 디지탈화되므로 사용자 정보를 보호하기 위한 기능을 비교적 저렴하게 사용자-망 인터페이스에서 제공할 수 있다. 그러나 음성, 화상, 데이타 등 정보의 종류가 다양하고 여러 채널을 통한 다양한 서비스 기능이 있으므로 실제적인 구현에는 많은 어려움이 따른다. 이러한 문제들을 고려하여 본 논문에서는 ISDN 사용자 정보의 비밀보장 서비스를 위한 키 분배 및 인증 방법을 제안하였다. 따라서 먼저 ITU-T(구 CCITT) 권고안의 표준을 중심으로 ISDN 사용자-망 인터페이스의 구조와 ISDN의 각종 서비스에서 우려되는 정보침해 요소를 분석한 후, 이 분석 자료를 근간으로 하여 비밀보장 서비스를 위한 기본적인 정책을 수립하고 적합한 프로토콜 구조를 제안하였다. 그리고 Diffie-Hellman이 제안한 공개키 분배방식을 기반으로 하여, 호(Call)설정시 Q.931 메세지 교환을 통하여 키 분배 및 인증이 안전하게 이루어지도록 적합한 키 분배 프로토콜을 제안하였으며, 키의 분배 및 인증의 명확성 여부를 GNY 로직을 이용하여 검증하였다.

1. 서론

ISDN망이 상용화되고 사용자들이 늘어나게 됨에 따라 좋은 품질의 서비스와 안전한 통신에 대한 요구도 점점 증대되어 가고 있다. 기존의 공중전화망(PSTN)을 근간으로 발전하는 협대역 ISDN은 음성, 화상, 데이타 등의 다양한 종류의 정보를 유통하는 종합정보통신망으로서 정보의 침해에 대해서 기존의 통신망보다 더욱 민감하다. 이미 기존의 여러 통신망 운영에서 보고되고 있는 정보에 대한 침해 사례를 보면 그 방법 및 기술면에서 점점 지능화되고 있으며, 특히 컴퓨터망이나 전화망을 통한 침해사건이 심각하게 증가하고 있음을 알 수 있다. 따라서, 기존의 통신망과 연동 또는 통합하며 다양한 서비스를 제공하는 ISDN을 위하여 사용자 정보에 대한 보안 서비스를 제공할 수 있도록 구체적인 방안이 마련되어야 하겠다.

기존의 아날로그 전화망에서는 고음질을 유지하며 음성정보의 보호를 실시간에 제공하는데 있어서 비용 등의 많은 부담이 있었다. 그러나 종합정보통신망인 ISDN은 사용자-망 인터페이스 부분이 디지탈화되므로 음성 및 데이타 신호의 종단간(End-to-end) 암호화를 비교적 저렴한 가격으로 가능하게 하며, 근시일에는 단일 세션 암호키로 종합 정보의 보호를 할 수 있을 것으로 기대된다. 또한, 밴드내 신호처리(In-band Signaling)를 하는 기존의 전화망과 달리 밴드외 신호처리(Out-of-band Signaling)를 하게 되는 ISDN은 정보의 암호화를 위한 키분배 등에 있어서 유리한 면을 갖고 있다. 그러나 제공되는 서비스가 다양하며 또한 기존 서비스의 폐지 및 새로운 서비스의 개시가 유동적이

므로 실제적인 구현에는 많은 어려움이 따른다. 특히 각 서비스별로 응용계층에서 보안기능을 구현할 경우에는 키 관리 부담 및 성능저하가 우려되므로, ISDN은 단일 세션키로 종합정보를 보호할 수 있도록 해야 한다.

본 논문에서는 ISDN 사용자 정보의 비밀보장을 위한 방법을 기본 액세스(2B+D) 사용자-망 인터페이스 구조상에서 검토해 보았고, 구체적인 키 분배 및 인증 방법을 제안하였다. 따라서 먼저 ITU-T 권고안을 중심으로 ISDN 사용자-망 인터페이스의 구조와 ISDN의 각종 서비스에서 우려되는 정보침해 요소를 분석하였고, 이 분석 자료를 근간으로 하여 비밀보장 서비스를 위한 기본적인 정책 및 적합한 프로토콜 구조를 제안하였다. 그리고 Diffie-Hellman이 제안한 공개키 분배방식을 기반으로 하여, 호(Call)설정시 Q.931 메세지 교환을 통해서 키 분배 및 인증이 안전하게 이루어지도록 적합한 키 분배 프로토콜을 제안하였으며, 제안한 프로토콜의 키 분배 및 인증 성능에 대한 평가는 GNY 로직을 이용하여 검증하였다.

2. ISDN의 구성 및 정보침해 요소

2.1 ISDN의 서비스

ISDN은 기존의 통신망과 달리 모든 정보를 디지탈 신호로 유통하며, 다양한 종류의 정보 서비스를 종합적으로 제공할 수 있다. ISDN의 사용자는 통신망 서비스의 전부 혹은 일부를 사용하게 된다. ISDN 서비스는 크게 기본 서비스와 보조 서비스로 구분되는데, 여기서 기본 서비스는 베어러 서비스(Bearer Service)와 텔리 서비스(Teleservice)로 나뉘어진다. 베어러 서비스란 OSI 참조모델의 1,2,3계층에 해당하는 하위계층 기능만을 제공하는 서비스를 의미하고, 텔리서비스란 하위계층 기능과 4,5,6,7계층 즉, 상위계층 기능을 모두 제공하는 서비스를 의미한다. 또한 보조 서비스란 기본 서비스의 기능 향상을 위해서 제공되는 부가적인 서비스로서 주로 사용자들에게 높은 수준의 편리함과 친숙함을 제공하기 위해서 이용된다.

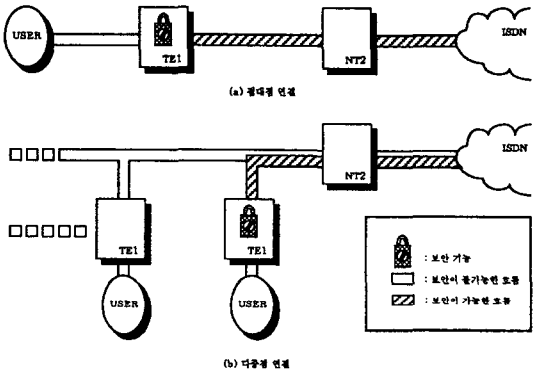
2.2 ISDN의 사용자-망 인터페이스

ISDN을 구성하는 기능 그룹은 크게 사용자 댁내 기능, 통신망 기능, 통신망 운용 관리 기능, 그리고 통신 처리 기능으로 구분된다. 이 중 사용자 댁내 기능은 사용자의 서비스 운용과 이에 사용되는 사용자 기기의 망 접속 및 이의 유지 보수 등을 포함한다. 사용자 댁내 기능의 표현을 위해서 사용자-망 인터페이스를 개념적으로 정의하는데 ISDN의 사용자-망 인터페이스 기능이란 사용자와 망 상호간의 통신을 위하여 제공되는 기능을 말한다. ISDN은 기존 통신망과 달리 다양한 서비스를 종합적으로 제공할 수 있어야 하므로 여러가지 서비스를 사용자가 제공받을 수 있는 통신 서비스 액세스 참조점(Reference Point)이 분명하게 제시되어 있다. 즉, ISDN의 사용자-망 인터페이스는 TE1, TE2, TA, NT1, NT2 등 기능 요소에 해당하는 각종 장치들과 액세스 지점의 특성을 표준화하는 참조점 R, S, T, U, V 등으로 구성된다. 사용자-망 인터페이스의 회선연결 방법에는 점대점연결과 다중연결이 있는데, 이 두가지 연결방법을 모두 고려하여 사용자 정보의 비밀보장 기능을 사용자-망 인터페이스에서 제공하도록 하는 개념도는 [그림 1]과 같다.

2.3 ISDN의 3계층 신호 프로토콜

협대역 ISDN은 사용자-망 인터페이스에서는 DSS1 신호 프로토콜을, 그리고 망내부의 교환국간에서는 SS#7 신호 프로토콜을 사용하며, DSS1의 2계층을 위해서 LAPD가 표준화되어 있다. DSS1의 3계층을 위해서는 ITU-T 권고안 Q.930에서 ISDN 사용자-망 인터페이스의 3계층 신호처리 및 호제어

에 대한 사항을 규정하고 있으며, ISDN 망연결을 설정확립(Establish), 유지(Maintain), 해제(Clear)하기 위한 프로토콜들을 정의하고 있다. ISDN의 망연결 형태에는 B채널을 이용하는 회선교환연결, D채널 또는 B채널을 이용하는 패킷교환연결, D채널을 이용하는 사용자간 신호연결 등이 있다. ITU-T 930에서 정의하는 3계층 신호 프로토콜은 기본적인 호제어를 위한 Q.931, 부가서비스를 위한 Q.932, 프레임릴레이를 위한 Q.933 등이 있다. ITU-T Q.931 신호 메세지의 최대크기는 260 옥텟(Octet)이며 호의 설정 및 유지, 해제 등을 위한 다양한 종류의 메세지와 각 메세지를 구성하는 다양한 정보원소들을 갖는다. 다음의 [표 1]은 중요한 메세지와 정보원소들을 나타내고 있다. 본 논문에서는 호설정시 Q.931 메세지에 암호화를 위해서 필요한 키 정보를 삽입하여 전송하도록 한다.



[그림 1] 사용자-망 인터페이스의 정보보호기능

	MORE DATA	REPEAT INDICATOR	BEARER CAPABILITY	CHANNEL IDENTIFICATION	END TO END TRANSIT DELAY	CALLING PARTY NUMBER	CALLED PARTY NUMBER	USER USER
CALL ESTABLISHMENT MESSAGES								
ALERTING				●				●
CALL PROCEEDING				●				
CONNECT				●	●			●
CONNECT ACKNOWLEDGE				●				
SETUP		●	●	●	●	●	●	●
CALL INFORMATION PHASE MESSAGES								
USER INFORMATION	●							●
CALL CLEARING MESSAGES								
DISCONNECT								●
RELEASE								●
RELEASE COMPLETE								●

[표 1] Q.931의 주요 메세지 및 정보원소

2.4 ISDN의 정보침해 요소

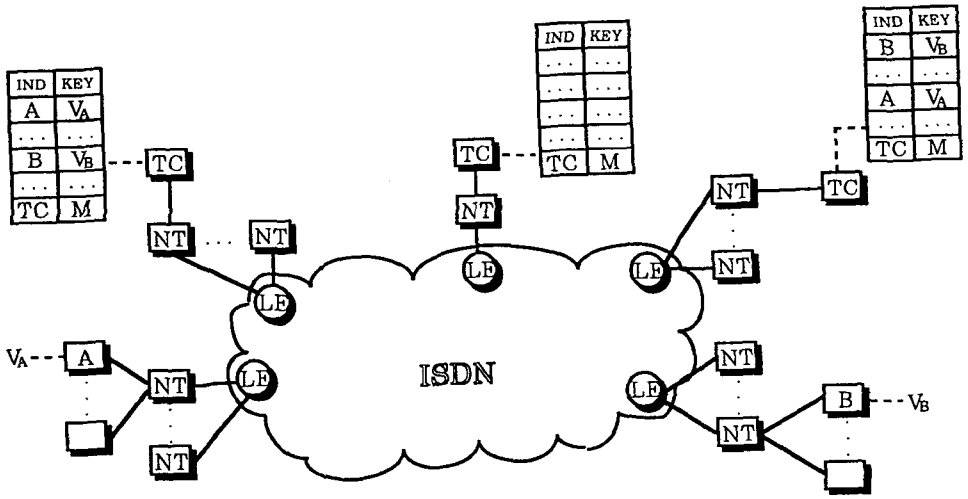
정보화사회의 고도화가 이루어지고 있는 현재 통신망 사용자들의 요구는 기존의 통신망들이 제공하던 정보서비스를 넘어서, 음성 정보, 문서 정보, 고화질의 정지화상 정보, 동화상 정보 등에 대한 다양한 정보서비스를 종합적으로 제공받기를 원하고 있는데, 이와 같은 요구를 충족시켜줄 수 있는 통신망이 ISDN이다. 그러나 점점 늘어나고 있는 통신망 정보의 유통은 사용자들에게 용이한 정보취득이란 편의를 제공하는 반면, 통신망으로 집중된 정보들에 대한 막대한 침해 피해를 더욱 증가시키고 있다. 따라서 모든 정보를 디지탈신호로 유통하며 기존의 통신망들과 통합 또는 연동하게 되는 ISDN에서는 더욱 다양한 정보침해가 우려된다. ISDN에서 우려되는 정보침해 요소는 다음의 [표 2]와 같이 분류할 수 있다.

(1) **통신정보의 비밀성(Secrecy) 파괴**
회선침입(Wiretapping)에 의한 디지탈 정보의 유출은 ISDN 사용자 정보의 비밀보장을 파괴한다.
(2) **통신정보의 무결성(Integrity) 파괴**
ISDN망은 디지탈신호로 정보를 유통하므로 불법자에 의한 정보 변조 및 수정이 쉽게 가능하다.
(3) **서비스 거부 - 가용성(Availability) 파괴**
ISDN의 망장비들에 대한 물리적인 공격이나 소프트웨어적인 침투로 사용자들에 대한 서비스가 중단될 수 있다.
(4) **원격접근침입(Remote Access Intrusion)을 위한 ISDN망 이용**
공중전화망을 통해서 자주 이루어지고 있는 원격접근침입은 공중 ISDN망에 연결된 시스템들에 대해서도 더욱 빈번해질 것이다.
(5) **망을 이용한 사기(Fraud)행위**
호출자의 익명성이 유지되고, 인증방법이 없는 공중 ISDN망에서는 통신을 이용한 사기 및 공갈행위가 우려된다.
(6) **키 갈취 및 세션 설정 방해 행위**
ISDN의 신호체계에 적합하지 않은 암호기법을 이용할 경우, 지능적인 키의 갈취 및 정상적인 세션 설정을 방해하는 행위가 우려된다.

[표 2] ISDN의 침해요소

3. ISDN 보안 정책

ISDN 사용자 정보의 비밀보장을 위해서는 각 사용자 영역에 보안 프로토콜을 구성해야 하며 빠르고 안전한 암호화 방법과 안전한 분배 및 인증이 가능한 키 관리 방법을 마련해야 한다. 본 논문에서는 키 분배 및 인증의 안전성을 위해서 가장 일반적인 공증 기법인 안전센터(TC:Trusted Center)를 지역적으로 구성하도록 한다. 사용자 영역의 단말기는 제작 당시에 고유의 일련번호가 할당되며, 이것은 TC와 비밀정보교환을 가능하게 하는 비밀키의 역할을 하게 된다. TC는 각 사용자 영역의 식별번호(ID)와 해당하는 일련번호 즉, 각 단말기의 비밀값을 해쉬테이블로 관리한다. 본 구성에서 가장 중요한 조건은 TC의 비밀값테이블(V-table)이 안전하게 유지되어야 한다는 것이다. TC는 키의 생성에 필요한 공증인 역할만 하게 되며 실제 정보를 암호화하는 세션키는 각 세션마다 통신자 당사자가 생성하도록 한다. 이것은 키분배 프로토콜을 Diffie-Hellman이 제안한 공개키분배방식을 기반으로 설계하였기 때문에 가능하며, TC는 이 방식에서 필요한 공통정보 g와 n을 사전에 안전하게 분배하도록 한다. TC는 지역을 단위로 존재하게 되며 각 지역의 TC는 계층적인 구조로 상위 TC와 정보를 유통하게 된다. 즉, 각 지역마다 새롭게 등록되는 비밀값은 상위 TC에 안전하게 전달해야 하며 타지역의 새로운 등록값은 상위 TC로부터 제공받게 한다. (5장 참조) 본 논문에서 제안하는 보안을 위한 ISDN의 구성은 다음의 [그림 2]와 같다.



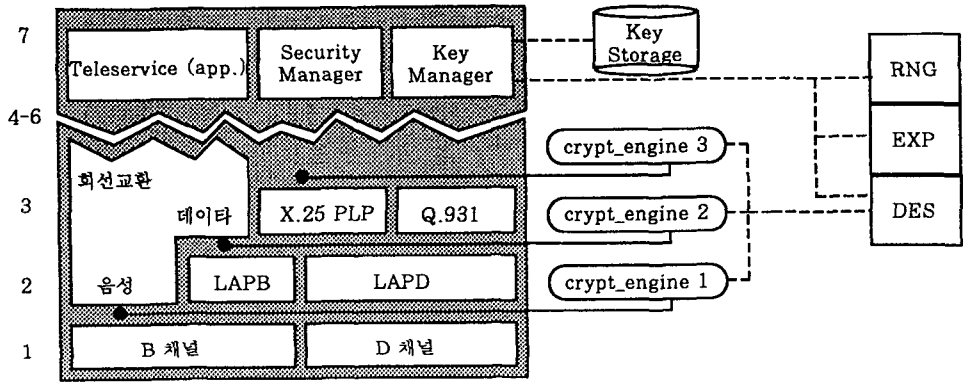
[그림 2] 보안을 위한 ISDN의 구성도

4. ISDN 보안 프로토콜

4.1 보안 프로토콜 구성

본 논문에서 고려하는 보안 프로토콜의 주요 기능은 ISDN을 통하여 유통되는 사용자 정보의 비밀성을 보장하도록 하는 것이며, 이 기능은 명확하고 안전한 암호 기술로써만 구현 가능하다. 제안하는 프로토콜 구조는 비밀보장 이외의 추가적인 보안 서비스 확장이나 광대역 ISDN에의 응용을 고려하여 유연하게 구성하였다. 본 논문의 보안 프로토콜 구성에서는 기본적인 프로토콜 스택 구조 및 각 기능부의 주요 기능, 안전한 키 분배 및 인증을 위한 기능부의 처리 절차의 제안만을 포함하

도록 한다. 한편, ISDN의 기본 액세스 인터페이스(2B+D)에서는 두개의 B채널과 하나의 D채널을 제공한다. 따라서 ISDN에서는 D채널을 이용한 밴드외 신호처리(Out-of-band Signaling) 및 회선교환 또는 패킷교환을 이용하는 다양한 서비스의 제공이 가능하며 각 채널 및 서비스 형태별로 프로토콜들이 구성된다. 본 논문에서는 이러한 사항들을 고려하였고, ISDN 사용자-망 인터페이스의 보안 프로토콜 스택 구성을 위해서 주요부(Primary Part)와 메카니즘부(Mechanism Part)로 구분되는 보안기능부를 기존의 프로토콜 구조에 추가하였다. 주요부는 Security Manager와 Key Manager, 그리고 1,2,3 각 계층의 Crypt Engine으로 구성되며 메카니즘부는 Key Storage, DES, EXP, RNG 등으로 구성된다. 보안 프로토콜의 구성도는 다음의 [그림 3]과 같다.



[그림 3] 사용자-망 인터페이스의 보안 프로토콜 구성도

4.2 보안기능부

(1) 주요부는 보안기능을 처리하고 제어하는 정책적 기능단위들로 구성된다.

- Security Manager : 전체 시스템을 제어하며, 사용자의 입력과 하위계층으로부터의 전달신호를 처리한다.
- Key Manager : 세션키를 생성하고 관리한다.
- Crypt_Engine 1 : B채널을 이용하는 회선교환 음성 신호를 1계층에서 암호화 및 복호화한다.
- Crypt_Engine 2 : B채널을 이용하는 회선교환 데이타 신호를 2계층에서 암호화 및 복호화한다.
- Crypt_Engine 3 : B채널 또는 D채널을 이용하는 패킷교환 데이타 신호를 3계층에서 암호화 및 복호화한다.

(2) 메카니즘부는 보안기능 수행 및 계산에 필요한 기술적 기능단위들로 구성된다.

- Key Storage : 생성된 세션키와 관련된 정보들을 관리하는 저장공간으로서 안전하게 유지되어야 하며 Key Manager외에는 접근할 수 없도록 구성한다. 특히 고유의 비밀값 V는 절대로 수정할 수 없도록 한다.
- DES : 비트 스트림을 블럭 암호화한다. Key Manager의 요구시 키분배에 필요한 암호화작업을 하며, Crypt_Engine의 요구시 제공된 키를 이용하여 사용자 정보를 암호화하게 된다.
- EXP : 고속의 지수계산을 한다. 키생성에 필요한 정보처리에 이용된다.
- RNG : 신뢰성 있는 난수를 발생한다.

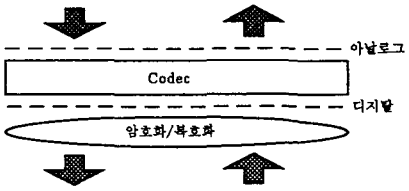
4.3 음성서비스를 위한 보안 프로토콜 기능 (Crypt_Engine 1)

아날로그 음성신호를 위한 대역폭은 3.1kHz이며 ISDN 단말기의 B채널 1계층에서 PCM방식으로

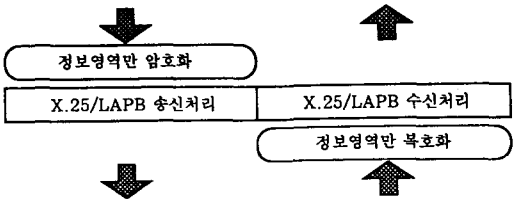
디지탈변환이 이루어진다. 음성정보의 암호화를 위해서는 정보 형태의 디지탈변환이 선행되어야 하므로 ISDN의 음성정보는 1계층에서만 안전한 암호화가 가능하다. 본 구조에서 음성정보의 암호화는 정보의 형태가 디지탈로 변환된 직후에 이루어지게 되며 수신측에서 복호화된 직후에 다시 아날로그 신호로 바뀌게 된다. 이 프로토콜을 위한 개념도는 다음 [그림 4]와 같다.

4.4 데이타서비스를 위한 보안 프로토콜 기능 (Crypt_Engine 2, 3)

ISDN의 데이타서비스는 회선교환으로 제공되는 방식과 패킷교환으로 제공되는 방식이 있다. 일반적으로 회선교환방식에서는 2계층 프로토콜인 LAPB만을 통해서 데이타전송처리가 이루어지며 패킷교환방식에서는 3계층의 X.25 PLP를 필요로 한다. 따라서 두 방식을 모두 고려하기 위한 방법으로 [그림 5]와 같이 2,3계층에 각각 보안 프로토콜 기능을 추가한다. 이 경우 암호화를 위해서는 ISDN 2,3계층 프로토콜 바로 위에서, 그리고 복호화를 위해서는 바로 밑에서 기능이 구현되며 B채널과 D채널의 패킷서비스에 대해서 유연하게 적용 가능하도록 구성된다. 데이타정보의 암호화는 해당 계층 데이타단위에서 헤더등을 제외한 순수한 정보 영역에 대해서만 적용된다.



[그림 4] 음성정보의 암호화



[그림 5] 데이타정보의 암호화

5. 키 분배 및 인증

5.1 암호화 방법

현대암호방식은 암호키와 복호키가 동일한 관용암호방식(Conventional Cryptosystem)과 암호키와 복호키가 서로 다른 공개키암호방식(Public Key Cryptosystem)으로 크게 분류된다. 관용암호방식은 암호화 및 복호화 작업시 수행시간이 비교적 적다는 장점이 있는 반면 대칭비밀키를 통신자간에 미리 안전한 경로를 통해서 분배해야 하는 부담이 있다. 또한 공개키암호방식은 비밀키분배를 할 필요가 없고 암호키의 공개가 허용되는 장점이 있지만 암호화 및 복호화 작업시 수행시간이 길어지는 문제점이 있다. 따라서 고속의 하드웨어가 제공되지 않는 경우 일반 통신망에서는 주로 관용암호방식이 사용된다.

본 논문은 사용자 정보의 암호화를 위해서, Diffie-Hellman이 제안한 공개키분배방식(Public Key Distribution Cryptosystem)을 근간으로 키 분배 및 인증을 하며 관용암호방식으로 정보를 암호화한다. 공개키분배방식은 통신자 서로간에 상대방의 공개값과 자신의 비밀정보를 이용해서 공통된 세션키를 생성하도록 하여 관용암호방식의 키분배 부담을 해결한 대칭 알고리즘 방식이다. 이 방식은 [표 3]에서 설명하는 조건으로, 관용암호방식에서 암호화 및 복호화 작업의 계산량이 적다는 장점과 공개키암호방식에서 암호키를 공개할 수 있다는 장점을 결합하게 된다. 따라서 키분배를 위해서 안전한 경로를 제공할 필요가 없고 많은 양의 사용자 정보를 공개키 방식의 느린 알고리즘으로 암호화하거나 복호화할 필요가 없다.

GP( ) : 공개값 생성 함수 GS( ) : 세션키 생성 함수	P_A , P_B : A,B의 공개값 S_A , S_B : A,B의 임의의 비밀값
① $GS(S_A,GP(S_B))=GS(S_B,GP(S_A))$식이 임의의 S_A,S_B에 대해서 성립해야 한다. ② GP( ), GS( )의 효율이 양호해야 한다. 즉, 계산량이 적어야 한다. ③ 불법자가 $GS(S_A,GP(S_B))=GS(S_B,GP(S_A))$를 얻기 위한 계산량이 커야한다.	

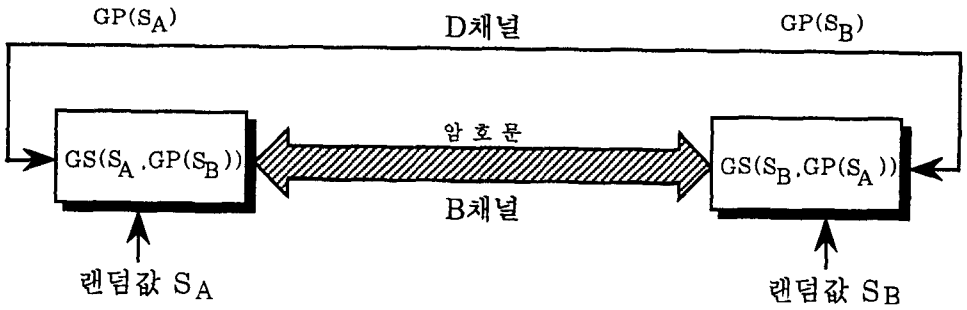
$P_A = GP(S_A) = g^{S_A} \bmod n \quad P_B = GP(S_B) = g^{S_B} \bmod n$

$K_{AB} = GS(S_A, P_B) = GS(S_A, GP(S_B)) = g^{S_AS_B} \bmod n$

$K_{BA} = GS(S_B, P_A) = GS(S_B, GP(S_A)) = g^{S_BS_A} \bmod n$

[표 3] 공개키분배방식의 조건

Difiie-Hellman이 제안한 키분배방식은 이산대수(Discrete Logarithm) 문제가 어렵다는 사실에 기반을 두고 있다. 위의 식에서와 같이, 암호화를 위한 세션키의 생성을 위해서 각 사용자측은 먼저 임의의 비밀값 S_A,S_B를 난수발생으로 얻은 후, 공개키 정보를 생성하여 상대방에게 전송한다. 이 식에서 n은 충분히 큰 소수이며, g는 GF(p)의 원시근이다. 그 후 상대방으로부터 받은 공개값을 이용해서 서로 같은 세션키를 얻는다. 본 논문에서 사용되는 암호방식의 개념도는 [그림 6]과 같다.



[그림 6] 공개키분배방식의 개념도

5.2 키 분배 및 인증 프로토콜

본 논문에서 제안하는 ISDN의 키 분배 및 인증 프로토콜은 다음과 같다. 본 프로토콜의 메세지들은 호연결을 위한 메세지에 내장되어 유통되며, 메세지를 주고 받는 쌍방간에는 서로의 ID를 호연결 메세지에 포함하는 것을 가정으로 한다. 따라서 A와 B가 연결한 후 B가 TC와 접속할 때는 A와 B, 그리고 B와 TC는 각각 서로를 알 수 있지만, TC는 A를 알 수 없다.

먼저 호출자(Caller) A는 난수 S_A를 생성한 후 공개값 P_A를 계산한다. 그리고 인식자(Recognizer) Σ와 함께, 자신의 비밀값 V_A로 DES를 이용하여 암호화한 후 피호출자(Callee) B에게 보낸다. 그리고 해쉬함수 H( )를 이용하여 P_A의 부분값 I_A를 쉽게 구한다. 한편 호 연결요구를 받은 B도 난수 S_B와 공개값 P_B를 구한 후 P_B , Σ 및 호출자의 ID를 자신의 비밀값 V_B로 DES를 이용하여 암호화한 후 TC에게 보낸다. 그리고 마찬가지로 해쉬함수 H( )를 이용하여 P_B의 부분값 I_B를 쉽게 구한다. B에게서 인증요구를 받은 TC는 먼저 B의 ID를 색인으로 하여 자신의 V-테이블 즉, 비밀키테이블에서 B의 비밀값 V_B을 찾은 후 B의 정보를 복호화한다. 인식자가 정상이면 다음 정보인 호출자의 ID를 얻고 마찬가지로 V-테이블을 참조하여 호출자의 비밀값을 얻는다. 또한 B의 공개값으로부터 부분값 I_B를 얻으며, 호출자 A의 인식자가 정상일 경우 A의 부분값 I_A도 구한다. 조건을 만족하지 않을 경우에는 B에게 인식실패 메세지와 함께 통신거부 신호를 보내게 된다. 조건을 만족할 경우 TC는 서로의 공개값을 바꾼 후 다시 각자의 비밀값으로 암호화 하여 B에게 보내게 된다. 이 때 각자의 부분값을 인식자로 사용하도록 한다. 각 인식자는 난수를 기반으로 한 세션값이므로 Nonce 즉, 현재 세션의 메세지임을 암시하게 된다. 특히 A에 대한 메세지에는 B의 ID를 포함하여 A에게도 인증 여부를 전달하게 된다. TC로부터 정보를 받은 B는 호출자 정보를 A에게 전달한 후 피호출자 정보를 복호화하여 I_B를 검사하고 A의 공개값 P_A를 얻게 된다. A도 역시 I_A를 검사하고 B의 공개값 P_B를 얻게 된다. 여기서 비록 세션키 K_{AB}를 각자 생성할 수 있지만 서로 같은 값이라는 것을 보증하기는

어렵다. 따라서 다시 상대방의 공개값으로부터 부분값을 구한 후 서로 상대방의 부분값을 자신이 생성한 세션키로 암호화하여 전송한다. 각자 자신이 생성한 세션키로 복호화했을 때 자신의 부분값이 정상이면 통신을 하게 되며, 조건을 만족하지 않을 경우에는 통신을 거부하게 된다. 따라서, 부분값은 Nonce 성질을 만족하므로 세션키의 Nonce 성질에 대한 보증을 가능하게 한다. 본 논문에서 제안하는 프로토콜은 다음과 같이 표현된다.

<A> { V_A , Σ }

. generate random S_A
. $P_A = GP(S_A) = g^{S_A} \bmod n$
. $V_A(\Sigma,P_A) = eDES(V_A,(\Sigma,P_A))$
. transfer $V_A(\Sigma,P_A)$ to B
. $I_A = H(P_A) = front\ octets\ of\ P_A$

. $(I_A,B,P_B) = dDES(V_A,V_A(I_A,B,P_B))$
if(I_A is correct)&&(B is correct){
} else DISCONNECT();
. $K_{AB} = GS(S_A,P_B) = P_B^{S_A} \bmod n$
$= g^{S_A S_B} \bmod n$

. $K_{AB}(I_B) = eDES(K_{AB},I_B)$
. transfer $K_{AB}(I_B)$ to B

. $I_A = eDES(K_{AB},K_{AB}(I_A))$
. if(I_A is correct){
} else DISCONNECT();

<B> { V_B , Σ }

. generate random S_B
. $P_B = GP(S_B) = g^{S_B} \bmod n$
. $V_B(\Sigma,A,P_B) = eDES(V_B,(\Sigma,A,P_B))$
. transfer $V_B(\Sigma,A,P_B)$,
$V_A(\Sigma,P_A)$ to TC
. $I_B = H(P_B) = front\ octets\ of\ P_B$

. transfer $V_A(I_A,B,P_B)$ to A
. $(I_B,P_A) = dDES(V_B,V_B(I_B,P_A))$
if(I_B is correct){
} else DISCONNECT();
. $K_{AB} = GS(S_B,P_A) = P_A^{S_B} \bmod n$
$= g^{S_A S_B} \bmod n$

. $K_{AB}(I_A) = eDES(K_{AB},I_A)$
. transfer $K_{AB}(I_A)$ to A

. $I_B = eDES(K_{AB},K_{AB}(I_B))$
. if(I_B is correct){
} else DISCONNECT();

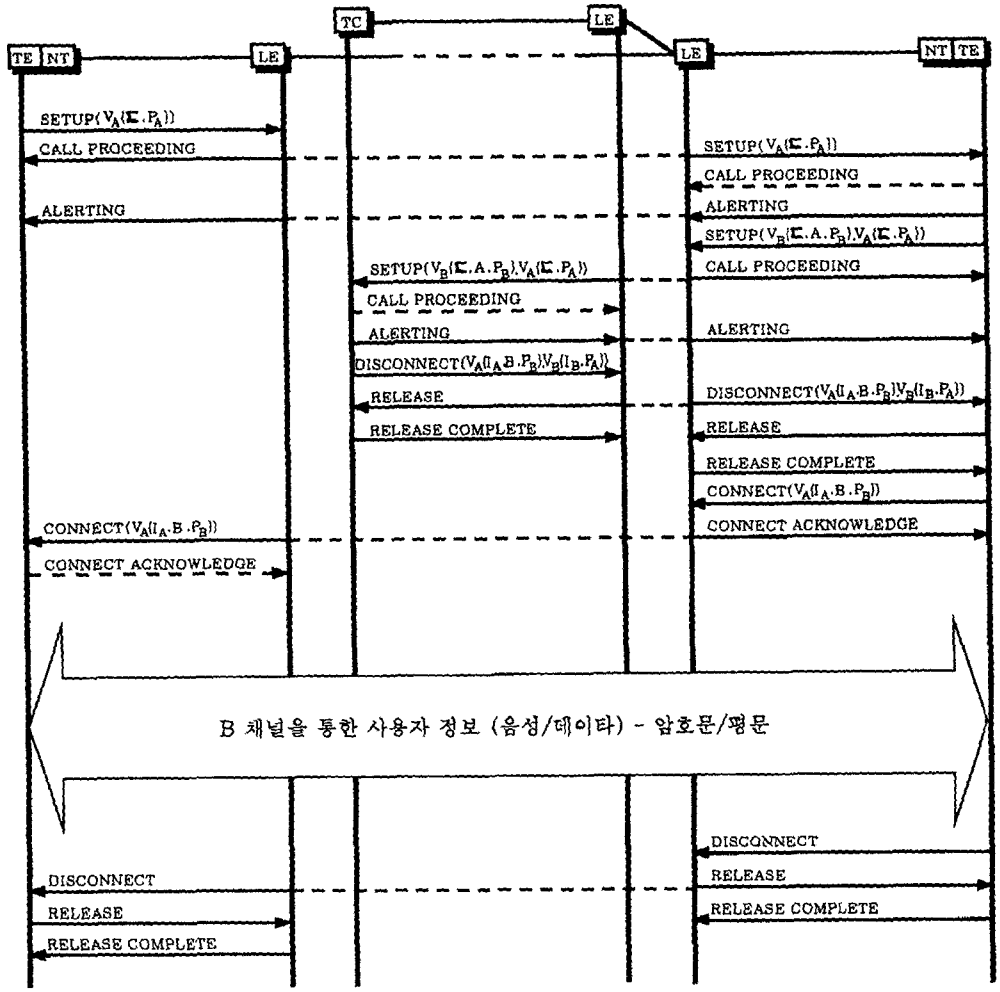
<TC> { [V_A , V_B , · · ·] , Σ }

. $(\Sigma,A,P_B) = dDES(V_B,V_B(\Sigma,A,P_B))$
if(Σ is correct){
caller = A; $I_B = H(P_B)$;
} else DENY();
. $(\Sigma,P_A) = dDES(V_A,V_A(\Sigma,P_A))$
if(Σ is correct){
$I_A = H(P_A)$;
} else DENY();
. $V_A(I_A,B,P_B) = eDES(V_A,(I_A,B,P_B))$
. $V_B(I_B,P_A) = eDES(V_B,(I_B,P_A))$
. transfer $V_A(I_A,B,P_B)$,
$V_B(I_B,P_A)$ to B

5.3 키 분배 및 인증을 위한 호제어

회선교환 호제어를 위한 메세지 중 호의 설정확립을 위해서 필요한 SETUP 메세지와 CONNECT 메세지, DISCONNECT 메세지는 발신 참조점과 수신 참조점을 포함하여 망전역에 관계되며 사용자간 정보전송을 위한 옵션인 User-user 정보원소를 정보영역에 포함할 수 있다. User-user 정보원소는 Q.931 메세지형식의 정보영역에서 쓰일 수 있는 여러가지 정보원소형식들 중 하나로서 가변길이 형식을 가지며 사용자간 정보를 망에 대해서 투명하게 운반한다. 따라서 호설정 시 호요청자의 SETUP 메세지와 호수신자의 CONNECT 메세지에 User-user 정보원소 영역을 할당하여 앞에서 설명한 키 분배 및 인증 정보를 전송하도록 한다. 본 논문에서는 기존의 Q.931 호제어 절차를 유지하며, 안전한 키 분배 및 인증이 가능한 방향으로 제안한다.

Q.931의 메세지는 260옥텟을 최대크기로 갖는다. 따라서 User-user 정보원소의 실제 크기는 약 200옥텟까지 가능하므로 본 프로토콜의 키분배에 필요한 정보의 최대크기인 149옥텟은 한 메세지에 충분히 포함될 수 있다. 구현을 할 경우 공개값 P는 최저 32옥텟(256비트)에서 최고 64옥텟(512비트)까지 책정할 수 있으며, 식별자 Σ 값과 I 값은 최저 3옥텟에서 최고 7옥텟까지로 정할 수 있다. 또한 ID 정보는 ISDN 사용자번호의 최대크기인 7옥텟까지 허용하는 것을 원칙으로 한다. 따라서 한 메세지에 포함될 수 있는 키분배 정보의 최대크기는 A, B 간에서 78옥텟, 그리고 B, TC 간에서 149옥텟이다. 키분배를 고려한 호제어는 다음의 [그림 7]과 같이 이루어진다.



[그림 7] 정보보호를 위한 회선교환 호제어

6. 제안한 방법에 대한 평가

6.1 GNY 로직을 이용한 검증 방법

본 논문에서 제안한 프로토콜의 검증에는 BAN 로직을 근간으로 제안된 GNY 로직을 이용하였다. BAN 로직과 GNY 로직은 프로토콜에서 통신자의 신뢰성에 대한 평가를 가능하게 하며 [표 4]와 같은 구성원으로 이루어진다. GNY 로직으로 검증을 하는 순서는 먼저, 본 프로토콜(Original Protocol)을 로직의 기호를 이용하여 이상 프로토콜(Idealized Protocol)로 바꾼 후, 통신 초기상태에서의 가정을 제시한다. 그리고 논리규칙을 가정과 각 메세지에 적용하여 프로토콜에서 통신자의 신뢰성에 대한 평가를 하도록 한다. GNY 로직을 이용할 경우 논리규칙을 통한 추론에서 얻게 될 최종 목표를 정하는 것이 중요하다. 키 분배 및 인증 프로토콜에서는 일반적으로 다음 조건을 만족하는 키가 분배되면 인증이 완전히 이루어진것으로 평가한다.

$A| \equiv A \xleftrightarrow{K_{ab}} B$, $B| \equiv A \xleftrightarrow{K_{ab}} B$, $A| \equiv B| \equiv B \xleftrightarrow{K_{ab}} A$, $B| \equiv A| \equiv A \xleftrightarrow{K_{ab}} B$

이 논리식의 의미는, 통신자 서로가 안전한 세션키를 공유하고 있음을 신뢰하고, 또한 상대방도 신뢰하고 있다는 사실에 대해서도 신뢰하도록 하는 것이다.

<table>
<tr><th>GNY 로직의 사용기호</th><th>본 논문에서 사용한 GNY 로직의 논리규칙</th></tr>
<tr><td>

$P \mid\equiv X$: P believe X
$P \lhd X$: P sees X
$P \mid\sim X$: P once said X
$P \mid\Rightarrow X$: P has jurisdictions over X
$\#(X)$: X is fresh
$P \overset{K}{\leftrightarrow} Q$: P and Q share secret key
$\{X\}_K$: X is encrypted under the key K
C1,C2 : Conjunction
$P \ni X$: P possesses X
$\phi(X)$: X is recognizable
$H(X)$: One-way function
$*$: Not-originated-here
$X \hookrightarrow C$: Precondition of X

</td><td>

1. Being-Told Rules
T1 $\frac{P \lhd *X}{P \lhd X}$
T2 $\frac{P \lhd (X,Y)}{P \lhd X}$
T3 $\frac{P \lhd \{X\}_K, P \ni K}{P \lhd X}$

2. Possession Rules
P1 $\frac{P \lhd X}{P \ni X}$
P2 $\frac{P \ni X, P \ni Y}{P \ni (X,Y), P \ni F(X,Y)}$
P3 $\frac{P \ni (X,Y)}{P \ni X}$
P4 $\frac{P \ni X}{P \ni H(X)}$
P5 $\frac{P \ni F(X,Y),\ P \ni X}{P \ni Y}$
P6 $\frac{P \ni K, P \ni X}{P \ni \{X\}_K, P \ni \{X\}_K^{-1}}$

3. Freshness Rules
F1 $\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,\ Y),\quad P \mid\equiv \#(f(X))}$
F2 $\frac{P \mid\equiv \#(X),\quad P \ni K}{P \mid\equiv \#(\{X\}_K),\quad P \mid\equiv \#(\{X\}_K^{-1})}$
F10 $\frac{P \mid\equiv \#(X),\quad P \ni X}{P \mid\equiv \#(H(X))}$

4. Recognizability Rules
R1 $\frac{P \mid\equiv \phi(X)}{P \mid\equiv \phi(X,Y), P \mid\equiv \phi(F(X))}$
R2 $\frac{P \mid\equiv \phi(X), P \ni K}{P \mid\equiv \phi(\{X\}_K), P \mid\equiv \phi(\{X\}_K^{-1})}$
R5 $\frac{P \mid\equiv \phi(X),\quad P \ni X}{P \mid\equiv \phi(H(X))}$

5. Interpretation Rules
I1 $\frac{P \lhd *\{X\}_K, P \ni K, P \mid\equiv P \overset{K}{\leftrightarrow} Q, P \mid\equiv \phi(X), P \mid\equiv \#(X,K)}{P \mid\equiv Q \mid\sim X, P \mid\equiv Q \mid\sim \{X\}_K, P \mid\equiv Q \ni K}$
I1′ $\frac{P \lhd \{X\}_K, P \ni K, P \mid\equiv P \overset{K}{\leftrightarrow} Q, P \mid\equiv \phi(X), P \mid\equiv \circledS(P)}{P \mid\equiv Q \mid\sim X, P \mid\equiv Q \mid\sim \{X\}_K}$
I6 $\frac{P \mid\equiv Q \mid\sim X, P \mid\equiv \#(X)}{P \mid\equiv Q \ni K}$
I7 $\frac{P \mid\equiv Q \mid\sim (X,Y)}{P \mid\equiv Q \mid\sim K}$

6. Jurisdiction Rules
J1 $\frac{P \mid\equiv Q \mid\Rightarrow C,\ P \mid\equiv Q \mid\equiv C}{P \mid\equiv C}$
J2 $\frac{P \mid\equiv Q \mid\Rightarrow Q \mid\equiv *,\ P \mid\equiv Q \mid\equiv (X \hookrightarrow C),\ P \mid\equiv \#(X)}{P \mid\equiv Q \mid\equiv C}$

</td></tr>
<tr><th>GNY 로직의 원소 표기</th><th></th></tr>
<tr><td>

Principals : P, Q, A , B, TC, · · ·
Formula : X, Y, S, P, K, · · ·

</td><td></td></tr>
<tr><th>BAN 로직의 유용한 논리 규칙</th><th></th></tr>
<tr><td>

1. message-meaning rule
$\frac{P \mid\equiv Q \overset{K}{\leftrightarrow} P,\ P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$

2. nonce-verification rule
$\frac{P \mid\equiv \#(X),\ P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$

</td><td></td></tr>
</table>

[표 4] GNY 로직

6.2 키 분배 및 인증 프로토콜의 평가

본 논문에서는 공개값을 TC의 공증을 통해서 서로 주고 받은 후 공통의 세션키를 생성하도록 하였으므로, 본 프로토콜을 다음과 같이 표현할 수 있다. 본 프로토콜의 앞부분 4단계는 서로 공개값

Original Protocol

$A \rightarrow B$: $A,\{\Sigma,P_A\}_{K_{VA}}$
$B \rightarrow TC$: $B,\{\Sigma,A,P_B\}_{K_{VB}},\{\Sigma,P_A\}_{K_{VA}}$
$TC \rightarrow B$: $\{I_A,B,P_B\}_{K_{VA}},\{I_B,P_A\}_{K_{VB}}$
$B \rightarrow A$: $\{I_A,B,P_B\}_{K_{VA}}$

$B \rightarrow A$: $\{I_A\}_{K_{AB}}$
$A \rightarrow B$: $\{I_B\}_{K_{AB}}$

Idealized Protocol

$B \lhd$: $*A,*\{*\Sigma,*P_A\}_{K_{VA}}$
$TC \lhd$: $*B,*\{*\Sigma,*A,*P_B\}_{K_{VB}},*\{*\Sigma,*P_A\}_{K_{VA}}$
$B \lhd$: $*\{*H(P_A),*B,*P_B\}_{K_{VA}},*\{*H(P_B),*P_A\}_{K_{VB}}$
$A \lhd$: $*\{*H(P_A),*B,*P_B\}_{K_{VA}}$

$A \lhd$: $*\{*H(P_A)\}_{K_{AB}}$
$B \lhd$: $*\{*H(P_B)\}_{K_{AB}}$

Assumptions

$A \ni K_{VA}$; $A \ni \Sigma$; $A \ni P_A$; $A \ni S_A$; $A \mid\equiv A \overset{K_{VA}}{\longleftrightarrow} TC$; $A \mid\equiv \#(P_A)$; $A \mid\equiv \varnothing(P_A)$
$B \ni K_{VB}$; $B \ni \Sigma$; $B \ni P_B$; $B \ni S_B$; $B \mid\equiv B \overset{K_{VB}}{\longleftrightarrow} TC$; $B \mid\equiv \#(P_B)$; $B \mid\equiv \varnothing(P_B)$
$TC \ni K_{VA}$; $TC \ni K_{VB}$; $A \ni \Sigma$; $TC \mid\equiv A \overset{K_{VA}}{\longleftrightarrow} TC$; $TC \mid\equiv B \overset{K_{VB}}{\longleftrightarrow} TC$; $B \mid\equiv \varnothing(\Sigma)$
$A \mid\equiv TC \Rightarrow TC \mid\equiv *$; $A \mid\equiv B \Rightarrow B \mid\equiv *$; $B \mid\equiv TC \Rightarrow TC \mid\equiv *$; $B \mid\equiv A \Rightarrow A \mid\equiv *$

을 안전하게 주고 받는 것을 목표로 하는데 즉, 받은 공개값이 상대방의 공개값이라는 사실을 TC의 공증을 통해서 신뢰하는 것을 목표로 한다. 또한 서로 상대방도 그와 같은 신뢰를 하고 있다는 것을 신뢰하도록 한다. 뒷부분 2단계는 앞단계에서 얻은 상대방의 비밀값을 이용하여 생성한 세션키로 서로의 Nonce값을 암호화하여 교환하므로써 각자 생성한 키가 이번 세션에 생성된 공개값을 기반으로 하는 것인지를 검사한다. 즉, 상대방의 공개값의 Nonce 성질을 서로 검사하게 되는데, 이것은 먼저 상대방의 세션키로 암호화 되어있는 Nonce값을 자신의 세션키로 복호화 한 후, Nonce값 검사를 하면 Nonce 여부와 함께 서로의 세션키가 같은가 아닌가를 쉽게 알 수 있게 한다. 따라서 최종적으로 안전한 키 분배 및 인증이 가능하게 된다. 이 프로토콜을 GNY 로직을 이용해서 검증하였다. 다음은 검증 과정의 핵심이 되는 부분들을 요약한 것이다.

<Message 1>
· T1, P1에 의해서 $B \ni (A,\{*\Sigma,*P_A\}_{K_{VA}})$ 를 얻는다.

<Message 2>
· T1, T2, T3, P1에 의해서 $TC \ni (\Sigma,A,P_B)$ 를 얻는다.
· R1, I1', I7, P3, P5에 의해서 $TC \mid\equiv \varnothing(\Sigma,A,P_B)$; $TC \mid\equiv B \mid\sim P_B$; $TC \ni A$
· T2, T3, P1에 의해서 $TC \ni (\Sigma,P_A)$ 를 얻는다.
· R1, I1', I7, P3에 의해서 $TC \mid\equiv \varnothing(\Sigma,P_A)$; $TC \mid\equiv A \mid\sim (\Sigma,P_A)$; $TC \mid\equiv A \mid\sim P_A$
· P3, P4, P2, P6에 의해서 다음의 식을 얻는다.
$TC \ni \{(H(P_A),B,P_B)\}_{K_{VA}} \hookrightarrow TC \mid\equiv B \mid\sim P_B$; $TC \ni \{(H(P_B),P_A)\}_{K_{VB}} \hookrightarrow TC \mid\equiv A \mid\sim P_A$

<Message 3>
· T1, T2, T3, P1에 의해서 $B \ni (H(P_B),P_A)$를 얻는다.
· R5, R1, F10, F1, P3, I1, I7, J2, J1에 의해서 다음의 식을 얻는다.
$B \mid\equiv \varnothing(H(P_B),P_A)$; $B \mid\equiv \#(H(P_B),P_A)$; $B \mid\equiv A \mid\sim P_A$
· P4, R5, F10, P6에 의해서 다음의 식을 얻는다.
$B \mid\equiv \varnothing(h_B(P_A))$; $B \mid\equiv \#(h_B(P_A))$; $B \ni \{H(P_A)\}_{h_B(P_A)}$

<Message 4>
· T1, T2, T3, P1에 의해서 $A \ni (H(P_A),B,P_B)$ 를 얻는다.
· R5, R1, F10, F1, P3, I1, I7, J2, J1에 의해서
$A \mid\equiv \varnothing(H(P_A),B,P_B)$; $A \mid\equiv \#(H(P_A),B,P_B)$; $A \mid\equiv B \mid\sim P_B$
· P4, R5, F10, P6에 의해서
$A \mid\equiv \varnothing(h_A(P_B))$; $A \mid\equiv \#(h_A(P_B))$; $A \ni \{H(P_B)\}_{h_A(P_B)}$

<Message 5>, <Message 6>
· T1, P1에 의해서 $A \ni \{H(P_A)\}_{h_B(P_A)}$, $B \ni \{H(P_B)\}_{h_A(P_B)}$를 얻으므로 다음의 결론을 얻을 수 있다.

$A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$; $A \mid\equiv B \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$
$B \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$; $B \mid\equiv A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B$

7. 결론 및 향후 연구 방향

공중망인 ISDN에서 사용자정보의 비밀보장을 위해서는 무엇보다 최적의 암호화 방법이 제안되어야 한다. ISDN을 위한 암호화 방법은 전송시 발생하는 비트에러에 강해야 하며 또한 실시간 처리를 위해서 빠르고 안전한 처리가 가능하도록 구현될 수 있어야 한다. ISDN은 음성, 화상, 데이타 등 다양한 종류의 정보를 유통하며 다자간 통화, 다중 서비스, 다중 번호체계를 제공하는 등 정보보호를 위한 메카니즘을 복잡하게 하는 요소가 많다. 그러나 정보가 국간과 사용자-망간에서 모두 디지탈형태로 전송되므로 적합한 암호화 알고리즘이 제안된다면 정보의 비밀보장 서비스를 비교적 저렴하고 안전하게 제공할 수 있다. 본 논문에서는 ISDN의 정보보호 기능구현을 위해서 필요한 기본적인 사항들과 보안 프로토콜의 구성 그리고 정보암호화를 고려한 호제어방법에 대해서 연구하였으며, 적합한 키 분배 및 인증 프로토콜을 제안 및 평가하였다. 특히 키 분배 및 인증을 위한 정보는 D채널을 통해서 이루어지도록 하였으며, 기존의 사용자-망 신호체계와 프로토콜구조를 유지하는 관점에서 연구를 진행하였다. 그러나 사용자 정보의 무결성을 제공하기 위해서는 데이타단위에 무결성검사값(ICV)의 추가가 필요한데 ISDN의 경우 LAPB 프레임의 크기가 충분히 크지 않으므로 무결성보장을 위해서는 기존의 체계에 수정이 필요할 것으로 평가된다. 앞으로의 연구에서는 실제 사용자 정보의 교환시 인증과 무결성보장 기능을 제공할 수 있는 방안에 대한 연구를 선행하며, ISDN의 사용자 정보보호 기능을 종합적으로 제공할 수 있도록 사용자-망 인터페이스 구조의 최적화와 ISDN을 위한 최적의 암호화 방법을 개발하는 방향으로 진행되어야 하겠다. 또한 광대역 ISDN의 신호체계에서도 적용 가능한 정보보호 체계의 표준을 마련하도록 해야 하겠다.

참 고 문 헌

[1] ITU-T Recommendation Q.931 Digital Subscriber Signalling System No.1 (DSS1), Network Layer, User-Network Management

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

[3] ITU-T Recommendation X.30 Support Of X.21, X.21 bis And Data Terminal Equipments (DTEs) By An ISDN

[4] Warren S. Gifford, "ISDN User-Network Interfaces," IEEE Journal on SAC, Vol. SAC-4, No. 3, pp. 343-348, May 1986

[5] Sadahiko Kano, "Layer 2 and 3 ISDN Recommendations," IEEE Journal on SAC, Vol. SAC-4, No. 3, pp. 355-359, May 1986

[6] Roger M. Needham, Michael D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Comm. of the ACM, Vol. 21, No. 12, pp. 993-999, Dec 1978

[7] Takeshi Chikazawa, Tohru Inoue, "A New Key Sharing System For Global Telecommunications," IEEE GLOBECOM, pp. 1069-1072, 1990

[8] Diffie W., Hellman M., "New Directions in Cryptography," IEEE Trans. Info. Theory, Vol. IT-22, No. 6, pp. 644-654, Nov 1976

[9] Brian O'Higgins, "Securing Information in X.25 Networks," IEEE GLOBECOM, pp. 1073-1078, 1990

[10] Charles Dinkel, "Secure Data Network System(SDNS) Network, Transport, and Message Security Protocols," NIST, Feb 1990

[11] Michael Burrows, Martin Abadi, Roger Needham, "A Logic of Authentication," ACM Transactions on Computer Systems, pp. 18-36, Feb 1990

[12] Li Gong, Roger Needham, Raphael Yahalom, "Reasoning about Belief in Cryptographic Protocols," Proceedings of IEEE Symposium on Research in Security and Privacy, pp. 234-248, 1990