通信情報保護學會論文誌
第 7 卷 第 1 號, 1997. 3

ATM 물리계층에서의 정보보호

서 정 욱*, 김 경 수*

A Security in the ATM Physical Layer

Chung-Wook Suh and Kyung-Soo Kim

요 약

본 논문은 정보보호 기능의 실시간 처리를 위한 초고속 정보통신망에서의 정보보호에 관한 것으로, 가입자-망이나 망-노드에서의 데이터 접속을 맡고 있는 ATM 물리계층내 구간처리기와 셀처리기에서의 정보보호 방안에 대하여 기술되었다.

아울러, 국제 표준안에 제안되어있는 물리계층의 각 기능이 분석되어 있으며, ATM 물리계층내 구간처리기와 셀처리기에서의 정보보호방안의 타당성에 관하여 기술되었다.

특히, DES 암호 알고리즘을 이용한 구간 처리기에서 정보보호 기능과 IDEA 암호 알고리즘을 이용한 셀처리기에서의 정보보호 기능이 시뮬레이션을 통하여 확인되었다.

아울러, 본 논문에서는 정보보호기능이 내장된 ATM 물리계층용 집적회로의 구현 가능성 및 그에 따른 효율성에 대하여 기술되었다.

Abstract

For the real-time processing of the security, this paper focused on the security for the section overhead processor or for the cell processor of the ATM physical layer which is charged with the data formatting for STM-n data in both of the user-network interface and the network-node interface.

In addition, in this paper, all the function of the physical layer recommended by ITU-T and ATM forum is analyzed and the feasibility of the security in the section overhead processor and the cell processor of the physical layer is described.

In particular, the functional simulation for the security application has been carried not only in the section overhead processor using DES cipher algorithm but in the cell processor using IDEA cipher algorithm.

---

* 한국전자통신연구원 반도체연구단

Finally, it is founded that the implementation of the security-built-in the physical layer IC is feasible as well as significantly efficient.

1. 서 론

향후 멀티미디어 서비스를 처리할 초고속 정보 통신망(Broadband Integrated Service Digital Network)의 핵심 기술인 ATM(Asyn-chronous Transfer Mode) 기술은 최근 들어 국내·외에서 관련 시스템의 구현 작업이 한창 진행 중에 있다. ATM 시스템의 구현은 향후 다양한 정보의 전달은 물론 고속 정보의 전달도 가능해 짐으로서, 컴퓨터 통신을 이용하려는 멀티 미디어 수요자들의 기대를 부풀려 놓았다. 그러나, ATM에 대한 이러한 기대는 요즈음 활동이 왕성한 해커(hacker)나 크래커(cracker)에 의한 각종 정보 손실에 대한 위협에 의하여 위축될 가능성이 커졌다. 특히, 해커나 크래커에 의한 초고속 정보 통신망에서의 정보 침해는 짧은 시간에 많은 데이터에 침범할 수 있기 때문에 초고속 정보 통신망에서의 정보 보호는 다른 어느 시스템보다 중요하다.

그러면, 이러한 정보의 침해를 막기 위하여 정보 보호 기능을 ATM 시스템에서 어디에 적용하고 어떻게 적용할 것인가 하는 점이 대두된다. ATM 시스템에서의 정보 보호를 위한 방안을 연구하기 위해서는 먼저 ATM 기술 및 시스템에 대한 분석이 필요하다.

ATM 기술은 시스템의 기능 분류에 따라서 크게 전송 기술과 교환 기술로 크게 나눌 수 있는데, 전송 기술과 교환 기술은 둘 다 기본적으로 데이터를 고속으로 처리해야 한다.[1] 이러한 이유때문에 ATM 시스템의 구현에 있어서 ATM 시스템의 많은 부분을 하드웨어로 구현해야 할 필요성이 대두되었다. 이에 따라, 세계 각국에서는 하드웨어를 이용하여 구현이 가능한 부분을 ITU-T(International Telecommunication Union-Telecommunication Standardization Sector)나 ATM forum에서 권고한 표준안에 따라 구현을 실현하고 있다. 본 연구에서는 현재까지 ITU-T나 ATM forum에서 권고된 표준안을 토대로, ATM 시스템 중 가장 하드웨어로의 구현이 용이한 물리 계층에 대한 분석과 아울러 정보 보호 기술의 적용 가능성을 연구하였다.

본 논문은 서론에 이어 제 2 장에서는 ATM 시스템에서의 정보 보호 기술의 적용이 가능한 부분에 대한 조사 및 분석에 관하여 기술하였고, 제 3 장에서는 ATM 정합부 내 물리 계층의 기능에 관하여 기술하였고, 제 4 장에서는 물리계층에서의 정보 보호 방안을 제시하였고, 제 5 장에서는 제안된 구간 처리기 및 셀 처리기에서의 정보 보호 방안의 실제 구성과 동작에 관하여 기술하였다.

2. ATM 시스템에서의 정보보호 방안 분석

국제 표준화 기구인 ITU-T나 ATM forum에서 제시한 초고속 정보통신망의 참조 모델을 보면, ATM 망이나 가입자 접속을 위한 물리 계층(Physical Layer)이 있고, 그 위에 ATM 계층, 그 위에 ATM 적응 계층(ATM Adaptation layer)이 있으며, 그 위에는 프로토콜과 관련된 상위 계층이 있다. ATM 적응 계층은 수렴 부계층(Convergence Sublayer)과 분리 및 재결합 부계층(Segmentation and Reassembly Sublayer)으로 구성되어, 상위 계

층의 정보에 대한 정당성을 점검하고, 셀 손실을 처리하며, 상위 계층으로 부터 오는 송신 정보의 분리, 수신 셀로부터 상위 계층의 정보로의 조립을 담당하는 등, 상위 계층과 ATM 계층과의 결합을 담당한다.[1]

ATM계층은 48바이트의 ATM 셀 정보에 5바이트의 ATM 셀 헤더를 붙여서 53바이트 길이를 갖는 ATM 셀을 만들기도 하고, 역으로 분리시키는 기능을 수행하면서 ATM 셀 단위의 비트 오류의 판정, 셀 폐기에 대한 일반적인 흐름 제어, 사용자와 망간의 정보 구분 등을 수행한다. 아울러, 5바이트의 ATM 셀 헤더는 ATM셀이 어떤 통로를 선택할 지를 나타내는 가상 채널 식별기(Virtual Channel Identifier, VCI)와 가상 통로 식별기(Virtual Path Identifier, VPI) 그리고, 각 단말에서 발생하는 트래픽의 흐름을 제어하기 위한 일반적인 흐름 제어(Generic Flow Control, GFC), 사용자 정보용 셀인지 네트워크 운반용 셀인지를 식별하는 페이로드 종류(Payload Type, PT), 셀 폐기의 우선순위를 나타내는 셀 손실 우선 순위(Cell Loss Priority, CLP), 헤더의 에러를 제어하고 ATM 셀 동기를 위한 헤더 에러 검사(Header Error Check, HEC)등으로 구성된다.[1]

물리 계층은 다시 전송 수렴 부계층(Trans-mission Convergence Sublayer)과 물리 매체 의존 부계층(Physical Media Dependent Sublayer)으로 나누어지고, 전송 수렴 부계층은 ATM 계층으로 부터 받은 ATM 셀들을 프레임 단위로 묶어서 전송하거나 반대로 전송 선로로부터 수신된 프레임 단위의 데이터를 ATM 셀 단위로 쪼개어서 ATM 계층으로 보내는 역할 등을 수행하며, 물리 매체 의존 부계층은 비트 단위 시간 처리 및 물리 매체 기능을 수행한다.[1][2][3][4]

초고속 정보 통신망에서의 상위 계층은 소프트웨어에 근거한 프로토콜로 이루어져 있기 때문에 그에 대한 하드웨어로의 구현이 용이하지 않을 뿐 만 아니라 향후 제공될 서비스의 종류에 따라서 그리고 그에 따른 표준화 작업에 따라서 향후 변화의 여지가 많기 때문에 정보 보호 기능의 적용이 적합하지 않음을 알 수 있다. 아울러, ATM 적응 계층도 상위 계층과 ATM 계층간의 결합 과정을 수행하기 때문에 정보의 분해 및 결합 과정에서의 정보 보호 기능의 적용은 타당치 않음을 알 수 있으며, ATM 계층에서는 셀 단위의 전송 및 교환, 비트 오류의 판정, 셀 폐기의 일반적인 흐름 제어, 사용자와 망간의 정보 구분 등을 수행하는데, 문제는 이러한 ATM 계층의 기능 정의가 아직도 확정이 되지 않았을 뿐만 아니라, 가입자 측이냐 교환기 측이냐에 따라 ATM 계층의 영역 설정이 명확하지 않기 때문에, 이러한 상황에서 당장 정보 보호 기능을 삽입하기 위한 적당한 곳을 찾기가 어렵기 때문에 본 논문에서는 ATM 계층에서의 정보 보호 기능의 설정은 제외하기로 하였다. 아울러, 본 논문은 정보 보호 기능을 집적회로로 구현하되 해당되는 기능과 통합하여 하나의 집적회로로 구현하여 정보 보호 기능을 실시간으로 처리하는 것을 목적으로 하기 때문에 ATM 표준안에서 기능 설정이 명확하지 않은 영역에서의 정보 보호 기능 수행은 본 고려에서 제외하였다.

마지막으로, 물리 계층은 ATM 셀에 대한 오버헤드를 첨가하여 가입자 및 망을 정합하는 구조로 되어 있다. 다시 말해서, ATM 셀에 대한 동기 기능과 경로(Path)에 대한 타이밍 제어, 구간(Section)에 대한 프레임 동기 기능을 수행함으로써, 기존 데이터의 동기 획득이 분명하기 때문에 물리 계층에서 정보 보호 기능을 부여하더라도 시스템 동기로 인한 부가적인 기능이 필요 없다. 아울러, 정보 보호 모드 설정에 있어서도, ATM 정합부에 있는 마이크로프로세서를 통하여 사용자에 의한 모드

설정이 가능하기때문에 모드 설정면에서도 편리하다. 아울러, 집적회로로 구현이 가능한 물리 계층에 정보 보호 기능 블럭을 추가하여 집적회로로 구현함으로써, ATM 정합부의 전체 구성이 간단해질 뿐만 아니라, 암호 알고리즘에 의한 암호화 및 복호화를 실시간으로 처리할 수 있는 장점을 갖는다.

3. 물리계층의 구성

ITU-T와 ATM forum에서 권고한 물리계층의 기능은 크게 전송 프레임의 생성 및 복원과 전송 오류 판정, 셀 동기, 유효 셀의 식별 등을 수행하는 전송 수렴 부계층과 비트 단위의 시간 처리 및 전송매체 기능을 담당하는 물리매체의존 부계층으로 구성된다. 전송 수렴 부계층은 프레임 정렬 및 삽입 기능 및 프레임 동기 스크램블링/디스크램블링 기능과 구간 오버헤드 처리 기능, 포인터 처리 기능, 경로 오버헤드 처리 기능, ATM셀 분리 및 삽입 기능, 유휴 셀 처리 기능, 자기 동기 스크램블링/ 디스크램블링 기능, ATM층과의 정합 기능(Universal Test & Operations PHY Interface for ATM, UTOPIA) 등을 포함한다.[2][3][4][5]

전송 수렴 부계층은 크게 송신부와 수신부, 물리계층 제어부로 나누어진다. 송신부는 ATM계층으로 부터 받은 ATM셀을 STM-n 데이터로 변환하여 전송 선로로 보내는 방향에서의 전송 수렴 부계층의 기능을 수행하고, 수신부는 전송 선로로 부터 받은 STM-n 데이터를 ATM계층으로 보내는 방향에서의 전송 수렴 부계층의 기능을 수행한다. 물리계층 제어부는 물리계층의 유지 보수를 위한 제어 및 유지 보수 정보를 처리한다.[2][3][4][5]

① 수신부

- 자국 루프 백
  - 송신부의 출력 데이터를 수신부의 입력으로 루프 백
- 구간 오버 헤드 처리부
  - 프레임 정렬 : A1, A2 바이트를 이용하여 프레임 정렬 기능 수행
  - 경보 처리 : loss of signal(LOS), loss of frame(LOF), multiplex section-alarm indication signal(MS-AIS), multiplex section-remote detect indication(MS-RDI) 검출
  - 성능 검사 : B1, B2 바이트 에러, out of frame(OOF) 및 multiplex section-remote error indication (MS-REI)에 대한 1 초 동안의 적분 값 계산
  - 데이터 통신 : 수신 구간의 성능 및 고장 처리를 위한 정보를 데이터 통신 채널을 통하여 수신 처리
  - 경로 오버 헤드 처리부에 강제로 "1"의 값을 삽입 : MS-AIS 발생시 재생기 구간 오버 헤드를 제외한 모든 STM-n 데이터에 삽입
  - 프레임 동기 디스크램블링 : $f(x)=x^7+x^6+1$ 특성 다항식을 이용
- 경로 오버 헤드 처리부
  - 포인터 해석 : H1, H2 바이트를 이용하여 포인터를 해석함으로써 VC-4 페이로드의 시작점 검출
  - 경보 처리 : loss of pointer(LOP), path-alarm indication signal(P-AIS), path-remote detect indication(P-RDI) 검출
  - 성능 검사 : B3 바이트 에러, pointer justification event 및 path-remote error indication(P-REI)에 대한 1 초 동안의 적분 값 계산
  - J1 바이트 추적

- 데이터 통신 : 수신 경로의 성능 및 고장 처리를 위한 정보를 데이터 통신 채널을 통하여 수신 처리
- 셀 처리부로 강제로 "1"의 값을 삽입

- 셀 처리부
  - 셀 분리 : 5 바이트의 셀 헤더에 대하여 $h(x)=x^8+x^7+x+1$ 특성 다항식을 이용한 CRC-8 수행
  - 경보 처리 : loss of cell delineation(LCD)
  - 성능 검사 : out of cell delineation(OCD)에 대한 1 초 동안의 적분 값 계산
  - 자기 동기 디스크램블링 : $g(x)=x^{43}+1$ 특성 다항식 이용
- 수신 UTOPIA 정합
  - UTOPIA 레벨 2 정합 규격 만족
  - ATM 계층으로 유효한 ATM 셀을 송신

② 송신부

- 원격 루프 백
  - 수신부의 입력 데이터를 송신부의 출력으로 루프 백
  - 구간 오버 헤드 처리부
  - 프레임 바이트 삽입 : A1, A2 바이트를 이용하여 프레임 바이트 삽입
  - 경보 정보 삽입 : K2(6~8비트)바이트를 이용하여 MS-AIS("111") 및 MS-RDI("110") 삽입
  - 성능 정보 삽입 : BIP-8을 이용한 B1 바이트 삽입, BIP-24n를 이용한 B2 바이트 삽입, 수신부에서의 MS-REI 에러 발생시 Z2(18~24비트)바이트를 이용한 수신 B2 오류 값을 삽입
  - 데이터 통신: 송신 구간의 성능 및 고장 처리를 위한 정보를 데이터 통신 채널을 이용
  - 프레임 동기 스크램블링 : $f(x)=x^7+x^6+1$ 특성 다항식 이용
- 경로 오버 헤드 처리부
  - 포인터 생성 : H1, H2 바이트를 이용하여 VC-4 페이로드의 시작점을 삽입
  - 성능 정보 삽입 : BIP-8을 이용하여 B3 바이트 삽입, 수신부에서의 P-REI 에러 발생시 G1(1~4비트)바이트를 이용하여 수신 B3바이트의 오류 값을 삽입
  - 데이터 통신: 송신 경로의 성능 및 고장 처리를 위한 데이터 통신 채널을 이용
  - 경보 정보 삽입 : 수신부에서의 LOS, LOF, LOP, LCD, MS-AIS 및 P-AIS 발생시 G1(5) 바이트를 이용하여 P-RDI('1')를 삽입
  - J1 바이트 삽입
- 셀 처리부
  - HEC(Header Error Checker) 바이트 삽입 : ATM 셀 헤더(1~4바이트)에 대하여 x^8+x^7+x+1 특성 다항식을 이용한 CRC-8 계산 후 HEC바이트에 삽입
  - 유휴 셀 삽입
  - 자기 동기 스크램블링 : $g(x)=x^{43}+1$ 특성 다항식 이용
- 송신 UTOPIA 정합
  - UTOPIA 레벨 2 정합 규격 만족
  - ATM 계층으로 부터 ATM셀을 수신

4. 물리계층에서의 정보 보호 방안

물리계층에서의 정보 보호 방안은 STM-n 데이터와 AU4-n 데이터, ATM 셀에 대한 정보 보호를 고려할 수 있다. 여기서, STM-n 데이터는 물리계층의 구간 처리기에서 처리하고, AU4-n은 경로 처리기에서, 그리고 ATM셀은 셀 처리기에서 각각 처리된다. 그러면, 세가지 방안에 대한 구성 및 데이터 처리 방법에 관하여 살펴 보도록 하자.

① 구간처리기에서의 정보 보호 방안

125μsec 의 한 프레임 구간은 총 270n×9바이트로 구성되는 데 그 중에는 [4(n-1)×9×8]바이트의 구간오버헤드와 [4(n-1)×9]바이트의 경로오버헤드, [4(n-1)×9]바이트의 AUG-n 포인터를 포함하고 있다. 특히 구간오버헤드의 첫번째 열에는 프레임 정렬을 위한 바이트들이 할당되어 있다.

초고속 정보 통신망에서의 프레임 동기는 물리 계층의 프레임 바이트를 이용하여 수행되기 때문에 STM-n 단위의 데이터 동기를 잡기 위해서는 구간 오버 헤드의 첫번째 열에 있는 A1과 A2바이트로 구성된 프레임 정렬 바이트들은 비화를 시키지 않아야 한다. 그러므로, STM-n 데이터 중 프레임 정렬 바이트 6n을 제외한 나머지 바이트들에 대하여 64비트 단위를 하나의 블럭으로 나눈 후, 각 블럭에 대하여 블럭 암호 알고리즘을 적용한다.[6] STM-n의 270n×9바이트 중에서 A1과 A2의 6n바이트를 제외한 2,424n바이트를 64비트로 나누면, 모두 303n블럭으로 나누어진다.

아울러, ECB(Electronic CodeBook) 운용 모드나 CBC(Cipher Block Chaining)모드에 대한 64비트 단위의 정보보호가 처리될 뿐만 아니라, CFB(Cipher FeedBack) 모드나 OFB(Out put FeedBack) 모드에서는 k비트 단위의 정보보호가 처리된다.[7]

이러한 정보보호 기능을 실시간으로 처리하기 위해서는 이러한 정보보호 기능을 물리계층용 집적회로에 포함해야 하기 때문에, 구간처리기에서의 정보보호 기능은 가입자 측이나 중계기 측에 함께 적용될 수 있다.

그림 1은 물리 계층의 구간 처리기에서의 정보 보호를 위한 구성도를 보여 준다.

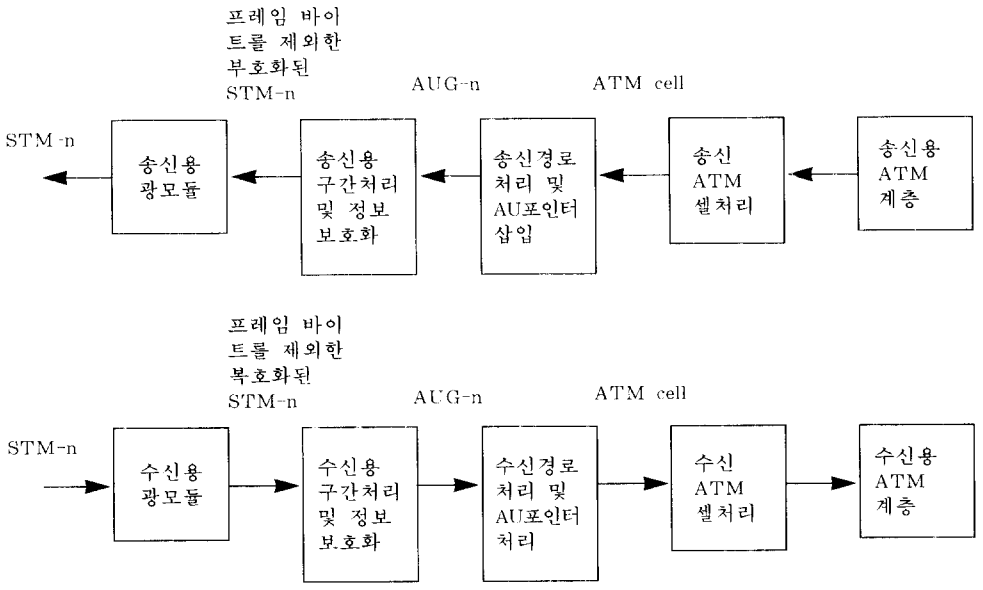

그림 1. 구간 처리기에서의 정보 보호를 위한 구성도

② 경로 처리기에서의 AUG4-n 데이터에 대한 정보 보호 방안

AUG4-n 데이터에 대한 정보보호 방안으로서, [4(n-1)×9+263n×9]바이트의 AUG4-n 데이터 중에서 [4(n-1)×9]바이트의 AUG4-n 포인터 중 VC4-n바이트의 시작점을 제어하는 6n의 H1과 H2바이트를 제외한 [263n×9+4n]바이트에 대하여 정보보호 기능이 수행된다.

초고속 정보 통신망에서의 VC4-n 데이터의 정렬은 AUG4-n포인터 중 H1과 H2바이트의 값에 따라서 이루어지기 때문에 6n의 H1과 H2바이트들은 비화를 시키지 않아야 한다. 그러나, AUG4-n 데이터 중 포인터 바이트 6n을 제외한 나머지 바이트들에 대하여 64비트 단위를 하나의 블럭으로 나누면 정확하게 나눌 수 없다. 그러므로, 이 방안에서는 블럭 암호 알고리즘용 4가지 표준 동작모드를 모두 적용하기가 곤란하기 때문에, 본 제안에서는 이 방안을 제외하였다.

③ 셀 처리기에서의 ATM셀에 대한 정보 보호 방안

ATM 셀은 ATM 셀의 구간을 확인할 수 있는 5바이트의 ATM 헤더와 48바이트의 정보 바이트로 구성되는 데, ATM 셀 헤더는 셀 동기와 관련이 있기 때문에, 비화를 하지 않고, 48바이트의 정보 데이터에 대해서만 비화하는 방안이다. 48바이트의 정보 데이터를 64비트 단위로 블럭화하여, 하나의 셀을 6개의 블럭으로 나눈다. 그림 2는 물리계층의 셀처리기에서의 정보 보호를 위한 구성도로써, 송신부에서는 UTOPIA를 거쳐서 ATM계층으로 부터 입력되는 유효한 ATM 셀에 대하여 비화를 수행하고 비화된 ATM 셀을 경로 단위로 매핑하여, 경로오버헤드와 포인터용 바이트를 포함한 AU4-n 데이터 형태를 만든 후, 구간오버헤드를 포함하는 STM-n 데이터를 만들어 상대 ATM 시스템으로 송신하고, 수신부에서는 광 모듈로 부터 수신된 데이터에 대하여 프레임 동기를 잡고, 이어 VC4-n 구간을 정렬하는

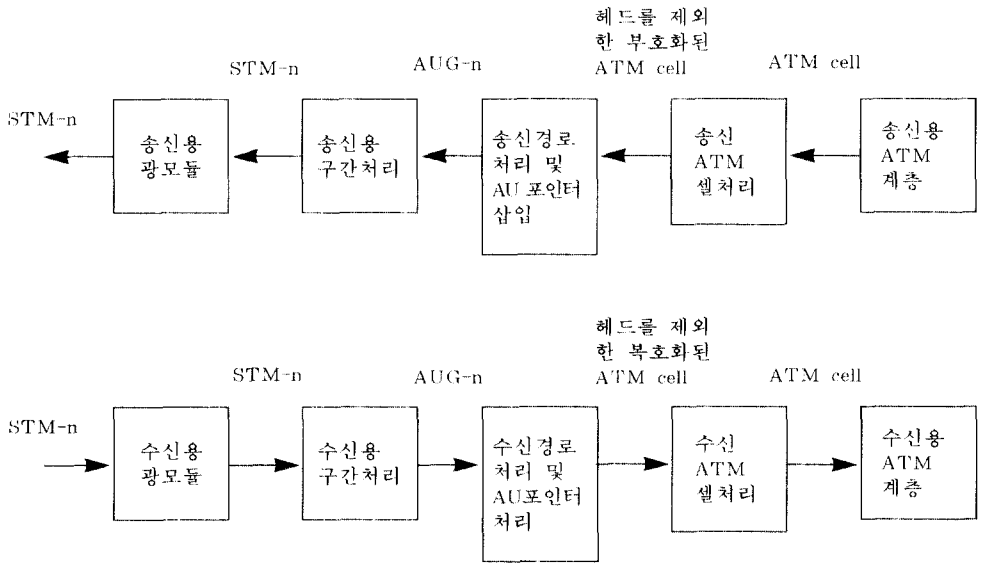

그림 2. 셀처리기에서의 정보 보호를 위한 구성도

등 기존의 물리계층의 수신 기능을 수행한 후, 셀 처리기에서 C4-n 데이터로 부터 ATM 셀 헤드용 5 바이트를 이용하여 셀 분리 기능을 수행한다. 그런 후, ATM 헤더용 5바이트를 제외한 정보용 48 바이트에 대하여 64비트 단위로 복호화를 수행한다.

5. 제안된 정보보호 방안의 세부 구조 및 효과

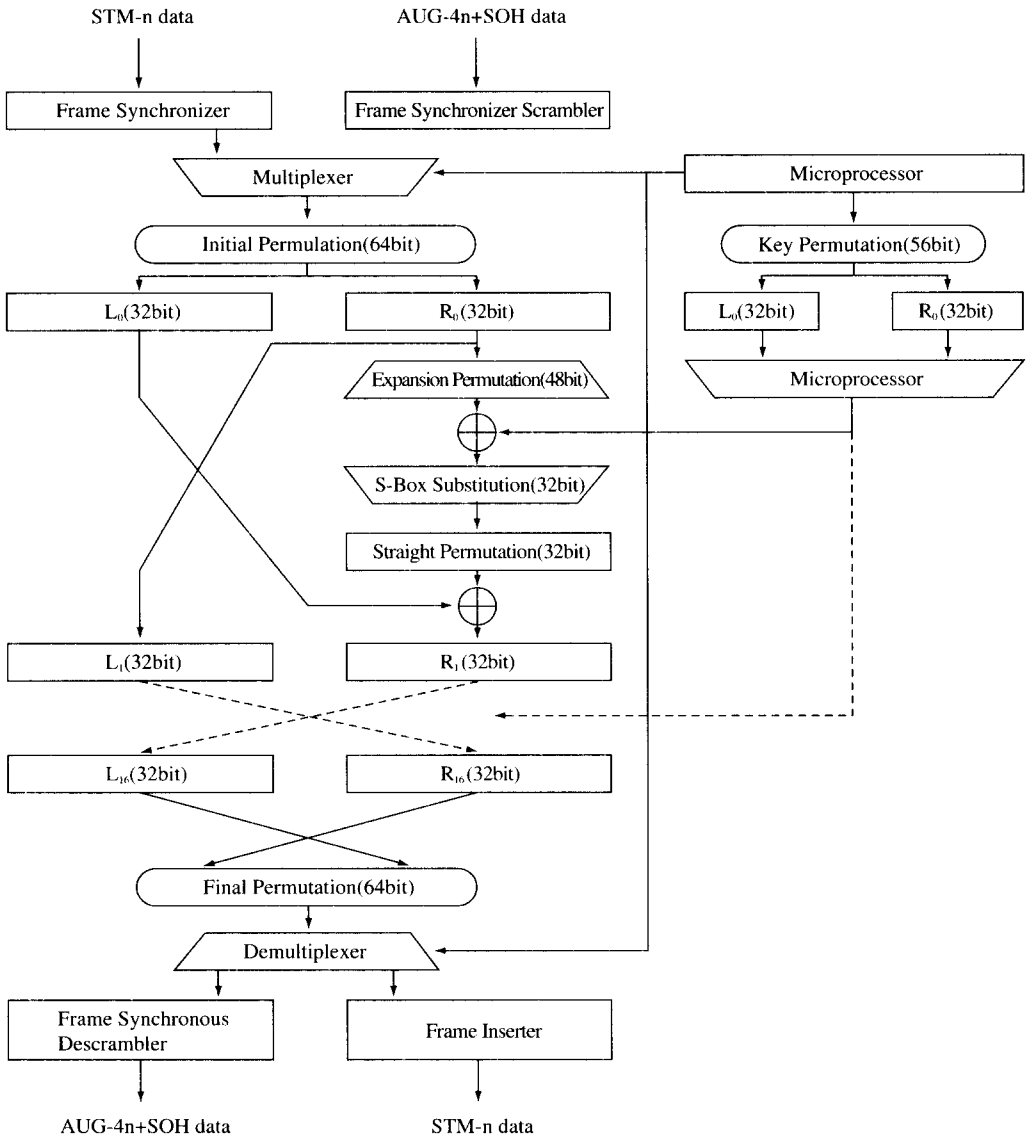

그림 3. DES(Data Encryption Standard)를 이용한 구간 처리기에서의 정보보호 블럭도

① 구간 처리기에서의 정보 보호를 위한 세부 구조

그림 3은 DES 암호 알고리즘을 이용하여 구간 처리기에서 정보보호 기능을 수행하기 위한 블럭 다이어그램으로써, VHDL 상위레벨 시뮬레이션을 이용하여 기능 동작을 확인하였다. 이러한 동작을 확인하기 위해서는 기본적으로 8-bit 버스 구조를 이용하는 병렬 처리 구조가 필요하다.

그림 3에서, 프레임 동기용 스크램블러는 AUG-n 데이터와 구간오버헤드로 구성된 (AUG-n+SOH) 데이터 중, 구간오버헤드 바이트의 첫번째 열을 제외한 모든 데이터에 대하여 $f(x)=x^7+x^6+1$의 특성 다항식을 이용한 프레임 동기용 스크램블링을 수행한다. 이어서, DES 암호 알고리즘을 이용한 암호화 회로는 스크램블링된 데이터와 다중화용 구간오버헤드의 첫번째 열중 A1과 A2 바이트를 제외한 3n의 나머지 바이트를 합한 2,424n바이트에 대하여 64비트 단위로 암호화를 수행한다. 이러한 암호화 과정에서 사용되는 암호 키는 마이크로프로세서 인터페이스 블럭으로 부터 입력된다. 암호화된 STM-n 데이터는 송신용 프레임 바이트 처리 회로에 의하여 프레임 바이트가 추가되어 송출한다. 한편, 수신부에서는 프레임 동기회로를 이용하여 수신된 STM-n 데이터로 부터 3n의 A1프레임 바이트와 3n 의 A2프레임 바이트를 연속해서 검출하고, 연속패턴 검출 회로를 이용하여 3n의 A1바이트와 3n의 A2바이트가 연속해서 두 번 발생되는 지를 확인 한 후 프레임 동기의 여부를 판정한다. 이어서, 프레임 동기회로로 부터 수신된 데이터는 Initial Permutation 블럭으로 입력되어 복호화가 수행된다. 이런 과정에서 프레임 동기된 STM-n 데이터 중, 다중화용 구간오버헤드의 첫번째 열중 A1과 A2바이트를 제외한 2,424n바이트에 대하여 64비트 단위로 복호화를 수행한다. 복호화에서 사용되는 암호 키는 사용자에 의하여 마이크로프로세서 인터페이스 블럭을 이용하여 입력된다. 이렇게 복호화된 데이터 중 다중화용 구간오버헤드의 첫번째 열을 제외한 2,421n바이트에 대하여 디스크램블링이 수행됨으로써 AUG-n 및 구간오버헤드 데이터가 송출된다.

본 구성에서 암호 키의 입력과 송수신 기능의 선택을 위하여 마이크로 프로세서 인터페이스 블럭을 만들어 사용하였는 데, 이것은 본 구성에 관련 레지스터들을 두어, 레지스터 어드레스 및 데이터 버스를 이용한 가상 마이크로프로세서 운영 환경을 꾸몄다.

② 셀 처리기에서의 정보 보호를 위한 세부 구조

그림 4는 IDEA 암호 알고리즘을 이용하여 셀 처리기에서의 정보보호를 수행하는 블럭도로써, 자기동화 스크램블러에서는 5바이트의 헤더 바이트를 제외한 48바이트의 정보 바이트에 대하여 $g(x)=x^{43}+1$의 특성 다항식을 이용하여 자기 동화 스크램블링을 수행하고, 이어서, 스크램블링된 48 바이트의 정보 데이터에 대하여 IDEA 암호 알고리즘을 이용하여 64비트 단위로 암호화를 수행한다. 이때, 사용되는 암호키는 마이크로프로세서 인터페이스 블럭으로 부터 입력된다. 헤더에러 제어기는 ATM셀의 헤더에 대하여 생성 다항식 $h(x)=x^8+x^2+x+1$을 이용하여 ATM 헤더 중 첫 4바이트에 대하여 HEC(Header Error Checker) 계산을 수행하고, 그 결과를 5번째 바이트인 HEC용 바이트에 삽입한다. 그리고, 수신부에서는 Cell Delineation 회로에 의하여 셀 동기를 추출하는 과정에서 C4-n 데이터는 ATM 셀 분리 회로에 의하여 ATM셀의 경계를 확인함으로써, ATM 셀에 대한 동기 기능을 수행하며,[40,42] shortened cyclic code를 사용

하여 5바이트의 셀 헤더에서 발생하는 비트 오류 중 1비트를 정정하고, 다중 오류를 검출한다. 이러한 과정을 거친 ATM 셀은 48바이트의 정보 데이터에 대하여 IDEA 암호 알고리즘에 의하여 64비트 단위로 ATM 셀 당 6개 블럭씩 복호화가 수행된다. 복호화된 정보 데이터는 자기동화 디스크램블러에 의하여 디스크램블링이 된다. 여기서도, 그림 3과 마찬가지로 마이크로프로세서 인터페이스를 이용하여 송수신 기능의 선택 및 암호키의 입력을 처리하였다.

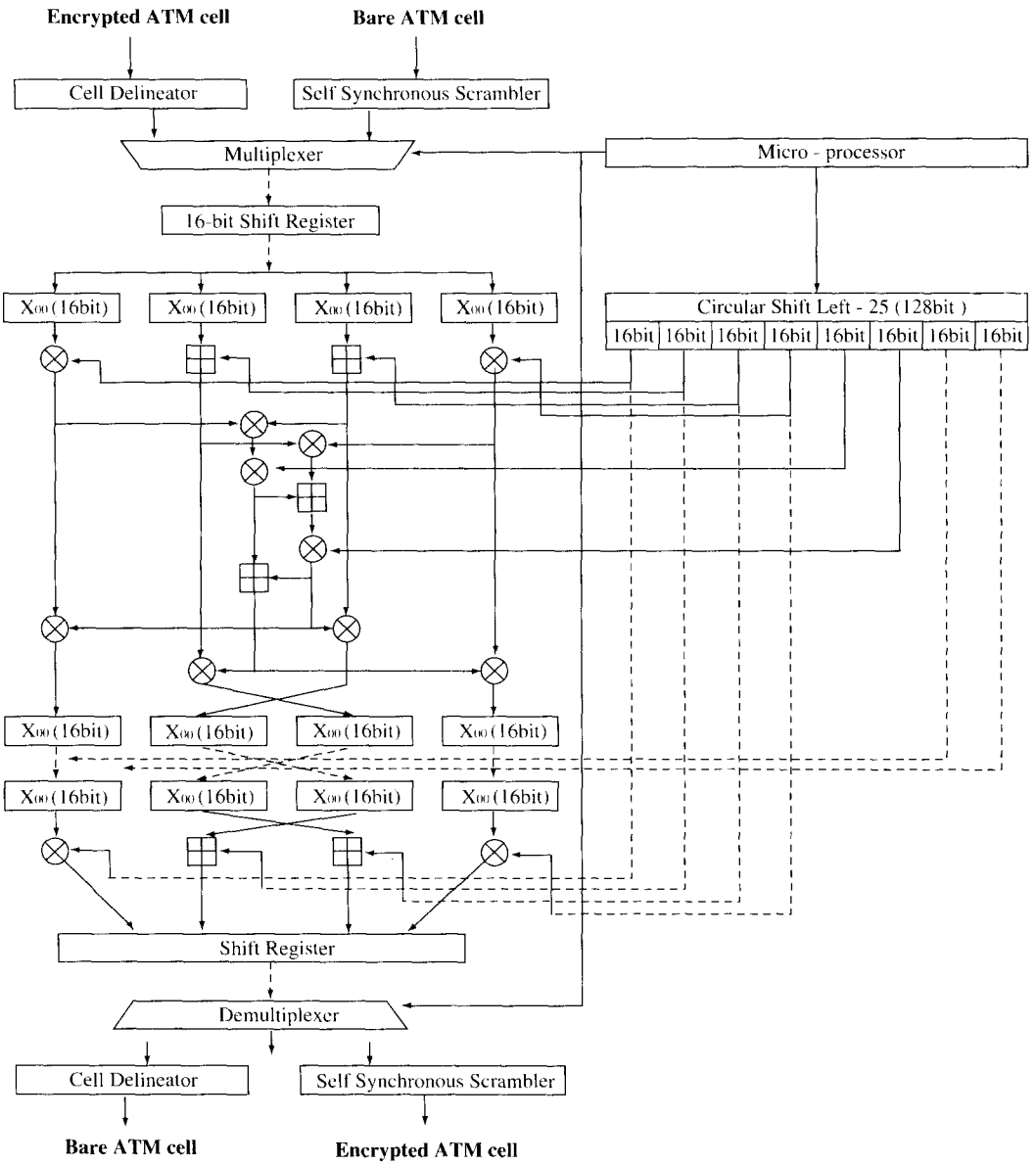

그림 4. IDEA를 이용한 셀 처리기에서의 정보 보호 블럭도

③ 제안된 정보 보호 방안의 유효성 검토

본 논문은 초고속 정보 통신망에서 정보보호 기능을 실시간으로 처리하기 위하여 구간 처리기나 셀 처리기에 기존의 블럭 암호 알고리즘을 적용하여 기능 시뮬레이션을 수행함으로써, ATM 물리계층용 집적회로의 구현 가능성을 타진하기 위하여 수행되었다. 특히, 표준안이 확정된 물리계층은 오늘날 집적회로로 구현되어 사용되고 있기 때문에 물리계층에서의 정보보호 방안은 가까운 시일 내에 수행할 수 있으리라 여겨진다.[8][9]

본 연구를 통하여 수행된 시뮬레이션 결과, 기존의 물리 계층용 집적회로에 들어 있는 구간 처리기나 셀 처리기용 정보보호 기능을 추가하여, 집적회로로 구현하는 것이 용이하다는 결론을 얻었다. 특히, 정보보호 기능의 집적회로 구현은 암호 및 복호화를 실시간으로 처리할 수 있으며, 아울러, ATM 시스템 내부의 CPU의 부담을 줄일 수 있고, 쓰기 전용 레지스터를 이용하여 암호 키를 저장할 수 있기 때문에 해커의 침입을 확실하게 방지할 수 있다. 그러므로, 집적회로화된 구간 처리기나 셀 처리기에 상기와 같은 정보 보호 기능을 하나의 집적회로로 구현할 경우 상당한 효과를 얻을 수 있다.

아울러, 본 제안에 따라 구간처리기에서 프레임 정렬 바이트를 제외한 데이터에 대한 정보 보호 기능과 셀 처리기에서 셀 헤드를 제외한 데이터에 대한 정보보호 기능을 집적회로로 구현을 하게 되면, 구성 및 운영이 간단하며, 동작 시 데이터 에러율이 작아 진다는 장점이 있다.

6. 결 론

본 논문은 ITU-T 및 ATM forum에서 권고하고 있는 물리계층의 기능과 DES 및 IDEA 암호 알고리즘을 이용한 ATM 물리계층에서의 정보 보호 방안을 제시하였다.

특히, 구간 처리기에서 STM-n의 270n×9 바이트 중에서 A1과A2 의 6n 바이트를 제외한 2,424n바이트에 대하여 DES 암호 알고리즘을 적용하여 구성하는 방안과, 셀 처리기에서 ATM셀 중 48바이트의 정보 데이터에 대하여 IDEA 암호 알고리즘을 적용하여 구성하는 방안을 제시하였다.

본 논문에서는 구간 처리기에서의 정보보호와 셀 처리기에서의 정보보호에 대한 기능 시뮬레이션을 통하여 정보보호 기능을 갖는 물리 계층용 집적회로의 구현에 대한 가능성을 타진하고자 하였다.[4][9]

본 연구의 기능 시뮬레이션에 따르면, 본 제안을 따를 경우, 초고속 정보통신망에서의 정보보호 기능을 실시간으로 처리할 수 있을 뿐만 아니라, ATM 정합부 내 CPU의 부담을 줄일 수 있으며, 암호 키를 쓰기 전용 레지스터에 저장함으로써 해커에 의한 초고속 정보통신망으로의 침해를 확실하게 막을 수 있으며, 아울러, 이러한 시도는 시스템의 소형화를 꾀할 수 있을 뿐 만 아니라, 가격 경쟁력을 향상시킬 수 있으며, 마지막으로 가입자-망 및 망-노드의 전송 성능을 더욱 더 향상시킬 수 있는 장점을 가질 것으로 사료된다.

참 고 문 헌

[1] Raifo.Onvural, Asynchronous Transfer Mode Networks : Performance Issues, Artech House, Inc., pp. 13-35, 1994.

[2] ITU-TSS Draft Recommendation G.70X, "Network Node Interface for the Synchronous Digital Hierarchy," ITU-TSS, Geneva, May 1994.

[3] ITU-TSS Revised Recommendation G.783, "Characteristics of Synchronous Digital Hierarchy (SDH) Equipment Functional Blocks," ITU-TSS, Geneva, 1994.

[4] ITU-TSS Draft Text of G.ATME-1 and G.ATME-2, "Types and General Characteristics of ATM Equipment," ITU-TSS, Geneva, Mar. 1994.

[5] The Tecnical Committee of the ATM Forum, "ATM User-Network Interface Specification(Version 3.1)," The ATM Forum, Sep. 1994.

[6] Man Young Rhee, "Cryptography and Secure Cummunications," McGraw-Hill Book Co., pp. 47-101, 1994.

[7] Bruce Schneier, "Applied Cryptography, Second edition Protocols, Algorithm, and Source Code in C," John wiley & Sons, Inc., pp. 189-211, 1996.

[8] Chung Wook Suh et al., "An Implementation of the 155M Physical Layer ASIC for ATM Network-Node Interface," IEEE Asia Pacific Conference on Circuits and Systems '96," pp.37-40, Nov. 1996.

[9] Chung Wook Suh et al., "An Implementation of the 155M Transmission Convergence ASIC for ATM User-network Interface and Network-Node Interface," ITC-CSCC'96, pp. 1330-1333, Jul. 1996.

□ 著者紹介

서 정 욱

1984년 홍익대학교 대학원 전자공학과 졸업(공학석사)
1992년 ~ 전자응용기술사
현재 한국전자통신연구원 과제책임자
"Security 집적회로 연구" 사업책임자
IEEE, KIISC, KITE 각 회원
※ 관심 분야 : VLSI 설계 분야
통신용 집적회로 설계 분야

김 경 수

1977년 서강대학교 전자공학과 졸업(공학사)
현재 한국전자통신연구원 집적회로연구부장
IEEE, KITE 각 회원