ATM 망을 위한 사용자 평면 시큐리티 서비스

이재근, 신상욱, 이경현
부경대학교 전자계산학과

User Plane Security Services for ATM networks

Jae-Keun Lee, Sang-Uk Shin, Kyung-Hyune Rhee
Dept. of Computer Science, PuKyong National University

요 약

본 논문에서는 ATM 네트워크 상에서의 발생 가능한 위협 요소들을 확인하고, 이러한 위협 요소들로부터 정보를 보호하기 위해 적용해야할 시큐리티 서비스들을 기술하고 ATM 사용자 평면(User Plane)에서의 시큐리티 서비스 모델을 제안한 후, RSA, Rabin, ElGamal, IDEA 등 다양한 암호 알고리즘들의 컴퓨터 시뮬레이션을 통해 알고리즘간의 성능을 비교 분석한다. 또한 ATM 네트워크에서 빈번한 키 갱신을 위해, 최근에 제안된 "Signcryption" 기법을 이용하여 기제안된 기법들보다 좀더 효율적인 세션 키 교환 기법을 제안한다.

1. 서론

Asynchronous Transfer Mode(ATM) 은 광대역 종합정보통신망(B-ISDN)구축의 핵심 기술로 이용되고 있으며 ATM Forum이 설립되면서 ATM 기술의 개발 및 보급이 더욱 활성화되었고 초고속 정보통신망을 통해 다양한 정보통신 서비스를 원활하게 이용할 수 있게 되었다. 이에 따라 ATM 네트워크를 통해 전송되는 정보에 대한 보호는 필수적인 요구사항이 되고 있다.

1997년에 ATM 포럼의 Security Working Group에 의해 Phase I Security Specification이 발표되었다[1]. 이 초안에서는 사용자 평면(User Plane)에서의 시큐리티 서비스와 제어 평면(Control Plane)에서의 인증 메커니즘을 포함하고 있고 제어 평면의 나머지 서비스와 관리 평면(Management Plane)의 시큐리티 서비스는 아직 연구 중이다. Deng 등[6]은 ATM 네트워크를 위한 시큐리티 요구 사항과 구조에 관해 논의했고, Chuang[4]은 안전한 ATM 네트워크의 도전과 시큐리티 메커니즘 위치, 시큐리티 요구 사항들을 기술했다. 또한 Stevenson 등[14]은 ATM 네트워크에서 시큐리티 위협 요소와 셀(cell) 암호화와 안전한 call setup 절차에 관해 기술했다. 서정욱, 김경수[5]는 ATM 물리 계층에서의 정보 보호에 관하여 연구하였다.

본 논문에서는 먼저 ATM 네트워크 상에서의 위협 요소들을 확인한 후, 이러한 위협 요소로부터 보호를 위해 적용해야 할 시큐리티 서비스들을 기술한 다음 ATM 포럼의 Security Working Group에 의해 제안된 시큐리티 서비스들을 근간으로 하여 ATM 시큐리티 서비스를 모델링한다. 제안된 모델에 다양한 암호 알고리즘을 적용하여 컴퓨터 시뮬레이션을 수행한 후 성능을 비교 분석한다.

2. ATM 망에서의 위협 요소와 시큐리티 서비스

ATM으로 연결된 망에서 전자우편, 화상회의와 같은 서비스가 증가함에 따라 통신 정보량도 늘고 특히 비밀을 요하는 민감한 정보도 증가 될 수밖에 없다. 이러한 정보들은 도청, 변조와 같은 위협의 대상이 될 수 있으므로 ATM 망에서의 시큐리티는 필수적이라 할 수 있다. ATM 네트워크에서 대표적인 위협 요소로

1) 도청(Eavesdropping)
2) 위장(Spoofing)
3) 서비스 거부(Denial of Service)

등이 있다[8,11]

이러한 위험 요소에 대해 ATM 네트워크를 보호하기 위해 다음의 시큐리티 서비스를 제공해야 한다.

1) 인증 서비스(Authentication Service)
2) 기밀성(Confidentiality Service)
3) 무결성(Integrity Service)
4) 접근 제어(Access Control Service)
5) 부인봉쇄(Non-repudiation Service)

3. ATM 망을 위한 사용자 평면 시큐리티 서비스 모델링

본 논문에서는 ATM의 3개 평면 중에서 사용자 평면(User Plane)에서의 시큐리티 서비스만을 제안한다. 현재 ATM 포럼 시큐리티 작업 그룹에서도 사용자 평면에서의 시큐리티 서비스를 중점적으로 정의하고 있으면, 제어 평면에서는 신호 인증만을 정의하고 있으며, 나머지 시큐리티 문제와 관리 평면에서의 시큐리티에 관해서는 계속 연구 중이다.

사용자 평면 시큐리티 서비스는 가상 연결(virtual connection)로 전송되는 사용자 정보에 대한 보호를 제공한다. 사용자 평면에서는 인증(authentication), 키 교환(key exchange), 무결성(integrity), 기밀성(confidentiality), 접근 제어(access control) 서비스를 제공해야 한다. 그리고 추가적으로 시큐리티 옵션 협정(negotiation of security options)을 제공해야 한다. ATM 네트워크에서는 다양한 트래픽 계층이 존재하기 때문에, 다른 시큐리티 옵션을 제공하는 것이 중요하다[3,8,9].

(1) 초기 인증, 키 교환, 시큐리티 옵션 협정

인증은 연결 설정 상황에서 두 당사자들이 서로를 확인하도록 하는 서비스이다. 이 서비스는 키 교환과 같은 다른 시큐리티 서비스에 대해 빈번하게 요구되기 때문에 매우 중요하다. 인증과 키 교환, 시큐리티 협정은 동일한 프로토콜을 사용하여 한꺼번에 제공될 수 있다. ATM 포럼 Security Working Group에서는 VCC(Virtual Channel Connection) 또는 VPC(Virtual Path Connection)의 설정동안 사용되는 프로토콜을 정의했다. 제안된 프로토콜은 인증, 키 교환, 시큐리티 옵션 협정을 수행한다. ISO/IEC 9594-8과 ISO/IEC 11770-2에 근간한 이 프로토콜은 two flows 또는 three flows를 사용하여 상호 인증(mutual authentication)을 제공한다[1,9]. 인증은 대칭 또는 비대칭 암호 알고리즘을 사용하여 수행되고, 일방향 또는 양방향 키 교환을 제공한다.

(2) 시큐리티 메시지 교환 프로토콜

two-way와 three-way 시큐리티 메시지 교환 프로토콜에서, 한 사용자는 프로토콜의 "개시(Initiating)" 역할을, 다른 사용자는 "응답(responding)" 역할을 가정한다.

시큐리티 메시지 교환 프로토콜에서 비대칭 키 알고리즘을 사용할 때 각 인증 개체 A와 B는 공개키와 비밀키 쌍을 소유하고 있다고 가정한다. K_a는 암호화에 사용되면 A의 공개키를, 디지털 서명(digital signature)에 사용되면 A의 비밀키를 나타낸다. 유사하게 K_b는 B의 공개키와 비밀키를 나타낸다. 대칭키가 사용될 때는 인증 개체 A와 B가 비밀키를 공유한다고 가정한다.

키 교환 옵션은 두 당사자들이 무결성과 기밀성 서비스를 위해 사용할 키에 동의하는 서비스이다. 이 키들은 직접적으로 사용될 수도 있지만, 짧은 기간동안 사용할 세션 키(session key)를 암호화하기 위한 마스터 키(master key)로 사용된다. 키 교환은 two-way와 three-way 프로토콜에서 "ConfPar" 변수를 통해 달성된다. 이 변수는 대칭 키나 비대칭 키를 사용하여 암호화되어야 한다. 키 교환이 한번 확립되면, 그 후에는 세션 키 갱신(session keyupdate) 프로토콜을 사용하여 주기적으로 변경되어야 한다. 시큐리티 협정은 "SecNeg" 파라메터를 사용하여 수행된다. 이 서비스는 사용자들이 사용하기 원하는 암호 알고리즘이나 프로토콜을 선택할 수 있도록 하는 유연성을 제공하게 된다.

three-way 시큐리티 메시지 프로토콜에 인증과 키 교환이 포함되면, 프로토콜은 nonce-based 상호 인증을 사용한다(R_a, R_b). Cert_a와 Cert_b는 A와 B의 인증서(certificate)이다. 그림 1은 three-way 인증, 키 교환, 시큐리티 협정 절차를 나타낸다.

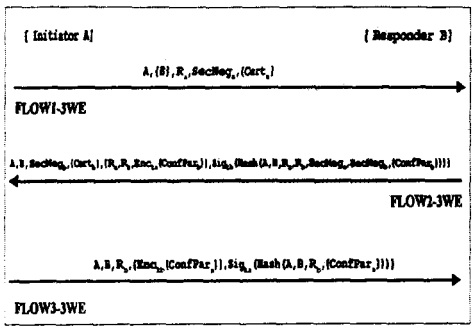

그림 1. 3방향 인증, 키 교환, 비밀협정 프로토콜

two-way 시큐리티 메시지 교환 프로토콜에서 개시자는 연결동안 어떤 시큐리티 서비스가 제공되는지를 지시하는 "SecOpt" 토큰을 사용한다. SecOpt는 연결을 위해 요구되는 시큐리티 서비스, 옵션, 파라메터들을 전송한다. 이것은 연결을 위해 제공되는 시큐리티 서비스들의 유형과 각 시큐리티 서비스에 사용되는 알고리즘과 동작 모드를 포함한다. 그림 2는 two-way 시큐리티 메시지 교환 프로토콜을 보여준다.

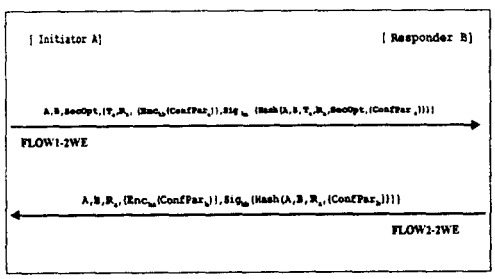

그림 2. 2방향 인증, 키 교환, 프로토콜

인증이나 키 교환이 포함되면, two-way 시큐리티 메시지 교환 프로토콜은 timestamp와 nonce-based 상호 인증을 사용한다(T_a, R_a).

(3) 무결성(Integrity)과 데이터 출처 인증(Data Origin Authentication)

무결성 서비스는 데이터 자체에 대한 변경여부 확인과 그 데이터를 누가 보냈는지 확인하는 것으로서 악의적인 불법수정이나 데이터 삽입 공격에 대한 보호를 하고 수신측이 잘못된 데이터를 수신하는 것을방지한다.[9,10].

(4) 기밀성(Confidentiality)

기밀성 서비스는 ATM 연결을 통해 전송되는 사용자 데이터가 비인가된 자에게로 유출되는 것을 막기 위한 암호학적 메커니즘을 제공하며 적절한 Key를 가진 수신자만이 데이터를 의미있는 것으로 복호화 할 수 있다는 것을 보장하기 위해서 암호화를 수행한다. 사용자 평면에서의 기밀성 서비스는 종단간, 그리고 스위치간 접속에서 정의된다.

데이터의 기밀성 서비스는 ATM 셀 레벨에서 서비스되며, 53 바이트 ATM 셀 중에서 5 바이트의 헤더(head)는 그대로 두고, 48 바이트의 payload 부분을 암호화시킨다. ATM 셀은 고정 길이(53-byte)로 되어 있기 때문에 빠른 속도로 동작하는 H/W의 기반 구현이 가능하고, 이것은 암호화 장비가 약 155Mb/s 속도로 동작하기 위해 특히 중요하다[9,10].

ATM 보안 규격(Security specification)에서는 DES, triple-DES, ECB, CBC, FEAL과 같은 대칭키 블록 암호화 알고리즘 모두 다 지원한다. 어떤 알고리즘이나 어떤 동작모드를 사용 할 것인지는 three-way security message 교환 프로토콜에서 연결 협정한다.

(5) 접근 제어(Access Control)

접근 제어 서비스는 연결 권한이 있는지를 결정하는 ATM security service이다. 접근 제어 메커니즘은 구현 제품에 따라 다르기 때문에, 접근 제어 장치에 의해서 요구되는 정보의 형태는 상호 운용이 가능하도록 표준화되어야 한다. 인증 프로토콜에 포함된 시큐리티 관련 정보에 추가로, ATM 보안 규격은 "label-based access control" 정보 요소를 정의한다[1,13]. 이것은 신뢰할 수 있는 호출 당사자가 요구되는 연결의 중요성을 구별하도록 한다. label이 허용 가능한 범위 내에 있으면, 그 연결 요구는 진행된다.

4. Signcryption을 이용한 세션 키 교환

연결이 설정될 때 무결성과 기밀성 서비스를 위한 키들은 협정되어야 한다. 그렇지만, 키들이 기밀성과 무결성 보호를 위해 사용될 때, 키들을 성공적으로 "cracking"하는 확률은 시간에 따라 증가한다. 그러한 공격을 방지하기 위해, 키들은 주기적으로 갱신되어야 한다[12]. 변경 빈도는 주어진 키로 변형되는 데이터 양에 의존한다. 이 목적을 위해 세션 키 갱신(session key update) 절차가 주기적인 키 변경을 지원하도록 정의되어야 한다. 이 절차는 짧은 기간 동안 사용되는 세션 키를 암호화하기 위해 사용되는 마스터 키(master key)를 사용한다. 마스터 키와 초기 세션 키는 초기 협정 단계동안 교환되지만 그 후의 세션 키들은 수신자가 그것들을 로드(load)하여 적절한 시간에 사용할 수 있도록 데이터 채널로 전송되어야 한다.

전송측과 수신측 사이에 세션 키를 교환할 때는 필수적으로 세션 키를 암호화하여 전송해야 하고 또한 인증과 무결성까지 제공되어야 한다. 이러한 세션 키 교환을 위한 방법으로 기존의 기법보다 좀더 효율적인 기법을 제안한다. 제안되는 기법에서는 최근에 Zheng에 의해 제안된 "signcryption" 기법을 적용함으로서 세션 키 교환을 위한 계산량과 전송량을 동시에 줄인다[15]. signcryption은 다음과 같이 수행된다.

[signcryption을 위한 파라메터]

(a) 모두에게 공개된 파라메터

p는 큰 소수, q는 $p-1$의 큰 소수인수

g는 1에서 $p-1$사이에서 임의로 선택된 위수

q mod p를 가진 정수

$hash$ 는 128 비트 이상의 출력을 가지는 일방향 해쉬 함수

KH 는 keyed 일방향 해쉬 함수

(E, D)는 비밀키 암호의 암호화, 복호화 알고리즘

(b) A의 키

x_a는 A의 비밀키, y_a는 A의 공개키 ($y_a = g^{x_a} \bmod p$)

(c) B의 키

x_b는 B의 비밀키, y_b는 B의 공개키 ($y_b = g^{x_b} \bmod p$)

[A에 의한 signcryption]

1. 1과 q사이에서 임의로 x를 선택, $k = hash(y_b^x \bmod p)$, k를 적당한 길이의 k_1과 k_2로 분할
2. $r = KH_{k_2}(m)$
3. $s = x - x_a \cdot r \bmod q$
4. $c = E_{k_1}(m)$
5. (c, r, s)를 B에게 전송

[B에 의한 unsigncryption]

1. r, s, q, p, y_a, x_b로부터 k를 복구
   ; $k = hash((g^s \cdot y_a^r)^{x_b} \bmod p)$
2. k를 k_1과 k_2로 분할
3. $m = D_{k_1}(c)$
4. $KH_{k_2}(m)$이 r과 같다면, m을 유효한 것으로 받아들인다.

이러한 signcryption을 이용하여 하나의 ATM 셀로 매우 안전하고 인증되는 키를 전송할 수 있다. 이를 위해 파라메터를 다음처럼 설정한다. p는 512 비트 이상, q는 160 비트, $KH(\cdot)$ 는 80 비트. 이와 같은 파라메터를 통해 최대 144비트까지의 키를 위조불가능하고 부인봉쇄 가능하게 전송하는 것이 가능하다.

그림 3 에 나타난 것처럼, ATM 셀은 5바이트의 헤더와 48 바이트의 payload로 구성된다. 그 중 48 바이트의 payload 부분에 인증되고 위조불가능한 키를 실어 전송한다. 전송되는 키 key는 최소 64 비트에서 최대 144 비트의 길이를 가진다. 이것은 DES의 경우에64 비트의 키가 필요하고, IDEA가 사용된다면 128 비트의 키가 필요하기 때문에 제안된 세션 키 교환 기법은 이들 모두에 적합하다(본 논문에서는 암호화를 위해 128 비트 키를 사용하는 IDEA를 적용한다). key가 144비트보다 적을 경우에는 나머지 부분은 timestamp로 사용할 수 있다. key는 $c = E_{k_1}(key)$로 암호화되어 전송된다.

$|p| \geq 512$, $|q| = 160$, $|KH(\cdot)| = 80$

$x \in_R [1, \cdots, q]$, $|k_1| \geq 64$, $|k_2| \geq 64$

$k_1 \| k_2 = hash(y_b^x \bmod p)$

$c = E_{k_1}(key)$, $r = KH_{k_2}(key)$

$s = (x - x_a \cdot r) \bmod q$

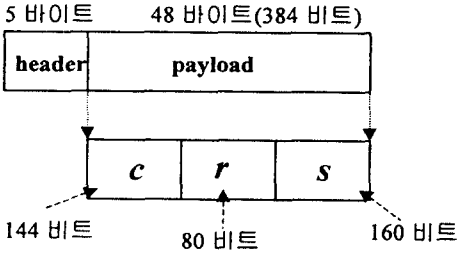

그림 3. ATM 셀로 Signcryption을 사용한 키 교환

위의 signcryption 기법을 적용했을 경우와 다른 기법들을 적용했을 때의 계산량과 전송량에 대한 비교가 표 1에 나타나 있다. 표 1에서 EXP는 모듈러 지수승(modulo exponentiation), MUL, DIV, ADD는 각각 모듈러 곱셈, 나눗셈, 덧셈을 나타내고, HASH는 일방향 또는 keyed 해쉬 함수 연산, ENC와 DEC는 비밀키 암호의 암호화 복호화를 나타낸다. 여기서는 RSA 기법에 기반한 경우와 (DSA + ElGamal) 기법에 기반한 경우 두 가지와 비교하였다. 각 알고리즘은 4.3.2 절에 설명되어 있다. 각 알고리즘이 같은 안전성을 가진다고 가정하고 파라메터는 RSA의 경우, $n_a = 512$, $n_b = 512$, DSA와 ElGamal의 경우, $|p| = 512$, $|q| = 160$ 을, 그리고 $|KH(\cdot)| = 80$ 을 고려한다[15].

표1을 보면, signcryption을 적용함으로서 다른 두 기법에 비해 계산량과 전송량이 상당히 줄어듬을 확인할 수 있고, 이는 아주 빠른 처리 속도를 요구하는 ATM의 경우에 signcryption의 사용은 다른 기법에 비해많은이점을 얻을 수 있다. 또한 안전하지만 인증되지 않는 RSA기반 키 교환 기법들에 비해, signcryption을 사용함으로서 위조 불가능성(unforgeability)과 부인 봉쇄(non-repudiation)까지 제공해 줄 수 있게된다[15].

표 1. Signcryption 기법과 다른 기법과의 계산량과 전송 비트 비교

기법	계산량	전송량 (bits)
RSA에 기반한 서명 후 암호화	EXP=2, HASH=1, ENC=1 [EXP=2, HASH=1, DEC=1]	1024 ($\|n_a\|$ + $\|n_b\|$)
DSA + ElGamal에 기반한 서명 후 암호화	EXP=3, MUL=1, DIV=1, ADD=1, HASH=1, ENC=1 [EXP=3, MUL=1, DIV=2, ADD=0, HASH=1, DEC=1]	832 ($2\|q\|$ + $\|p\|$)
signcryption	EXP=1, MUL=1, DIV=0, ADD=1, HASH=2, ENC=1 [EXP=2, MUL=3, DIV=0 ADD=0, HASH=2, DEC=1]	240 ($\|KH(\cdot)\|$ + $\|q\|$)

5. 컴퓨터 시뮬레이션 및 분석

이 장에서는 앞 절에서 기술한 시큐리티 프로토콜에 대하여 대칭키 암호 알고리즘으로 IDEA(International Data Encryption Algorithm), 해쉬 함수(hash function)로 SHA-1(Secure Hash Algorithm-1)을 사용하고, 디지털 서명 알고리즘으로 DSA(Digital Signature Algorithm), RSA(Ron Rivest, A.Shamir, Len Adelman), ElGamal, Rabin 알고리즘을 적용하여 프로토콜을 컴퓨터 시뮬레이션한 후 결과를 분석한다. 시뮬레이션 환경은 MicroSparc II 85MHz, Solaris 2.5, 32MB 시스템에서 gcc 컴파일러를 사용하였다.

4가지 알고리즘이 거의 유사한 안전성을 가지도록 하기 위해 RSA에서 모듈러 n, Rabin에서 모듈러 n, ElGamal 알고리즘에서 모듈러 p, 그리고 DSA에서 모듈러 p는 512비트로 선택하여 시뮬레이션하였다. 또한 DSA에서 q는 160 비트를 사용하였고, 각 서명 알고리즘에서 서명하기 전에 사용되는 해쉬 함수는 SHA-1을 적용하였다.

표 2. 4가지 서명 알고리즘의 성능

알고리즘	서명 시간 (seconds)	검증 시간 (seconds)
RSA	0.079	0.000
Rabin	0.090	0.000
ElGamal	0.040	0.270
DSA	0.040	0.050

표 3. 4 가지 서명 알고리즘에서 생성된 서명 길이

알고리즘	서명 길이 (bits)
RSA	512
Rabin	512
ElGamal	(512 + 511)
DSA	(160 + 160)

표 4. 프로토콜에서 총 수행 시간과 전송 비트

알고리즘	수행 시간 (seconds)	전송량 (bits)
RSA	0.158	1024
Rabin	0.180	1024
ElGamal	1.340	2046
DSA	0.180	640

시뮬레이션 결과를 보면, RSA와 Rabin의 서명 생성 시간이 DSA와 ElGamal 기법에 비해 많이 걸리는 것을 알 수 있다. 즉, 프로토콜 수행시 two-way에서는 첫 번째 흐름에서 initiator A의 서명 생성, three-way에서는 두 번째 흐름에서 responder B의 서명 생성 그리고 세 번째 흐름에서 initiator A의 서명 생성에 많은 계산량이 요구된다. DSA와 ElGamal 기법의 서명 생성 시간은 같게 나타난다. 검증 시간을 비교해보면, 서명 생성 시간과 반대로 DSA와 ElGamal 기법이 RSA와 Rabin 기법에 비해 상당히 많은 시간을 소비한다. 그리고 ElGamal 기법이 DSA에 비해서 많은 시간을 소비한다. 검증 시간이 많이 소비된다는 것은 two-way의 경우 첫 번째 흐름에서 responder B의 서명 검증과 두 번째 흐름에서 initiator A의 서명 검증, three-way에서 두 번째 흐름에서 initiator A의 서명 검증, 세 번째 흐름에서 responder B의 서명 검증에 많은 시간이 소비된다. 서명 생성과 검증 시간 모두를 고려하면, ElGamal이 가장 많은 시간이 걸리고 DSA의 경우는 서명 생성과 검증 시간이 거의 비슷한 시간을 소비하는 것으로 나타난다. 프로토콜 흐름에서 보면, two-way인 경우, responder B는 initiator A로부터의 서명을 검증하고 난 후 A에게 다시 자신의 서명을 생성하여 전송해야 하기 때문에 두 번째 흐름에서 responder B에 가장 많은 부하가 걸린다. three-way인 경우는 두 번째 흐름의 initiator A에서 가장 많은 계산량이 요구된다.

4가지 알고리즘의 서명 길이를 비교해보면, 같은 시큐리티를 가진다고 가정하면 DSA가 다른 기법에 비해 작은 서명 길이를 가지며 ElGamal 기법의 서

명이 가장 크다. 프로토콜에서 나머지 파라메터는 적용되는 서명 알고리즘에 무관하게 같은 길이를 가진다. 서명 길이가 길다는 것은 전송 시간에 영향을 미친다. 4가지 알고리즘이 모두 SHA-1의 160 비트 해쉬 결과를 입력으로 받아 서명을 생성하게 되는데 ElGamal의 경우 1023 비트의 서명을 생성하여 6배 이상 전송량이 증가하게 된다. DSA의 경우는 2배가 증가하게 된다.

표 4는 서명 생성과 검증만을 고려했을 때 4가지 알고리즘에서 프로토콜 수행을 위해 필요한 총 수행 시간과 전송 비트를 나타낸다. 서명 길이에서는 DSA 기법이, 수행 시간에서는 RSA 기법이 이점이 있고 ElGamal 기법이 가장 좋지 않음을 알 수 있다.

6. 결론

초고속 정보 통신망에서 ATM 사용으로 인해 ATM 네트워크에서 시큐리티 서비스는 필수적인 요구 사항이다. 본 논문에서는 ATM 네트워크에서 발생할 수 있는 여러 가지 위협 요소들(도청, 위장, 서비스 거부 등)을 확인하였고, 이러한 위협 요소에 대해 안전한 정보를 전달하기 위한 시큐리티 서비스를 기술하였다. 그리고 ATM 보안 규격에 기반하여 ATM의 세 가지 평면 중에서 사용자 평면(User Plane)에서의 시큐리티 서비스 모델을 제안하였다. 제안된 모델에 대칭 키 암호 알고리즘으로 IDEA, 해쉬 함수로 SHA-1을, 그리고 서명 알고리즘으로 RSA, Rabin, ElGamal, DSA 서명 알고리즘을 적용하여 컴퓨터로 시뮬레이션하여, 4 가지 서명 알고리즘의 성능을 수행 시간과 전송 비트 관점에서 비교 분석하였다. 또한 최근에 Zheng에 의해 제안된 "Signcryption" 기법을 적용하여 기 제안된 기법보다 좀더 효율적인 세션 키 교환 기법을 제안하였다.

향후 연구과제로는 ATM의 제어 평면과 관리 평면에서의 위협 요소 확인과 적용 가능한 시큐리티 서비스에 대해 연구할 계획이다.

[참 고 문 헌]

[1] ATM Forum/BTD-SECURITY-01.02, "Phase 1 ATM Security Specification(Draft)", Feb. 1997.

[2] M. Bacon, Security: a question of confidence, Telecommunications (int.ed.) (USA) Vol. 23, No. 11, pp51-52, Nov. 1989.

[3] Rao J. cherukuri , Mohammad Peyravian , Shyhtsun F.Wu, "A User Plane Security Protocol for ATM Networks", October 9. 1996

[4] Shaw-Cheng Chuang: "Securing {ATM} Networks", 3rd{ACM} Conferrence on Computer and Communications Security, New Delhi, India, 1996, pp.19-30

[5] Chung-Wook Suh, Kyung-Soo Kim, "A Security in the ATM Physical Layer", 통신정보보호학회 논문지, 제7권, 제1호, 1997.

[6] R. H. Deng, Li Gong, Aurel A. Lazar, "Securing Data Transfer in Asynchronous Tranfer Mode Networks", Proceedings of GLOBECOM'95, Singapore, Nov, 1995, pp. 1198-1202

[7] Warwick Ford, *Computer Communications Security, Principles, Standard protocols and Techniques*, Prentice Hall, 1994

[8] Donglin Liang, "A Survey on ATM Security", http://www.cis.ohio-state.edu/~jain/cis788-97/atm_security/index.html

[9] M. Peyravian Thomas D. Tarman, "Asynchronous Transfer Mode Security", IEEE Network, May/June 1997

[10] M. Peyravian et al., "User Plane Data Integrity Mechanism", ATM Forum/96-1020, June. 1996

[11] L. Pierson, et al., "Threat-Asset Analysys for ATM" ATM Forum/96-0229, Feb. 1996.

[12] Schneier, Bruce, *Applied Cryptography Second Edition: protocols, algorithms, and source code in C*, John Wiley&Sons, 1996

[13] D. Schnackenberg, "A Proposed Label-Based Access Control information Element", ATM Forum/96-1020, June. 1996.

[14] D. Stevenson and N. Hillery and G. Byrd, "Secure communications in {ATM} networks", Communications of the ACM, Volume 38, No 2, pp 45--52, Feb, 1995.

[15] Yuliang Zheng, "Digital signcryption or how to achieve cost (signature&encryption) << cost(signature) + cost(encryption)", In Advances in Cryptology-CRYPTO'97,volume 1294 of Lecture Notes in Computer Science, pages 165-179, Berlin, New York, Tokyo, 1997. Springer-Verlag.