한국산업정보학회논문지 제7권 제5호 (2002. 12)

IPv6 및 ATM에서의 보호에 관한 연구

(A Study on Security for IPv6 and ATM)

박 영 호*
(Young-Ho Park)

요 약 본 논문에서는 IPv6, ATM 및 IP/ATM에서의 보호에 관하여 기술한다. IPv6에서는 보호서비스를 제공하기 위하여 인증 헤드와 ESP를 사용하고 있으며 이러한 인증 헤드와 ESP에서의 보호서비스 제공에 관하여 기술한다. ATM에서의 보호체계는 ATM 포럼에서 지금까지 연구한 ATM 보안 규격 내용을 보호서비스 측면에서 소개한다. 또한, IP/ATM의 특성을 고려하여 IP/ATM에 적합한 보호서비스와 보호기술들을 기술한다.

Abstract This paper presents IPv6, ATM, and IP/ATM security systems for computer network. IPv6 uses authentication header and ESP to provide security services. Authentication header provides integrity and authentication services and ESP provides integrity, authentication and confidentiality services. User plan of ATM provides authentication, integrity, confidentiality and access control services and control plan of ATM provides authentication and integrity services. IP/ATM security services are also presented.

1. 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 네트워크에 연결되어 있는 상황에서는 더욱 심각하다. 따라서 이를 막을 수 있는 대책이 필요하다.[1,2] IPv6에서의 새로운 특징 중에 하나는 기존에는 고려하지 않았던 보호서비스를 제공하기 위하여 인증헤드와 ESP(encapsulating security payload)를 사용한다.[3-5]

ATM에 관한 규격은 ATM 포럼 등에서 이루어지고 있으며 ATM 보호에 관한 연구는 ATM 포럼의 기술위원회 산하에 보안 작업 그룹을 두어 ATM에서의 보호 정책에 관한 표준화 작업이 이루어지고 있다. ATM 포럼에서는 ATM 보안을 위해 요구되는 요구사항을 연구하여 사용자 망간(UNI:User Network Interface) 또는 망간(NNI:Network-Node Interface) 접속부에서 암호학적으로 안전한 프로토콜과 알고리즘을 정의하고 이를 바탕으로 한 ATM 보안규격을 개발하는 것을 목표로 ATM 보안규격 개발작업이 진행되고 있으며 보안 규격서[6]를 발행하였다.

ATM 망이 공중망으로 구축되어야 하는 시점에서 IP 프로토콜을 사용하는 기존의 방대한 LAN 응용을 효율적으로 접속하여 기존의 서비스를 그대로 이용할 수 있어야 한다는 것은 필수적인 요인이라 하겠다. 이러한 요구에 따른 ATM LAN에 대한 표준화는 ATM 포럼과 IETF를 중심으로 이루어지고 있다. 기존 LAN과 ATM의 연동을 위해서 LAN의 특징인 공유 매체를 사용한 비연결성 서비스를 ATM망에서 어떻게 제공하게 할 것인가 하는 문제가 야기된다. 이러한 문제를 위한 해결 방법으로 ATM 포럼에서는 LAN 에뮬레이션[7]을 제안하였고 IETF(Internet Engineering Task Force)에서는 Classical IP over ATM(IP/ATM)의 rfc 문서를[8] 제시하고 있다. IP/ATM은 IP를 ATM상에서 사용하여 비연결형 연결을 지원하는 방식으로 상위의 네트워크 계층에서 인터넷 프로토콜만을 지원한다는 단점이 있지만 그 구현의 오버 헤드가 적으며 구현이 용이하다는 장점이 있다.

본 논문에서는 인터넷 기반인 IPv6에서의 보호체계와 초고속정보통신망의 기반인 ATM 및 IP/ATM에서의 보호체계에 관하여 기술한다. IPv6에서의 새로운 특징 중에 하나는 기존에는 고려하지 않았던 보호서비스를 제공하기 위하여 인증 헤드[3]와 ESP[4]를 사용한다는 것이다[5]. 본 고에서는 이러한 인증 헤드와 ESP에서의 보

* 상주대학교 전자전기공학부 부교수(yhpark@sangju.ac.kr)

호서비스 제공에 관하여 기술한다. ATM에서의 보호 체계는 ATM 포럼에서 지금까지 연구한 ATM 보안 규격 내용을 보호서비스 측면에서 소개한다. 또한, IP/ATM은 하부 기반이 ATM으로 IP 레벨의 패킷이 ATM 망을 통과하므로 기존의 ATM에서 보호서비스가 제공될 수 있지만 IP 레벨의 라우터를 거치는 경우에 생기는 AAL SDU내의 IP 헤드의 문제로 그대로 적용하기가 힘든 부분이 존재한다. 따라서 이러한 문제를 고려하여 IP/ATM에 적합한 보호서비스와 보호기술들을 기술한다.

2. IPv6에서의 보호

IPv6는 확장헤드를 가지며 다음 헤드 영역에서 규정한다. 확장헤드는 패킷이 IPv6 헤드의 목적지 주소영역에서 정의한 노드에 도착하기 전에는 어떠한 노드에서도 처리되지 않으며 hop-by-hop 옵션 헤드, 라우팅 헤드, 단편 헤드, 인증 헤드 및 종단간 헤드들이 있다. IPv6는 보호서비스를 제공하기 위하여 인증 헤드와 ESP를 사용한다. 인증 헤드는 IP 데이타그램에 무결성과 인증서비스를 제공하며 ESP는 IP 데이타그램에 무결성, 인증 및 기밀성 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 네트워크가 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 시스템사이에 수행된 사용자 데이타(TCP 혹은 UDP)만을 암호화하는데 ESP를 사용한다. 무결성이 제공되지 않은 라우팅 헤드는 소스 라우팅 공격등과 같은 다양한 공격을 받을 수 있기 때문에 수신측에서 무시된다.

(1) 보호연관

보호연관은 두 통신자간에 보호를 제어하는 보호속성들의 집합이며 인증 알고리즘과 알고리즘 모드, 암호화 알고리즘과 알고리즘 모드, 인증 및 암호화 키 등으로 구성된다. 송신 호스트는 적당한 보호연관을 설정하기 위하여 송신 사용자 식별과 목적지 주소를 사용하며 수신 호스트는 정확한 보호연관을 구분하기 위하여 SPI(security parameter index) 값과 목적지 주소를 사용한다. 보호연관은 일반적으로 일방향이며 SPI값과 목적지 주소에 의해 유일하게 규정된다. 목적지 주소는 유니캐스트 주소 혹은 멀티캐스트 그룹 주소일 수 있다. 멀티캐스트 트래픽인 경우 몇몇 시스템은 멀티캐스트 그룹을 대표하여 SPI를 선택하는 것이 필요하고 멀티캐스트 그룹의 호스트들과 그 정보를 통신한다. 멀티캐스트 그룹의 송신자들은 모든 트래픽에 대해서 하나의 보호연관을 사용할 수 있다. 이 경우, 수신자는 수신된 메세지가 멀티캐스트 그룹을 위한 보호연관임을 안다. 또한 멀티캐스트 트래픽은 멀티캐스트 그룹의 각 송신자들을 위한 분리된 보호연관을 사용할 수 있다.

(2) 인증 헤드

인증 헤드는 호스크 간, 게이트웨이 간 그리고 호스트와 게이트웨이 간의 IP 데이타그램에 무결성과 인증서비스를 제공한다. 인증 헤드 구현시, IP 데이타그램은 인증정보를 가지며 이 인증정보는 인증 키와 인증함수를 사용하여 데이타그램상의 인증정보를 가지며 이 인증정보는 인증키와 인증함수를 사용하여 데이타그램상의 전송 중 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 종단간 헤드 뒤에 위치한다. 부인봉쇄 서비스는 RSA와 같은 비대칭키 암호화 방식에 기초한 인증 알고리즘을 사용하여 제공될 수 있으나 기밀성 서비스는 인증 헤드에서 송수신측에서의 인증계산 때문에 IP 프로토콜 처리비용 및 통신도달 시간을 증가시킨다. 기본적으로 설정된 인증 알고리즘은 MD5이다. 이방식은 대칭키 암호화방식으로 부인봉쇄 서비스를 제공하지 못한다.

인증 헤드의 처리과정은 다음과 같다. IP 패킷에 인증 헤드를 부가시, 송신자는 우선 적당한 보호연관을 가져야 한다. 모든 보호연관은 일 방향이며 IP 패킷에 대한 보호연관은 사용자 식별과 목적지 주소에 의존한다. 선택된 보호연관은 전송패킷에 사용된 보호알고리즘, 알고리즘 모드, 키 등의 보호성질을 나타낸다. 송신자는 인증된 IP 패킷을 전송하기 전에 인증값을 계산하여 부가한다. 모든 IPv6 선택형은 그 부가 데이타가 인증 계산시 포함되어질 것인지를 나타내는 하나의 비트(third-highest-bit)가 있다. 만약, 그 비트가 0이면 부가 데이타가 인증계산시 포함되며 1이면

부가 데이타가 인증계산시 0으로 된다. 단편화는 전송 패킷의 인증 헤드 처리 후와 수신패킷의 인증 헤드 처리 전에 발생한다. IP 패킷 수신시 수신자는 정확한 보호연관을 가지기 위해 목적지 주소와 SPI값을 이용한다. 수신자는 수신된 IP 패킷의 인증값을 이용하여 수신된 IP 패킷을 검증한다. 인증데이타 값이 정확하면 수신된 데이타그램을 받이들이며 정확하지 않으면 수신된 데이타그램을 버리고 시스템 로그와 감시 로그에 인증 실패를 기록한다. 기록된 로그 데이타는 SPI 값, 수신시간, 송수신주소등을 기록한다.

그림 1은 인증 헤드의 구조를 나타낸 것이다. 다음 헤드 영역은 8비트이며 인증 헤드 후의 헤드를 나타낸다. 길이 영역은 8비트이며 인증 데이타 영역의 길이를 32비트 단위로 나타낸다. 예약 영역은 16비트이며 미래사용을 위한 영역이다. 전송시 이 영역은 0으로 둔다. SPI 영역은 32비트이며 데이타그램의 보호연관 식별자를 나타낸다. SPI 값이 0이면 보호연관이 존재하지 않음을 나타낸다. 인증 데이타 영역은 32비트 단위의 가변길이를 가지며 패킷의 인증값을 나타낸다.

Next Header(8)	Length(8)	Reserved (16)
Security parameter index(32)		
Authentication data(variable number of 32-bit word)		

<Figure 1> Structure of authentication header.

(3) ESP

ESP는 호스트간, 게이트웨이 사이 간 그리고 호스트와 게이트웨이 간의 IP 데이타그램에 무결성 및 기밀성 서비스를 제공하며 사용하는 알고리즘에 따라 인증 서비스를 제공할 수 있다. ESP는 터널 모드와 트랜스포트 모드가 있다. 터널 모드는 ESP 헤드내의 모든 IP 데이타그램을 암호화하는 방식이며 트랜스포트 모드는 ESP 헤드내의 상위계층 프로토콜인 UDP나 TCP만을 암호화하고 평문 IP헤드를 부가하는 방식이다. 통신 호스트들이 보호 게이트웨이의 간섭없이 통신하고자할 때 트랜스포트 모드를 사용할 수 있다. 이때 트랜스포트 모드는 전체 IP 데이타그램에 기밀성을 원하지 않는 호스트들에게 처리 비용을 감소시킨다. ESP는 IP 단편화 후와 IP 재결합 전에 이루어진다. ESP의 사용은 IP 프로토콜 처리시간을 증가시키며 증가된 시간은 암호화 알고리즘, 키 등의 변수에 의존한다.

그림 2는 ESP의 구조를 나타낸 것이다. ESP 헤드는 IP 헤드 후에 트랜스포트 계층 프로토콜 전에 위치한다. ESP의 프로토콜 식별자는 50이며 IP 프로토콜의 다음 헤드 영역에 50이 설정되어야 ESP가 수행된다. ESP는 암호화되지 않은 헤드 영역과 암호화된 데이타 영역으로 구성된다. 암호화된 데이타 영역은 보호된 ESP 헤드와 보호된 사용자 데이타로 이루어지며 보호된 사용자 데이타는 전체 IP 데이타그램이거나 상위계층 프로토콜 프레임이다.

←---- Unencrypted ------→			← Encrypted →
IP header	Other IP header	ESP header	Encrypted data

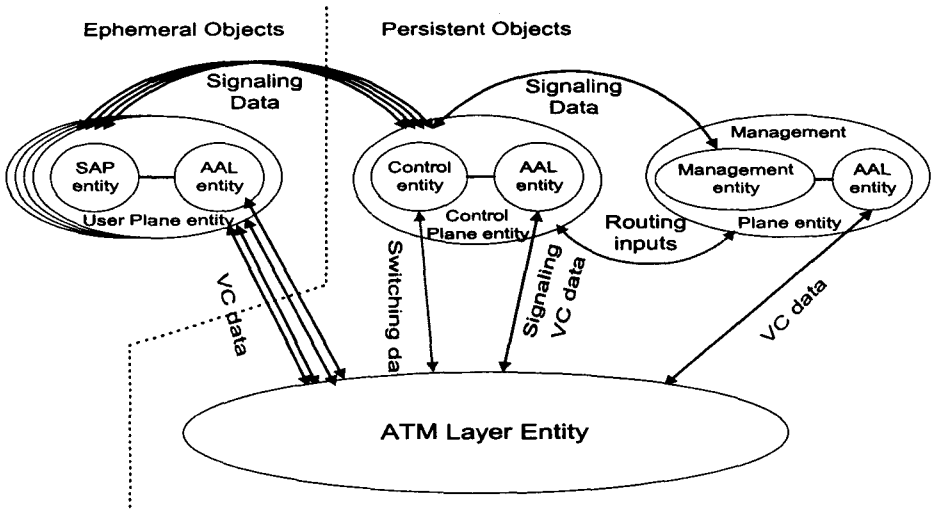
<Figure 2> Structure of ESP.

그림 3은 ESP 헤드의 구조를 나타낸 것이다. ESP 형태는 미래에 적용될 부가적인 암호화 알고리즘을 지원하도록 구성된다. SPI 영역은 적용된 데이타그램의 보호연관을 나타내는 32비트 값이다. 만약, 보호연관이 설정되지 않았다면 SPI 값은 0x00000000이다. 0x00000001에서 0x000000FF까지의 SPI 값은 미래사용을 위해 IANA(internet assigned members authority)에 예약되어 있다.

Security association identifier (SPI), 32 bits
Opaque transform data, variable length

<Figure 3> Structure of ESP header.

ESP는 인증 헤드와 함께 사용되면 데이타 무결성 및 기밀성 서비스 뿐만 아니라 인증 서비스도 제공할 수 있다. ESP와 인증 헤드를 함께 사용하는 방법은 두 가지가 있다. 첫 번째는 송신자가 원하는 데이타에 마지막으로 IP 인증 헤드를 부가한다. 이때, 수신자는 먼저 전체 데이타그램에 대하여 인증검사를 한다. 인증결과가 정확하면 ESP 처리를 수행하여 암호화된 데이타를 복호하여 결과 데이타를 상위계층에 보낸다. 두 번째는 인증이 단지 터널 모드 ESP에 의해 보호된 데이타그램에 적용하는 경우이며 이때 인증 헤드는 보호된 데이타그램내에 위치한다. 그러나 인증이 트랜스포트 모드 ESP에 의해 보호된 데이타그램에 적용되면 인증 헤드는 보호된 데이타그램을 처리하여 ESP내에 그리고 전체 데이타그램에 대한 인증 헤드가 존재한다.



<Figure 4> ATM Network Element Object Model.

3. ATM에서의 보호

(1) 보안 참조모델

ATM에서는 보안 규격의 범위와 요구되는 기능을 효율적으로 규정하기 위해서 두 가지의 참조 모델을 정의한다. 하나는 단일 ATM 망 요소들 사이의 관계를 표시하는 객체 모델이고 다른 하나는 ATM 보호 접속부와 상호동작에 대한 참조 모델이다. 그림 4는 객체 모델로 ATM 프로토콜 참조모델에 근거하고 있다. 이 모델을 통해서 ATM 프로토콜에서 정의되고 있는 서로 다른 평면과 각 객체에 대한 보안 기능을 규정해야 함을 알 수 있다. 그림 5는 ATM 보호 접속부와 상호동작에 대한 참조모델을 나타낸 것이다. 이 모델은 접속부의 종단간, 스위치간 및 종단-스위치간 등과 같은 다양한 상호 접속의 경우에 대한 보안 기능을 규정하고 있다.

(2) 보안규격 범위

ATM에서의 보안규격 범위는 그림 6과 같다. 그림 6에서는 보안 규격에서 고려하고 있는 ATM의 각 평면에서의 보호 기능들에 대한 범위를 나타낸 것이다. 보안 규격에서는 ATM에서의 보호 기능을 위해 크게 사용자 평면에서 제공되는 보호서비스, 제어 평면에서 제공되는 보호서비스 및 지원 서비스로 규정하고 있다. 사용자 평면에서 제공되는 보호서비스들로는 접근제어, 인증, 기밀성, 데이타 무결성 서비스가 있으며 제어 평면에서 제공되는 보호서비스들로는 인증과 데이타 무결성 서비스가 있으며 지원 서비스들로는 보호메세지 교환 및 협상, 키 교환, 세션키 갱신 그리고 Certification Infrastructure이 있다.

	User Plane	Control Plane	Management Plane
Authentication	■	■	
Confidentiality	■		
Date Integrity	■	■	
Access Control	■		

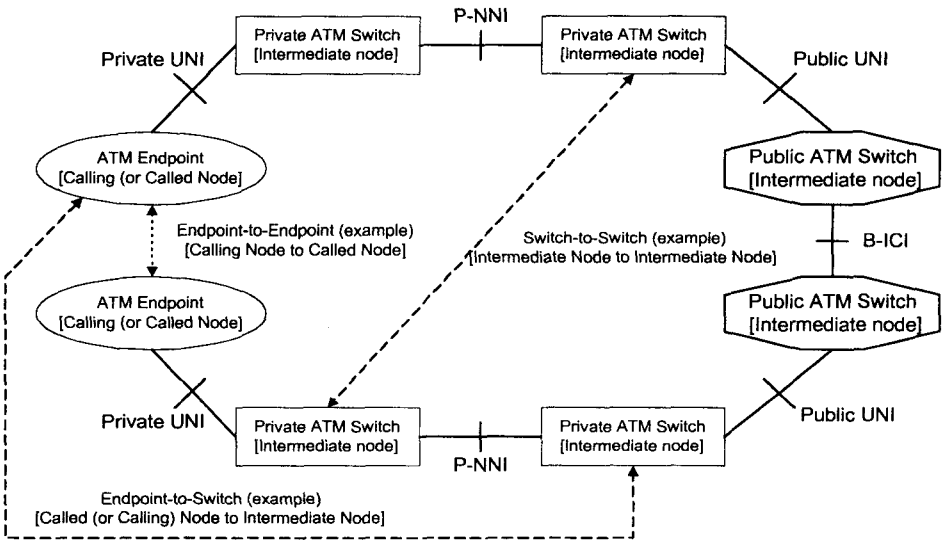
<Figure 6> Scope of Phase I Specification.

1) 사용자 평면에서의 보호서비스

사용자 평면에서의 보호서비스는 VC(VCC 혹은 VPC) 기초 단위로 적용되며 제공되는 보호서비스는 인증, 기밀성, 데이타 무결성 및 접근제어 서비스이다.

① 인증 서비스

인증 서비스는 송신자와 수신자의 실체를 보장해준다. 또한 인증은 많은 다른 보호서비스들을 지원해주는 서비스이기도 하다. 인증은 노드들 간의 안전한 통신을 수행하기 위한 첫 번째 단계이다. 실체의 인증으로 노드는 접속의 초기에 다른 노드의 신원을 확인할 수 있다. 스푸핑(spoofing) 등에 대한 공격을 막기 위해 노드의 인증은 안전한 통신을 수행하기 위해서 필



<Figure 5> ATM Security Interface and Interactions Reference Model.

수적이다. 또한 실체 인증은 노드들간의 키 교환 및 보호협상 변수들의 교환과 같이 다른 보호서비스들을 위해 사용되는 보조 서비스이기도 하다.

인증은 단방향 혹은 양방향 인증에 의해 제공될 수 있다. 인증은 DES와 같은 대칭키 암호 알고리즘이나 RSA와 같은 비대칭키 암호 알고리즘을 이용하여 이루어질 수 있다. 비대칭키 암호 알고리즘을 이용하는 경우에는 인증이 이루어지기 전에 두 노드간의 비밀키 교환이 선행되어야 하고 비대칭키 암호 알고리즘을 이용하는 경우는 노드는 단지 다른 노드의 공개키만 알면 된다.

② 기밀성 서비스

기밀성 서비스는 VC상에서 사용자의 데이타가 비인가된 실체에게 노출되는 것을 막아주며 이를 위해 암호학적인 메카니즘이 사용된다. ATM 셀의 고정된 길이는 효율적인 암호를 허용하므로 기밀성 서비스는 ATM 셀 레벨에서 제공된다. 즉, 셀의 48 바이트 payload 영역은 암호화되며 5 바이트 헤드영역은 평문으로 전송한다. 따라서, 암호화된 셀은 각 hop에서 복호 할 필요가 없다. ATM 보안 규격에서는 기밀성 서비스를 제공하기 위해 대칭키 알고리듬을 사용하도록 정의하고 있다. 이는 대칭키 알고리듬이 비대칭 알고리듬보다 속도가 빨라 ATM 암호화에 적합하기 때문이다.

③ 데이타 무결성 서비스

데이타 무결성 서비스는 사용자의 데이타와 데이타의 순서가 변경되지 않았음을 보장해준다. 데이타 무결성 서비스는 AAL3/4와 AAL5를 위한 AAL SDU에서 종단간에 제공된다. 데이타 무결성 서비스에서는 2가지의 옵션이 아래와 같이 제공된다.

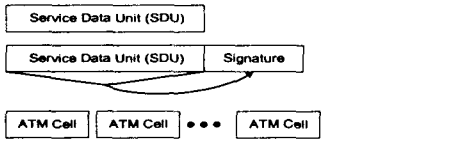
ⓐ 재연/재순서(replay/reordering)의 보호가 없는 데이타 무결성

ⓑ 재연/재순서(replay/reordering)의 보호가 있는 데이타 무결성

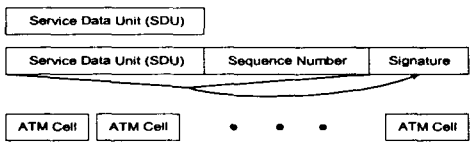
ⓐ번 옵션이 제공될 때 송신측에서 암호학적인 서명 값을 각 AAL-SDU의 끝 부분에 부가한다. 이것은 그림 7의 a)에서 보여 주고 있다. 수신 측에서는 AAL-SDU의 수신시 이 서명을 검증하여 만약 서명이 올바르지 않으면 이 AAL-SDU를 폐기한다. 이 옵션은 자신의 순서번호를 제공한 상위계층 프로토콜에 유용하다. 왜냐하면 ALL에 순서번호 기능을 중복적으로 부가할 필요가 없기 때문이다.

ⓑ번 옵션이 제공될 때는 데이타 무결성 서비스는 재연과 재순서에 의한 공격에 대한 보호를 제공한다. 이때는 송신측에서 AAL-SDU의 끝부분에 순서번호를 먼저 첨가한 후에 이 순서번호를 포함하는 AAL-SDU의 전체에 대한 서명을 다시 부가한다. 이것은 그림 7의 b)에 나타낸다. 순서번호는 연결 설정시나 데이타 무결성을 위한 세션키가 갱신될 때마다 0으로 설정된

다. 순서번호는 송신측에서 AAL-SDU를 송신할 때마다 증가하며 6 바이트의 수를 가진다. 수신측에서는 AAL-SDU 수신시 서명이 유효한지를 검증한다. 만약 서명이 유효하지 않으면 AAL-SDU를 폐기하고 서명이 유효시에는 순서번호가 유효한 지를 조사한다. 순서번호를 검사하는 방법은 다음과 같다.



a) Integrity without replay/reordering protection



b) Integrity with replay/reordering protection

<Figure 7> AAL-SDU Level Data Integrity.

첫번째로 앞서 받은 유효한 AAL-SDU가 있을 경우에는 현재 AAL-SDU의 순서번호가 가장 최근에 받은 유효한 AAL-SDU의 순서번호보다 클 경우에만 이 순서번호는 유효하다. 앞서 받은 유효한 AAL-SDU가 없는 경우는 현재 AAL-SDU의 순서번호는 유효하다고 채택한다. 수신측에서는 다음번에 받을 AAL-SDU의 순서번호를 조사하기 위해서 가장 최근의 유효한 순서번호를 기억하고 있어야 한다. ATM 보안 규격에서는 데이타 무결성 서비스를 제공하기 위해 기밀성 서비스와 마찬가지로 대칭키 알고리듬을 사용하도록 정의하고 있다.

④ 접근제어 서비스

접근제어 서비스는 ATM 연결 서비스와 자산들에 대한 접근을 허용할 것인가를 규정하며 VC 상에서 제공된다. 접근제어 서비스는 일반적으로 보호메세지 교환 및 네트워크 구성 파라메터들이 포함된 정보에 기초하여 연결설립 동안 수행된다. 접근제어는 서비스 요구에 대한 규칙들의 집합 응용이다. 이러한 규칙들은 실체와 같은 요구 개체의 속성들, 목적지 주소와 같은 참조된 파라메터들의 속성들, 시간과 같은 시스템 속성들 그리고 현재의 클라이언트 개체 그리고/또는 다른 클라이언트 개체에 의한 이전의 요구들의 기록에 의존할 수도 있다. 접근제어 규칙들은 위와 같은 모든 속성들에 의해 형성된 상태 공간상의 내용으로 간주될 수도 있다. 만약 내용이 만족되면 요구된 서비스가 수행되지만 만족되지 않으면 요구된 서비스는 수행되지 않는다.

사용자 평면의 접근제어는 ATM 내에 연결에 대한 접근이 보장되어야 하는지를 결정하기 위하여 접근제어 정보를 사용하는 메카니즘 뿐만 아니라 연결 설정동안에 사용된 접근제어 정보를 전송하는 메카니즘을 요구한다. 사용자 평면의 접근제어는 보호 라벨들, 송신지 또는 목적지 사용자 실체들, 시간, 서비스 종류, 상위 계층 프로토콜 필드 또는 연결설정 동안에 결정될 수 있는 다른 파라메터들에 의존할 수 있다. 사용자 평면의 접근제어는 종단-스위치, 스위치간과 같은 각 ATM 인터페이스에 대해 정의된다. 각 경우에 있어서 사용자 평면의 접근제어는 ATM 계층에서 제공된다.

2) 제어 평면에서의 보호서비스

제어 평면은 장치들로 하여금 가상 회선를 설정하는 것과 같은 어떤 목적을 이루기 위해서 망을 구성하는 메카니즘이다. 제어 평면의 메시지들은 망의 상태와 가용성에 영향을 미칠 수 있으므로 여기에 대한 보호가 매우 중요하다. 보호 규격에서는 재연/재순서화 보호를 가진 강한 암호학적 데이타 무결성을 제공할 수 있는 신호를 위한 메카니즘이 정의된다. 이 메카니즘은 요구에 대한 자원이 할당되기 전에 ATM 제어 평면 개체들이 송신자와 신호 메시지의 내용들을 검증할 수 있도록 한다.

제어 평면에서 제공되는 인증과 무결성 서비스는 ATM 신호 메시지와 메시지의 송신자를 결합하는 ATM 보호서비스이다. 이러한 결합을 생성함으로써 메시지 수신자는 메시지가 자신이 요구한 송신자로부터 온 것이지를 확실하게 검증할 수 있다. 이 서비스는 또한 스푸핑과 악의를 가진 수정 위협들을 방어할 수 있다.

3) 지원 서비스

지원서비스들은 통신 실체 사이에 직접적인 보안 서비스를 제공하는 것은 아니지만 앞서 기술된 서비스들에서 원하는 서비스를 제공하기 위해서 마련된 것으로 보안 메세지 교환 및 협상 프로토콜, 키 교환, 세션 키 갱신 그리고 Certification Infrastructure 서비스들이 있다.

(3) ATM에서의 키 갱신 프로토콜

초기자 또는 응답자가 새로운 세션 키를 사용하기를 원할 경우, 사용자 데이터 흐름 안에 키 갱신 OAM 셀들을 전송한다. 세션 키 갱신 프로토콜은 두 당사자간

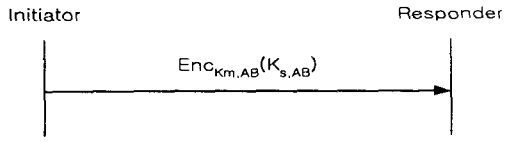
에 세션 키를 교환하는 과정(SKE : Session Key Exchange)과 새로운 세션 키를 변경(SKC : Session Key Changeover)하는 두 과정으로 이루어진다

1) 세션 키 교환과정(SKE)

송신지에서 목적지까지 다음에 사용할 세션 키를 안전하게 전송하기 위해서 SKE OAM 셀이 사용된다. 각각의 키 갱신은 암호학적 보호와 더불어 발신지와 목적지의 동기를 위해서 32bit 크기의 순차적인 키 번호를 사용한다. 다음에 사용할 세션 키는 안전한 호 설정동안에 얻어진 마스터 키를 사용하여 암호화된다. 세션 키를 위한 영역은 앞으로의 사용과 현재의 상황을 고려하여 256 bit의 크기가 할당되어 있다. 키 교환에 사용될 해쉬 함수는 초기 연결 설정시에 협상되어질 것이다. 여기에서는 RFC-1321의 MD5[11]방법을 사용하여 SKE를 정의하고자 한다. 이 Scheme에서는 공유된 마스터 키 $K_{m,AB}$의 크기는 특정한 크기로 제한되지 않는다. 새롭게 생성된 세션 키를 암호화하기 위한 과정은 다음과 같다.

$HalfMask1 = MD5(K_{m,AB}, KeyFill, A, KN_A, c1, K_{m,AB}, MD5Fill)$
;
if(세션 키 > 128bits)
$HalfMask2 = MD5(K_{m,AB}, KeyFill, A, KN_A, c2, K_{m,AB}, MD5Fill)$
;
else
$HalfMask2 = 0$;
$Mask = (HalfMask1, HalfMask2)$;
($c1 = 0000\ 0000\ hex, c2 = 5555\ AAAA\ hex$: 개시자
$c1 = 00FF\ FF00\ hex,\ c2 = 6666\ CCCC\ hex$: 응답자)
$Enc_{K_{m,AB}}(K_{s,AB}) = (ZeroPad, K_{s,AB}) \oplus Mask$;

위의 과정을 나타내면 그림 8와 같으며 세션 키 교환을 위한 OAM 셀 형식은 그림 9와 같다.



<Figure 8> Session key update in ATM Forum.

단계 1 : 송신측에서는

$Enc_{K_{m,AB}}(K_{s,AB}) = (ZeroPad, K_{s,AB}) \oplus Mask$

를 계산한 후 수신측으로 전송한다.

단계 2 : 수신측에서는

$K_{s,AB} = Enc_{K_{m,AB}}(K_{s,AB}) \oplus Mask$

를 복호화한다.

위와 같이 세션 키를 교환했을 경우 CRC에 의한 비트 에러 검사과정 외에는 키 확인 과정이 없기 때문에 전송도중 임의의 공격자에 의해 변경될 위험이 있다. 따라서 이러한 위협에 대한 암호학적인 대책이 필요하다.

GFC/VPI[11:8]	VPI[7:4]		1	ATM addr.
VPI[3:0]	VCI[15:12]		2	ATM addr
VCI[11:4]			3	ATM addr
VCI[3:0]	PTI	CLP	4	ATM addr, PT
HEC[7:0]			5	Header Ck
1 1 1 1	0 0 0 1		6	OAM+Ftype
Relative ID	0 0 0 1		7	RID, FID
	Reserved		8	BID, RES
Reserved			9	Reserved
Reserved			46-51	Reserved
0 0 0 0 0 0		CRC[9:8]	52	0,CRC
CRC-10[7:0]			53	CRC-10

<Figure 9> SKE OAM cell format.

2) 세션 키 변경과정(SKC)

세션 키 교환과정(SKE)이 끝난 후에 송신측에서는 수신측에서 변경된 키를 언제부터 사용할 지를 가리키기 위해 세션 키 변경과정(SKC)을 수행한다. 이는 그림 10과 같은 SKC OAM 셀을 전송함으로써 가능하다.

GFC/VPI[11:8]	VPI[7:4]		1	ATM addr.
VPI[3:0]	VCI[15:12]		2	ATM addr
VCI[11:4]			3	ATM addr
VCI[3:0]	PTI	CLP	4	ATM addr, PT
HEC[7:0]			5	Header Ck
1 1 1 1	0 0 1 0		6	OAM+F type
Relative ID	0 0 0 1		7	RID, FID
BANK ID	Reserved		8	BID, RES
Reserved			9	Reserved
Key Number			10-13	KN
State Vector(SV)			14-21	SV
Reserved			22-51	Reserved
0 0 0 0 0 0		CRC[9:8]	52	0,CRC
CRC-10[7:0]			53	CRC-10

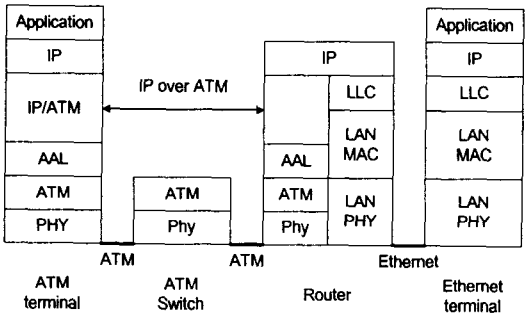
<Figure 10> SKC OAM cell format.

4. IP over ATM에서의 보호

ATM은 효과적인 대역폭 사용을 지원하고 고속의 멀티미디어 서비스에서 저속 데이타에 이르기까지 다양한 트래픽을 수용할 수 있어 차세대 초고속정보통신망으로 각광 받고 있다. 그러나 이러한 ATM 상에서 순수 ATM 응용 서비스의 개발은 아주 미미한 상태이다. 또한 ATM망이 공중망으로 구축되어야 하는 시점에서 IP 프로토콜을 사용하는 기존의 방대한 LAN 응용을 효율적으로 접속하여 기존의 서비스를 그대로 이용할 수 있어야 한다는 것은 필수적인 요인이라 하겠다. 이러한 요구에 따른 ATM LAN에 대한 표준화는 ATM 포럼과 IETF를 중심으로 이루어지고 있다.

기존 LAN과 ATM의 연동을 위해서 LAN의 특징인 공유 매체를 사용한 비연결성 서비스를 ATM망에서 어떻게 제공하게 할 것인가하는 문제가 야기된다. 이러한 문제를 위한 해결 방법으로 ATM 포럼에서는 LAN 에뮬레이션을 제안하였고 IETF에서는 Classical IP/ATM을 표준안으로 제시하고 있다. IP/ATM은 인터넷 프로토콜을 ATM상에서 사용하여 비연결형 연결을 지원하는 방식으로 상위의 네트워크 계층에서 인터넷 프로토콜만을 지원한다는 단점이 있지만 그 구현의 오버 헤드가 적으며 구현이 용이하다는 장점이 있다. 그림 11은 IP/ATM의 프로토콜 스택을 나타낸 것이다.

개방형 통신망을 위한 보호서비스로는 인증, 기밀성, 무결성, 접근제어 및 부인봉쇄 서비스를 들수 있으며[9] IP/ATM에서도 이러한 보호서비스들이 제공되어져야 한다. IP/ATM은 ATM을 하부구조로 하여 IP레벨의 패킷을 ATM망을 통해서 전송되어지므로 보호서비스의



<Figure 11> Protocol stack of IP/ATM.

적용 레벨이 모호하다. 보호서비스를 제공해 주기 위해서는 사전에 보호연관 설정이 필요하며 이는 연결 설정시에 이루어진다. IP/ATM에서의 연결은 ATM VCC로 이루어지므로 보호연관 설정이 VCC 설정시 이루어져야 한다. 따라서 보호연관 설정은 ATM 포럼에서 제시된 보호연관을 따를 수 있다.

IP/ATM은 하부 기반이 ATM으로 IP레벨의 패킷이 ATM 망을 통과하므로 기존의 ATM에서 보호서비스가 제공될 수 있지만 IP레벨의 라우터를 거치는 경우에 생기는 AAL SDU내의 IP 헤드의 문제로 그대로 적용하기가 힘든 부분이 존재한다. 본 장에서는 이러한 문제를 고려하여 IP/ATM에 적합한 보호서비스와 보호기술들을 기술한다.

① 인증 서비스

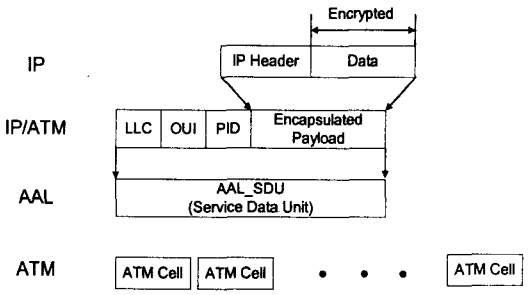
IP/ATM에서의 인증은 송신자와 수신자의 실체를 보장해준다. 실체의 인증으로 호스트는 접속의 초기에 다른 노드의 신원을 확인해야 하며 이는 보호연관 설정시에 같이 이루어진다. VCC 설정시에 이러한 인증과정을 제공하여 실체 인증이 이루어져야 한다. 동일 LIS(logocal IP subnet)내에서의 인증은 호스트 쌍방간의 VCC 설정 초기에 이루어 져야 하고 다른 LIS간에 존재하는 호스트간의 인증은 송신자와 라우터간의 VCC 설정시와 라우터와 수신자간의 VCC 설정시에 모두 이루어져야 한다.

인증을 위한 프로토콜은 비대칭키 방법과 대칭키 방법 중에 하나를 사용할 수 있다. 그러나 이러한 인증 프로토콜이 수행될 때 두 당사간에 먼저 이러한 알고리즘이 협상되어있어야 하므로 협상 과정이 먼저 수행된다. 이러한 협상과정은 순수 ATM에서의 그것과 동일하다. 비대칭키를 이용한 인증 방법으로는 RSA, DSA, Elliptic Curve/DSA 및 ESIGN과 같은 알고리즘을 사용할 수 있으며 대칭키를 이용한 방법으로 DES, DES40 및 FEAL 등의 알고리즘을 사용할 수 있다. 또한 인증시에는 해쉬함수가 필요하며 SHA나 MD5와 같은 함수를 사용할 수 있다.

② 기밀성 서비스

기밀성 서비스는 IP/ATM 상에서 사용자의 데이타가 비인가된 실체에게 노출되는 것을 막아주며 이를 위해 암호학적인 메카니즘이 사용된다. 데이타 기밀성 서비스는 IP계층의 payload에 대해서 적용된다. 기존의 ATM 망에서는 ATM 셀 레벨에서 암·복호가 이루어진다. 그러나 IP/ATM 구조에서는 동일 LIS내에 존재하는 호스트간의 통신과 다른 LIS간에 존재하는 호스트간의 통신을 모두 고려하여야 하므로 ATM 셀 레벨에서의 암·복호화는 라우터에서 해석되어야 할 IP 레벨 패킷의 헤드정보의 암호로 라우팅이 되지 않게 된다. 그러므로 IP/ATM 망에서는 그림 12와 같이 IP레벨에서의 암·복호가 필수적이다.

기밀성 서비스를 제공하기 위하여 사용되어질 수 있는 알고리즘은 다음과 같다. 이 때 암호 알고리즘의 선택 및 키 교환은 미리 이루어지는 보호연관 설정시에 협상으로 이루어진다. 사용자 측면의 기밀성을 위해서는 56비트의 유효키를 가지는 DES, 40비트의 유효키를 가지는 DES40, 112비트의 유효키를 가지는 Triple DES, 그리고 64비트의 키를 가지는 FEAL중에 하나가 사용되어질 수 있다.



<Figure 12> Confidentiality on IP/ATM.

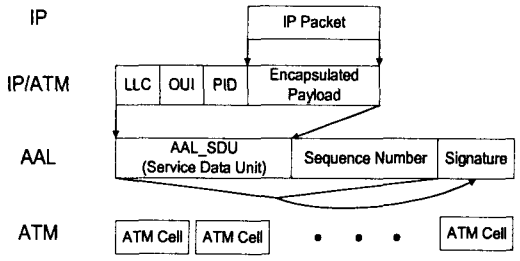
③ 데이타 무결성 서비스

IP/ATM에서의 데이타 무결성 서비스는 사용자의 데이타, 데이타의 순서 및 헤드가 변경되지 않았음을 보장해준다. 일반적으로는 암호학적 서명 방식으로 MAC(message authentication code)를 계산하여 이를 각 데이타 단위에 부가한다.

데이타 무결성은 AAL3/4와 AAL5 서비스 데이타 단위에 부가되는 암호학적인 점검값(해쉬 코드, MAC 등)에 의해 제공된다. 데이타 무결성 서비스를 AAL-SDU 레벨에서 지원되어야 하는데 그 이유는 전송 정보량이 지나치게 늘어나는 것을 막기 위함이다. 만약 ATM 계층에서 데이타 무결성 서비스를 제공하면 보호하고자 하는 단위 데이타마다 16바이트(128 bits) 길이의 서명값을 48바이트 길이를 갖는 ATM 셀 payload마다 첨부해야 하므로 33% 정도의 전송 오버헤드가 발생된다. 따라서 AAL-SDU단위로 무결성 서비스를 지원하는 것이 효율적이다. 데이타 무결성이 제공될 때는 송신측에서 MAC를 각 AAL-SDU의 끝 부분에 부가한다. 이때 재연과 재순서에 의한 공격에 대한 보호를 제공하기 위해 AAL-SDU의 끝부분에 순서번호를 먼저 첨가한 후에 이 순서번호를 포함하는 AAL-SDU의 전체에 대한 MAC를 부가한다. 그림 13은 IP/ATM에서의 무결성 서비스를 나타낸 것이다. 수신측에서는 AAL-SDU의 수신시 이 서명을 검증하여 만약 서명이 올바르지 않으면 이 AAL-SDU를 폐기한다.

④ 접근제어 서비스

접근제어는 서비스의 요구에 대한 규칙들의 집합이다. 이러한 규칙들은 식별자와 같은 서비스 요청 개체의 속성, 목적지 주소와 같은 참조된 파라미터들의 속성, 시스템의 속성 그리고 이전의 요구에 대한 기록 등에 의



<Figure 13> Integrity on IP/ATM.

해서 결정된다. IP/ATM에서의 접근제어는 연결 설정시에 사용되어지는 접근제어 정보들을 전송할 수 있는 메카니즘이 필요하다. IP/ATM에서의 접근제어는 송신 및 수신지의 식별자, 시간 정보, 서비스의 종류, 상위 계층의 프로토콜(IP) 및 다른 파라미터들과 같은 보호 레이블에 기초를 두고 제공될 수 있다.

⑤ 지원 서비스

IP/ATM에서 인증, 비밀 보장, 무결성 및 접근제어 등의 보호서비스를 제공하기 위해서는 이들 보호서비스에서 필요로 하는 기능들을 추가로 지원해주기 위한 서비스들이 필요하다. 보호연관 설정이나 키 교환 또는 갱신 및 안전한 메시지를 전송하기 위해 안전한 메시지 교환 프로토콜이 필요하며 이는 순수 ATM망에서의 안전한 메시지 교환 프로토콜과 마찬가지로 3방향 프로토콜과 2방향 프로토콜로 나눌 수 있다. 또한 키 교환을 위한 프로토콜과 키 갱신 프로토콜이 필요하며 공개키 확인 기능이 필요하다. 키 교환과 키 갱신 프로토콜은 ATM망에서의 그것과 동일하게 사용될 수 있으며 공개키 확인을 위해서는 X.509[10]을 이용하여 공개키 확인기능을 제공해 줄 수 있다.

5. 결 론

본 논문에서는 인터넷 기반인 IPv6에서의 보호체계 및 초고속정보통신망의 기반구조가 될 ATM 및 IP/ATM에서의 보호체계에 관하여 기술하였다. IPv6에서는 보호서비스를 제공하기 위하여 인증 헤드와 ESP를 사용하고 있다. 인증 헤드는 IP 데이타그램에 인증 및 데이타 무결성 서비스를 제공하며 ESP는 IP 데이타그램에 인증, 데이타 무결성 및 기밀성 서비스를 제공

한다. ATM에서의 보호체계는 사용자 평면과 제어 평면으로 분류하여 분석하였다. ATM의 사용자 평면에서는 인증, 데이타 무결성, 기밀성 및 접근제어 서비스가 제공되며 ATM의 제어 평면에서는 인증 및 데이타 무결성 서비스가 제공된다. IP/ATM은 하부 기반이 ATM으로 IP레벨의 패킷이 ATM 망을 통과하므로 기존의 ATM에서 보호서비스가 제공될 수 있지만 IP레벨의 라우터를 거치는 경우에 생기는 AAL SDU내의 IP 헤드의 문제로 그대로 적용하기가 힘든 부분이 존재한다. 따라서 이러한 문제를 고려하여 IP/ATM에 적합한 보호서비스와 보호기술들을 기술하였다.

참 고 문 헌

[1] W. Ford, Computer Communications Security, Prentice Hall, New Jersey, chap. 1-2, 1994.

[2] D. W. Davies and W. L. Price, Security for Computer Network, Wiley Interscience, New York, chap. 1, 1989.

[3] Network Working Group, IP Authentication Header, RFC 1826, Aug. 1995.

[4] Network Working Group, IP encapsulating Security Payload(ESP), RFC 1827, Aug. 1995.

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

[6] Thomas D. Tarman, ATM Security Specification, ATM Forum STR-SEC-01.01, ATM Forum/Security WG, Feb. 1998.

[7] LAN Emulation SWG Drafting Group, LAN Emulation of ATM: Draft Specification - Revision 2, ATM Forum/94-0035R2+, April, 1994.

[8] M. Laubach, Classical IP and ARP over ATM, RFC-1577, IETF, Jan. 1994.

[9] ISO/IEC 7498-2, Information Processing Systems - OSI Basic Reference Model - Part 2 : Security Architecture, 1989.

[10] ITU-T Recommendation X.509, The Directory : Authentication Framework, ITU-T, 1993.

[11] IETF Network Working Group, The MD5 Message Digest Algorithm, RFC 1321, April 1992.

박 영 호 (Young-Ho Park)

1989년 경북대학교 전자공학과 (공학사)
1991년 경북대학교 대학원 전자공학과 (공학석사)
1995년 경북대학교 대학원 전자공학과 (공학박사)
1996년 3월 ~ 현재 : 상주대학교 전자전기공학부 부교수
<관심분야> 정보보호, 컴퓨터통신, 이동통신 등