論文 98-23-1-18

ATM 방식의 고속 통신망에서 비밀성 보장을 위한 구조와 암호 알고리즘에 관한 연구

正會員 신 효 영*, 유 황 빈**

A study on the structure and encryption algorithm for securing ATM based network

Hyo-Young Shin*, Hwang-Bin Ryou** *Regular Members*

요 약

ATM 방식은 B-ISDN 망의 스위칭 기술로 채택되어 사용이 확산되고 있다. ATM망에서 제공되는 서비스가 다양해짐에 따라 병원의 진료기록, 기업간의 사업관련 정보, 일반인의 신용카드 번호 및 비밀번호와 같은 민감한 정보들의 전송이 증가될 것이다. 이러한 서비스를 제공할 때 전송되는 중요 정보자원에 대한 비밀을 보장하여 주는 것은 매우 중요한 문제로 대두되고 있다.

본 논문에서는 통신정보의 비밀성을 보장하기 위하여 ATM 망의 각 계층내에 정보보호 기능을 두었을 경우의 장, 단점을 분석한 후 정보보호 구조를 설계하였으며, 해쉬 함수를 이용한 암호 알고리즘을 제안 및 구현하였다. 제안된 암호 알고리즘은 안전성 면에서 DES에 뒤지지 않을 뿐만 아니라 속도면에서도 우수함을 보여 주었다.

ABSTRACT

The use of ATM is growing as it is chosen for the switching technology of B-ISDN. As various services of ATM is created, the transfer of sensitive information such as the medical record of patient, business information, and credit card number, will be increased . It is important that the network system guarantees confidentiality when these services are provided for users.

This paper analyzes the tradeoff of security function when it is located in each layer and designs the security structure for securing ATM network. And we propose an encryption algorithm using hash function. We prove that proposed algorithm is more fast as well as not less secure than DES.

*경성전문대학 사무자동화과
**광운대학교 전자계산학과
論文番號:97294-0823
接受日字:1997年 8月 23日

Ⅰ. 서 론

지난 수년간 고속 통신망의 기술과 표준화에 많은 발전이 있었으며, B-ISDN 망은 여러 부류의 응용 서비스와 사용자들을 지원하는 일반적인 망으로 자리 잡고 있다. B-ISDN 망은 품질이나 전송속도면에서 다양한 미래의 통신 서비스를 만족시킬 기술이라 할 수 있다. ATM(Asynchronous Transfer Mode) 방식은 B-ISDN을 구현할 스위칭 기술로 ITU에 의해 선정되어 근거리 통신망 뿐만 아니라 광역 통신망에서의 주요 정보 전송 기술로 사용되고 있다[1]. ATM을 기반으로하는 망에서 사용되는 서비스가 다양해짐에 따라 환자의 의료기록, 회사의 사업에 관련된 정보, 신용카드 번호와 같은 민감한 정보들의 전송이 증가될 것이다. 이러한 서비스를 제공할 때 사용자들에게 통신 정보의 비밀을 보장하여 주는 것은 중요한 일이다.

다른 통신망과 같이 ATM 망도 도청과 비인가된 접근에 취약하다. ATM 망에서의 정보보호 위협요소는 비밀성, 무결성, 인증, 액세스 제어의 네 가지로 분류 할 수 있다[2]. 비밀성은 통신 내용의 도청을 방지하는 것이며, 암호화를 통하여 해결할 수 있다. 무결성은 정보를 변경한 시도를 발견해내는 것이며, 해쉬 함수를 이용한 전자서명을 이용하여 만족시킬 수 있다. 인증은 송, 수신자의 신분을 상호 검증하는 것이며, 이를 위해 인증 프로토콜을 사용한다. 액세스 제어는 보안정책의 정의와 구현을 통하여 자원의 접근을 제한하는 것이다.

최근 ATM 망의 정보보호를 위한 연구가 활발히 진행되고 있으며, 이들은 암호 장치를 내부망에 방화벽과 같은 개념으로 운영하는 방법과[2, 4], ATM 교환기의 계층내에 정보보호 기능을 두는 방법[3]으로 구분된다. 본 논문에서는 주로 통신정보의 비밀성을 보장하기 위하여 ATM 망의 각 계층내에 정보보호 기능을 두었을 경우의 장, 단점을 분석한 후 정보보호 구조를 설계하였다. 또한, 비밀성을 보장하기 위하여 해쉬 함수를 이용한 암호 알고리즘을 제안하고, 이를 구현하였다.

Ⅱ. ATM 통신 방식의 구조

ATM 프로토콜 참조 모델은 ITU-T에 의해 개발된 표준안에 기초하고 있다. ATM은 그림 1과 같이 제어 평면, 사용자 평면, 관리자 평면의 세 가지로 나뉘며, 각각 AAL(ATM Adaptation Layer) 계층, ATM 계층, 물리계층으로 구성된다.

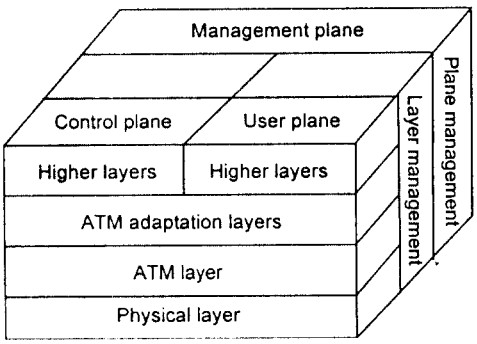

그림 1. ATM 구조
Fig. 1 The structure of ATM

AAL 계층은 상위 계층에서 요구되는 서비스들과 ATM 계층에 의해 사용되는 ATM 셀들사이의 연결 기능을 제공한다. AAL 계층은 출발지와 목적지의 시간관계, 비트율의 가변성, 연결모드에 따라 4개의 등급으로 분류된다.

ATM 계층은 AAL 계층과 물리계층 사이의 인터페이스를 제공한다. 이 계층은 AAL 계층으로부터 물리계층으로의 전달을 위해 중계 셀들을 처리하며, 단말 시스템에서의 사용을 위하여 물리계층으로부터 AAL 계층으로의 중계 셀들을 처리한다. ATM 계층은 종단 시스템에 위치하는 경우, 스트림 셀들을 물리계층으로부터 수신하여 새로운 데이터를 가진 셀들을 전송하며, 전송할 데이터가 없으면 빈 셀들을 전송한다. ATM 계층이 스위치내에 있는 경우, ATM 계층은 입력되는 셀들이 어디로 전달되어야 하는가를 결정하고, 관련된 연결 식별자를 재설정하여 셀들을 다음 링크로 전송한다. 또한 송, 수신 셀들에 대한 버퍼링을 수행하며, 셀손실 우선순위, 과잉 밀집 표시, 포괄적인 흐름제어와 같은 다양한 트래픽 관리 기능들을 처리한다.

물리계층은 사용중인 통신 매체상의 전송 및 수신을 위하여 데이터를 적절한 전자적, 광학적 파형으로 변, 복조하는 것이다. 물리계층은 또한 셀 윤곽설정

기능, HEC 생성과 처리, 성능 감시, 이 계층에서 사용되는 다른 전송 형식들의 payload을 매칭 등의 기능들을 제공한다.

Ⅲ. ATM 망을 위한 정보보호 구조

3.1 관련 연구

Stevenson[2] 등은 링크 레벨에 key agility 기능을 하드웨어로 구현하였으며, 손실된 셀을 단일한 암호 체인으로 한정시키기 위하여 동기 셀을 사용하였다. 이 방식은 링크 레벨에서 암호화가 수행되어 ATM LAN과 ATM WAN 사이에 보안 게이트웨이가 필요할 때 효과적일 수 있으나 스위치만을 보호하게되어 같은 스위치에 연결된 종단 시스템간의 공격이 가능한 단점이 있다.

Deng[3]의 연구에서 상호 시스템간의 인증, 보안 association의 설정, 암호키 분배와 같은 보안 관련 기능은 제어 면에서 수행되며, 사용자 트래픽의 보호는 사용자 면에 DPL(Data Protection Layer)을 정의함으로써 이루어진다. DPL은 AAL 계층의 SAR 부분에 위치하며, 제어 면에서의 자료전송은 DPL에 의해 보호되지 않는다. 이 방법은 AAL TYPE 1, 2, 3/4, 5의 각 형태별로의 구현이 필요한 단점이 있으며, time-stamp를 기반으로한 인증 프로토콜을 사용하여 동기화된 클럭이 유지되어야 한다.

Chuang[4]은 암호화 장치를 이용하여 ATM 계층에 비밀성 기능을 구현하였다. AAL5의 PDU 토큰을 이용하여 새로운 키와 초기화 벡터 등을 갱신하여 다음 블럭의 데이터를 암/복호화 하는데 이용하도록 하였다. 그러므로 키나 초기화 벡터가 변경되면, AAL 계층에서 ATM 계층으로 인터럽트가 발생하여 ATM 계층의 작업을 잠시 중단 시킨채 ATM 계층의 키와 초기화 벡터 변경 작업을 수행한다. 이 방법은 동기화를 시켜주는 계층과 암호화를 수행하는 계층이 다른 문제점이 있을뿐만 아니라 하위 계층이 상위 계층의 PDU 구조를 이해하고 있어야 하는 문제점이 있다.

3.2 제안구조

물리계층에 암호화 기능을 두는 경우, ATM 망으로 전송되는 모든 데이터들을 암호화하여 데이터 비밀성뿐만 아니라 트래픽 비밀성을 제공할 수 있다. 이는 헤더를 포함한 전체 메시지를 암호화하기 때문에 중간 스위칭 노드들에서 라우팅을 위해 복호화가 필요하게 되며, 이 과정에서 메시지 수정, 삽입, 순서 변경 등의 공격에 취약할 수 있다. 또한 전체 메시지를 암호화하므로써 암호화 과정을 채널의 속도와 정합시켜서 운영하는데 문제가 될 수 있다. 이러한 문제점들로 인하여 물리계층에 정보보호 기능을 두는 것은 적합하지 않다고 볼 수 있다.

ATM 계층에 암호화 기능을 두는 경우, 헤더 부분을 제외한 메시지를 암호화하게 됨으로 물리계층에서의 암호화보다 적은 비트율을 이용하게 된다. 그러나, ATM 계층은 헤더 정보가 생성되어 셀에 추가되는 곳이므로 암호화를 시키기 위해서는 부적절할 수 있다. 중간망의 노드들이 ATM 계층에서 셀 스위칭을 하므로 전체 망에서 암호 장비가 필요한 단점이 있다.

암호화 기능을 AAL 계층 이상에 두는 경우 보호 기능을 종단 사용자들에게까지 확장시킬 수 있으며, 하나의 ATM VC상에 멀티플렉스되는 여러 세션들에 대해 각기 다른 보호 기능을 둘 수 있다. 그러나 이 방법은 하위 계층에 보호기능을 두는 경우보다 비용이 많이들 수 있다. AAL 계층의 상위계층에는 현재 여러가지 전송 프로토콜과 응용프로그램들이 존재할 수 있으며, 이러한 모든 프로토콜상에 보호 서비스를 구현해야 함을 의미한다.

AAL 계층은 프로토콜 스택상의 상위계층에서 요구되는 기능들을 지원하며, 서비스 사용자들의 요구를 충족시키기 위하여 AAL 형태 1, 2, 3/4, 5 등의 프로토콜을 지원한다. AAL 계층은 CS와 SAR 부계층으로 구성되며, AAL 계층에 암호화 기능을 부여하는 방안에는 CS내, CS와 SAR 사이, SAR 내에 위치시키는 세 가지 방법이 있을 수 있다. 암호화 기능을 CS내에 두는 경우에는 AAL 형태별로 필요한 요구사항들을 모두 고려해주어야 하므로 작업이 번거로워진다. SAR는 CS PDU를 48 바이트로 분할 시키는 곳이며, 암호화로 인하여 데이터가 확장되는 경우의 처리가 어려워져 암호 알고리즘 선택에 대한 유연성이 줄어든다. CS와 SAR 사이에 두는 경우 암호화로 인하여 데이터가 확장되더라도 SAR로 데이터가 전송되기 이전이므로 확장으로 인한 영향을 받지 않으며, 정보보호와 관련된 추가의 기능들을 쉽게 구현 가능

하다.

(1) ASP 부계층의 위치

위에서 분석한 것과 같이 AAL 계층의 CS와 SAR 사이에 정보보호 기능을 두는 것이 가장 적합한 것으로 분석되어졌다. CS와 SAR 사이에 정보보호 기능을 위치시킴으로서 다음과 같은 장점을 가질 수 있다. ASP(ATM Security Protocol) 부계층은 CS와 SAR에 투명하게 동작하여 ASP 부계층으로 인한 영향을 받지 않는다. 암호화나 해쉬 함수의 사용으로 인하여 데이터가 확장되더라도, 이를 SAR 부계층에서 분할/조립하므로 별도의 기능을 추가하지 않아도 자연스럽게 처리될 수 있다. 그림 2는 정보보호를 위한 ASP 부계층의 위치를 나타낸다.

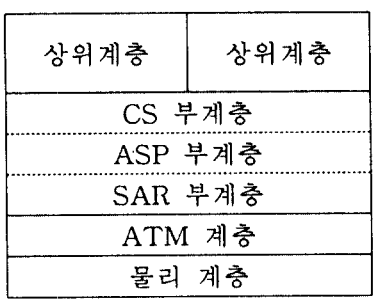

그림 2. ATM 정보보호 프로토콜 구조
Fig. 2 The protocol stack for ATM security

(2) ASP 부계층을 위한 프리미티브

ASP 부계층을 위하여 기본적으로 ASP-UNITDATA-invoke, ASP-UNITDATA-signal 프리미티브가 필요하다. 부계층 사이에는 SAP가 존재하지 않기 때문에 이를 구분하기 위하여 request와 indication 대신에 invoke와 signal을 사용한다. ASP 부계층은 CS PDU의 암호화와 메시지 인증을 위한 처리를 수행하고 기존의 SAR-UNITDATA-invoke와 SAR-UNITDATA-signal의 매개변수들을 SAR와 CS에 전달하여 주는 기능을 수행한다. 따라서, ASP-UNITDATA-invoke와 ASP-UNITDATA-signal의 매개변수에는 기존의 SAR-UNITDATA-invoke와 SAR-UNITDATA-signal의 매개변수에 암호화와 메시지 인증에 필요한 매개변수들을 추가하였다.

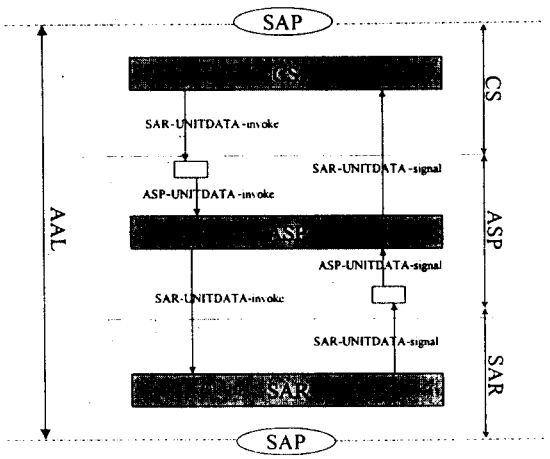

그림 3. ASP 부계층을 위한 프리미티브
Fig. 3 The primitives for ASP sublayer

ASP-UNIT-DATA-invoke, ASP-UNIT-DATA-signal을 위하여 기존의 프리미티브들에 추가된 내용들은 다음과 같다.

```
typedef struct {
  Algrithm_Type;      /* 알고리즘 종류 */
  Initial_Vector;     /* 초기화 벡터 */
  Key;                /* 세션키 */
  ASP_SDU;            /* ASP SDU */
} ASP-UNIT-DATA-invoke, ASP-UNIT-DATA-signal;

typedef struct {
  More;
  SAR_LP;             /* SAR-Loss Priority */
  SAR_CI;             /* SAR-Congestion Indication */
  Interface_Data;     /* SAR-SDU */
} SAR-UNIT-DATA-invoke, SAR-UNIT-DATA-signal;
```

(3) 송신측에서의 메시지 처리절차

ASP 부계층은 AAL 계층의 CS와 SAR 사이에 위치한다. 송신측에서 먼저 상위계층의 PDU가 CS에서 캡슐화된후 ASP PDU에서 암호화된다. ASP PDU는 SAR로 전송되어 분할이 이루어지며, 그림 4는 이 과정을 나타낸다.

ASP-PDU의 구조는 다음과 같이 정의한다.

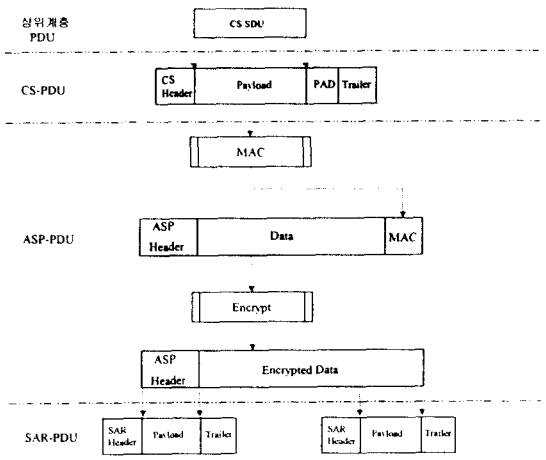

그림 4. 송신측에서의 메시지 처리
Fig. 4 The message processing at sending system

```
typedef struct {
  Length;              /* ASP-PDU의 길이 */
  Algrithm_Type;       /* 알고리즘 종류 */
  Initial_Vector;      /* 초기화 벡터 */
  Enc_Area Enc_Block;  /* 비밀성 영역 */
} ASP-PDU
```

여기서 비밀성 영역의 구조는 다음과 같이 정의한다.

```
typedef struct {
  Next_Key;      /* 다음의 세션키 */
  Key_Seq;       /* 키순서 */
  Data;          /* CS PDU */
  Pad[];         /* 패딩 */
  Pad_Length;    /* 패딩 길이 */
  MAC;           /* 메시지 인증 코드 */
} Enc_Area;
```

ASP에서는 CS PDU에 대한 암호화와 메시지 인증 코드를 생성한다. 암호 알고리즘은 크게 비밀키 방식과 공개키 방식으로 분류할 수 있다. ASP는 이들 다양한 암호 알고리즘을 수용할 수 있도록 설계되었다. MAC 코드를 생성할 때는 일방향 해쉬 함수를 이용하여 메시지의 변조를 방지하도록 한다. 알고리즘 1은 송신측 ASP내에서의 처리과정을 보여주고 있다.

알고리즘 1. 송신측 처리 알고리즘
Algorithm 1. The processing algorithm for transfer

```
Procedure Message-Transfer
  /* MAC 생성 */
  CS_PDU = SAR-UNIT-DATA-invoke.Interface_Data
  Key = ASP-UNIT-DATA-invoke.Key
  Initial_Vector = ASP-UNIT-DATA-invoke.Initial_Vector
  MAC = MAC_Calcu(CS_PDU, Key, Initial_Vector)

  /* 다음 세션키 생성 */
  Next_Key = Generate_Key( )

  /* 전송 순서 번호 증가 */
  Key_Seq = Key_Seq +1

  /* 패딩 길이 계산 */
  Pad_Length = block_unit -((MAC +Next_Key
  +Key_Seq +Data) mod block_unit)

  /* ASP PDU 생성 */
  ASP_PDU.Enc_Block.MAC = MAC
  ASP_PDU.Enc_Block.Next_Key = Next_Key
  ASP_PDU.Enc_Block.Key_Seq = Key_Seq
  ASP_PDU.Enc_Block.Pad_Length = Pad_Length
  for (cnt = 0; cnt < Pad_Length; cnt++)
    ASP_PDU.Enc_Block.Pad[i] = 0

  /* 알고리즘 종류에 따른 암호화 */
  Alg_Type = ASP-UNIT-DATA-invoke. Alg_Type
  Encrypt(Alg_Type, ASP_PDU.Enc_Block, Key,
  Initial_Vector)

  /* SAR-UNIT-DATA-invoke 메시지 내용 생성 */
  SAR-UNIT-DATA-invoke.More = ASP-UNIT-
  DATA-invoke.More
  SAR-UNIT-DATA-invoke.Loss_Prio = ASP-
  UNIT-DATA-invoke.Loss_Prio
  SAR-UNIT-DATA-invoke.interface_data = ASP_PDU
End Procedure
```

알고리즘 1에서 무결성을 지원하는 부분은 CS-PDU 필드이고, CS-PDU를 포함하여, AT, NK, KS, PAD, PAL, MAC 필드의 암호화를 통하여 무결성을 지원한다. 암호화시에는 알고리즘 형태를 검사하여 이에 해당하는 암호 알고리즘을 사용한다.

(4) 세션키 변경

키의 사용시간이 길어질수록 키에 대한 공격 가능성은 커지게 된다. Chuang[4]은 세션키 변경을 위하여 CryptoTag를 사용하는 방법을 제안한 바 있으며 그 절차는 다음과 같다.

- 송신측에서 현재 프레임내에 다음에 사용될 세션키를 수신측으로 전송한다.
- 수신측에서는 수신된 세션키가 현재의 세션키와 다르면 세션키를 갱신한다.

그러나 이 방법은 다음과 같은 문제점을 갖는다. 전송하여 수신측에서 이를 비교하여 세션키를 갱신한다. 즉 이후에 수신되는 메시지는 갱신된 세션키를 사용하여 복호화 한다는 것이다. 그러나 이 방법은 다음 세션키를 포함하고 있는 PDU에 손실이 생길 경우 이후에 수신되는 메시지를 복호화할 수 없는 심각한 단점이 있다.

따라서 메시지 손실시에도 손실된 이후의 메시지들을 복호화 시킬 수 있는 세션키 변경방법이 필요하다. 이러한 문제를 해결하기 위하여 ASP 헤더내에 세션키 순서번호 필드와 OAM 셀을 사용하는 방법을 제안한다. 세션키 순서번호는 PDU 손실로 인한 세션키 손실을 발견하기 위하여 사용하며, OAM 셀은 세션키 재동기를 이루기 위하여 사용한다. 그림 5는 송신측과 수신측의 메시지 교환중의 PDU 손실로 인하여 재동기화가 이루어지는 절차를 보여준다.

위 절차에서 첫번째와 두번째 메시지는 정상적으로 전송이 되었으나 세번째 메시지에 손실이 발생된 예이다. 수신측에서는 현재 수신된 세션키 순서 번호와 다음에 받을 것으로 기대된 번호가 일치하는 가를 비교하여 메시지가 손실되었는지를 판단할 수 있다. 세션키 정보가 손실되어 송, 수신측은 세션키에 대한 동기를 재 설정 해 주어야하며, 이는 OAM 셀을 이용하여 세션키를 재 설정해 주도록 한다. 이때 인위적

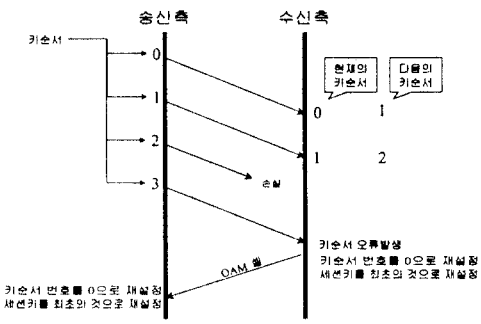

그림 5. 세션키 손실 처리 절차

Fig. 5 The procedure for lost session key

으로 키 순서 오류를 발생 시키는 것을 방지하기위하여 ASP PDU의 키순서 필드는 비밀성을 지원한다. 알고리즘 2는 수신측에서의 세션키 재설정 절차를 나타내고 있다.

알고리즘 2. 수신측에서의 세션키 재설정 알고리즘

Algorithm 2. The algorithm for resynchronize session key at receiver

```
declare Recvd_SeqNo /* 메시지에 송신된 키순서 번호 */
declare Curr_SeqNo /* 현재 수신측에서 저장한 키순서 번호 */
declare Curr_SessionKey /* 현재 사용중인 세션키 */
Procedure Resync_Session_Key
    if (Rcvd_SeqNo == (Curr_SeqNo +1)
                        /* 세션키가 갱신된 경우 */
      Use Curr_SessionKey to decrypt received message
      Update Curr_SeqNo to (Curr_SeqNo +1)
    else                /* 재동기화가 필요한 경우 */
      Update Curr_SessionKey to initial session key
      Send OAM cell to sender for resynchronyzing
    end if
End Procedure
```

Ⅳ. 해쉬 함수를 이용한 인증 및 암호화 기법

ATM망의 비밀성은 암호 알고리즘을 통하여 구현된다. 암호화 방식에는 공개키 방식과 비밀키 방식의 알고리즘이 있다. 공개키 방식은 비밀키 방식에 비하여 속도가 느리기 때문에 키분배와 VC 인증시에 사

용하고, ATM 데이터들의 암호화에는 비밀키 방식을 사용하여야 한다. 비밀키 방식의 암호 알고리즘에는 DES, FEAL, IDEA등이 있으나, 이들의 사용에는 수출규제, 특허 등의 제약사항이 따르므로, ATM 망에서의 암호 알고리즘은 사용자의 선택을 최대한 허용하여야 한다. 또한 ATM과 같은 고속 통신망에서의 암호 알고리즘은 안전하면서도 속도가 빨라야한다. 본 장에서는 Luby-Rackoff 등에 의하여 제안된[5, 6] 해쉬 기반의 암호 알고리즘에 RIPEMD-160 해쉬 함수를 적용한 암호 알고리즘을 구현하였다. 제안된 암호 알고리즘은 AAL 계층에서의 데이터 송수신 처리시 알고리즘 1에서의 암호 알고리즘 종류 매개변수를 이용하여 ATM의 비밀성 보장을 위한 절차에 적용한다.

4.1 해쉬 함수를 이용한 블록 암호화 기법

대부분의 비밀키 암호 알고리즘은 Feistel 블록 암호의 구조를 따르고 있다. 본 논문에서는 Feistel 블록 암호에서의 F-function을 해쉬알고리즘을 이용하여 블록 암호기법을 제안한다. 사용한 해쉬알고리즘은 RIPEMD-160 해쉬알고리즘을 사용하였으며, keyed hash function 기법 중 enveloping method를 이용하였다. 또한 본 논문에서 제안한 블록 암호기법은 기존의 Feistel 블록 암호 형태에서와 같이 입력을 두 개의 블록으로 나누어 처리하는 방법 이외에, 입력을 4개의 블록으로 나누어 처리하는 방법 또한 제안한다. 고속으로 암호화/복호화를 위해서 nesting method 대신, 해쉬연산을 한번만 수행하는 enveloping method를 사용하였으며, 사용되는 키는 128비트 길이를 갖도록 하였다.

본 논문에서 제안한 블록 암호화 기법은 ATM을 기반으로한 통신망에 적용하기 위해, 2개의 블록으로 나누어 처리하는 방법에서는 입력을 24 옥텟으로 하고, 이를 두 개의 블록(각각 12 옥텟)으로 나누어 암호화/복호화를 2번 수행하도록 하였으며, 4개의 블록으로 나누어 처리하는 방법에서는 각각의 블록을 12옥텟으로 하여 암호화/복호화를 수행하도록 하였다.

2개의 블록으로 나누어 처리하는 방법은 4라운드 이상을 갖도록 하였으며, 4개의 블록으로 나누어 처리하는 방법은 5라운드 이상을 갖도록 하였다. 본 논문에서 제안한 블록 암호화 기법의 암호화/복호화 과정은 다음과 같다.

(1)2 블록 암호화/복호화 기법

· 기호
- r: 블록 암호의 라운드 수 ($r \geq 4$)
- b: 암호문/복호문의 비트 길이 (192 비트)
- t: 해쉬코드의 비트 길이 (160 비트)
- X: 해쉬 입력 블록의 비트 길이 (96 비트)
- K: 암호화/복호화에 사용되는 키
- H: 해쉬 함수 (RIPEMD-160)

· 부분 키 생성 방법:

$K_i = (k1_i \| k2_i) = H(u_i, K)\ i = 1, 2, 3, \ldots, r$
$(u_0 = 0xb7e15163,\ u_i = u_{i-1} + 0x9e3779b9 \quad (i \geq 1))$

· F-function의 구성:

$F(K_i, X) = H(k1_i \| X \| k2_i) \bmod 2^{b/2}$
$(|k1_i| = |k2_i| = t/2,\ |X| = b/2)$

· 암호화 과정:

$P = L_0 \| R_0\ (|L_0| = |R_0| = b/2)$
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus F(K_i, R_{i-1})\ i = 1, 2, \ldots, r$
$C = R_r \| L_r$

· 복호화 과정: 부분 키들의 순서를 역순으로 하여 암호화 수행

(2)4 블록 암호화/복호화 기법

· 기호
- r: 블록 암호의 라운드 수 ($r \geq 5$)
- b: 암호문/복호문의 비트 길이 (384 비트)
- t: 해쉬 코드의 비트 길이 (160 비트)
- X: 해쉬 입력 블록의 비트 길이 (96 비트)
- K: 암호화/복호화에 사용되는 키
- H: 해쉬 함수 (RIPEMD-160)

· 부분 키 생성 방법:

$K_i = (kL_i \| kR_i) = H(u_i, K)\ i = 1, 2, 3, \ldots r$
$(u_0 = 0xb7e15163,\ u_i = u_{i-1} + 0x9e3779b9\ (i \geq 1)$

· F-function의 구성:

$F_1(kL_i, X) = H(kL_i \| X \| kL_i) \bmod 2^{b/4}$
$F_2(kL_i, X) = H(kR_i \| X \| kR_i) \bmod 2^{b/4}$
$(|kL_i| = |kR_i| = t/2,\ |X| = b/4)$

· 암호화 과정:

$P = A_0 \| B_0 \| C_0 \| D_0$
$A_i = B_{i-1}$
$B_i = C_{i-1} \oplus F_2(kR_i, D_{i-1})$
$C_i = D_{i-1}$
$D_i = A_{i-1} \oplus F_1(kL_i, B_{i-1})$
$C = A_r \| B_r \| C_r \| D_r \qquad i = 1, 2, \ldots, r$

· 복호화 과정:

$C = A_r \| B_r \| C_r \| D_r$
$A_{i-1} = D_i \oplus F_1(kL_i, A_i)$
$B_{i-1} = A_i$
$C_{i-1} = B_i \oplus F_2(kR_i, C_i)$
$D_{i-1} = C_i$
$P = A_0 \| B_0 \| C_0 \| D_0 \qquad i = r, r-1, \ldots, 2, 1$

V. 안전성 및 성능 분석

5.1 안전성 분석

Luby/Rackoff는 pseudo-random 치환은 3~4개의 pseudo-random 함수로 구성될 수 있음을 증명하였다. 또한 DES와 같은 Feistel 블록 암호의 F-function이 Feistel 형태의 블록 암호 설계시 중요하게 고려되어지며, F-function이 pseudo-random 치환임을 증명하였다. 그리고 Luby/Rackoff는 이러한 F-function을 이용하여 3 라운드 연산을 수행하는 블록 암호는 선택 평문 공격(chosen plaintext attack)에 대해서 안전하고, 4 라운드 연산을 수행하는 블록 암호는 선택 평문/암호문 공격(chosen plaintext/ciphertext attack)에 대하여 안전함을 밝힌바 있다 [5, 6].

본 논문에서 제안한 블록 암호화 기법의 안전성은 전적으로 해쉬 함수가 pseudo-random하고, 해쉬 함수가 안전하다는 가정 하에 안전성을 보장받을 수 있는데, 해쉬 함수는 pseudo-random에 가장 근접한 것으로 판명된 바 있다 [8]. 또한 본 논문에서 제안한 2 블록 암호화 기법이나, 4 블록 암호화 기법 모두가 해쉬 연산을 4번 이상 수행하기 때문에 선택 평문 공격이나 선택 평문/암호문 공격에 대해서 안전성을 보장받는다. 그리고 블록 암호의 라운드 함수로 사용되고 있는 keyed hash function에는 해쉬 함수의 특성상, 입출력 변화/선형근사(differential/linear)의 특성이 DES에 비하여 거의 나타나지 않기 때문에 입출력 변화 공격(differential cryptanalysis) 및 선형근사 공격(linear cryptanalysis)에 대해서도 안전성을 보장받는다[8]. 본 논문에서 사용하고 있는 해쉬 함수는 지금까지 개발된 전용 해쉬 함수 중에서 비교적 안전성이 뛰어난 RIPEMD-160 알고리즘을 채택하여 사용하고 있으며, 사용되는 키의 크기를 128 비트로 하였기 때문에, exhaustive key search에 대해서도 또한 안전성을 보장받는다.

블록 암호 알고리즘에서 입력에 대한 약간의 변화가 출력에 많은 변화를 주어야 함은 가장 기본적인 성질이다. 이러한 성질 중 입력에 대한 한 비트의 변화가 출력에 어느 정도 영향을 미치는 가를 측정하는 것이 avalanche 효과이다. 본 논문에서는 avalanche 효과를 측정하기 위해서, 2 바이트 값이 0xab, 0xcd로 가정하여 1비트씩 변화를 주었다.

표 1은 평문과 키의 비트를 변화 시켰을 때의 avalanche 효과를 나타낸 것이다.

블록 암호에서의 avalanche 효과는 한 비트의 입력 비트 변화가 출력 비트에 절반정도의 영향을 주는 것이 안전한 것으로 본다. 본 논문에서 제안한 암호화

표 1. avalanche 효과
Table 1. The avalanche effect

	DES	2 블록 암호	4 블록 암호
평문에서 1개 비트의 변화	31.06	95.89	191.57
사용된 키에서 1개 비트의 변화	32.88	96.02	193.71

기법의 입력은 2 블록 암호화에서는 24 옥텟이기 때문에 96 비트에 가까워야 하고, 4 블록 암호화에서는 입력이 48 옥텟이기 때문에, 192 비트에 가까워야 한다. 따라서, 표 2에서 보는 바와 같이 본 논문에서 제안한 암호화 기법은 DES와 마찬가지로 avalanche 효과에 있어서 안전성을 보장받는다.

5.2 성능 분석

본 논문에서 제안한 블록 암호화 기법은 2 블록 암호화에서는 4라운드 연산을 수행하고, 4 블록 암호화는 5라운드 연산을 수행하도록 하였다. 따라서 2 블록 암호화 기법은 ATM 셀을 암호화하기 위해서는 24 옥텟의 암호화 연산을 2 번 수행하여야 하기 때문에 키 스케쥴링 해쉬연산까지 포함하면 16번의 해쉬 연산이 필요하고, 4 블록 암호화 기법은 48 옥텟 암호화 연산을 한번을 수행하기 때문에, 키 스케쥴링 연산까지 15번의 해쉬 연산을 한다.

보통의 전용 해쉬 함수와 DES의 수행 속도를 비교하면 전용 해쉬 함수가 20배정도 빠르고[7], 본 논문에서 제안한 암호화 기법에서 사용되는 해쉬 연산이 20번 이하이기 때문에 DES와 수행속도면에서 비교하였을 때 우수한 결과를 얻는다.

본 논문에서 제안한 암호화 기법의 수행 속도를 측정하기 위한 성능 분석 프로그램은 ATM 기반의 네트웍을 고려하여 ATM 셀을 초당 몇 개를 암호화/복호화 할 수 있는가를 테스트한 프로그램으로, 시스템 환경은 Sun Sparc 20이며, 사용 언어는 GNU 컴파일러 gcc 2.7.2를 사용하였다. 성능 분석 프로그램은 1 메가 개수의 ATM 셀을 입력받아, 암호화/복호화하는데 소요되는 시간을 측정하여, 이를 다시 초당 몇 개의 ATM 셀을 암호화/복호화 할 수 있는가를 계산하였다. 본 논문에서 제안한 블록 암호화 기법과 DES와의 수행속도 결과는 다음 표 2와 같다.

표 2. 성능 평가(수행 속도)
Table 2. The performance evaluation of processing speed

	DES	2 블록 암호	4 블록 암호
암, 복호화된 ATM 셀/초	157.53개	817.92개	852.52개
KBps (Bytes per second)	7.38	38.34	39.96

VI. 결 론

ATM은 B-ISDN 망의 스위칭 기술로 채택되어 사용이 확산되고 있다. ATM 망에서의 서비스가 증가함에 따라 통신 정보의 비밀유지의 필요성도 증가되고 있다. 본 논문에서는 ATM을 기반으로 하는 망에서의 비밀성 보장을 위한 정보보호 구조와 해쉬 함수를 이용한 암호 알고리즘을 제안하였다.

ATM 프로토콜 스택상에서 정보보호를 위하여 AAL 계층의 CS와 SAR사이에 암호화를 위한 부계층을 두는 것이 가장 적합한 것으로 분석되어졌다. ASP (ATM Security Protocol) 부 계층을 두는 경우 다음과 같은 장점을 가지게 된다. ASP(ATM Security Protocol) 부계층은 CS와 SAR에 투명하게 동작하여 ASP 부계층으로 인한 영향을 받지않는다. 암호화나 해쉬 함수의 사용으로 인하여 데이터가 확장되더라도, 이를 SAR 부계층에서 분할/조립하므로 별도의 기능을 추가하지 않아도 자연스럽게 처리될 수 있다.

본 논문에서 제안한 해쉬 함수를 이용한 암호화 기법은 키의 크기와 블록의 크기에 제약을 받지 않고, 임의의 크기로 정할 수 있어서, 기존의 블록 암호화 알고리즘에 비해서 좀 더 실용적이라 할 수 있다. 또한 성능 면에서 DES보다 우수한 것으로 나타났으며, 안전성 면에서도 해쉬 함수가 안전하다는 가정하에 문제가 없는 것으로 나타났다. ATM과 같은 고속망에서 DES보다 속도가 빠르면서 특히 키의 길이가 128 비트인 암호화 알고리즘을 사용하는 것은 중요한 의미를 갖는다. ASP 부계층은 다양한 암호 알고리즘을 지원하도록 설계 하였으므로, 제안된 암호 알고리즘을 ASP 부계층에 적용하여 비밀성 기능을 제공할 수 있다.

본 논문에서는 주로 ATM을 기반으로 하는 망에서의 통신정보에대한 비밀성 보장을 위한 정보보호 구조및 암호 알고리즘에 관한 연구를 수행하였으며, 사용자 인증, 키 분배등에관한 내용은 추후 연구 사항이다.

참 고 문 헌

1. Ronald J. Vetter, "ATM Concepts, Architectures, and Protocols", Communications of the ACM Vol.

38, No. 2, pp. 30-38, Feb. 1995.
2. Daniel Stevenson, Nathan Hillery, and Greg Byrd, Secure communication in ATM Networks, Communications of the ACM, Vol. 38, No. 2, p. 46-52, February 1995.
3. Robert H. Deng, Li Gong, Aurel A. Lazar, Securing Data Transfer In Asynchronous Tr ansfer Mode Networks, IEEE GLOBECOM '95, 1995.
4. Shaw-Cheng Chuang, Securing ATM Networks, 3rd ACM Conference on Computer and Communication Security, p. 19-30, March, 1996.
5. Ueli M. Mauere, "A Simplified and Generalized Treatment of Luby-Rackoff Pseudorandom Permutation Generators", Advances in Cryptology-EUROCRYPT'92 LNCS, Berlin, Springer-Verlag, vol. 658, 1992, pp. 239-255.
6. M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudo-ranndom functions", SIAM Journal on Computing, Vol. 17, No. 2, 1988, pp. 373-386.
7. R. Merkle, "One way hash functions and DES", Advances in Cryptology, Proc. Crypto'89, LNCS 435, G. Brassard, Ed., Springer-Verlag, 1990, pp. 428-446.
8. M. Bellare, R. Guerin and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols", In Proc, 1st ACM Conference on Computer and Communications Security, ACM Press, 1993, pp. 62-73.

신 효 영(Hyo-Young Shin)정회원

1986년 2월 : 광운대학교 전자계산학과 졸업(이학사)
1988년 2월 : 광운대학교 대학원 전자계산학과(이학석사)
1996년 8월 : 광운대학교 대학원 전자계산학과 박사과정 수료
1988년~1993년 : LG 소프트웨어(주)
1994년~현재 : 경성전문대학 사무자동화과 전임강사
※관심분야 : B-ISDN, 네트워크 보안, 멀티미디어 통신

유 황 빈(Hwang-Bin Ryou) 정회원

1975년 2월 : 인하대학교 전자공학과(공학사)
1977년 7월 : 연세대학교 대학원(공학석사)
1989년 2월 : 경희대학교 대학원(공학박사)
1994년 2월~1995년 2월 : 美 UCSD 교환교수
1995년~1997년 : 광운대학교 전자계산소장
1981년~현재 : 광운대학교 전자계산학과 교수
1995년~현재 : 광운대학교 신기술 연구소 연구원
1997년~현재 : 광운대학교 도서관장
※관심분야 : ATM, B-ISDN, 멀티미디어 통신, VOD