ATM 망을 위한 보호프로토콜 스택의 제안

[0]유형소* 이원철* 박영호** 유주열*** 정호석*** 문상재*
* 경북대학교 전자전기공학부
** 상주대학교 전자전기공학과
*** (주) 삼성 SDS

A Proposal of security protocol stack for ATM network

Hyung-So Yoo*, Won-Cheol Lee*, Young-Ho Park**
Ju-Yeol Yu*, Ho Suk Chung*** Sang-Jae Moon***
*** School of Electronics and Electrical Eng., Kyungpook National University**
**** Dept. of Electronics and Electrical Eng., Sangju National University**
***** Samsung SDS Co.**

요 약 문

본 논문에서는 ATM 망에서 정보보호 서비스를 제공하기 위해 기존의 ATM Forum에서의 보호 프로토콜 스택을 분석하여 새로운 보호프로토콜 스택을 제안한다. 제안된 보호프로토콜 스택은 ATM 계층에서 기밀성과 무결성 서비스를 제공하기 때문에 기존의 ATM 프로토콜 스택에 대한 변경을 최소화하며 또한 종단시스템간, 종단시스템-스위치간, 스위치간 보호 서비스를 제공할 수 있는 장점이 있다.

1. 서 론

컴퓨터와 통신기술의 발전과 함께 다양한 멀티미디어 응용 서비스가 출현하면서 통신망의 고속화 및 광대역화가 요구되게 되었고, 이러한 요구사항을 효율적으로 만족시켜 줄 수 있는 통신 프로토콜 기술로 ATM(asynchronous transfer mode)기술이 개발되었다[1]. 기존의 인터넷이나 패킷망에서와 마찬가지로 ATM 망을 통해 전송되는 정보 역시 정보의 누설, 전송중의 정보에 대한 조작, 정당한 네트워크 개체에 대한 위장 등과 같은 다양한 위협에 노출되고 있다. 이와 같은 위협에 대해 ATM 망을 보호하기 위해서는 정보보호 기술이 필요하다[2, 3].

ATM 망에서의 정보보호 필요성이 증가함에 따라 ATM Forum에서는 1995년 6월

에 Security Ad Hoc 그룹을 정식으로 설립하였고, 이는 1995년 12월에 독립적인 작업반으로 바뀌어 현재의 보안 작업반으로 개편되어 ATM 보안규격 개발작업을 진행하고 있다[4]. 현재 ATM Forum에서 개발되고 있는 보안규격에서는 기밀성과 무결성 서비스를 제공하기 위한 계층을 정의하고 있다. 기밀성 서비스는 ATM 계층에서 지원하도록 하고 있고, 무결성 서비스는 AAL(ATM adaptation layer)에서 지원하도록 되어 있다. ATM Forum에서 제시하고 있는 보호 프로토콜 스택에서는 기밀성과 무결성 서비스를 각각 다른 계층에서 제공하고 있다. 따라서, AAL과 ATM 계층에 대한 변경을 고려하여야 하므로 기존의 프로토콜 스택에 대한 많은 변경이 필요하며, 무결성 서비스의 경우 AAL 에서 제공되므로 종단간에만 제공될 수 밖에 없다는 단점이 있다.

본 논문에서는 이러한 ATM Forum에서의 문제점을 해결하기 위하여 새로운 보호프로토콜 스택을 제안하고 제안한 구조에 적합한 무결성 서비스를 제공하는 메카니즘을 소개한다. 제안한 보호프로토콜 스택은 통신정보의 기밀성과 무결성 서비스를 ATM 계층에서 제공함으로써 기존의 프로토콜 스택에 큰 변화를 주지 않고 한 계층내에서 통합된 보호 서비스를 제공할 수 있으며, 종단 시스템간, 스위치간, 그리고 종단 시스템-스위치간 보호 서비스를 제공할 수 있는 장점이 있다. ATM 계층에서 무결성 서비스를 제공하기 위한 알고리즘은 XOR MAC 구조를 가지며 이는 하드웨어로 구현시 병렬 처리가 가능해 지기 때문에 ATM망과 같은 고속의 네트워크 상에서 효율적으로 보호 서비스를 제공할 수 있는 장점이 있다[5].

2. ATM Forum에서의 보호 프로토콜 스택

ATM Forum에서의 보호 프로토콜 스택에서는 사용자 평면에서 기밀성과 무결성 서비스를 제공하기 위해서 제공되는 보호 서비스마다 다른 계층을 사용한다. 즉, 기밀성 서비스의 경우 ATM 계층에서 제공하도록 정의되어 있고, 무결성 서비스의 경우 AAL에서 제공하도록 되어 있다[4]. ATM Forum에서의 보호 프로토콜 스택은 그림 2.1과 같다.

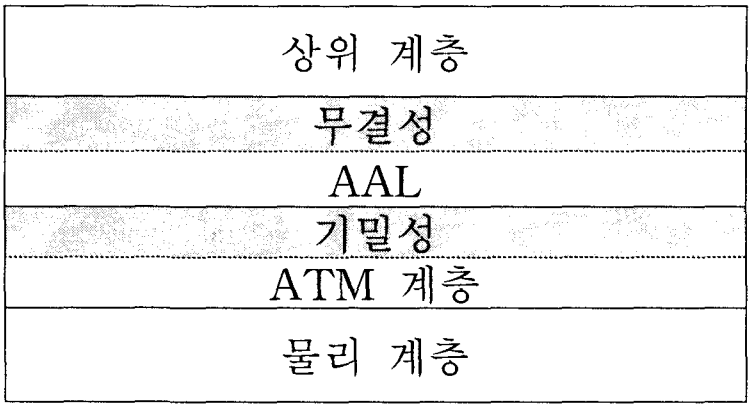

그림 2.1. ATM Forum에서의 보호 프로토콜 스택
Fig. 2.1. Security protocol stack in ATM Forum.

사용자 평면의 기밀성 서비스는 종단 시스템간, 스위치간의 두 가지 시나리오에 대해 정의되어 있으며, 종단 시스템간 기밀성 서비스, 스위치간 기밀성 서비스 모두 ATM 계층에서 제공하도록 되어 있다. ATM 계층에서 기밀성 서비스를 제공할 경우 암호화할 데이터의 길이가 48byte로 고정되어 있기 때문에 효율적인 암호화를 수행할 수 있다. 예를 들어 하나의 ATM 셀은 6개의 DES 블록으로 이루어져 있다. ATM Forum에서의 보호 규격에서는 대칭키 알고리즘을 사용하여 사용자 평면의 기밀성 서비스를 제공하도록 되어 있으며, 정의된 알고리즘으로는 56 bit 키를 가지는 DES[9], 40bit 키를 가지는 DES40[4], 112 bit 키를 가지는 3중 DES[10], 64 bit 키를 가지는 FEAL[11]이 있으며, 사용 가능한 모드로는 Cipher Block Chaining(CBC)[12], Counter 모드[12], Electronic codebook(ECB) 모드[12]가 있다. ATM 계층에서 암호화가 이루어지는 과정은 그림 2.2와 같다.

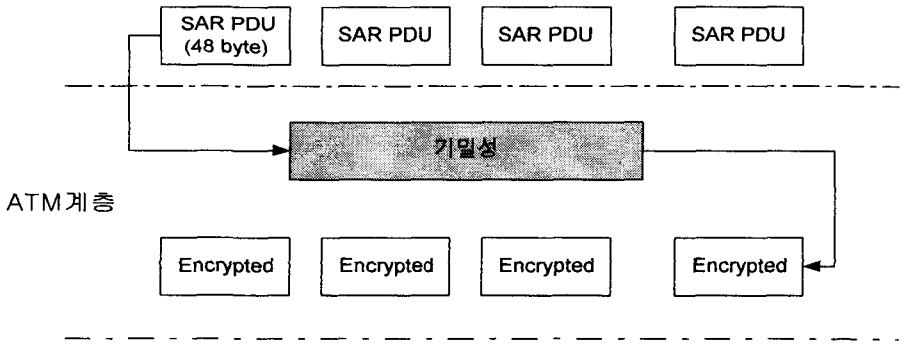

그림 2.2. ATM 계층에서의 기밀성 서비스
Fig. 2.2. Confidentiality at ATM layer.

ATM Forum에서의 데이터 무결성 메카니즘은 AAL-SDU(AAL-service data unit) 레벨에서 지원하도록 하고 있다. 즉, AAL3/4 와 AAL5 Common Part SDU에 암호학적 체크섬(해쉬 코드, 메시지 인증 코드(MAC : message authentication code), 메시지 다이제스트)을 덧붙여서 데이터 무결성을 제공한다. AAL 계층에서의 무결성은 재연/재순서화 공격을 방지할 수 있도록 순서 번호를 사용하는 것과 사용하지 않는 것 두 가지를 선택적으로 사용할 수 있다. ATM Forum에서 정의되어 있는 무결성 서비스를 제공하기 위한 알고리즘으로는HMAC-MD5[13,14],HMAC-SHA-1[13,15],HMAC-RIPEMD-160[13,16], DES/CBC MAC, DES40/CBC MAC, 3중 DES/CBC MAC, FEAL/CBC MAC이 있다. AAL에서 무결성 서비스를 제공하는 과정은 다음 그림 2.3과 같다.

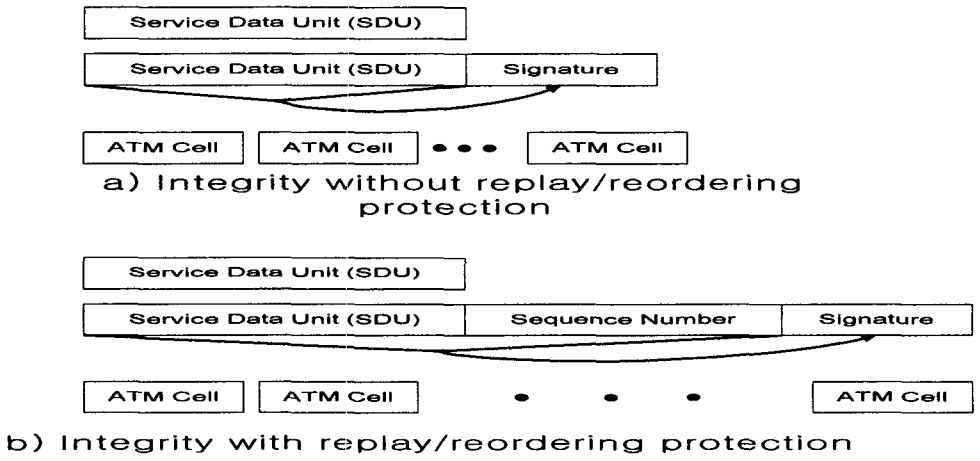

그림 2.3. AAL 에서의 무결성 서비스

Fig. 2.3. Integrity at AAL.

3. 제안된 보호프로토콜 스택

본 장에서는 ATM Forum에서의 보호 프로토콜 스택과 달리 기밀성과 무결성 서비스를 ATM 계층에서 제공할 수 있는 보호프로토콜 스택을 제안하고 제안된 보호프로토콜 스택에 적합한 무결성 서비스를 제공하는 메카니즘을 소개한다.

3.1 ATM 계층에서의 통합 보호프로토콜 스택

기밀성과 무결성 서비스를 각각 다른 계층에서 제공하게 되면, 각각의 보호 서비스가 제공되는 계층에 대한 수정이 필요하게 되고, 보호 서비스를 AAL에서 제공하

면 스위치에서는 AAL이 없기 때문에 중간 노드에서의 보호 서비스의 적용이 어렵다. 또한, ATM 계층은 모든 종류의 트래픽에 대해서 공통적으로 적용되는 반면, AAL은 트래픽의 종류에 따라 다른 형태로 적용된다. 따라서 ATM 계층에서 보호 서비스를 제공하는 것이 바람직하다. 제안한 보호프로토콜 스택은 그림 3.1과 같다.

그림 3.1 제안한 보호프로토콜 스택

Fig. 3.1. Proposed security protocol stack.

ATM 계층에서 기밀성 서비스를 제공할 경우 암호화할 데이터의 길이가 48byte로 고정되어 있기 때문에 효율적인 암호화를 수행할 수 있다[17]. ATM Forum에서의 보호 규격에서는 대칭키 알고리즘을 사용하여 사용자 평면의 기밀성 서비스를 제공하도록 되어 있으며, 정의된 알고리즘으로는 56 bit 키를 가지는 DES, 40bit 키를 가지는 DES40, 112 bit 키를 가지는 3중 DES, 64 bit 키를 가지는 FEAL이 있다. 사용 가능한 모드로는 Cipher Block Chaining(CBC), Counter 모드, Electronic codebook(ECB) 모드가 있다. 제안된 보호프로토콜 스택에서도 ATM Forum에서의 권고를 사용한다. ATM 계층에서 기밀성 서비스가 제공되는 과정은 그림 3.2와 같다.

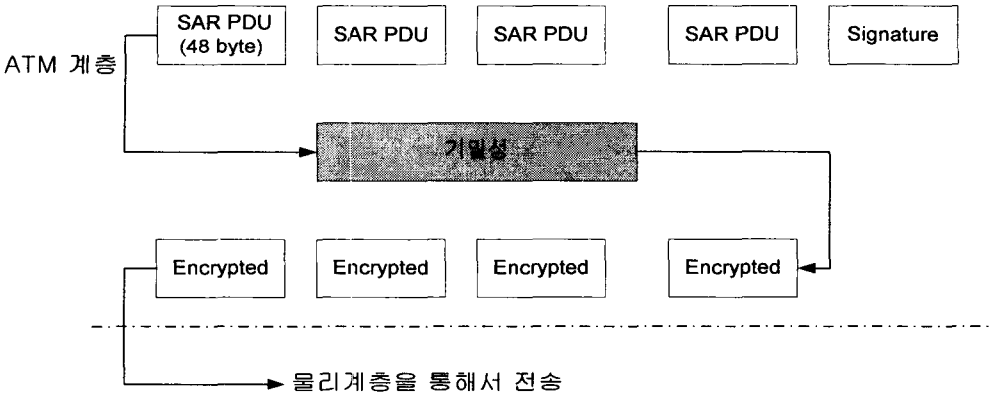

그림 3.2 ATM 계층에서의 기밀성 서비스
Fig. 3.2. Confidentiality at ATMlayer.

제안된 보호프로토콜 스택에서는 무결성 서비스 역시 ATM 계층에서 48바이트 단위로 제공된다. ATM Forum에서와 같이 CPCS-SDU 단위로 무결성 서비스를 제공할 경우 상위 계층에서의 데이터 형식이 무결성을 제공하기 위한 알고리즘에 적합한 형식이 되도록 데이터를 패딩시키는 작업이 필요하다. 하지만, ATM 계층에서 셀 단위로 무결성 서비스를 제공할 경우 데이터의 길이가 48byte로 고정되어 있기 때문에 효율적으로 알고리즘을 수행할 수 있다. ATM 계층에서 무결성 서비스를 제공하기 위해서 기존의 DES CBC 메카니즘을 사용하면 오버헤드가 많아지기 때문에 제안된 보호프로토콜 스택에서는 DES 기반의 XOR MAC 구조[5]를 가지는 메카니즘을 사용한다. DES기반의 XOR MAC을 사용하면 오버헤드를 줄일 수 있고, 병렬처리가 가능하기 때문에 하드웨어로 구현시 효율성이 뛰어나며, 특히 ATM 과 같은 고속의 네트워크에 있어서 뛰어난 성능을 가진다. ATM 계층에서 무결성 서비스가 제공되는 과정은 그림 3.3과 같다.

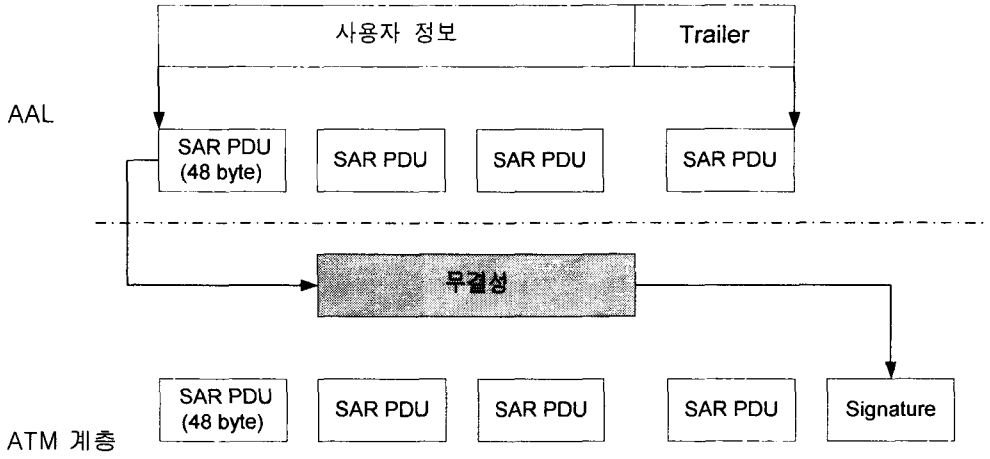

그림 3.3. AAL 에서의 무결성 서비스
Fig. 3.3. Integrity at AAL.

3.1.2 XOR MAC 메카니즘

XOR MAC을 사용하여 MAC을 생성하는 방법은 다음과 같다.

- Spec. of the scheme
  - F : 키 길이 k, 입력 길이 l, 출력 길이 L을 가지는 함수의 집합
  - C : 카운터
  - $a \in \{0,1\}^k$: 공유된 키
  - <i> : 블록 순서의 bit 열 표현

단계 1: 메시지 M(ATM Cell)을 블록단위로 encode한다.

- M=M[1]M[2]...M[n]

단계 2: 각 블록에 대하여 PRF(Pseudo Random Function)을 적용하여 PRF 상을 생성한다.

- 각 블록에 대하여 PRF 상을 생성한다.

  $F_a(0.C), F_a(\text{셀순서번호}.1.\langle 1\rangle.M[1]), \cdots, F_a(\text{셀순서번호}.1.\langle n\rangle.M[n])$

단계 3: PRF 상들을 XOR하여 MAC을 생성한다.

- $z_1 = F_a(0.C) \oplus F_a(\text{셀순서번호}.1.\langle 1\rangle.M[1]) \oplus \cdots \oplus F_a(\text{셀순서번호}.1.\langle n\rangle.M[n])$

단계 4: 각각의 ATM Cell들에 대한 결과값을 xor한다.

- MAC= $z_1 \oplus z_2 \oplus \cdots \oplus z_n$

단계 5: (C, MAC)이 메시지 M의 서명값이 된다.

XOR MAC을 사용하여 무결성 서비스를 제공할 경우 ATM 셀들에 대한 병렬 처리가 가능하기 때문에 고속 처리가 가능하다. 실제 계산량에서는 DES CBC MAC의 경우 하나의 셀을 처리하는데 6번의 DES계산이 필요한 반면 XOR MAC에서는 하나의 셀을 처리하는데 8번의 DES 계산이 필요하게 된다[5]. 하지만 DES CBC MAC의 경우 병렬 처리가 불가능하지만 XOR MAC의 경우에는 병렬 처리가 가능하다. 따라서 하드웨어로 구현할 경우 두 개 이상의 DES 하드웨어를 사용하면 하드웨어에 비례한 성능 향상을 가져올 수 있다. 오버헤드의 측면에서도 기존의 방식으로 ATM 계층에서 무결성 서비스를 제공할 경우 ATM 셀 단위마다 오버헤드가 발생했지만 XOR MAC을 사용하면 AAL-SDU 단위마다 오버헤드가 발생하기 때문에 향상된 결과를 얻을 수 있다.

4. 분석

제안된 보호프로토콜 스택은 ATM Forum에서의 보호 프로토콜 스택과 비교하면 다음과 같은 장점이 있다. 지원되는 보호서비스 측면에서는 ATM Forum에서와 같이 기밀성 서비스와 무결성 서비스를 모두 제공할 수 있으며, 보호 서비스가 제공되는 계층은 ATM Forum에서는 기밀성 서비스는 ATM 계층에서, 무결성 서비스는 AAL에서 제공되지만, 제안된 보호프로토콜 스택에서는 ATM 계층내에서 기밀성과 무결성 서비스가 제공된다. 또한, ATM Forum의 경우 기밀성 서비스는 ATM 계층에서 제공이 가능하지만, 무결성 서비스가 AAL 에서 제공되므로 단지 종단 시스템간에만 제공될 수 있는 반면, 제안된 보호프로토콜 스택에서는 기밀성과 무결성 서비스 모두 종단 시스템간, 스위치간, 종단 시스템-스위치간 보호 서비스를 제공할 수 있는 장점이 있다. 기존의 프로토콜 스택에 대한 변경 측면에서 살펴보면, ATM Forum 의 경우 무결성 서비스는 AAL, 기밀성 서비스는 ATM 계층에서 제공되므로 보호 서비스를 제공하기 위해서는 ATM 계층과 AAL 모두에 대한 변경이 필요하지만 제안된 보호프로토콜 스택에서는 ATM 계층에서의 변경만으로도 보호 서비스를 제공할 수 있다. 여러 가지 특성을 기반으로 하여 제안된 보호프로토콜 스택의 효율성을 분석하면 ATM 계층내에서 통합된 보호 서비스가 제공될 경우 ATM Forum의 보호 프로토콜 스택에 비하여 향상된 성능을 가져올 수 있다. 표 4.1은 ATM Forum의 보호 프로토콜 스택과 제안한 보호프로토콜 스택을 비교한 것이다.

표 4.1. ATM 보호 프로토콜 스택 분석

Table 4.1. Analysis of ATM security protocol stack

보호 프로토콜 스택 / 특 성		ATM Forum 보호 프로토콜 스택	제안된 보호프로토콜 스택
제공 서비스	기밀성	O	O
	무결성	O	O
제공되는 계층	기밀성	ATM Layer	ATM Layer
	무결성	AAL Layer	ATM Layer
보호범위	기밀성	End-to-end End-to-Sw Sw-to-Sw	End-to-end End-to-Sw Sw-to-Sw
	무결성	End-to-End	End-to-end End-to-Sw Sw-to-Sw
프로토콜 스택 변경		AAL, ATM계층	ATM 계층

또한 ATM 망에서 보호 서비스를 제공하기 위해서는 기존의 네트워크의 서비스 품질을 떨어뜨려서는 안된다. 현재까지의 상용 암호 칩의 처리 속도와 ATM 망과 같은 초고속망에서의 전송 속도를 살펴보면 표 4.2[18,19] 와 표 4.3과 같다. 표에서 알 수 있는 것처럼 암호 칩의 처리 속도가 망의 전송 속도를 따라가지 못한다. 따라서 암호 칩의 처리 속도와 망의 전송 속도를 일치시키기 위하여 병렬 처리의 필요성이 제기된다. 제안된 보호프로토콜 스택에서 무결성 서비스를 제공하기 위한 XOR MAC 메카니즘은 기존의 DES CBC 모드와 달리 병렬 처리가 가능하기 때문에 망의 전송 속도에 맞추어 보호 서비스를 제공할 수 있다.

표 4.2. 상용 DES chip
Table 4.2 Commercial DES chip

제조회사	칩	연도	클럭	처리속도
CE-Infosys	SuperCrypt CE99C003	1994	30MHz	160Mbps
Hi/fn	7711 Encryption processor	1998		225Mbps
VLSI Tech.	6868	1995	32MHz	512Mbps
Newbridge	CA95C68/18/09 PCC100	1993	33MHz	117Mbps
Semaphore Communications	Roadrunner284	?	40MHz	284Mbps

표 4.3 SDH와 SONET의 전송 속도 표준
Table 4.3 Standard of transmission rate in SDH and SONET

SDH	SONET	전송속도
STM-16	OC-48	2488.32Mbps
STM-4	OC-12	622.08Mbps
STM-1	OC-3	155.52Mbps

망의 전송속도를 따라가기 위해 사용되는 암호 칩의 개수에 따른 성능을 비교하면 다음 표 4.4와 같은 결과를 얻을 수 있다.

표 4.4. 칩 개수에 따른 성능 비교

Table 4.4. Comparision of performance depending on the number of chip

보호 프로토콜 스택 / Chip No.	ATM Forum 보호 프로토콜 스택	제안한 보호프로토콜 스택
1	1	1.165
2	0.5	0.665
3	0.5	0.5
4	0.5	0.33

표 4.4에서는 ATM Forum에서 제시한 방법으로 DES chip 한 개를 사용하여 ATM 셀 하나에 대한 기밀성과 무결성 서비스를 처리하는 시간을 1이라고 가정하였다. DES chip 이 한 개일 경우 제안한 보호프로토콜 스택에서의 처리 시간은 1.165가 된다. DES chip이 두 개일 경우 ATM Forum에서의 보호 프로토콜 스택에서는 처리 시간이 1/2로 줄어들게 되며, 제안한 보호프로토콜 스택에서는 0.665로 줄어들게 된다. 위의 표 4.4에서 알 수 있는 것처럼 실제 DES chip의 개수가 3개까지는 제안한 보호 프로토콜 스택보다 ATM Forum 에서의 방식이 동일하거나 더 나은 성능을 가질 수 있으나 이 경우에는 ATM 망의 처리속도를 따라가지 못한다. 따라서, ATM망의 처리 속도에 정합하기 위해서는 제안한 보호프로토콜 스택에서와 같이 DES chip을 늘려서 속도를 향상시킬 수 있어야 한다.

5. 결 론

본 논문에서는 ATM 망에서 효율적이고 안전한 데이터를 전송하기 위하여 ATM Forum에서의 보호 프로토콜 스택을 분석하였고, 이를 바탕으로 새로운 보호프로토콜 스택을 제안하였다. 제안된 보호프로토콜 스택에서는 기밀성과 무결성 서비스를 ATM 계층에서 통합적으로 제공할 수 있으므로 ATM 프로토콜 스택에 대한 변경을 최소화할 수 있으며, 종단 시스템간, 종단 시스템-스위치간, 스위치간 보호 서비스를 제공할 수 있다. 또한, 무결성을 제공하는 메카니즘으로 XOR MAC을 사용함으로써

효율적인 데이터 처리를 할 수 있다. 본 논문의 내용은 추후 ATM Forum 의 국제 표준화에 반영할 수 있는 것으로 여겨진다.

참 고 문 헌

[1] J.Y.Le Boudec, "The Asynchronous Transfer Mode : a turorial," *Computer Networks and ISDN Systems*, Vol. 24, pp. 279-309, 1992.

[2] Daniel Stevenson, Nathan Hillery, and Greg Byrd, Secure communication in ATM Networks, *Communications of the ACM*, Vol.38. No.2, pp.46-52. Feb. 1995.

[3] Robert H.Deng, Li Gong, Aurel A. Lazar, "Securing Data Transfer In Asynchronous Transfer Mode Networks," *IEEE GLOBECOM '95*, 1995.

[4] ATM Forum Technical Committee, *Phase I ATM Security Specification (Draft)*, ATM Forum/Security WG, Jul. 1998.

[5] M.Bellare, Roch Guerin, and P.Rogaway, "XOR MACs:New Methods for Message Authentication Using Finite Pseudorandom Functions," *Advances in Cryptology-Crypto 95 Proceedings, Lecture Notes in Computer Science* Vol. 963, D.Coppersmith ed., Springer-Verlag, 1995.

[6] ITU-T Recommendation I.432 (03/93) - *B-ISDN user-network interface - Physical layer specification*

[7] ITU-T Recommendation I.361 (11/95) - *B-ISDN ATM layer specification*

[8] ITU-T Recommendation I.363 (03/93) - *B-ISDN ATM adaptation layer (AAL) specification*

[9] Federal Information Processing Standards Publication 46-2(FIPS PUB 46-2), "*Data Encryption Standard(DES)*," Dec.30, 1993.

[10] X9.17. *Financial Institution Key Management*, April 1985.

[11] Miyaguchi, S., et. al., "Expansion of FEAL Cipher," *NTT Review*, Vol.2, No.6, pp.117-127, Nov. 1990.

[12] Federal Information Processing Standards Publication 81(FIPS PUB 81), "*DES Modes of Operation*," Dec. 1980.

[13] IETF Network Working Group, "*HMAC:Keyed-Hashing for Message Authentication*," RFC 2104, Feb., 1997.

[14] IETF Network Working Group, "*The MD5 Message Digest Algorithm*," RFC

1321, April 1992.

[15] Federal Information Processing Standards Publication 180-1(FIPS PUB 180-1), "*Secure Hash Standard,*" April 1995.

[16] RIPE Consortium : RIPE Integrity Primitives - Final Report of RACE Integrity Primitives Evaluation(R1040), *Lecture Notes in Computer Science,* vol.1007, Springer-Verlag, 1995.

[17] Rao J.Cherukuri, Mohammad Peyravian, Shyhtsun F.Wu, "A User Plane Security Protocol for ATM Networks," *Network Security'96*

[18] Bruce Schneier, *Applied Cryptography,* John Wiley & Sons, 1996

[19] http://www.hifn.com/ds-0001-01-7711Frm.htm