초고속정보통신기반의 기술적 보호

Technical Prevention Scheme for the Information-Superhighway Infrastructure

박정현(J. H. Park) 초고속연구기획실 선임연구원
김성연(S. Y. Kim) 초고속연구기획실 선임연구원, 실장
김성규(S. K. Kim) 초고속정보통신연구본부 책임연구원, 본부장
박영호(Y. H. Park) 상주산업대학교 정보통신공학과 교수

초고속정보통신기반에서의 보호는 크게 사용자 측면, 서비스 측면, 네크워크 측면 그리고 관리 측면으로 분류할 수 있다. 본 논문에서는 이러한 측면들 가운데 초고속정보통신기반 보호기술이 가장 절실한 네트워크 측면에서의 보호를 크게 OSI, TCP/IP, ATM으로 나누어 검토하여, OSI 참조모델을 위한 NLSP와 TLSP방식, TCP/IP를 위한 IP보호방식, 그리고 ATM 보호방식을 각각 제시했다.

I. 서 론

초고속정보통신기반은 정부 및 국민들에게 경제적, 사회적 및 문화적 이익을 줄 수 있으며 원격교육 및 원격진료 서비스 등의 제공으로 국민 생활의 질을 향상시킬 수 있다. 그러나 초고속정보통신기반에서의 범죄로 인하여 초고속정보통신기반을 신뢰할 수 없다면 사회적인 문제가 야기될 수 있다. 여러 선진국에서는 초고속정보통신기반 구축 과정에서 발생되는 범죄들로부터 정보를 안전하게 보호하기 위하여 정부 차원의 정책 및 보호기술 개발을 통해 효율적인 초고속정보통신기반을 구축하고 있다.

초고속정보통신기반에서의 보호는 크게 사용자 측면, 서비스 측면, 네트워크 측면 그리고 관리 측면으로 분류할 수 있다. 사용자 측면에서의 보호는 스마트 카드, off-line 암호화 등으로 구현될 수 있고, 서비스 측면에서의 보호는 X.400, X.509, 인증 등으로 구현될 수 있고, 네트워크 측면에서의 보호는 NLSP, TLSP, IP 보호프로토콜 등으로 구현될 수 있으며, 관리 측면에서의 보호는 보호관리 구조, 키관리, 감사(audit) 등으로 구현될 수 있다.

본 논문에서는 초고속정보통신기반하에서의 기술적 보호대책을 모색하며 특별히 네트워크 측면의 기술적 보호를 크게 OSI, TCP/IP, ATM 측면으로 제시한다. 또, 본 논문에서는 기술적 방지대책, 물리적 방지대책, 관리적 방지대책 그리고 법적·제도적 방지대책 가운데서 기술적 방지대책에 관하여 중점적으로 다루며 초고속정보통신기반하에서 이용되는 서비스들을 보다 안전하게 사용하기 위해서는 법적·제도적, 관리적 그리고 물리적 방지대책과 병행하여 기술적 방지대책이 이

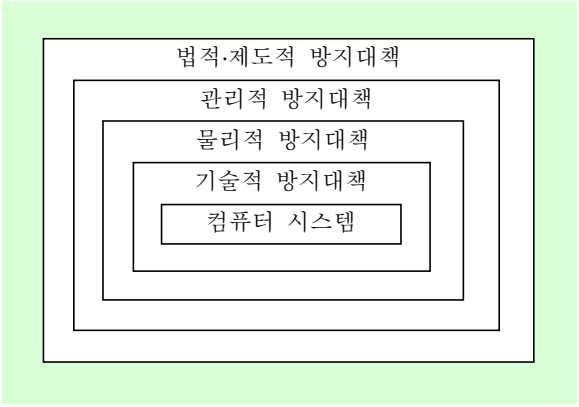
루어져야 효과적으로 범죄를 예방할 수 있다.

II. 초고속정보통신기반에서의 보호 메커니즘

일반적으로 사람들은 세가지 이유로 범죄 행위를 자제하고 있다. 첫째로는 도덕적 양심 때문이며, 둘째로는 범죄를 일으킬 기회가 사실상 없기 때문이며, 셋째로는 범죄 수행 후 발각되어 처벌받을 것이 두렵기 때문이다. 이에 따라 컴퓨터 범죄를 막기 위해서는 다음과 같은 점을 고려해야 한다.

첫째, 내부 직원 또는 사회인의 도덕성을 높여야 한다. 오늘날의 사회는 전반적으로 배금주의가 팽배하고 도덕 관념이 크게 떨어져 있는 상태에서 급속히 고도 정보화 사회로 이행하여 가고 있다. 이러한 상태를 방치하게 되면 머지않아 많은 모순이 노출되고 사회 각 분야에서 혼란이 발생할 것으로 예상되므로 국민 전체의 도덕성을 확보하기 위한 행정 당국의 구체적인 대책이 필요하고 기업에서는 직원들간의 융화를 도모하기 위한 노력이 이루어져야 할 것이다.

둘째, 범죄를 일으킬 수 있는 기회를 가능한 한 줄임으로써 범죄 충동을 줄여야 한다. 이를 위해서는 한 직원이 접근할 수 있는 자료나 그 직원이 수행할 수 있는 작업의 범위를 줄여야 한다. 예를 들어, A 파일은 볼 수 없다든가, B 파일은 볼 수는 있으나 그 내용을 고칠 수는 없다든가, 또는 C 파일은 내용 수정은 가능하나 작업 처리는 할 수 없다든가 등의 제한이다. 이러한 제한을 정하는 데에는 그 직원이 담당업무를 수행하는데 필요한 내용 및 작업으로만 한정한다는 것이 원칙이다. 이렇게 되면 단독 범행은 불가능하고 몇 명의 공동 범행만이 가능하게 되는데 이 경우에는 범죄 수행이 더욱 어려워지고, 또 범행 후에도 이 사실이 노출될 가능성이 높아지게 된다.



(그림 1) 컴퓨터 범죄 방지 대책

셋째, 범죄 수행 후 발각될 가능성을 높이고 그것이 발견되는 경우 적절한 처벌을 함으로써 범죄에 대한 두려움을 높여야 한다. 이를 위해서는 한 업무를 직원들간에 적당히 분리하여 옆사람이나 상사가 그 직원이 하는 일과 연관이 되게 함으로써 직원들간의 견제 효과를 도입하여야 한다. 또한 정보시스템에 있는 데이터나 프로그램 등을 주기적으로 적절히 감사하여 부정을 발견하는 노력이 이루어 져야 하고 범죄 발견시 이를 입증할 수 있는 증거 자료의 확보가 중요하다. 컴퓨터 범죄의 경우 실제로 범죄를 적발한 경우에도 증빙자료의 확보가 어렵거나 또한 현행 법규상으로 범죄로 인정하기 힘든 이유로 말미암아 무죄 또는 가벼운 처벌만으로 끝나는 경우가 많다. 이는 발각 때의 두려움을 경감시켜서 컴퓨터 범죄를 더욱 조장하는 결과가 되고 있다. 따라서 저지른 범죄에 합당

〈표 1〉 보호서비스와 메커니즘과의 관계

Service / Mechanisms	E	D.S	A.C	D.I	A.E	T.P	R.C	N
Peer Entity Authentication	Y	Y			Y			
Data Origin Authentication	Y	Y						
Access Control Service			Y					
Connection Confidentiality	Y						Y	
Connectionless Confidentiality	Y						Y	
Selective Field Confidentiality	Y							
Traffic Flow Confidentiality	Y					Y	Y	
Connection Integrity with Recovery	Y			Y				
Connection Integrity without Recovery	Y			Y				
Selective Field Connection Integrity	Y			Y				
Connectionless Integrity	Y	Y		Y				
Selective Field Connectionless Integrity	Y	Y		Y				
Non-repudiation, Origin		Y		Y				Y
Non-repudiation, Delivery		Y		Y				Y

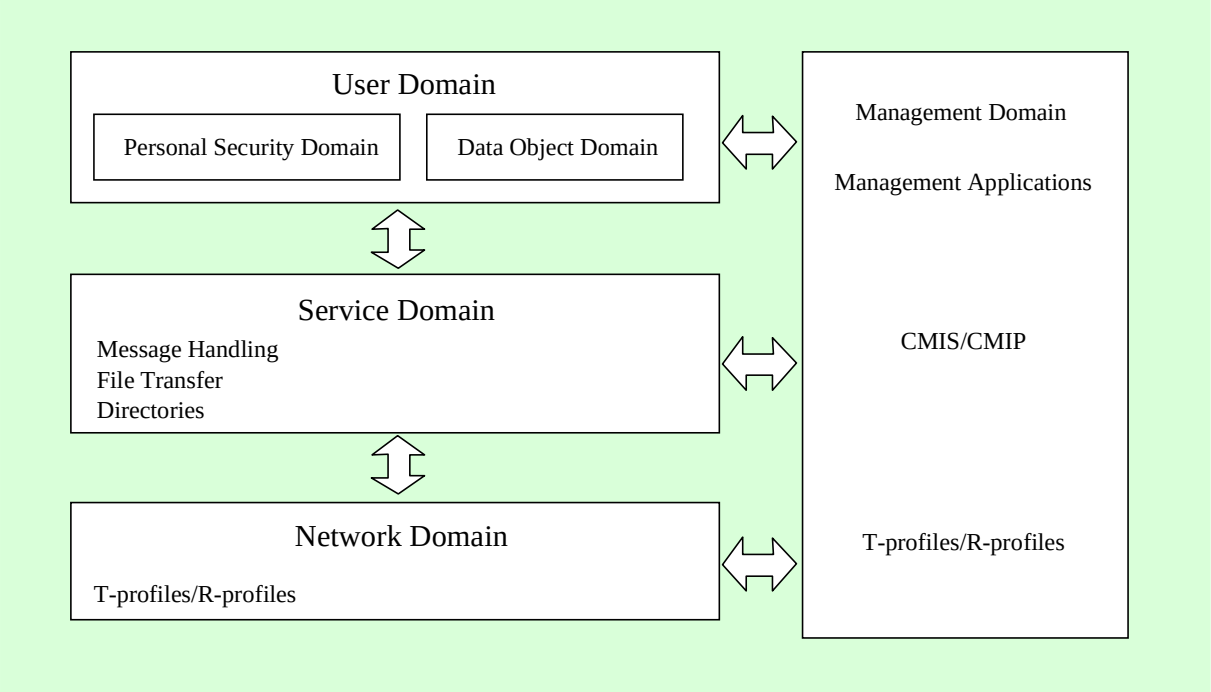
Legend: The mechanism is considered not to be appropriate. Y(Yes): the mechanism is considered to be appropriate, either on its own or in combination with other mechanisms. The mechanism is considered not to be appropriate. where, E : Encipherment, D.S: Digital Signature, A.C: Access Control, D.I: Data Integrity, A.E: Authentication Exchange, T.P: Traffic Padding, R.C: Routing Control, N. : Notarization

하는 적절한 처벌을 가할 수 있는 컴퓨터 범죄 관련 형법의 제정 등 적절한 법률적 방지대책이 필요하다.

이와 같은 세가지 사항에 근거하여, 컴퓨터 범죄로부터 시스템을 보호하기 위한 방지대책을 (그림 1)과 같이 4가지의 계층으로 나누어 생각할 수 있다. 즉, 기술적인 통제 방안을 이용하는 기술적 방지대책, 물리적으로 시스템 환경을 안전하게 보호하기 위한 물리적 방지대책, 컴퓨터 시스템의 관리 및 운영적인 측면에서의 관리적 방지대책, 마지막으로 국가적인 차원에서 지원해야 하는 법적·제도적 방지대책 등으로 나누어 진다[5].

이러한 방지대책 가운데서 개방형시스템의 보호체계를 통한 기술적 방안으로 ISO 7498-2[6]에서는 보호서비스와 보호메커니즘 그리고 이들간의 관계 등을 정의하고 있다. 보호서비스들로는 비밀보장, 신분인증, 접근제어, 데이터 무결성 그리고 부인봉쇄 서비스들이 있으며, 보호 메커니즘들로는 암호화, 인증, 데이터 무결화,접근제어, 디지털서명, 트래픽 패딩, 경로제어, 공증 등이 있다.

〈표 1〉은 보호서비스와 메커니즘의 관계를 나타낸 것이다. 여기서 하나의 서비스에 대해 타당한 메커니즘이라고 표시한 것이 절대적인 것은 아니다. 즉, 타당하다고 표시된 메커니즘은 그 메커니즘 하나 혹은 표시된 다른 메커니즘과 함께 적



(그림 2) 개방환경에서 통신시스템에 대한 보호 측면

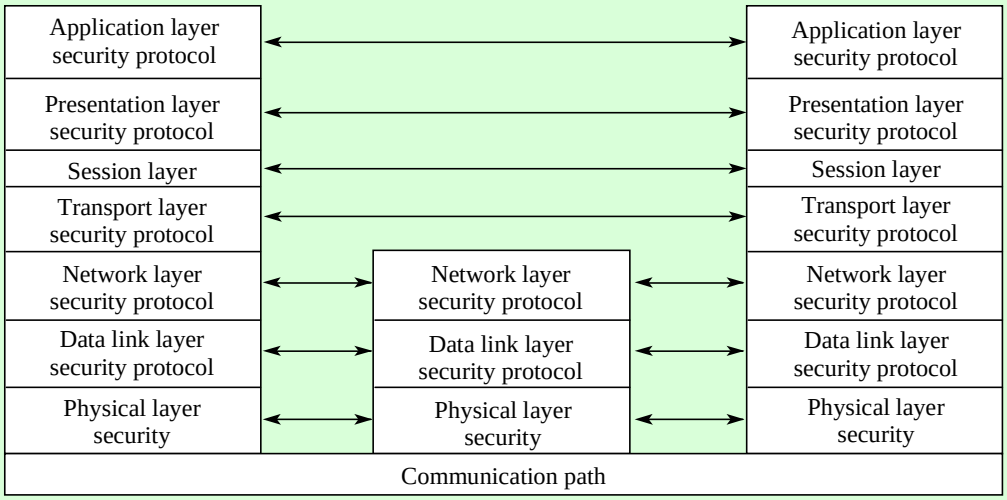
용될 수도 있다.

III. 초고속정보통신기반하에서의 보호방식

초고속정보통신기반에서의 보호는 (그림 2)와 같이 크게 사용자 측면, 서비스측 면, 네트워크 측면 그리고 관리 측면으로 분류할 수 있다[7]. 사용자 측면에서의 보호는 스마트 카드[8, 9], off-line 암호화 등으로 구현될 수 있고, 서비스 측면에서의 보호는 X.400[10], X.509[11], 인증[12] 등으로 구현될 수 있고, 네트워크 측면에서의 보호는 NLSP[13-15], TLSP[16-18], IP 보호프로토콜[19-21] 등으로 구현될 수 있으며 관리 측면에서의 보호는 보호관리 구조, 키관리, 감사(audit) 등으로 구현될 수 있다. 본 절에서는 네트워크 측면에서의 보호방식을 OSI 측면, TCP/IP 측면, 그리고 ATM 측면에서 기술한다. OSI 참조모델에서의 보호를 위한 NLSP와 TLSP는 국제 표준안이며 TCP/IP에서의 보호를 위한 IP 보호프로토콜은 현재 표준화 작업중이며 ATM에서의 보호는 현재 연구중이다.

1. OSI 보호방식

전형적인 OSI 참조모델과 호환되는 보호모델의 구조와 각 계층의 보호 프로토콜은 (그림 3)과 같다. 물리계층에서의 보호는 ISO 9160에서 정의하고 있으며 전송되는 비트 모두를 암호화한다. 데



(그림 3) OSI참조 모델에서 보호 프로토콜의 위치

이터 링크 계층의 보호를 위한 보호 서비스는 규정되어 있으나, 다양한 프로토콜에 사용될 수 있는 구체적인 보호 메커니즘은 정해지지 않고 있다. 반면에, 근거리 통신망에서의 보호를 위해 IEEE 802.10은 제 2계층 보호 프로토콜을 규정하고 있으며 위성통신망 보호를 위해 2계층 보호 프로토콜을 사용할 수 있다. 네트워크 계층과 트랜스포트 계층에서의 보호는 SDNS(Secure Data Network System) 프로젝트에 의한 SP3(Security Protocol 3)과 SP4(Security Protocol 4)가 정의되어 있으며 ISO와 IEC의 JTC1/SC6에서는 네트워크 계층과 트랜스포트 계층 보호 프로토콜의 표준안을 발표하였다. 세션 계층에서는 보호 서비스가 제공되지 않는다. 프리젠테이션 계층에서 제공되는 기능들은 암호에 기초한 데이터의 구문적인 부호화이다. 응용 계층에서의 보호는 MHS(Message Handling System) 보호, FTAM(File Transfer, Access, and Management) 보호와 디렉토리 보호 등이 있으며 현재 CCITT(Consultative Committee for International Telegraph and Telephone) X.400, ISO 8571, CCITT X.507 등에서 연구중이다.

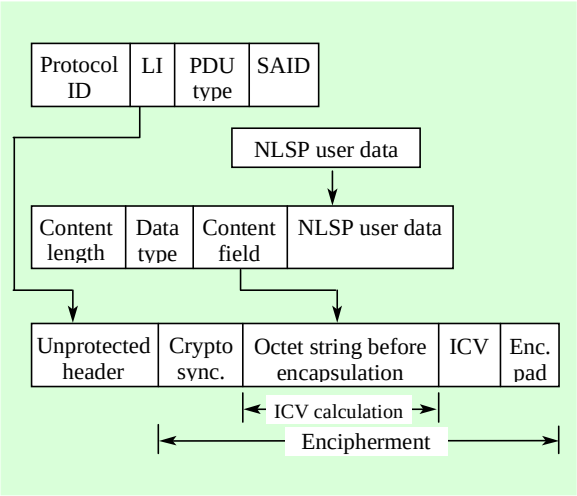
가. NLSP

NLSP는 네트워크 계층에서 보호 서비스를 제공하기 위하여 종단 시스템 및 중간 시스템에서 구현될 수 있으며 네트워크 계층의 부계층으로 동작된다. NLSP는 비접속 네트워크 계층 보호 프로토콜(NLSP-CL) 및 접속 네트워크 계층 보호 프로토콜(NLSP-CO)로서 동작 가능하다. NLSP는 ISO 7498-2에서 명시하는 네트워크 계층 보호 서비스인 인증, 접근 제어, 비밀보장, 무결성 서비스를 제공한다. NLSP는 암호화 메커니즘을 사용하여 보호서비스들을 지원하고, 보호 속성은 보호 관리에 의해 미리 설정되거나 보호 연관 프로토콜을 사용

하여 설정된다.

NLSP에서의 보호는 모든 서비스 파라미터 보호, NLSP 사용자 데이터 보호, 그리고 비보호가 있다. 모든 NLSP 서비스 파라미터 보호는 주소와 사용자 데이터를 포함하는 모든 파라미터들을 보호하며 보호연관 속성 Param_Protec이 True일 때 선택된다. NLSP 사용자 데이터 보호의 경우 사용자 데이터는 보호하나 다른 NLSP 서비스 파라미터들은 보호하지 않으며 보호연관 속성 Param_Protec이 False일때 선택된다. 비보호의 경우 모든 NLSP 서비스 파라미터들은 UN(Underlying Network) 서비스 파라미터들로 복사되며 모든 NLSP 절차들은 수행되지 않는다. NLSP-CO와 NLSP-CL은 SDT(Secure Data Transfer) PDU를 사용함으로써 모든 NLSP 서비스 파라미터들을 보호할 수 있으며 NLSP-CO는 No-header 형으로써 NLSP 사용자 데이터를 보호할 수도 있다. NLSP에서 사용되는 PDU는 SDT PDU, CSC(Connection Security Control) PDU, 그리고 SA(Security Association) PDU의 세가지 방식이 있다.

SDT PDU 구조는 (그림 4)와 같다. SDT PDU는 무결성 서비스를 제공하기 위하여 무결성 검사 값을 첨가하고 비밀보장 서비스를 제공하기 위하여 보호영역을 암호화 한다. 비보호 헤더 영역 구조는 프로토콜 식별자, 길이, PDU 형태 그리고 보호연관 식별자 영역으로 구성된다. 프로토콜 식별자 영역은 NLSP 식별자를 나타내며 길이 영역은 PDU 형태와 SAID 영역을 합한 길이를 나타낸다. PDU 형태 영역은 SDT PDU임을 나타내기 위하여 0100 1000의 값을 가지며 SAID 영역은 상



(그림 4) SDT PDU 구조

대 객체 보호연관 식별자를 나타낸다. 암호 동기 영역은 선택 영역이며 특정 암호화 알고리듬을 위해 사용될 수 있다. ICV(Integrity Check Value)는 무결성 검사 값을 포함하며 보호 연관 속성에 포함된 ICV 알고리듬 식별자에 의해 정의된다. 암호화 패딩 영역은 비밀보장 서비스를 위한 블록 암호화 알고리듬을 제공할 목적으로 사용된다.

나. TLSP

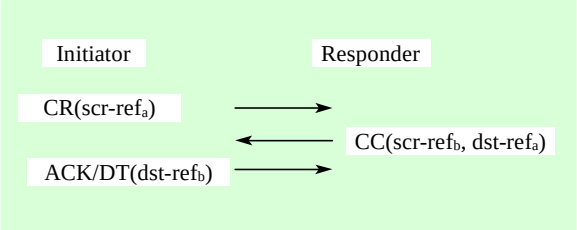
TLSP는 ISO/IEC 8073 및 ISO 8602의 확장이며, 접속 및 비접속형 TPDU(Transport Protocol Data Unit)의 전송에 대한 데이터 보호 및 비보호를 허용한다. TLSP는 ISO 7498-2에서 명시하는 트랜스포트 계층 보호 서비스인 대등 실체 확인, 데이터 발신처 확인, 접근제어, 접속 비밀보장, 비접속 비밀보장, 복구기능을 갖는 접속 무결성, 복구기능이 없는 접속 무결성 그리고 비접속 무결성 서비스들을 제공한다. 접속형으로 사용되는 TLSP는 대등실체 확인, 접근제어, 접속 비밀보장,

복구기능을 갖는 접속 무결성과 복구기능이 없는 접속 무결성 서비스들을 제공하며, 비접속형으로 사용되는 TLSP는 비접속 무결성, 비접속 비밀보장, 접근제어 그리고 데이터 발신처 확인 서비스들을 제공한다.

TLSP는 암호화 메커니즘을 사용하여 이 서비스들을 지원하고, 보호 라벨링(Labelling), 키 및 식별자와 같은 보호 속성은 보호 관리에 의해 미리 설정되거나 보호연관 프로토콜을 사용하여 설정된다. 키의 재설정은 보호 연관 프로토콜이나 프로토콜의 외적 수단을 통하여 지원된다.

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. Decapsulation은 디멀티플렉싱 후와 다른 프로토콜 처리 기능을 수행하기 전에 수행된다.

TLSP의 기능은 데이터 암호화 기능, 무결성 기능, 보안 라벨 기능, 보호 페딩 기능, 대등 실체 인증 기능 및 보호 연관 기능로 나눌 수 있다. 첫째, 암호화 기능은 데이터 비밀보장 기능을 제공하며 각 SE TPDU는 복호화를 위한 충분한 정보를 가진다. 이 정보는 복호화에 필요한 SA-ID의 인덱스뿐만 아니라 암호동기와 알고리듬 초기화열을 포함한다. 둘째, 무결성 기능은 비접속 무결성과 데이터 발신처 신분확인 혹은 접속 무결성 서비스를 제공한다. 셋째, 보호 라벨은 데이터의 민감도를 나타내는 선택적 기능이며 접근 제어 메커니즘을 지원한다. 넷째, 보호 페딩은 캡슐화된 TPDU 셋의 길이를 확장하기 위하여 사용하는 선택적 기능이며, 비밀보장과 무결성을 위한 암호화 알고리듬 요구를 지원한다.



(그림 5) 피어들간의 인증절차

다섯째, 대등 실체 인증은 (그림 5)에서 나타낸 것처럼 접속 식별자를 가지고 있는 접속 설정 PDU의 교환을 통하여 이루어 진다. 근원지와 목적지참조는 보호된 무결성과 무결성 키의 수명시간내에서 유일해야 한다. 마지막으로 보호연관 기능은 트랜스포트 계층 내에서 SA-P를 사용하여 제공될 수 있다.

보호연관 프로토콜은 SA PDU들의 전송을 지원하기 위하여 ISO 8073에 정의된 절차들을 사용하여 초기화될 수 있다. 그러나 초기화는 트랜스포트 접속의 수립전에 이루어지거나 논리적 관리 채널을 통하여 이루어져야 한다. 로컬 참조 번호는 SA의 설정, 유지 및 해제 동안 트랜스포트 계층에서 사용되는 유일한 식별자이다.

2. TCP/IP 보호방식

TCP/IP는 1969년부터 미 국방성 프로젝트가 진행이 되어 1980년대가 되어서야 완전한 프로토

콜로 형성되었다. 처음 인터넷의 주소를 만들 때에는 이렇게 인터넷이 크게 성장할줄 몰랐으며 그 시절에 생각할 수 있는 최대한의 주소 체계를 잡은 것이 바로 현재의 IP Address이다. 현재의 IP Address는 32비트 체계로 구성이 되어 있으며 가장 많이 사용을 할 때 2^{32} 만큼의 주소를 부여할 수 있다. 그러나 기존 주소의 부여는 클래스라는 개념을 두어 부여를 하였기 때문에 실제 사용할 수 있는 주소는 극히 일부밖에 되지 않는 실정이다. 이렇게 무분별한 주소의 관리에서부터 많아진 사용자의 요구를 들어주기엔 32비트의 주소 체계는 더 이상 주소를 부여할 수 없게 되었다. 또한 원격 회의, 원격 교육, 원격 영화 감상 등의 요구가 늘어남에 따라 좋은 품질의 선로뿐만 아니라 서비스의 질을 높여야 했다. 이렇게 늘어나는 요구에 수용하다 보니 새로운 프로토콜을 만들게 되었다.

IPng는 Ipv4에서 설계된 프로토콜로서 새로운 버전을 6으로 할당함에 따라 Ipv6로 명명하였다. 또한 Ipv4에서 동작하던 기능을 그대로 Ipv6에 옮겼으며 Ipv4에서 사용하지 않던 기능은 삭제하였다. Ipv6의 대표적인 특징들은 확장된 주소체계와 경로체계, anycast라는 주소의 탄생, multicast의 지원, 헤드의 단순화, QoS(Quality of Service)를 지원 그리고 보호기능의 지원이다.

IPv6는 확장 헤드를 가지며 next header 영역에서 규정한다. 확장 헤드는 패킷이 IPv6 헤드의 목적지 주소영역에서 정의한 노드에 도착하기 전에는 어떠한 노드에서도 처리되지 않으나 hop-by-hop option 헤드는 패킷의 경로를 따라 모든 노드에서 처리된다. 확장 헤드의 순서는 IPv6 헤드, hop-by-hop option 헤드, routing 헤드, fragment 헤드, authentication 헤드, end-to-end option 헤드이다.

IPv6는 보호서비스를 제공하기 위하여 인증 헤드와 ESP를 사용한다. 인증 헤드는 IP 데이터그램에 무결성과 인증 서비스를 제공하며 ESP는 IP 데이터그램에 무결성, 인증 및 비밀보장 서비스를 제공한다. 인증 헤드와 ESP는 호스트 간, 게이트웨이 사이 간 그리고 호스트와 게이트웨이 간에 보호를 제공한다. 보호 게이트웨이는 외부의 비신뢰 시스템과 자신의 부 네트워크에 있는 신뢰된 호스트들 사이에 통신 게이트웨이로 동작한다. 보호 게이트웨이가 신뢰된 부 네트워크상에서 하나 혹은 많은 호스트를 대신하여 보호서비스를 제공하는 경우, 보호 게이트웨이는 신뢰된 호스트를 대신하여 보호연관을 설립하고 외부 시스템들과 보호서비스를 제공한다. 이 경우, 보호 게이트웨이는 인증 헤드 및 ESP를 구현하고 신뢰된 부 네트워크의 모든 시스템들은 인증 헤드 및 ESP 보호서비스를 갖는다.

만약, 접속상에 보호 게이트웨이가 없다면 두 종단 시스템은 단지 두 시스템 사이에 수행된 사용자 데이터(TCP 혹은 UDP)만을 암호화하는데 ESP를 사용한다. 무결성이 제공되지 않은 routing 헤드는 source routing 공격 등과 같은 다양한 공격을 받을 수 있기 때문에 수신측에서 무시된다.

가. 보호연관

보호연관은 두 통신자간에 보호를 제어하는 보호속성들의 집합이며 인증 알고리듬과 알고리듬 모드, 암호화 알고리듬과 알고리듬 모드, 인증 및 암호화 키 등으로 구성된다. 송신 호스트는 적당한 보호연관을 설정하기 위하여 송신 user-id와 목

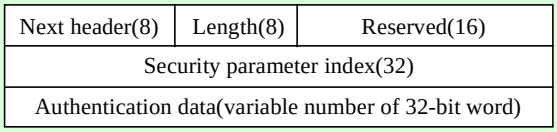
적지 주소를 사용하며 수신 호스트는 정확한 보호연관을 구분하기 위하여 SPI 값과 목적지 주소를 사용한다. 보호연관은 일반적으로 일방향이며 SPI(Security Parameter Index) 값과 목적지 주소에 의해 유일하게 규정된다. 목적지 주소는 unicast 주소 혹은 multicast 그룹 주소일 수 있다. Multicast 트래픽인 경우 몇몇 시스템은 multi-cast 그룹을 대표하여 SPI를 선택하는 것이 필요하고 multicast 그룹의 호스트들과 그 정보를 통신한다. Multicast 그룹의 송신자들은 모든 트래픽에 대해서 하나의 보호연관을 사용할 수 있다. 이 경우, 수신자는 수신된 메시지가 multicast 그룹을 위한 보호연관임을 안다. 또한, multicast 트래픽은 multi-cast 그룹의 각 송신자들을 위한 분리된 보호연관을 사용할 수도 있다.

나. 인증 헤드

인증 헤드는 호스트 간, 게이트웨이 사이 간 그리고 호스트와 게이트웨이 간의 IP 데이터그램에 무결성과 인증 서비스를 제공한다. 인증 헤드 구현시, IP 데이터 그램은 인증정보를 가지며 이 인증정보는 인증 키와 인증함수를 사용하여 데이터그램상의 전송중 변하지 않는 모든 영역을 계산하여 부가된다. Hop count, time to live, routing pointer 등과 같이 전송중 변하는 영역은 인증값 계산시 0으로 둔다. 인증 헤드는 ESP와 트랜스포트 계층 헤드 앞, 단편화와 end-to-end 헤드 뒤에 위치한다. 부인봉쇄 서비스는 RSA와 같은 비대칭키 암호화 방식에 기초한 인증 알고리듬을 사용하여 제공될 수 있으나 비밀보장 서비스는 인증 헤드에서 제공되지 않으므로 트래픽 해석과 같은 공격을 막을 수 없다. 인증 헤드는 송수신측에서의 인증계산 때문에 IP 프로토콜 처리비용 및 통신 도달 시간을 증가시킨다. 기본적으로 설정된 인증 알고리듬은 MD5이다. 이 방식은 대칭키 암호화방식으로 부인봉쇄 서비스를 제공하지 못한다.

인증 헤드의 처리과정은 다음과 같다. IP 패킷에 인증 헤드를 부가시, 송신자는 우선 적당한 보호연관을 가져야 한다. 모든 보호연관은 일방향이며 전송 IP 패킷에 대한 보호연관은 user-id와 목적지 주소에 의존한다. 선택된 보호연관은 전송 패킷에 사용된 보호알고리듬, 알고리듬 모드, 키 등의 보호성질을 나타낸다. 송신자는 인증된 IP 패킷을 전송하기 전에 인증값을 계산하여 부가한다. 모든 IPv6 option type는 그 부가 데이터가 인증계산시 포함되어질 것인지를 나타내는 하나의 비트(third-highest-bit)가 있다. 만약, 그 비트가 0이면 부가 데이터가 인증 계산시 포함되며, 1이면 부가 데이터가 인증 계산시 0으로 된다. 단편화는 전송패킷의 인증 헤드 처리 후와 수신패킷의 인증 헤드 처리전에 발생한다. IP 패킷 수신시 수신자는 정확한 보호연관을 가지기 위해 목적지 주소와 SPI 값을 이용한다. 수신자는 수신된 IP 패킷의 인증값을 이용하여 수신된 IP 패킷을 검증한다. 인증데이터 값이 정확하면 수신된 데이터그램을 받아들이며 정확하지 않으면 수신된 데이터그램을 버리고 system log와 audit log에 인증 실패를 기록한다. 기록된 log 데이터는 SPI값, 수신 시간, 송수신 주소 등을 기록한다.

(그림 6)은 인증 헤드의 구조를 나타낸 것이다. Next header 영역은 8비트이며 인증 헤드후의 헤드를 나타낸다. Length 영역은 8비트이며 인증 데이터 영역의 길이를 32비트 단위로 나타낸



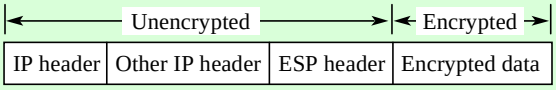
(그림 6) 인증헤드 구조

다. Reserved 영역은 16비트이며 미래 사용을 위한 영역이다. 전송시 이 영역은 0으로 둔다. Security parameter index 영역은 32비트이며 데이터그램의 보호연관 식별자를 나타낸다. SPI 값이 0이면 보호연관이 존재하지 않음을 나타낸다. Authentication data 영역은 32비트 단위의 가변길이를 가지며 패킷의 인증값을 나타낸다.

다. ESP

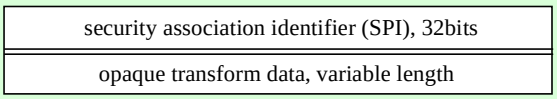
ESP(Encapsulating Security Paylord)는 호스트 간, 게이트웨이 사이 간 그리고 호스트와 게이트웨이 간의 IP 데이터그램에 무결성 및 비밀보장 서비스를 제공하며 사용하는 알고리듬에 따라 인증 서비스도 제공할 수 있다. ESP는 터널 모드와 트랜스포트 모드가 있다. 터널 모드는 ESP 헤드내의 모든 IP 데이터그램을 암호화하는 방식이며 트랜스포트 모드는 ESP 헤드내의 상위계층 프로토콜인 UDP나 TCP만을 암호화하고 평문 IP 헤드를 부가하는 방식이다. 통신 호스트들이 보호 게이트웨이의 간섭 없이 통신하고자 할 때 트랜스포트 모드를 사용할 수 있다. 이때 트랜스포트 모드는 전체 IP 데이터그램을 비밀보장을 원하지 않는 호스트들에게 처리 비용을 감소시킨다. ESP는 IP 단편화 후와 IP 재결합 전에 이루어진다.

ESP의 사용은 IP 프로토콜 처리시간을 증가



(그림 7) ESP 구조

시키며 증가된 시간은 암호화 알고리듬, 키 등의 변수에 의존한다. 기본적으로 설정된 ESP의 알고리듬은 DES CBC 모드이다. (그림 7)은 ESP의 구조를 나타낸 것이다. ESP는 IP 헤드 후와 트랜스포트 계층 프로토콜전에 어느곳이나 위치한다. ESP의 프로토콜 수는 50이며 IP 프로토콜의 next header 영역에 50이 설정되어야 ESP가 수행된다. ESP는 암호화되지 않은 헤드 영역과 암호화된 데이터 영역으로 구성된다. 암호화된 데이터 영역은 보호된 ESP 헤드와 보호된 사용자 데이터로 이루어지며 보호된 사용자 데이터는 전체 IP 데이터그램이거나 상위계층 프로토콜 프레임이다.



(그림 8) ESP 헤더 구조

(그림 8)은 ESP 헤드의 구조를 나타낸 것이다. ESP 형태는 미래에 적용될 새롭거나 부가적인 암호화 알고리듬을 지원하도록 구성된다. SPI 영역은 적용된 데이터그램의 보호연관을 나타내는 32비트 값이다. 만약, 보호연관이 설정되지 않았다면 SPI 값은 0×00000000이다. 0×00000001에서 0×000000FF까지의 SPI 값은 미래사용을 위해 IANA(Internet Assigned Numbers Authority)에 예

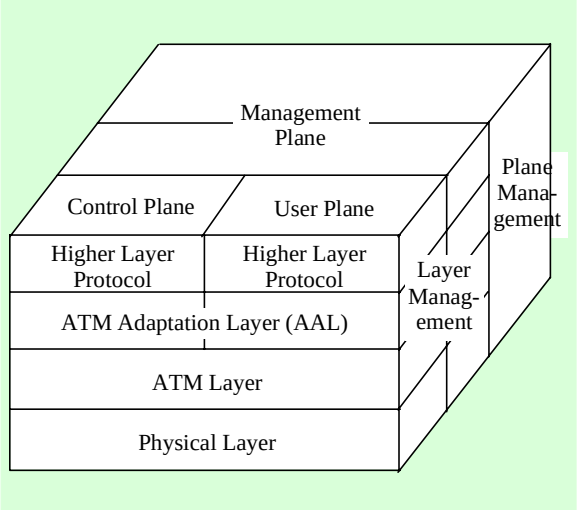
약되어 있다.

ESP는 인증 헤드와 함께 사용되면 무결성 및 비밀보장 서비스뿐 아니라 인증 서비스도 제공할 수 있다. ESP와 인증 헤드를 함께 사용하는 방법은 두가지가 있다. 첫번째는 송신자는 원하는 데이터에 ESP를 적용하여 비밀보장 서비스를 부가한 후 평문 IP 헤드를 부가하며 마지막으로 IP 인증 헤드가 부가된다. 이 때, 수신자는 먼저 전체 데이터그램에 대하여 인증 검사를 한다. 인증 결과가 정확하면 ESP 처리를 수행하여 암호화된 데이터를 복호하여 결과 데이터를 상위계층에 보낸다. 두번째는 인증이 단지 터널 모드 ESP에 의해 보호된 데이터그램에 적용하는 경우이며 이때 인증 헤드는 보호된 데이터그램내에 위치한다. 그러나 인증이 트랜스포트 모드 ESP에 의해 보호된 데이터그램에 적용되면 인증 헤드는 보호된 데이터그램을 처리하여 ESP 내에 그리고 전체 데이터그램에 대한 인증 헤드가 존재한다.

3. ATM 보호방식

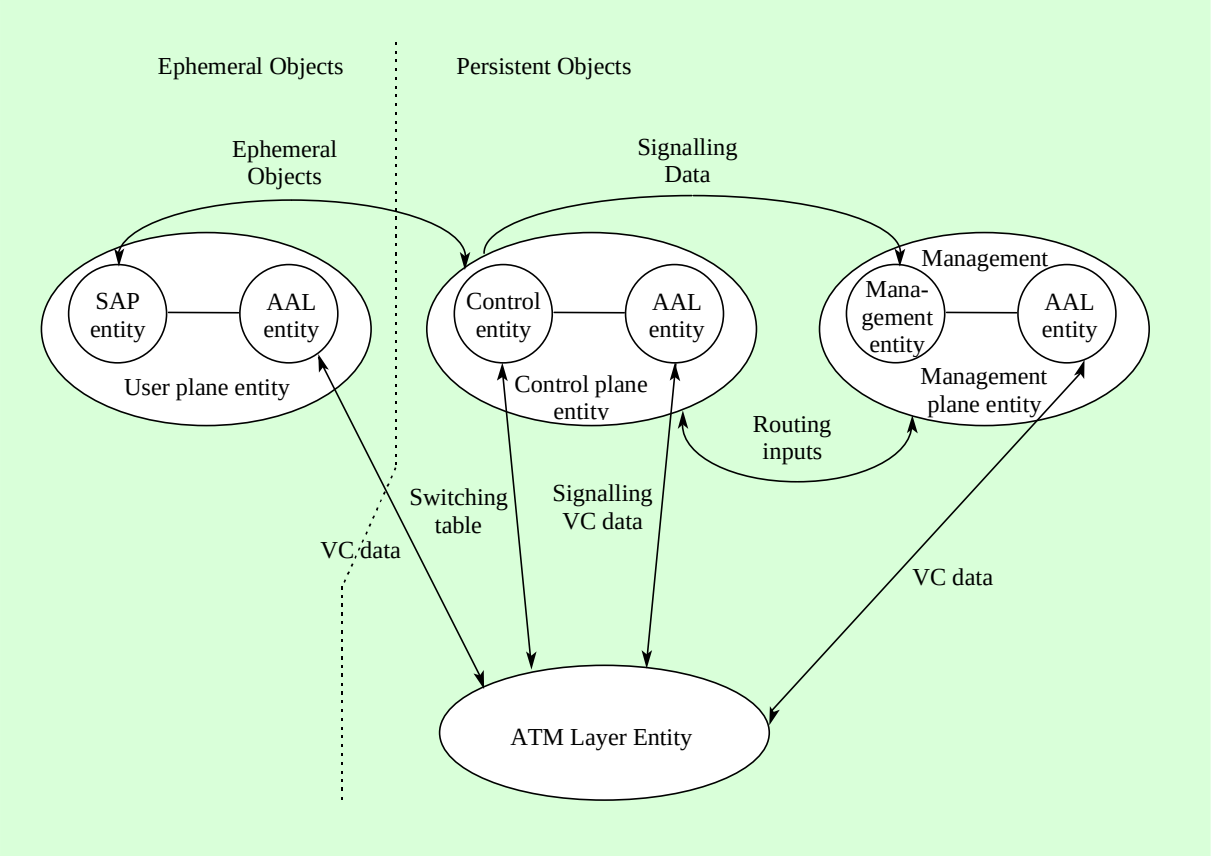
B-ISDN은 차세대 초고속 정보 통신망의 기반 구조라 할 수 있다. B-ISDN에서는 통신망에서 존재하는 모든 서비스를 수용하는 것을 목표로 하고 있으며 이러한 B-ISDN망을 구현하기 위한 통신 방식으로 ATM이 있다. ATM에 관한 규격은 ATM Forum에서 현재 이루어지고 있으며 ATM 보호에 관한 내용은 현재 연구 진행중이다.

ATM에서의 보호은 ATM을 구성하고 있는 객체들의 성질과 상관관계를 고려해야 한다. ATM을 구성하고 있는 이 객체들의 성질과 상관관



(그림 9) ATM 참조 모델

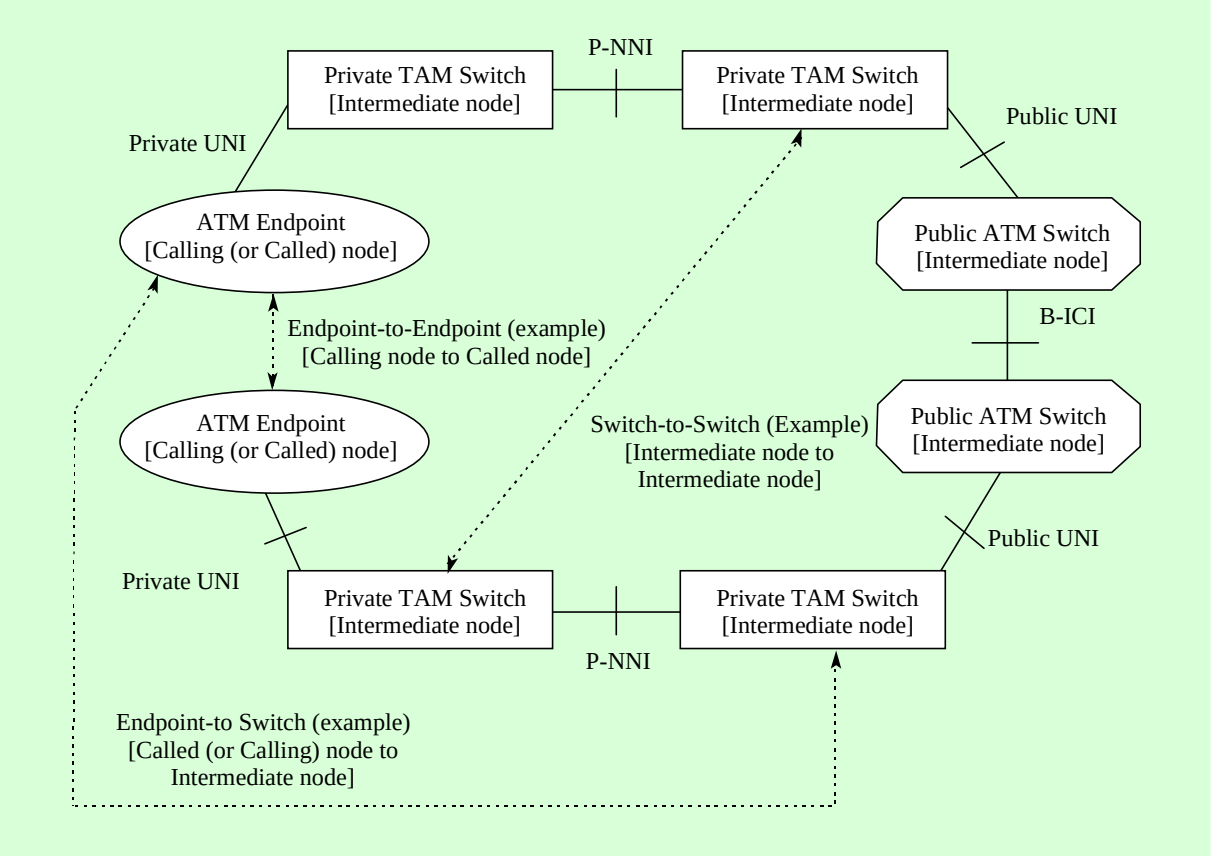
계는 ATM 참조 모델에서 정의되어 있으며 그 구성은 (그림 9)와 같다. ATM에서 계층은 응용 계층, AAL계층, ATM계층, 물리 계층으로 이루어져 있다. AAL계층은 상위 계층과 하위의 ATM계층 사이에서 상위 계층의 정보를 ATM계층으로의 적절한 전달을 맡고 있다. 즉 상위 계층의 서비스 요구를 ATM계층에 적용시키는 것이다. AAL계층은 상위 계층의 사용자 서비스 정보를 PDU 로 만들어주는 수렴 부계층(Convergence Sublayer: CS)와 ATM 계층과의 통신에서의 PDU 절단 및 재결합(Segmentation And Reassembly: SAR) 부계층으로 구성된다. ATM 계층은 주로 사용자 노드와 네트워크 노드간의 셀 전달에 관한 일을 한다. 물리 계층은 송 수렴 부계층과 물리 매체 부계층으로 구성되는데, 전송 수렴 부계층의 기능은 셀 속도의 분리, 헤더오류 제어용 바이트의 발생 및 확인, 셀 경계점의 검출 등을 한다. 또한 동기식 디지털 계위에 의거하여 전송하는 경우에는 전송 프



(그림 10) ATM 망 요소 객체 모델

레임의 발생 및 확인 기능도 수행한다. 물리 매체 부계층은 광섬유나 동축 케이블을 통한 최종 전송 단계를 의미한다.

ATM은 사용자 측면, 제어 측면 및 관리 측면으로 구분될 수 있으며 각각의 측면은 여러개의 계층으로 구성 되어 있다. 먼저 사용자 측면은 주로 사용자의 데이터와 관련되어 사용자 정보전달, 흐름 제어, 에러 복구 등의 기능을 주로 한다. 사용자 측면은 ATM을 통해서 데이터를 전달할 경우에 생성되며 가상회로마다 하나의 사용자 측면을 가지므로 다른 객체보다 짧은 활성 기간을 가진다. 사용자 측면은 ATM 서비스 접근 포인트(SAP: Service Access Point)에서 ATM 가상회로를 요구할 경우에 생성된다. 요청이 계속 영향을 미칠 때까지는 지속되는데 요구가 스위치 서비스이면 SVC(Switched Virtual Circuit) SETUP으로 계속 남아 있다가 SETUP이 되면 회선이 끊어질 때까지 남아 있는다. SETUP이 실패하면 알리고 사라진다. PVC(Permanent Virtual Circuit)의 경우에는 관리자의 정의에 의해서 생성되고 소멸된다. 제어 측면과 가상회선의 연결과 해제에 관하여 상호작용을 하며 ATM 네트워크에 사용자 데



(그림 11) ATM 시큐리티 정합 참조 모델

이터를 보내고 받기 위해서 ATM 계층과 상호작용을 한다.

ATM에서 네트워크의 연결과 해제에 관한 기능과 연결들의 관리에 관한 기능을 가지는 것이 제어 측면이다. 제어 측면은 사용자 측면과 다르게 네트워크가 활성 중이면 항상 활동한다. 제어 측면은 ATM 계층의 스위치 테이블의 관리와 신호 메시지를 신호 채널로 전송하는 것을 관여하며 관리 측면에 필요한 가상회선의 연결과 해제, PNNI(Private Network Network Interface) 라우팅 기능으로부터 라우팅을 결정하기 위한 정보에 관여한다. 관리 측면은 사용자 측면과 제어 측면을 조정, 관리하는 기능을 한다. 관리 측면은 PNNI 기능을 가지며 이는 라우팅 기반을 확립하는 기능을 한다. 네트워크가 활성 중이면 항상 활동을 하며 가상회선으로 관리 데이터를 받고 보내기 위해서 ATM 계층과 연결된다.

ATM에서의 보안 구조는 (그림 11)과 같이 종단간(Endpoint to Endpoint), 종단에서 중간 노드간(Endpoint to Switch) 및 중간 노드간(Switch to Switch)에 보호를 제공할 수 있다. 종단간에 보호를 제공하는 경우, 보호 서비스는 전 연결 경로에

대해서 제공하며 종단에서 중간 노드간 보호를 제공하는 경우, 보호서비스는 종단에서 중간 노드로의 연결 경로 일부분만을 보호하고, 중간 노드간 보호를 제공하는 경우, 보호서비스는 중간 노드에서 중간 노드의 연결 경로의 일부분만으로 제한된다. 이를 기초로 하여 참조 모델의 보호 적용범위를 정의하고 있다. 사용자 측면 보호는 사용자 사이에 확립된 가상회선에 대한 보호를 다루며 종단간 및 중간 노드간에 보호서비스를 제공한다. 종단간에는 인증, 비밀보장, 데이터 무결성의 보호서비스가 제공되며 중간 노드간에는 인증 및 비밀보장 서비스가 제공된다. 제어 측면 보호는 제어 측면 사이의 메시지 교환에 대한 보호을 다루며 종단간, 종단에서 중간 노드간 및 중간 노드간에 인증 서비스를 제공한다.

IV. 결 론

본 논문에서는 초고속정보통신기반하에서의 기술적 보호대책을 모색하였으며 이러한 보호대책은 초고속정보통신기반 구축에 활용될 것이다. 다음은 주요 결과를 간단히 정리하였다.

(1) 범죄의 방지대책으로 기술적인 통제방안을 이용하는 기술적 방지대책, 물리적으로 시스템 환경을 안전하게 보호하기 위한 물리적 방지대책, 컴퓨터 시스템의 관리 및 운영적인 측면에서의 관리적 방지대책, 그리고 국가적 차원에서 지원해야 하는 법적·제도적 방지대책으로 구분할 수 있다. 본 연구에서는 범죄 보호 메커니즘을 제시하였으며 특별히 기술적 방지대책, 물리적 방지대책, 관리적 방지대책 그리고 법적·제도적 방지대책 가운데서 기술적 방지대책에 관하여 중점적으로 다루었다.

(2) 초고속정보통신기반에서의 보호는 크게 사용자 측면, 서비스 측면, 네트워크 측면 그리고 관리 측면으로 분류할 수 있다. 본 연구에서는 이러한 측면들 가운데 초고속정보통신기반 보호기술이 가장 절실한 네트워크 측면 보호방식들을 OSI 참조모델을 위한 NLSP와 TLSP 방식, TCP/IP를 위한 IP 보호방식 그리고 ATM을 위한 보호방식차원에서 제시하였다. 현재 ATM 보호에 관한 연구는 국제적으로 초보적인 단계이며 앞으로 연구가 계속 수행되어져야 할 분야이다.

그리고 초고속정보통신기반하에서 이용되는 서비스들을 보다 안전하게 사용하기 위해서는 법적·제도적, 관리적 그리고 물리적 방지대책과 병행하여 기술적 방지대책이 이루어져야 효과적으로 범죄를 예방할 수 있다.

참 고 문 헌

[1] Cohen, Protection and Security on the Information Superhighway, Wiley, 1995.

[2] Lawrence J. Haas, "*NII security: The federal role*," National Information Infrastructure Security Issues Forum, June 1995.

[3] Whitfield Diffie and David Gifford, "Security and privacy technologies," National Information Infrastructure Security Issues Forum, 1995.

[4] 김세헌, 컴퓨터범죄와 프라이버시 침해, 희성출판사, 1989년 10월.

[5] 박영호, 문상재, 김세헌, 강신각, 임주환, "컴퓨터범죄 방지를 위한 정보통신망의 보호반안에 관한 연구," 통신정보보호학회지, 제 4권 , 제 2호, pp. 47-57, 1994년 6월

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

[7] EWOS, "Model for management of the EII security work programme," Feb. 1996.

[8] EURESCOM project P401, Definition of a Pan-European IC-Card for Authentication, 1995.

[9] Daniel Minoli, Telecommunications Technology Handbook, Artech House, 1991.

[10] CCITT, The Directory Authentication Framework, CCITT Recommendation X.509, Geneva, 1991.

[11] ISO/IEC 10181-2, Information Technology - Security Frameworks in Open Systems - Authentication Frameworks, 1992.

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

[13] ISO/IEC JTC 1/SC 6, Information Technology - Telecommunications and Information Exchange Between Systems - Network Layer Security, DIS Ballot Text of ISO/IEC 11577, Jan. 1993.

[14] 박영호, 문상재, "OSI 참조모델의 네트워크 계층 보호 프로토콜," 통신정보보호학회지, 제 5권, 제 2호, pp. 64-73, 1995년 6월.

[15] SDNS Program Office, Security Protocol 4(SP4), SDN.401, Revision 1.3, May. 1989.

[16] ISO/IEC JTC 1/SC 6, Information Technology - Telecommunications and Information Exchange Between Systems - Transport Layer Security, Draft of the New DIS Test, Oct. 1992.

[17] 박영호, 김기현, 문상재, 강신각, "OSI 트랜스포트 계층에서의 보호시스템 개발," 통신정보보호학회 논문지, 제 5권, 제 1호, pp. 65-84, 1995년 3월.

[18] R. Atkinson, "Security architecture for the Internet protocol," RFC 1825, Aug. 1995.

[19] R. Atkinson, "IP authentication header," RFC 1826, Aug. 1995.

[20] R. Atkinson, "IP encapsulating security payload (ESP)," RFC 1827, Aug. 1995.

[21] ATM Forum, "ATM security specification," ATM Forum/95-1473R4, Aug. 1996.

[22] ATM Forum, "UNI signaling addition to support user plane security," ATM Forum/96-1019, Aug. 1996.

[23] ATM Forum, "User plane data integrity mechanisms," ATM Forum/95- 1473R4, Aug. 1996.

[24] NTIA Privacy Report, "Privacy and the NII: safeguarding telecommunications -related personal information," U.S. Department of Commerce, Oct. 1995.

[25] Leonardo Chiariglione, "The development of the GII: a process driven by producers and consumers of information," CSELT, Torino, Italy, 1995.