ATM 망에서의 보안서비스 적용과 성능 평가
(Performance Evaluation and Application of Security Services in ATM Networks)

이 지 은 † 채 기 준 ††
(Jieun Lee) (Kijoon Chae)

요 약 초고속 통신망에서의 정보 침해는 짧은 시간에 많은 데이타의 손실을 초래할 수 있기 때문에 정보보호의 필요성이 제기되고 있다. ATM 망에서의 정보보안을 위해 보안 서비스를 ATM 계층과 AAL 계층에 적용시킬 수도 있고, 이 계층들 사이에도 적용시킬 수 있으며 보안 계층을 따로 두어 보안 서비스를 하나의 계층에서 다양하고 투명하게 적용할 수 있다. 그러나 이러한 연구들의 결과가 이론에 그치고 있고, 실제로 암호 알고리즘 등의 보안 서비스를 적용한 망에서의 성능을 평가하는 부분에 대해서는 연구가 부족한 상황이다.

본 논문에서는 사용자 평면에서 데이타의 비밀성, 무결성, 데이타 원천 인증 등의 보안 서비스를 적용한 보안 계층을 구현하고, SDL이라는 모델링 툴을 이용하여 망에서의 메시지 전달 지연 시간 등을 측정한 후 그 성능을 비교·분석하였다. 모델링 하는 세 가지 종류의 망은 첫 번째는 보안 서비스가 적용되지 않은 ATM 망이고, 두 번째는 보안 계층이 CS 부계층과 SAR 부계층 사이에 삽입된 망이며, 세 번째는 보안 계층이 ATM 계층과 AAL 계층 사이에 삽입된 망이다.

Abstract It needs to provide information security in ATM network because the information hacking in high speed network causes a heavy data loss in relatively short time. The current methods providing information security in ATM network propose various solutions which apply security services to each layer according to ATM reference model. But most of those researches are not implemented practically and remains theoretical. In particular, performance evaluation in ATM network applying security services such as cryptography algorithm has not been dealt with seriously.

In this paper, the performance of ATM network including security services is evaluated by measuring message transfer delay time. The security services provide data confidentiality, integrity and data origin authentication in user plane. These security services are implemented using three block cryptography algorithms, a hash function and a random number generator. Moreover three kinds of modeling including optional security layer are performed by using SDL simulation tool. The first network environment of modelings is normal ATM network not providing any security services. The second is the ATM network in which a security layer between CS sublayer and SAR sublayer is inserted. The last is the ATM network in which a security layer between ATM layer and AAL layer is inserted.

1. 서 론

초고속 종합통신망의 핵심 기술인 ATM(Asynchronous Transfer Mode)은 최근 국내외적으로 보급이 확산되고 있는 실정이다. ATM 시스템의 구현은 데이타 정보뿐만 아니라 멀티미디어 정보와 같은 다양한 정보를 전달함과 더불어 고속으로 정보를 전달하게 하여, 컴퓨터 통신을 이용하려는 멀티미디어 수용자들의 기대에 부합하여 중요 기술로 자리를 잡았다. 그러나 인터넷을 이용하는 사용자들이 급격히 늘어남에 따라 해커나 크래커에 의한 정보 손실의 위험성이 점점 커지고 있어 이에 대한 보안이 시급한 실정이다. 특히, 해커나 크래

† 비 회 원 : LG전자 정보통신 단말연구소 연구원
jieunlee@lgic.co.kr
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
kjchae@ewha.ac.kr
논문접수 : 2000년 1월 14일
심사완료 : 2000년 9월 6일

커에 의한 초고속 정보통신망에서의 정보 침해는 짧은 시간에 많은 데이타의 손실을 초래할 수 있기 때문에 초고속 통신망에서의 정보보호는 다른 어느 시스템 보다 중요하고 보안을 제공하기 위한 필요성도 나날이 증가되고 있다.

ATM 망에서의 보안을 제공하기 위한 연구는 ATM 포럼에서 1995년 Security Ad Hoc 그룹을 설립하면서부터 본격적으로 시작되게 되었다. 현재 ATM 포럼을 중심으로 ATM 보안 규격[1]이 개발 작업 중에 있고. 그 외 Chuang[2], R.H. Deng[11], D. Stevenson[5], Laurent[8], R. Shankaran[12] 등의 연구자들을 포함하여 여러 그룹들이 다양한 해결책을 고안해 내고 있다. 이러한 연구들은 B-ISDN 모델을 참조하여 각 계층별로 암호 서비스를 적용시키는 쪽으로 진행되고 있지만, ATM 각 계층 별로 암호화 알고리즘을 적용시킨 결과에 대한 장단점 비교 및 분석과 체계적인 연구는 아직 진행되지 않고 있다. 따라서 ATM의 다양한 계층에서 ATM 포럼의 보안 규격에 정의된 사용자측면, 제어측면, 관리측면에서의 보안 서비스를 적용하여 구현하고, 또 새로운 계층을 만들어 장단점을 비교하여 ATM 망 보안을 위한 최상의 해결방안을 모색하는 작업이 필요하게 되었다.

ATM 망에서 보안 유지를 제공하는데 중요하게 고려되어져야 할 점은 먼저 ATM 구조를 분석해야 하는 것과 ATM 보안 서비스가 제공되어야 하는 범위를 구분하는 일이다[4]. 따라서 본 논문에서는 보안 서비스가 적용되지 않은 망과 보안 서비스가 구현된 보안 계층이 ATM 계층들 사이에 삽입될 때와 다양한 암호 알고리즘이 적용되었을 때의 망의 성능을 모델링 및 성능 분석 툴인 SDL(Specification and Description Language)툴을 이용하여 분석한다. 본 논문의 목적은 ATM 망에서의 사용자 데이타를 다양한 암호화 알고리즘을 사용하여, 이를 ATM 계층별로 적용시켜 망의 성능을 분석하려는데 있다. 보안 서비스를 적용하지 않은 망과 보안 서비스가 적용된 망과의 성능을 비교·분석하여 ATM 망에서 보안 서비스들이 연구되어야 할 방향을 제시한다. 적용할 보안 서비스들은 사용자 평면에서의 비밀성, 무결성, 데이타 원천 인증 서비스이다. 비밀성을 제공하기 위해서 IDEA, DES, SAFER 등의 블록 암호 알고리즘을 사용하며, 무결성과 데이타 원천 인증 서비스를 제공하기 위해서 RIPEMD-128 해쉬함수를 이용한다.

본 논문의 구성은 다음과 같다. 2장에서는 ATM 프로토콜 참조 모델의 정의를 알아보고, ATM 보안 위협 요소를 분석하여 이를 예방할 수 있는 보안 서비스들에 대해 설명한다. 그리고 ATM 계층별 보안 메커니즘에 대해 기술한다. 3장에서는 기존의 암호 메커니즘들을 고찰한다. 4장에서는 다양한 암호 알고리즘을 ATM 계층별로 적용한 망을 모델링하고 SDL 툴을 이용하여 망의 성능을 분석하며 마지막으로 5장에서는 본 논문의 연구결과와 향후 연구 계획에 대해서 기술한다.

2. 기존의 ATM 보안 메커니즘

2.1 ATM 프로토콜 참조 모델

ATM 프로토콜의 참조 모델은 ITU-T에 의해 개발된 표준안에 기초하고 있으며, 그림 1과 같다. 이 모델은 사용자 평면, 제어 평면, 관리자 평면과 같이 세 가지 평면으로 나뉘어져 있다. 사용자 평면은 사용자 정보의 전달을 담당하고, 제어 평면은 호 제어와 연결 제어 기능을 수행하고 호와 연결의 설정, 감시, 해제를 위한 신호 기능을 수행한다. 관리자 평면은 전체 시스템에 관련된 관리 기능과 모든 평면과의 협조 기능을 수행한다. 또한 그림 1에서 보는 것과 같이 ATM 프로토콜 참조 모델은 AAL (ATM Adaptation Layer), ATM 계층, 물리 계층으로도 나누어진다.

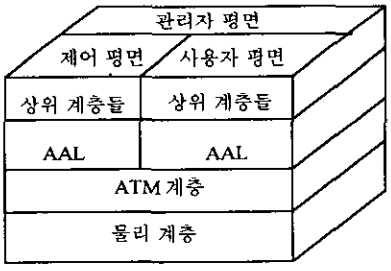

그림 1 ATM 프로토콜 참조 모델

2.2 ATM 보안 위협 요소

다른 망과 마찬가지로 ATM 망 역시 보안을 위협하는 많은 요소들로부터 위협을 받는다[4,11,21]. 전형적인 위협 요소로는 도청과 위장, 서비스 부인, VC(Virtual Channel) 훔치기, 트래픽 분석 등이 있는데, 이 중 VC 훔치기와 트래픽 분석은 오직 ATM 망에서만 나타나는 위협 요소이다.

- VC 훔치기 : 만약 ATM망 내의 두 스위치가 협상한다면, 이 때 침입자는 다른 사용자로부터 VC를 훔칠 수 있다. QoS(Quality of Service)를 보장해야 하는 ATM 망의 경우 침입자는 자신이 접근할 수 없는 더 상위의 채널을 얻을 수 있게 되고, 이럴 경우 이 상위의

채널을 사용하는 사용자는 피해를 입게 된다.

▪ 트래픽 분석 : 트래픽 분석[13]은 침입자가 VC의 규모, 타이밍, 통신자와 같은 자료를 분석/수집함으로써 정보는 얻는 것을 말한다. 암호화 과정이 자료의 규모와 타이밍에는 영향을 미치지 않으므로, 자료가 암호화되더라도 규모와 타이밍은 침입자에게 많은 정보를 누출시킨다. 발신자와 수신자에 대한 정보도 셀 헤더와 라우팅 테이블로부터 유추해낼 수 있다.

2.3 ATM 보안 서비스

ATM 보안 시스템을 만들기 위해서 먼저 해야하는 것은 ATM 상에서 안전한 통신을 하기 위한 요구사항을 규명하는 것이다[9]. ATM 보안 프레임워크 1.0[17]의 목적은 ATM 망상에서 제공되어지는 서비스의 요구사항을 밝히는 것이다. 보안 객체들을 위협하는 요소에 따라 많은 요구사항을 필요로 한다. 표 1은 보안 요구사항과 이 요구사항들을 만족시켜 줄 수 있는 보안 서비스간의 연관성을 보여주고 있다.

표 1 보안 요구사항과 보안 서비스들과의 매핑

Functional Security Requirement	*Security Services*
Verification of Identities	User Authentication Peer Entity Authentication Data Origin Authentication
Controlled Access and Authorization	Access Control
Protection of Confidentiality: Stored Data	Access Control
Protection of Confidentiality: Transferred Data	Confidentiality
Protection of Data Integrity: Stored Data	Access Control
Protection of Data Integrity: Transferred Data	Integrity
Strong Accountability	Non-repudiation
Activity Logging	Security Alarm,, Audit Trail and Recovery
Alarm Reporting	Security Alarm,, Audit Trail and Recovery
Audit	Security Alarm,, Audit Trail and Recovery
Security Recovery/Management of Security	-

2.4 ATM 계층별 보안 메커니즘

ATM 보안 시스템의 요구를 분석하는 것 외에 주요하게 생각해야 할 것은 ATM 망에서 보안 서비스를 구현하는 방법이다[4,19]. 즉, 보안 서비스를 ATM 프로토콜 참조 모델내의 어느 계층에서 구현하느냐에 따라 망의 성능이 달라질 수 있다. 본 논문에서 제공되는 보안 서비스는 사용자 평면에서의 비밀성과 무결성, 데이타 원천 인증 서비스이다. 이러한 서비스는 ATM 참조 모델에서 다른 계층에서 구현될 수 있지만, 같은 계층에서 구현되는 것이 유리하다. 왜냐하면 기존의 프로토콜 스택에 대한 수정을 최소화시킬 수 있고, 보안 메커니즘들이 같은 암호화 요소를 공유할 수 있으며, 더불어 암호화 메커니즘을 위한 동기화 스킴을 간단히 구현할 수 있기 때문이다. 이론적으로, 보안 메커니즘은 다음과 같이 세 개의 주요 계층 사이나 내부에서 구현될 수 있다.

2.4.1 물리 계층 내부, 물리 계층과 ATM 계층 사이, ATM 계층 내부

보안 계층이 물리 계층 내에 있으면, ATM 셀의 전체 53 바이트를 모두 암호화한다. 이것은 트래픽 흐름의 비밀성 및 사용자 데이타의 비밀성을 완벽히 보장할 수 있게 된다. 또한 상위 계층에 완전히 투명하게 작동하게 되는 것이다. 그러나 여기에는 치명적인 단점이 있는데, 스위치가 헤더를 읽어야 셀을 스위칭할 수 있으므로 스위치마다 모든 셀을 복호화 하고 다시 암호화를 해야하는 부담을 갖게 되어 성능이 저하되고 사용자의 데이타를 노출시킬 수 있는 위험을 안게 되므로 큰 공중망에서는 부적절하다. 그리고 이 계층에서 무결성 체크를 한다면 새로운 데이타들이 늘어날 것이므로 부가적인 셀의 분할 요구가 생길 것이다.

Stevenson 방안[5]

연결마다 하나의 세션키로 ATM 셀들을 암호화하는 암호화 유닛(프락시)을 정의하여 여러 연결의 ATM 셀들을 각각 독립적으로 암호화하기 충분한 속도로 키가 스위칭 되어야 하는 문제를 연구하였다. 동기화 문제는 OAM 셀에 동기화 정보를 삽입함으로써 해결하였다.

Chuang 방안[2]

VC 연결마다 하나의 세션키를 가지고 ATM 계층에서 사용자 데이타를 암호화하는 크립토노드(Crypto-Node)라는 디바이스를 정의하였다. 동기화는 AAL 계층에서 수행되는데, 이는 다음 데이타 블록들을 복호화하는데 사용되어지는 새로운 키 번호들과 초기화 벡터들을 포함하는 AAL5 PDU 토큰들을 삽입함으로써 가능해진다. 그러나 암호화/복호화와 암호 동기화가 다른 계층에서 이루어지기 때문에 문제가 생길 수도 있다. 즉, 동기화 셀이 같은 가상 채널로 사용자 데이타와 같이 섞여서 전송된다면, AAL 계층에서 동기화 셀이 처리되는 동안 많은 사용자 데이타들이 낡은 암호화 정보를 이용하여 ATM 계층에서 복호화될 수 있는 문제가 발생할 수 있는 것이다.

ATM 포럼[1]

ATM 포럼의 규격안은 사용자 데이타의 비밀성, 무결성,을 보장하고 재순서/재수신 감지는 선택적으로 보

장한다. 데이타의 비밀성은 ATM 계층에서 수행되고, 무결성과 선택적 재순서/재수신 감지는 AAL 계층에서 AAL SDU를 암호화함으로써 이루어진다.

2.4.2 ATM 적응 계층 내부

53 바이트를 모두 암호화/복호화하는 데서 생기는 문제점은 스위치마다 복호화/재암호화를 해야하는 부가적인 작업이 생긴다는 점이다. 이를 해결하기 위한 방법은 5바이트 헤더를 붙이기 전에 48바이트 SAR PDU를 암호화하는 것이다. 보안 계층이 AAL 내부에 위치하게 되면 SAR 부계층과 CS 부계층 사이에 명확한 계층이 생기게 되고, 이 계층에서 SAR-PDU로 분할되기 전의 CS-PDU에 비밀성과 무결성 서비스를 적용하게 된다. 전형적인 무결성 체크는 16-32 바이트의 데이타를 증가시키고 이 증가된 데이타는 SAR 부계층이 분할 기능을 실행하기 전에 CS-PDU에 덧붙여진다.

이 방법의 문제점은 비록 데이타 비밀성은 제공되어지지만, 트래픽 흐름 비밀성은 제공되어지지 못한다는데 있다. 왜냐하면 ATM 계층에서 추가되는 5바이트의 헤더를 암호화하지 않고 그냥 전송하므로, 침입자가 데이타 흐름을 분석하여 침입할 수도 있기 때문이다.

Deng et al. 방안[11]

CS 부계층과 SAR 부계층 사이에 DPL(Data Protection Layer)이라는 새로운 계층을 추가하였다. Deng이 제안한 방안은 데이타의 비밀성과 무결성, 선택적 재순서 감지 서비스를 제공할 수 있다. DPL 계층에서의 DPL SDU는 연결 설정시 협상되었던 키와 DPL SDU의 암호화되지 않은 헤더에 있는 초기화 벡터에 의해서 독립적으로 암호화되고, 서명되므로 동기화가 불필요하다고 주장한다.

신효영 방안[20]

ATM 방식의 초고속 통신망에서 정보 보호를 위한 구조를 사용자 평면과 제어 평면으로 나누어 제시하였으며, 비밀성과 무결성을 제공하기 위하여 해쉬 함수를 이용한 암호 알고리즘을 제안하였다. 또 제어 평면에서의 정보 보호를 위하여 호 설정시 송·수신자의 신원을 확인하기 위한 인증 절차 및 키 분배 프로토콜을 제안하였다. 사용자 평면에서의 정보 보호를 위하여 ATM 통신 구조에서 AAL 계층의 CS와 SAR 사이에 ASP(ATM Security Protocol) 부계층을 두었으며, ASP 부계층을 위한 서비스 프리미티브 및 메시지 처리 절차 등을 정의하였다. ASP 부계층은 사용자 평면에 대한 데이타 비밀성, 데이타 무결성, 원천 인증 및 세션 키 변경 등의 기능을 제공한다.

2.4.3 AAL 계층과 ATM 계층 사이

ATM 계층과 AAL 계층 사이에 보안 계층을 두는 것은 보안 서비스가 고정된 크기를 갖는 SAR-PDU에 적용되는 것을 의미한다. 일반 암호 알고리즘은 데이타 증가를 유발시킬 수 있으나 피드백 체이닝 기술이나 스트림 암호 알고리즘을 사용하면 48바이트 셀이 데이타의 증가 없이 암호화되어 ATM 계층에서 5바이트 헤더를 덧붙이게 된다.

ATM 계층과 AAL 계층 사이에서 무결성을 체크하는 것은 부가적인 셀 분할을 요구한다. 일반적으로 무결성 체크는 ICV(Integrity Checksum Value)를 계산하여 데이타에 추가시킨다. 그리고 비밀성과 무결성을 제공하기 위해 Chaining 기술을 사용할 경우는 IV(Initial Vector)를 필요로 한다. 그러므로 새로이 추가된 ICV와 IV를 상대방에게 전달할 때, ICV는 메시지의 끝에 추가시키고 IV는 다음 메시지의 시작을 가리키는 부분에 삽입되어져야 한다. 마지막 SAR-PDU에 여유공간이 없을 경우가 있을 수 있으므로 새로운 SAR-PDU를 만들어 거기에 이 정보들을 넣는다. 예를 들어, 그림 2와 같이 5번 메시지의 끝에 5번 메시지를 계산한 ICV와 6번 메시지의 IV를 새로운 SAR-PDU에 넣어 두 메시지 사이에 삽입하면 된다. 그리고 새로이 삽입되는 SAR-PDU는 암호 동기화의 목적으로도 사용되어질 수도 있다. 암호 동기화는 네트워크를 통해 정보가 전달될 경우에 반드시 필요한 필수적인 요구사항이다. ICV와 IV를 SAR-PDU에 넣고 이것을 암호 동기화에 사용한다면, 암호 동기화를 위하여 새로이 추가되는 부분을 생략할 수 있으므로 오버헤드를 줄일 수 있을 것이다.

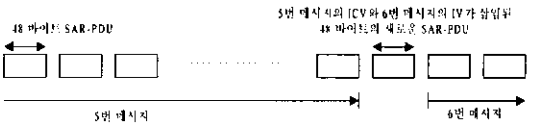

그림 2 새로운 SAR-PDU

Varadharajan 방안[12]

ATM과 AAL 계층사이에 보안 계층을 삽입하여 비밀성, 무결성, 데이타 원천 인증 서비스를 제공한다. 그리고 새로운 AAL PDU를 정의하여 암호화/복호화 디바이스 동기화에 독점적으로 사용한다. 다른 사용자 AAL PDU와의 혼잡을 막기 위해서 보안 AAL PDU 앞에 데이타 프레임의 끝을 나타내는 식별자로 구분된다. 그러나 보안 계층이 AAL PDU를 감지하기 위해서 AAL PDU의 세그먼트 타입 필드(Segment Type Field)를 분석해야 하기 때문에 AAL 계층 일부분을 처리해야 하는 단점을 가진다.

3. 기존의 암호 메커니즘 고찰

이 절에서는 비밀성 서비스를 제공해 주는 대칭형 암호 알고리즘, 무결성, 데이타 원천 인증 서비스를 제공해 주는 해쉬함수, 세션키 생성과 관련 있는 난수 발생기에 대해서 살펴본다.

3.1 대칭형 암호 알고리즘

본 논문에서 사용할 대칭형 암호 알고리즘은 암호화와 복호화할 때 사용되는 키가 같은 단일키 암호 알고리즘이다[18]. 그래서 단일키 암호 알고리즘을 개인키(private key) 알고리즘이라고도 한다. 비밀리에 정보를 교환하고자 하는 스테이션 A와 B는 비밀키를 공유하여 정보를 암호화하여 전송하거나 수신한 정보를 같은 키로 복호화한다. 키가 안전하게 유지되는 한 시스템은 승인된 송신자가 아닌 다른 사람에 의해 조작되지 않았다는 것을 증명하는 인증을 제공해야 한다.

3.1.1 DES (Data Encryption Standard)

DES는 IBM에서 Lucifer 시스템을 개선하여 개발한 암호 알고리즘으로, 1977년 미국 상무성의 국립 표준국(NBS, National Bureau of Standard)에서 미국 표준 암호 알고리즘으로 채택한 64비트 블록 암호 알고리즘이다. 64 비트의 키블록 중 56 비트가 암호화 및 복호화에 사용되고 나머지 8비트는 키블록의 패리티 검사용으로 사용된다[18].

본 논문에서는 64비트의 키를 이용하는 DES-CBC를 사용한다.

3.1.2 IDEA(International Data Encryption Algorithm)

IDEA는 스위스의 ETH Zurich에서 개발된 암호 알고리즘이다[3]. 이 알고리즘은 128 비트의 키를 사용하며, 일반적으로 안전도가 높다고 평가되며, 현재 많이 사용되는 알고리즘의 하나이다.

본 논문에서는 CBC 모드에서 IDEA 알고리즘이 사용되었다.

3.1.3 SAFER

SAFER는 IDEA 개발자 중 하나인 J. L. Massey가 개발하였다. SAFER 알고리즘은 8 비트 프로세서에서 조차 빠르게 실행되는 장점을 가지고 있다[10].

본 논문에서는 CBC 모드에서 SAFER 알고리즘이 사용되었다.

3.2 해쉬함수

ATM 망에서의 무결성 보장은 일반적으로 ICV를 계산하여 송·수신자간에 ICV를 비교한다. ICV는 MAC(Message Authentication Code)라고 하여 해쉬함수를 이용하여 계산되어진다. ATM 포럼에서는 SHA-1, MC5, RIPEMD-160 함수의 사용을 권장하고 있다[1]. 본 논문에서는 RIPEMD-128라는 해쉬함수를 사용한다.

3.3 난수 발생기(Random Number Generator)

일반적으로 암호 알고리즘은 침입자에 의해서 예측할 수 없는 강력한 난수들이 필요하다[3]. 난수들은 세션키를 만드는데 사용되어지며, 결과적으로 시스템의 성능에 큰 영향을 미친다.

본 논문에서는 SPRNG(Scalable Parallel Random Number Generators)[15]라는 알고리즘을 이용하여 의사 난수를 만든다.

4. 보안 서비스를 적용한 ATM 망의 모델링 및 성능평가

4.1 모델링 도구 : SDL

통신 시스템 개발용 명세 언어인 SDL(Specification and Description Language)은 시스템을 명세화하고 기술하는 표준화된 언어이다. 현재 ITU-T로 명칭이 바뀐 CCITT에 의해 개발되었으며 ITU-T Recommendation Z.100으로 표준화되었다. SDL은 시스템을 계층적으로 표현하기 위해 제안되어 여러 동시 작업과 상호 동작이 중요시되는 사건 중심의 실시간 시스템을 기술하는데 적합하다. 이에 따라 통신 시스템의 동작을 기술해 주는 사용자와 개발자들의 공통언어로 사용되고 실시간 시스템의 구조, 동작 기능 및 데이타를 표시할 수 있는 장점을 보유하며 시스템 분석과 설계에 적용이 가능하다. 프로토콜을 구현할 경우에는 다음과 같은 장점이 있다. 보다 편리하고 빠른 시간 안에 구현이 가능하며, 명확하게 구현할 수 있고, 명시한 사실이 바뀌더라도 간편하게 변경 내역을 수정할 수 있다. 계층 구조를 그래픽으로 표현함으로 C로 구현하는 것보다 쉽게 이해되고, 구현된 시스템에 대한 단계적인 분석이 가능하여 기능에 따른 모델링 및 검증이 용이하다[14].

4.2 망 모델

4.2.1 망모델 구조

그림 3은 ATM 망의 환경을 나타내는 간소화된 구조이다. 본 논문에서 실행할 모델링 망 환경은 보안 서비스가 적용되지 않은 망과 보안 서비스가 적용된 보안 계층을 포함하는 ATM 망이다. 각 ATM 망은 두 개의 종단 호스트와 두 종단 호스트 사이에 있는 ATM 백본으로 구성되며, 이 백본은 두 개의 ATM 스위치로 대표될 수 있다.

보안 서비스가 적용되지 않은 망에서는 사용자의 데이타가 AAL 계층을 통하여 48바이트 SAR-PDU 데이타 형식으로 ATM 계층으로 전달되고, ATM 계층을

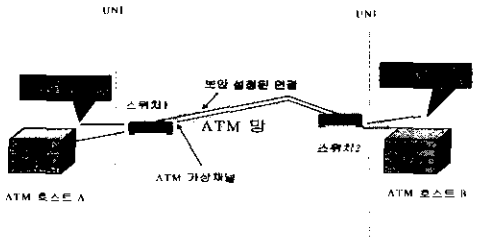

그림 3 보안 계층이 적용된 ATM 망

통하면 VPI/VCI를 포함한 5바이트 헤더를 추가하여 망으로 전달된다. 망에서는 VPI/VCI를 분석하여 목적지로 스위칭한다. 일단 목적지에 도착하면 ATM 계층에서 ATM 헤더를 제거하여 AAL 계층으로 전달하고, AAL에서는 재조립하여 사용자 계층으로 사용자 데이타를 전송한다. 이 과정이 보안 서비스가 제공되지 않은 망에서의 데이타 전달 절차이다.

보안 서비스를 적용하는 망은 보안 계층이 B-ISDN 참조 모델에서 어디에 삽입되냐에 따라 그 과정이 달라진다. 본 논문에서 보안 서비스를 제공할 보안 계층 모델을 두 종류로 제안한다. 첫째는 보안 계층을 AAL내의 CS 부계층과 SAR 부계층 사이에 삽입하는 것이고, 둘째는 보안 계층을 ATM 계층과 AAL 사이에 삽입하는 것이다. 보안 계층에서 하는 일은 데이타를 암호화하는 비밀성을 제공하고, 데이타 원천을 보증해 주는 데이타 원천 인증을 수행한다. 마지막으로 데이타 전송도중에 데이타의 변화가 있는지 체크하는 무결성을 제공한다.

4.2.2 암호 알고리즘의 적용

본 논문에서 사용하는 암호 알고리즘은 대칭키 알고리즘과 MAC을 만들기 위한 해쉬함수, 그리고 세션키를 만드는데 사용하는 의사난수함수 등이다. 암호 알고리즘으로는 IDEA, DES, SAFER 알고리즘을 사용하였고 해쉬함수로는 RIPEMD-128 알고리즘을 사용하였으며 세션키를 생성하는 프로그램은 SPRNG이다. IDEA 알고리즘의 경우 128비트 세션키를 사용하고, DES, SAFER 알고리즘은 64비트 세션키를 사용한다. 본 논문에서 모델링에 사용한 도구는 SDL 툴이며, 이 툴은 C의 코드를 연결하여 C의 함수들과 서로 호환할 수 있는 기능을 제공한다. 그리고 본 논문에서 다룬 암호화 알고리즘들은 모두 C로 구현되어 있으므로 실제 데이타들을 암호화함으로써 그 성능을 분석할 수 있었다. 자세한 내용은 3.1절을 참고로 한다.

4.3 성능 분석 결과

본 절에서는 앞의 망모델을 사용하여 수행한 모델링 결과를 분석한다. 본 논문에서는 SDL이라는 모델링 툴을 사용하여 수행되었다. 보안 서비스를 적용하는 곳은 ATM 망의 종단 호스트이다. ATM 망에서의 보안 서비스는 스위치와 종단 호스트에서 제공될 수 있다. 본 모델링은 보안 계층이 AAL 계층 내에 삽입되는 경우도 고려하므로 스위치보다는 종단 호스트에 적용하기로 한다. 모델링의 결과를 분석하기 전에 보안 서비스를 적용하지 않은 망을 CASE A라 가정하고, 보안 계층이 CS 부계층과 SAR 부계층에 삽입되는 경우는 CASE B라 가정하며 보안 계층이 ATM 계층과 AAL 계층 사이에 삽입되는 경우를 CASE C라 가정한다. 모델링의 분석 결과는 메시지의 전달 지연 시간으로 측정이 된다. 메시지 전달 지연 시간이란 메시지가 발생해서 모든 처리가 끝나고 사라질 때까지의 암호화 시간, 복호화 시간, 전송 시간, 대기 시간 등이 모두 포함된 시간을 의미한다. 암호화가 적용되지 않은 CASE A 경우에서의 메시지 전달 지연 시간의 측정은 송신자가 보내려는 사용자 데이타를 ATM 계층을 통해 망으로 전달하는 지연 시간을 계산하고, 암호화 서비스들이 적용된 CASE B, C의 경우에서의 메시지 전달 지연시간은 CASE A에서의 전달 지연 시간에 데이타의 비밀성, 무결성, 원천 인증 서비스를 모두 적용하여 망에서 소비한 전달 지연시간을 추가로 더하여 측정한다.

본 모델링은 Ultrasparc SUN OS 5.6 버전의 운영체제를 사용하고, CPU가 167MHz, RAM이 132M인 워크스테이션에서 실행되었다.

4.3.1 보안 서비스가 적용되지 않은 ATM 망(CASE A)

보안 서비스가 적용되지 않은 망을 SDL을 이용하여 모델링하였다. 송신자가 전송하는 데이타의 종류는 TELNET, HTTP, FTP 트래픽이며 각각의 크기는 64, 417, 1514 바이트이다.

ATM 망을 SDL로 모델링할 때 블록으로 망의 노드들을 표시할 수 있고, 프로세스로 각 계층을 정의할 수 있다. 그림 4는 메시지가 전달되는 ATM 망을 표현한 SDL의 시스템 블록도이고, 그림 5는 한 개의 64 바이트 TELNET 트래픽이 보안 서비스가 적용되지 않은 ATM 망에서 전달될 때의 SDL MSC(Message Sequence Chart)의 일부분이다. SDL MSC는 각 프로세스가 어떤 순서로 어떠한 신호를 서로 주고받는지 알기 쉽도록 보여준다.

그림 4에서처럼 USER 블록에서는 사용자의 데이타를 만들어 ATM_SRC 블록으로 전달하고, ATM_SRC 블록에서는 AAL 계층과 ATM 계층을 포함하여 각각의 기능을 수행하도록 하였으며 ATM_NW 블록으로

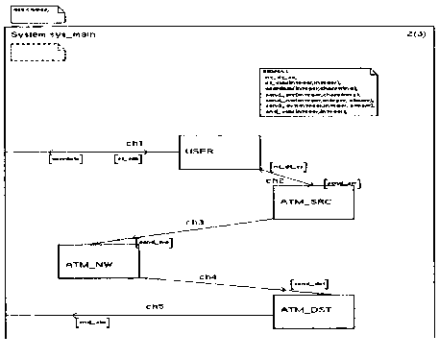

그림 4 SDL에서의 시스템 블록도(보안 서비스가 적용되지 않은 ATM 망)

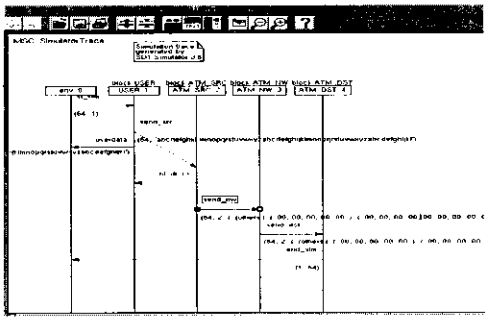

그림 5 송·수신간의 데이터 전달 과정(CASE A)

데이타를 전송하게 하였다. ATM_NW 블록은 데이타를 전송하는 ATM 망의 기능을 수행하며 ATM_DST는 목적지 호스트에서의 ATM 계층, AAL 계층의 역할을 수행한다. 이 블록들은 다음 두 모델링에서도 공통적으로 수행되는 블록들이다. 각 블록들은 채널을 통하여 신호를 보낼 수 있으며, 이 신호에는 다음 블록들에 전달되는 파라미터의 값들이 포함될 수 있어 블록간의 통신이 가능하도록 하였다.

CASE A에서 메시지 전달 지연 시간을 측정 할 때는 암호화 시간과 복호화 시간이 포함되지 않고 순수하게 데이타 전송시간과 각 계층에서의 대기 시간만이 포함된다(표2). 하나의 메시지를 전달하는 과정을 모델링

표 2 데이타 전달 지연 시간(CASE A)

데이타크기		TELNET (64바이트)	HTTP (417바이트)	FTP (1514바이트)
트래픽 수	100	7	10	22
	500	40	53	115
	1000	81	108	228
	2000	164	212	443

한 결과를 자세히 살펴보면 프로세스들의 처리 시간 중 소스와 목적지의 CS 계층에서 사용자 데이타와 통신스트림과의 변환 과정에서 처리되는 시간이 86%를 차지하였고, 메시지 전달 시간의 나머지 14%가 SAR에서 데이타를 분할/재조립하고 ATM 계층에서 헤더를 삽입/제거하며 망에서의 스위칭 시간, 그리고 큐에서의 대기 시간을 포함하는 것으로 나타났다.

4.3.2 보안 계층이 CS 부계층과 SAR 부계층 사이에 삽입된 경우(CASE B)

본 절에서는 보안 계층이 AAL 내의 CS 부계층과 SAR 부계층 사이에 삽입되는 망을 모델링하였다. ATM 소스 호스트에서의 보안 계층은 CS에서 받은 48 바이트로 분할하기 전의 데이타를 가지고 MAC 계산을 하여 원래의 데이타에 추가시키고, MAC이 추가된 데이타를 암호하화여 SAR 계층으로 내려보내고, 목적지에서의 보안 계층은 SAR 계층에서 재조립하여 전달한 MAC이 추가된 데이타를 복호화하여 다시 MAC 계산을 한 후 데이타 무결성과 데이타 원천 인증을 체크한다. 모델링에 사용되는 데이타는 CASE A에서 모델링한 TELNET, HTTP, FTP 트래픽들이다. 그리고 적용할 암호 알고리즘은 IDEA, DES, SAFER 블록 암호 알고리즘이고, RIPEMD-128 해쉬 알고리즘이 MAC을 계산하는데 사용되어진다. 이 알고리즘들은 각각 C로 구현되어 있고, SDL 언어와 연동하여 사용되어진다.

메시지 한 개를 전송할 때 걸리는 메시지 전달 지연 시간을 측정한 결과 전체 메시지 전달 지연 시간에서 보안 계층에서 처리되는 시간의 비율이 약 8.3% (IDEA), 8.1%(DES), 8.1%(SAFER) 미만을 차지하는 것을 볼 수 있었다. IDEA 알고리즘을 적용한 보안 계층에서의 처리 시간이 DES 알고리즘을 적용한 보안 계층의 처리 시간보다 0.2% 정도 더 걸리기는 했지만, SDL의 내부 시간 단위가 1초임을 고려해볼 때 세 가지의 암호 알고리즘을 이용해 하나의 메시지를 암호하는데 걸리는 시간들을 보고 암호 알고리즘의 성능을 평가한다는 것이 어렵다는 것을 알 수 있다. 따라서 메시지들의 크기와 전송횟수를 다양하게 모델링을 하여 세 알고리즘의 성능을 분석해야 한다.

전송할 메시지들의 수와 메시지의 길이를 다양하게 하여 모델링을 한 결과를 살펴보면 그림 6, 7, 8에서처럼 그 차이를 확실히 알 수 있게 한다. 보안 계층을 제외한 나머지 계층에서의 처리시간이 비슷한 상황을 고려할 때, 다음 그래프들의 차이는 보안 계층에서의 처리 시간의 차이임을 알 수 있다. 64 바이트 TELNET 트래픽을 100개 전송하여 얻은 메시지 전달 지연 시간보

다 1514 FTP 트래픽을 2000개 전송하여 얻은 메시지 전달 지연 시간을 보면 그 성능의 차이가 크게 나타난다. 비밀성 서비스를 지원하는 암호 알고리즘 성능의 차이는 한번에 암호화하는 데이타의 크기보다는 암호화 알고리즘을 적용하는 횟수에 의해 영향을 받는 것으로 밝혀졌다. 결국 CASE B에서 비밀성과 무결성, 데이타

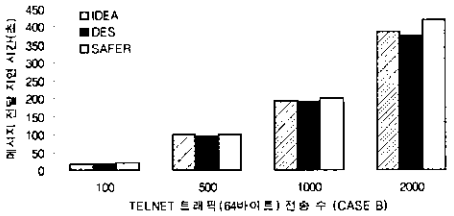

그림 6 TELNET 트래픽(64바이트)을 반복 발생시킬 때의 데이타 전달 시간 (CASE B)

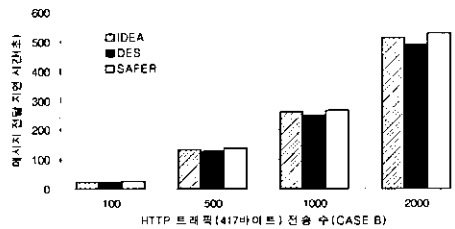

그림 7 HTTP 트래픽(417바이트)을 반복 발생시킬 때의 데이타 전달 시간 (CASE B)

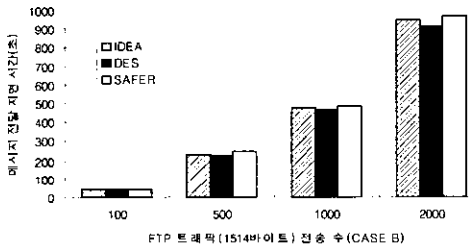

그림 8 FTP 트래픽(1514바이트)을 반복 발생시킬 때의 데이타 전달 시간 (CASE B)

인증 서비스를 제공하는 조건에서 그 성능을 보면 DES 암호 알고리즘을 적용한 것이 그 성능이 다른 두 알고리즘에 비해 높다는 것을 알 수 있다.

그림 9는 두 개의 IDEA 알고리즘을 이용하여 암호화 서비스를 적용한 모델링 결과이다. 본 논문에서 사용된 IDEA 알고리즘은 Finnish University and Research network FUNET에서 개발한 알고리즘[6]과 넷스케이프사가 개발한 암호 알고리즘인 SSL의 공개버전인 SSLeay 알고리즘[7]이다. CASE B에서 두 개의 알고리즘을 적용하여 FTP 트래픽을 모델링한 메시지 전달 지연 시간의 결과를 살펴보면 메시지의 크기와 트래픽 수에 비해 그 성능의 차이가 거의 드러나지 않았다.

4.3.3 보안 계층이 ATM 계층과 AAL 계층 사이에 삽입될 경우(CASE C)

본 절에서는 보안 계층이 ATM 계층과 AAL 계층 사

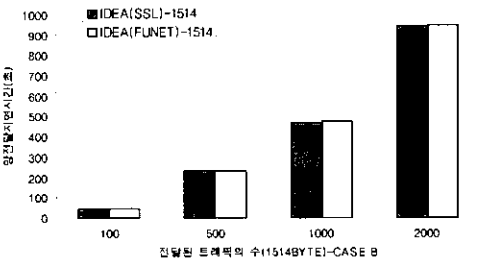

그림 9 두 IDEA 알고리즘의 비교(CASE B)

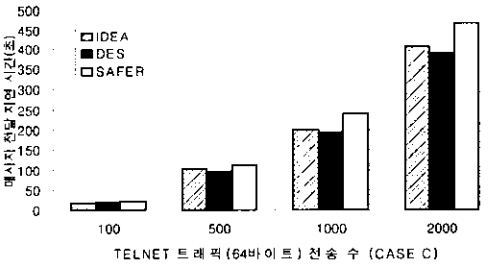

그림 10 TELNET 트래픽(64바이트)을 반복 발생시킬 때의 데이타 전달 시간 (CASE C)

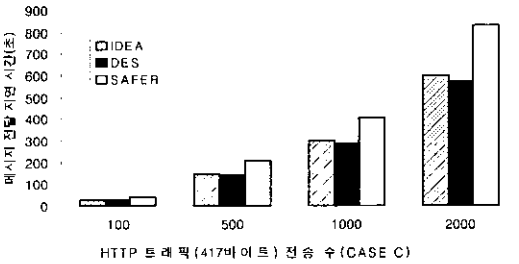

그림 11 HTTP 트래픽(417바이트)을 반복 발생시킬 때의 데이타 전달 시간 (CASE C)

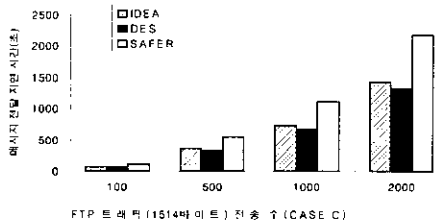

그림 12 FTP 트래픽(1514바이트)을 반복 발생시킬 때의 데이타 전달 시간 (CASE C)

이에 삽입될 경우를 모델링하였다. 보안 계층에서는 데이타의 비밀성, 무결성, 데이타 원천 인증 서비스가 적용된다. 각각은 4.3.2절에서처럼 세 가지의 암호화 알고리즘과 해쉬 함수를 적용하였다. 보안 계층에서는 이미 48 바이트로 분할된 SAR-PDU 스트림을 이용하여 MAC을 계산한 후 새로운 SAR-PDU에 삽입하고 이 셀들을 암호/복호화 과정을 거쳐 다음 계층으로 전달시킨다.

그림 10, 11, 12는 TELNET, HTTP, FTP 트래픽들이 IDEA, DES, SAFER 등의 암호 알고리즘을 적용한 보안 계층을 거쳐 ATM 망을 통과하는 경우로 데이타의 길이가 각각 64바이트, 417 바이트, 1514바이트일 때의 메시지 전달 지연 시간을 측정한 결과이다. 결과 값을 보면 트래픽의 길이가 짧고 트래픽의 발생 수가 작을수록 메시지 전달 지연 시간의 차이가 작고, 트래픽의 길이가 길고 트래픽의 발생 수가 많을수록 성능의 차이가 크게 드러남을 알 수 있다. 하나의 메시지를 전송할 때의 지연 시간을 측정해 보면 보안 계층에서 처리되는 시간의 비가 각각 45.3%, 42.9%, 50%으로 나타났다. CASE B에서는 하나의 메시지의 경우 전달 지연 시간의 차이가 거의 나지 않았지만, CASE C에서는 SAFER 암호 알고리즘을 적용한 경우의 보안 계층에서의 처리시간이 다른 두 알고리즘에 비해 길어지는 것으로 나타났다. 따라서 메시지의 크기와 전송횟수를 다양하게 적용할 경우 그 성능의 차이가 더 확실히 나타나게 된다. 결론적으로 보면 CASE B와 마찬가지로 모델링에 사용된 세 가지 암호 알고리즘 중 DES 알고리즘의 경우가 가장 성능이 좋았다. IDEA 알고리즘의 경우는 DES와 약간의 차이만 날 뿐이지만 SAFER 알고리즘의 경우는 데이타의 크기가 커질수록 성능의 저하가 큰 폭으로 늘어났다.

CASE C의 경우가 CASE B에 비해 처리시간의 차이가 큰 이유는 이미 48 바이트의 데이타로 나누어진 데이타를 다시 합쳐서 MAC을 계산하는데 처리하는 시간과 48 바이트의 SAR-PDU마다 암호/복호 알고리즘을 적용하여 계산하는 시간이 포함하는데서 찾을 수 있다.

그림 13은 두 개의 IDEA 알고리즘을 이용하여 암호화 서비스를 적용한 모델링 결과이다. 적용한 알고리즘은 CASE B와 같다. CASE C에서 두 개의 알고리즘을 적용하여 FTP 트래픽을 모델링한 메시지 전달 지연 시간의 결과를 살펴보면 CASE B에 비해 메시지의 크기와 트래픽수에 비해 그 성능의 차이가 더 확실히 드러났다. 이것은 앞에서 언급했듯이 암호화되는 메시지의 크기보다 암호 알고리즘이 호출되는 빈도수가 성능의 차이에 영향을 미치는데서 그 원인을 찾을 수 있다. CASE C에서는 비록 같은 알고리즘이라 하더라도 구현을 어떻게 했느냐에 따라 망에 미치는 영향이 CASE B에 비해 더 클 것으로 예상할 수 있다.

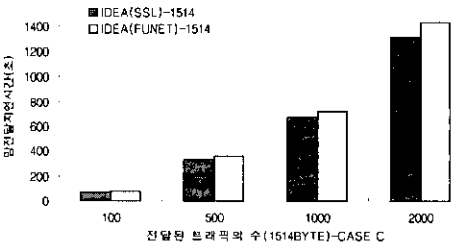

그림 13 두 IDEA 알고리즘의 비교(CASE C)

4.3.4 모델링의 결과 비교 및 분석

그림 14, 15, 16은 CASE A, B, C에서 다양한 길이를 가진 데이타들의 메시지 전달 지연 시간을 모델링한 결과이다. 데이타의 크기와 상관없이 보안 서비스를 적용하지 않은 망인 CASE A와 보안 서비스를 적용한 망인 CASE B, C 에서의 메시지 전달 지연 시간의 차이가 분명하게 나는 것을 알수 있다. CASE A의 경우보다 CASE B, C의 경우에서의 데이타 전달 지연 시간이 크다는 것은 보안 계층이 삽입될 경우에는 세션키를 만들어 데이타의 MAC을 계산하는 시간과 다시 이 데이타들을 암호화하는 시간이 추가되는 것을 고려해 볼 때 충분히 예측할 수 있는 사실이다. 그리고 보안 계층을 제외한 나머지 계층에서의 처리 시간은 거의 같다고 가정할 수 있다.

메시지의 크기가 작을 때 CASE B, C에서의 메시지 전달 지연 시간의 차이는 크게 드러나지 않지만, 전송되는 메시지의 크기가 크고 수가 많을수록 메시지 전달

지연 시간의 차이가 크게 드러남을 알 수 있다. 그림 16의 경우 하나의 메시지를 전달하는 시간을 분석해보면 CASE C의 경우가 CASE B에 비해 메시지 전달 지연 시간이 거의 두 배가 나온다. 그리고 CASE B에서 CS 계층에서의 처리 시간은 전체의 처리 시간의 80.5%를 차지하였고, 보안 계층에서의 처리 시간은 8.5%를 차지하는 결과를 보였지만, CASE C의 경우는 CS 계층에서의 처리 시간이 전체 처리 시간의 46.9%를 차지하고, 보안 계층이 45.3%, 나머지 계층에서의 처리 시간과 대기 시간이 7.8%를 차지하는 결과를 보였다. CASE C의 경우가 CASE B에 비해 보안 계층에서의 처리 시간이 크게 늘어났음을 알 수 있었다. 이것은 CASE B 경우

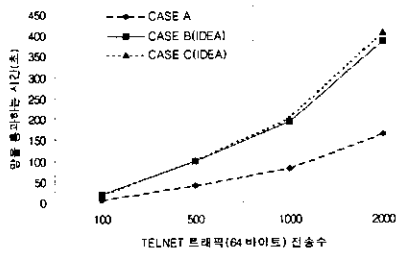

그림 14 CASE A,B,C에서의 TELNET(64바이트) 트래픽 전달 지연 시간

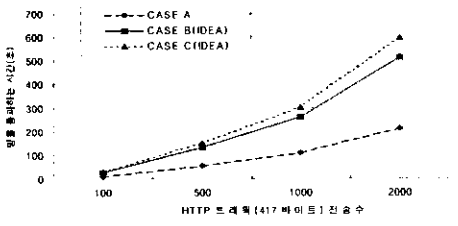

그림 15 CASE A, B, C에서의 HTTP(417바이트) 트래픽 전달 지연 시간

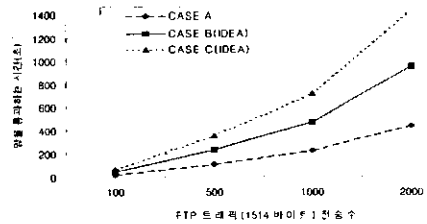

그림 16 CASE A,B,C에서의 FTP(1514바이트) 트래픽 전달 지연 시간

의 보안 계층에서 CS 부계층에서 받은 데이타를 그대로 이용하여 MAC 계산하고 CS PDU에 이 MAC 데이타에 추가시킨 뒤 암호 서비스를 적용하는데 비해, CASE C에서의 보안 계층은 이미 분할된 48바이트의 셀들 하나하나 암호 서비스를 적용하는데 걸리는 시간과 이미 분할된 데이타들로 MAC을 계산하기 위해 처리하는 시간을 포함하는데서 발생하는 결과로 볼 수 있다.

결론적으로 말하자면, 보안 계층이 CS 부계층과 SAR 부계층 사이에 삽입된 망(CASE B)의 경우 보통의 망에 비해 보안 계층에서의 처리시간이 크게 늘어나지 않았지만, 보안 계층이 ATM 계층과 AAL 계층사이에 삽입된 망(CASE C)에서의 데이타 전달시간이 보통 망에서의 데이타 전달 시간보다 데이타의 길이가 커질수록 그 차이가 늘어나는 것을 알 수 있었다. 즉, 메시지의 전달 지연 시간의 증가는 데이타의 길이가 길어질수록 증가하는 경향이 있지만, 암호 서비스를 적용시키는 빈도수에 따라 메시지 전달 지연 시간에 더 영향을 미치는 것으로 밝혀졌다. 이는 이미 분할된 데이타를 이용하여 MAC을 계산하는데 처리되는 시간이 증가되었고, 분할된 셀마다 암호/복호 알고리즘을 적용해야하는 부담이 늘어났기 때문으로 분석된다.

5. 결 론

ATM 망에서의 보안을 제공하기 위한 연구는 ATM 포럼을 중심으로 이루어져 왔다. 본 논문에서는 먼저 ATM 구조를 설명하였고, 보안 유지를 제공하기 위해 필요한 요구사항과 이를 만족시키는 보안 서비스들을 분석하였다. 그리고 이러한 보안 서비스를 ATM 구조에 적용시키는 여러 방안에 대한 장단점을 살펴보았다.

본 논문에서는 보안 서비스를 계층별로 적용한 ATM 망과 보안 서비스를 적용하지 않은 ATM 망의 성능을 비교·분석하여 ATM 망에서 보안 서비스들이 연구되어야 할 방향을 제시하였다. 모델링은 세 가지 종류의 망으로 나누어 구현되었다. 보안서비스가 적용되지 않은 망과 보안 서비스가 ATM의 각 계층별로 적용된 망에서의 성능을 비교한 결과를 살펴보면 메시지의 전달 지연 시간의 증가는 데이타의 길이가 길어질수록 그 차이가 증가하는 경향이 있지만, 암호 서비스를 적용시키는 빈도수에 따라 메시지 전달 지연 시간에 더 영향을 미치는 것으로 나타났다. 이는 이미 분할된 데이타를 이용하여 MAC을 계산하는데 처리되는 시간이 증가되었고, 분할된 셀마다 암호/복호 알고리즘을 적용하는 부담이 늘어났기 때문이다. 그리고 여러 암호 알고리즘을 사용

하여 성능을 비교한 결과를 봤을 때, 그 성능의 차이가 CASE B보다 CASE C에서 영향을 더 미친 것도 이런 이유에서 비롯한 것으로 볼 수 있다.

안전한 ATM 망을 제공하기 위해서 주의해야 하는 것 중 하나가 ATM의 고속의 스위칭 속도에 맞게 암호화 메커니즘을 적용하는 것이다. 그러나 현재까지 사용되는 암호 알고리즘으로는 ATM에서 요구하는 속도를 따라갈 수 없다고 알려져 있다. 따라서 ATM 망에서 제공해야하는 보안 서비스는 접근제어, 비밀성, 무결성, 인증 등과 같은 일반적인 보안 서비스와 ATM의 고속 셀 스위칭 속성으로 인하여 생기는 위협을 방지하는 보안 서비스를 제공해야 한다. 그리고 ATM 망에서는 특별히 보안 서비스 제공으로 인해 과도한 지연 시간의 방지, 셀 수준의 멀티플렉싱을 수용할 수 있는 세션키 변환과 빠른 키 변환이 요구되는 조건에서 적용할 수 있는 암호 알고리즘을 개발해야 한다.

참 고 문 헌

[1] "ATM Security Specification Version 1.0," ATM Forum/AF-SEC-0100.000,Feb, 1999.

[2] Chuang, "Securing ATM networks," Cambridge University ATM Document Collection 4(The Green Book), 1995. http://www.itr.unisa.edu.au/~dstowww/atm_security/.

[3] Cryptographic Algorithms, http://www.ssh.fi/tech/crypto/algorithms.html.

[4] D. Liang, "A Survey on ATM Security," http://www.cis.oio-state.edu/~jain/cis/788-97/atm_security/index.html.

[5] D. Stevenson, N. Hillery, G. Byrd, "Secure Communications in ATM Netwroks," Communications of the ACM, V.38 N.2, pp.46-52, 1995.

[6] ftp://ftp.ox.ac.uk/pub/crypto/SSL/SSLeay.

[7] ftp://ftp.funet.fi/pub/crypt/cryptography/symmetric/.

[8] M. Laurent et al, "Securing Communications over ATM networks," In Proceedings of IFIP SEC'97 Security Conference, Copenhagen, 1997. http://www.rennes.enst-bretagne.fr/~mlaurent/index-engl.html.

[9] M. Peyravian, E.V. Herreweghen, "ATM Security Scope and Requirements," ATM Forum/95-0579, 1995.

[10] Massey, J.L., "SAFER K-64: A Byte-Oriented Block Ciphering Algorithm," pp. 1-17 in Fast Software Encryption (Ed. R. Anderson), Proceedings of the Cambridge Security Workshop, Cambridge, U.K., Dec. 1993.

[11] R. Deng, et al, "Securing Data Transfer in Asynchronous Transfer Mode Networks," Proceedings of GLOBECOM '95, Singapore, pp.1198-1202, Nov. 1995,

[12] R. Shankaran, V. Varadharajan, "Secure Signaling and Access Control for ATM Networks," Proceedings of the Fourteenth Annual Computer Security Applications Conference, pp.212-222, 1998.

[13] R. Taylor, G. Findlow, "Asynchronous Transfer Mode: Security Issues," Proc. Austrailian Telecommunication Networks and Applications Conference, pp.161-166, 5-7 Dec. 1995.

[14] Rolv Braek, "SDL Basics," Computer Networks and ISDN Systems 28, pp.1585-1602, 1996.

[15] Scalable Paralle Random Number Generators Library for Parallel Monte Carlo Computations, http://www.ncsa.uiuc.edu/Apps/SPRNG.

[16] SDT Getting Started "Chapter 1. Introduction to Languages and Notations," SDL 매뉴얼.

[17] Security Working Group, "Security Framework for ATM Networks," ATM FORUM/97-0068, Feb. 1997.

[18] 김철, "암호학의 이해", 영풍문고, 1996.

[19] 신효영, 유황빈, "ATM 망에서의 정보보호에 관한 연구", 한국정보처리학회 춘계 학술발표논문집 제4권 제1호, pp.748-751, 1997.

[20] 신효영, "ATM 초고속 통신망에서의 정보 보호 모델과 암호 알고리즘에 관한 연구", 박사학위논문, 광운대학교, 1998.

[21] 한치문, "ATM Network Security 표준화 현황", 제 2회 정보통신 표준화 심포지엄(SSIT '99), pp.397-412, 1999.

이 지 은

1997년 이화여자대학교 컴퓨터학과 학사. 2000년 이화여자대학교 컴퓨터학과 석사. 2000년 1월 ~ 현재 LG 전자 정보통신 단말연구소 연구원. 관심분야는 무선 데이타통신, 무선 데이타에 대한 암호 처리.

채 기 준

정보과학회논문지 : 정보통신
재 27 권 제 2 호 참조