IEEE 802.11i MAC Layer 설계 및 구현

준회원 홍 창 기*, 정회원 정 용 진*

Design and Implementation of IEEE 802.11i MAC Layer

Chang-Ki Hong* *Associate Member*, Yong-Jin Jeong* *Regular Member*

요 약

IEEE 802.11i에서는 기존의 802.11a,b,g가 가지고 있던 보안상 문제점을 보완하기 위해서 RSNA(Robust Security Network Association)를 새로이 규정하고 있다. RSNA에서는 기존의 데이터 암호화를 위한 WEP(Wired Equivalent Privacy)을 대신하여 좀 더 견고한 데이터 암호화를 위하여 TKIP(Temporal Key Integrity Protocol)와 CCMP(Counter with CBC-MAC Protocol)를 사용하고 있다. 본 논문에서는 WEP, TKIP, CCMP의 암.복호 엔진을 설계하여 IEEE 802.11i를 지원하는 MAC Layer를 설계, 구현 하였다. WEP은 기존의 IEEE 802.11 legacy MAC과의 호환성을 보장하기 위하여 구성되었고, TKIP와 CCMP는 IEEE 802.11i에서 규정한 데이터 보안을 보장한다. 본 논문의 CCMP 블록은 동작 주파수 134MHz에서 최대 816.7Mbps의 데이터의 처리속도를 가짐으로써 802.11n의 성능을 보장 한다. 또한 2단 파이프 라인 구조를 가지는 AES 구조를 제안하여 CCMP에서의 동작 모드인 CBC 모드와 CTR 모드를 1개의 AES 코어에서 처리하도록 하여 적은 면적의 하드웨어를 가지도록 하였다.

Key Words : 802.11i, WLAN, TKIP, CCMP, SoC

ABSTRACT

IEEE 802.11i is an amendment to the original IEEE 802.11/b,a,g standard specifying security mechanism by stipulating RSNA for tighter security. The RSNA uses TKIP(Temporal Key Integrity Protocol) and CCMP(Counter with CBC-MAC Protocol) instead of old-fashioned WEP(Wired Equivalent Privacy) for data encryption. This paper describes a design of a communication security engine for IEEE 802.11i MAC layer. The design includes WEP and TKIP modules based on the RC4 encryption algorithm, and CCMP module based on the AES encryption algorism. The WEP module suffices for compatibility with the IEEE 802.11 b,a,g MAC layer. The CCMP module has about 816.7Mbps throughput at 134MHz, hence it satisfies maximum 600Mbps data rate described in the IEEE 802.11n specifications. We propose a pipelined AES-CCMP cipher core architecture, which has lower hardware cost than existing AES cores, because CBC mode and CTR mode operate at the same time.

I. 서 론

현대 사회는 인터넷을 이용한 멀티미디어 서비스를 어디에서나 이용할 수 있는 정보화 사회로 급진전하고 있다. 이에 무선랜의 성장은 국내에서 2012년까지 연평균 15%의 빠른 성장률을 보일 것으로 예상된다[1]. 무선랜은 브로드캐스팅 통신이므로 통신 서비스 셋 안에 있는 모든 단말기는 다른 단말기의 통신 내용을 수신 할 수 있어 보안상 취약점을 가지고 있다. 기존의 무선랜에서 사용되는 RC4

※ 본 논문은 IDEC의 툴 지원과 ETRI 시스템 반도체진흥 센터에서 수행한 IT SoC 핵심설계인력양성사업 및 서울시 산학연 협력사업 (KU080661)의 지원으로 수행되었습니다.

* 광운대학교 전자통신공학과 실시간 구조 연구실(hckllsks@kw.ac.kr, yjjeong@kw.ac.kr)

논문번호 : KICS2009-04-181 , 접수일자 : 2009년 4월 29일, 최종논문접수일자 : 2009년 8월 12일

(Rivest Cipher 4)를 이용한 WEP은 여러 가지 보안상 문제점을 노출하게 된다[2][3]. 이에 IEEE 802.11i Gn에서는 WEP의 보안 취약점을 보완하기 위하여 RSN(Robust Security Network)를 새롭게 정의하였다. RSN은 데이터의 암호화를 위하여 TKIP과 CCMP을 사용하고 있다[2].

본 논문에서는 기존 무선랜과의 호환성을 위한 WEP과 IEEE 802.11i를 지원하기 위한 TKIP, CCMP의 효율적인 구현을 보여 주고 있다. 또한 차세대 무선랜 표준으로 주목 받고 있는 IEEE 802.11n에서 데이터의 암호화는 CCMP를 이용하여 데이터를 암호화를 하고, 빠른 데이터 전송을 위하여 MAC 계층에서 100Mbps 이상의 데이터 전송이 이루어 져야 한다[4]. 이에 802.11n에서도 사용이 가능하도록 CCMP 블록의 설계는 빠른 데이터 암호화에 초점을 맞추어 설계를 하였다.

본 논문은 IEEE 802.11i의 개요를 시작으로 WEP, TKIP, CCMP, 802.11 MAC layer의 하드웨어 구현에 대하여 기술하였다. 마지막으로 설계된 하드웨어의 검증 및 성능 평가를 하고, 결론을 맺는다.

Ⅱ. IEEE 802.11i의 개요

WEP의 보안상 문제점으로는 Week Key의 취약점을 들 수 있다. RC4에서 사용되는 seed값 중에서 24비트의 IV(Initialization Vector)는 암호화되지 않고 평문으로 노출되어 전송된다. 또한 세션이 연결 중에는 비밀 공유키가 갱신되지 않기 때문에 동일한 IV를 가지는 암호문을 수집하면, 키 스트림을 복원해 낼 수 있다. 이러한 방법은 참고 논문[5]를 통해 확인 할 수 있다. TKIP는 WEP의 보안상의 취약점을 보완하기 위하여 Wi-Fi 연합체에서 표준화한 것으로써, 802.11i의 일부로 채택되었다. CCMP는 128비트 블록 키를 사용하는 CCM모드의 AES(Advanced Encry -ption Standard) 블록 암호 알고리즘을 사용한다.

Ⅲ. WEP, TKIP 하드웨어 구현

3.1 WEP 알고리즘 개요

WEP은 64비트 혹은 128비트의 키를 이용하여 RC4에서 데이터 암호화를 위한 난수 스트림을 생성한다. 그림 1은 WEP의 암호화 과정을 간단한 블록도로 나타낸 그림이다. 암호화 동작에서는 WEP

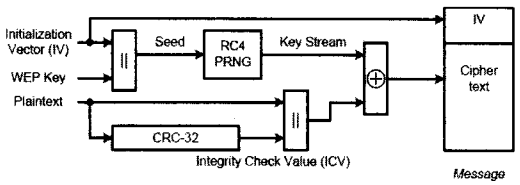

그림 1. WEP 암호화 과정 블록도
Fig. 1. WEP encapsulation block diagram

키와 IV가 결합된 값이 RC4의 seed 값으로 입력되고, RC4에서는 암호화에 필요한 난수 스트림을 생성한다. 생성된 스트림은 데이터와 1바이트씩 EXOR 연산을 통해 암호화되어 진다.

3.2 WEP 알고리즘 하드웨어 구현

본 논문에서 설계한 WEP 암호화 블록은 그림 2에서 보이는 것과 같이 크게 2개의 블록으로 구성되어 있다. 왼쪽 블록은 WEP Header를 생성하고 RA (Receiver Address) 따라 WEP키를 찾는 블록이고, 오른쪽 블록은 왼쪽 블록에서 생성된 WEP키를 이용하여 난수 스트림을 생성하는 RC4, CRC-32 연산을 이용하여 ICV를 생성하는 블록이다.

S배열을 하드웨어로 구현할 때, 크게 Register로 구현하는 방법과 SRAM을 이용하여 구현하는 방법이 있다. Register로 구현할 경우, S배열을 1~255 초기화할 때 지연 시간 없이 초기화 할 수 있는 이점이 있지만, 하드웨어의 많은 면적을 차지하게 된다. 그러므로 본 논문에서는 RC4의 효율적인 구현을 위해서 S배열을 SRAM을 이용하여 구현하였으며, S배열의 초기화를 위한 지연 시간을 줄이기 위하여 256비트 Valid Register를 이용하였다[6].

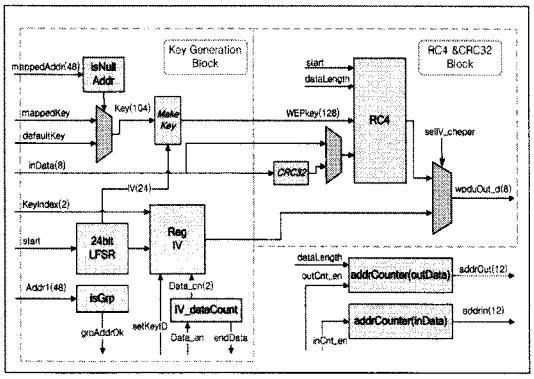

그림 2. WEP 하드웨어 구조
Fig. 2. WEP hard ware block diagram

3.3 TKIP 알고리즘 개요

TKIP는 WEP과 같이 RC4를 기반으로 하는 스트림 암호화 알고리즘이다. 하지만 WEP은 정적인 고유 비밀 키를 사용하는 반면에, TKIP는 인증과정에서 동적으로 생성된 TK(Temporal Key)와 MPDU마다 증가하는 카운터인 TSC(TKIP Sequence Counter)를 이용하여 공유 비밀키를 생성하여 데이터를 암호화 한다.

TKIP는 기존의 WEP의 보안상 문제점을 보완하기 위해 하드웨어로 구성된 RC4는 그대로 사용하고, 소프트웨어를 개선하여 사용할 수 있도록 함으로써 이미 배치되어 사용 중인 무선랜의 보안 문제점을 해결하자는 취지에서 개발된 보안 프로토콜이다[7]. TKIP는 TK와 TSC를 통해 MPDU(MAC Protocol Data Unit)가 전송될 때마다 다른 RC4의 seed값을 생성한다. seed값이 생성되는 과정은 크게 2단계의 과정을 통해 생성된다. 그림 3은 TKIP를 이용한 데이터 암호화를 나타내고 있다. Phase1에서는 TA(Transmitter Address)와 TK, TSC를 이용하여 128비트의 길이를 가지는 TTAK를 생성한다. Phase2에서는 Phase1에서 생성한 TTAK와 TK, TSC를 이용하여 RC4의 128비트 seed값을 생성한다. 각각의 연산 16비트 덧셈과 16비트 EXOR, 시프트로 이루어져 있다[2].

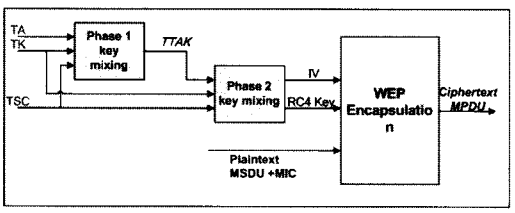

그림 3. TKIP 암호화 과정 블록도
Fig. 3. TKIP encapsulation block diagram

3.4 TKIP 알고리즘 하드웨어 구현

앞서 언급한 것과 같이 TKIP 알고리즘은 기존의 WEP으로 구성되어 있는 무선랜 장비에 소프트웨어를 패치 하여 보안의 취약성을 보완하기 위해서 채택된 알고리즘이다. 그러나 본 논문에서는 TKIP를 하드웨어로 구성하였다. TKIP에서 키를 동적으로 생성하는 연산인 Phase 1과 Phase 2연산은 소프트웨어로 구성하였을 때, 하드웨어로 구성하였을 때보다 많은 오버헤드를 발생 시킨다. 그림 4는 Phase 연산을 소프트웨어로 동작시켰을 때와 하드웨어로 동작시켰을 때의 오버 헤드를 비교한 그림이다.

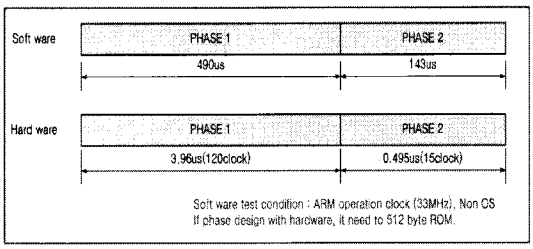

그림 4. TKIP Phase 연산의 동작 시간 비교
Fig. 4. Operation delay of the TKIP Phase

비교에 사용한 소프트웨어의 동작은 33MHz로 동작하는 ARM 프로세서를 이용하여 802.11i의 표준 문서의 참조 C언어 코드를 이용하여 동작시킨 것이다. Phase1에서의 동작 시간은 490us가 걸리고, Phase2에서는 143us가 걸렸다. 이에 비해 본 논문에서 제안하는 하드웨어 설계를 이용하여 동작을 하였을 경우에는 이보다 적은 3.96us와 0.495us가 소요되었다. 이러한 오버 헤드는 하나의 데이터를 전송 할 때마다 발생하게 된다. 그러므로 전송에 대한 오버헤드를 줄이기 위해서는 TKIP의 Phase 연산 또한 하드웨어로 구성하는 것이 올바른 선택이다.

Ⅳ. CCMP 하드웨어 구현

4.1 CCMP 알고리즘 개요

CCMP는 AES의 동작 모드 중에서 데이터의 기밀성을 위한 CTR (Counter mode) 모드와 인증 및 데이터의 무결성 검증을 위한 CBC-MAC (Cipher -Block Chaining Message Authentication Code)모드로 구성되어 있다[8]. CCMP에서 사용되는 AES는 128bit 크기의 비밀키와 128bit의 데이터 블록으로 암·복호 연산을 한다.

4.1.1 무결성 검증을 위한 CBC-MAC 모드

CBC-MAC 모드는 인증과 전송 데이터의 무결성을 검증하기 위한 MIC(Message Integrity Code)를 생성한다. 128비트의 MIC_IV는 TK를 키값으로 AES에 의해 암호화된다. 128비트의 암호화된 데이터는 다시 MIC_ HEADER1과 EXOR 연산된 후에 다시 AES에 의해 암호화된다. 그 결과 값은 다시 MIC_HEADER2와 EXOR 연산을 하고 AES에 의해 암호화 된다. 위와 같은 방법으로 CBC-MAC은 체인형태의 연산을 통해 최종적으로 MIC를 생성한다.

4.1.2 기밀성을 위한 CTR 모드

CTR 모드는 AES가 블록 암호 알고리즘으로 채

택되면서 새롭게 추가된 모드이다[9]. CTR 모드는 AES의 복호 연산 없이 데이터의 암호화와 복호화가 가능한 구조로 되어 있어, 적은 하드웨어를 통해 구현이 가능하다. CTR 모드는 128비트의 카운터 값을 AES로 암호화 하고, 그 결과 값을 평문의 128비트와 EXOR 연산을 통해 데이터를 암호화 한다. 암호화에 사용되는 카운터는 MPDU의 헤더로 구성된 Nonce와 16비트 카운터로 구성되어 있다.

4.2 CCMP 하드웨어 구현

CCMP은 IEEE 802.11n에서 규정하고 있는 HT(High Throughput) STA에서 기본적으로 사용되는 알고리즘이다. 추후 IEEE 802.11n에서도 사용이 가능하도록 로직의 크기보다는 빠른 동작속도에서 동작하도록 설계를 하였다. 또한 기존 논문에서는 1개의 AES 코어를 통해 순차적으로 CBC-MAC 모드와 CTR 모드를 연산 하거나, 2개의 AES 코어를 통해 2가지의 모드를 연산하는 것에 비해 효율적인 하드웨어 면적을 위해 동시에 1개의 AES 코어를 이용하여 2가지의 모드를 동시에 동작하도록 설계되었다. 그러기 위해서 본 논문에서의 AES 코어는 2단의 파이프 라인으로 동작하도록 설계되었다.

그림 5는 본 논문에서 제안하는 CCMP의 블록도이다. 입출력 인터페이스는 8비트로 설계되었으며, start 신호가 'Active high'가 되면 MAC Layer의 전 블록인 fragment 블록에서 MPDU의 헤더 정보를 읽어와 CBC-MAC 모드에서 사용할 데이터를 생성한다. MIC_HEADER2가 AES에서 암호화되는 동안 8비트 입력 포트를 통해 평문을 입력 받게 된다. 2번째 평문이 암호화 되는 동안 CTR 모드를 통해 암호화된 1번째 128비트 데이터는 8비트씩 출력포트를 통해 다음 블록인 전송 버퍼에 저장된다.

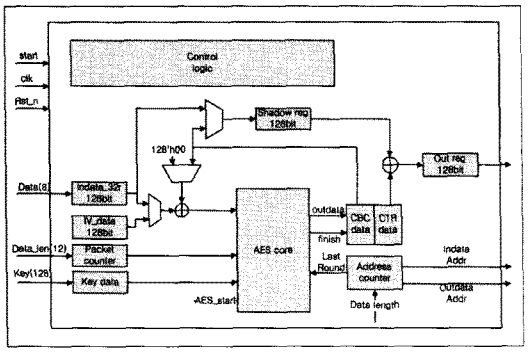

그림 5. 설계된 CCMP의 블록도
Fig. 5. diagram of the designed CCMP core

AES에서 가장 많은 로직을 필요로 하는 부분은 SubBytes를 연산 할 때 사용되는 S-BOX 부분이다[10]. 본 논문에서는 composite field 연산 방법을 이용하여 S-BOX를 구현하여 하드웨어의 면적을 최소화하도록 하였다[11].

V. 802.11i MAC Layer 하드웨어 구현

5.1 802.11 MAC Layer의 구조

802.11의 MAC Layer에서는 무선 매체에 접근하기 위한 방법으로 경쟁 기반의 분산 조정 함수(DCF : Distributed Coordination Function)와 비경쟁 기반의 포인트 조정 함수(PCF : Point coordination Function)를 사용한다. DCF는 CSMA/CA(Carrier Sensing Multiple Access with Collision Avoidance)를 기반으로 하고 있다. DCF를 통해 채널에 접근을 원하는 단말기들은 프레임을 전송하기 전에 채널이 사용 중인지를 확인하고, 채널이 비어 있을 경우에 충돌을 피하기 위해 프레임을 전송하기 전에 임의 시간동안 백오프를 수행한다[2], [3]. PCF는 DCF보다 우선권을 가지고 있지만 이 기능은 선택적으로 구현될 수 있으며, 현재 출시된 제품에서는 대부분 구현되어 있지 않다[3]. 따라서 본 논문에서 설계한 MAC layer는 DCF만을 통해 무선 채널에 접근을 한다. MAC Layer는 무선 채널의 접근을 관리하는 것 외에도 MPDU 송수신, 주소할당, 프레임 형성, 에러검사, 조각화(Fragment)와 조립(Defragment)을 수행한다.

5.2 802.11i MAC Layer 하드웨어 구현

본 논문에서 사용하고 있는 IEEE 802.11 MAC layer 하드웨어는 참고 논문[12]에서 설계된 하드웨어를 이용하였다. 해당 MAC layer 하드웨어는 MAC 프로토콜을 제어하는 부분과 MSDU 및 MPDU를 생성하여 PHY layer로 전송하는 부분을 하드웨어로 설계하여 소프트웨어에서 Aggregation 기능을 추가할 경우, IEEE 802.11n에서도 사용 가능하도록 설계되어 졌다.

그림 6은 본 논문에서 사용하는 802.11i MAC layer 하드웨어 구조를 나타낸 블록도이다. 그림6에서 TxCoord 블록과 RxCoord 블록은 MAC layer에서 핵심이 되는 기능인 DCF 컨트롤 블록으로 빠른 데이터 처리를 요구하는 연산 블록은 없지만, 프로토콜을 제어하기 위한 복잡한 제어 신호를 처리 할 수 있도록 FSM(Finite State Machine)기반의 구조

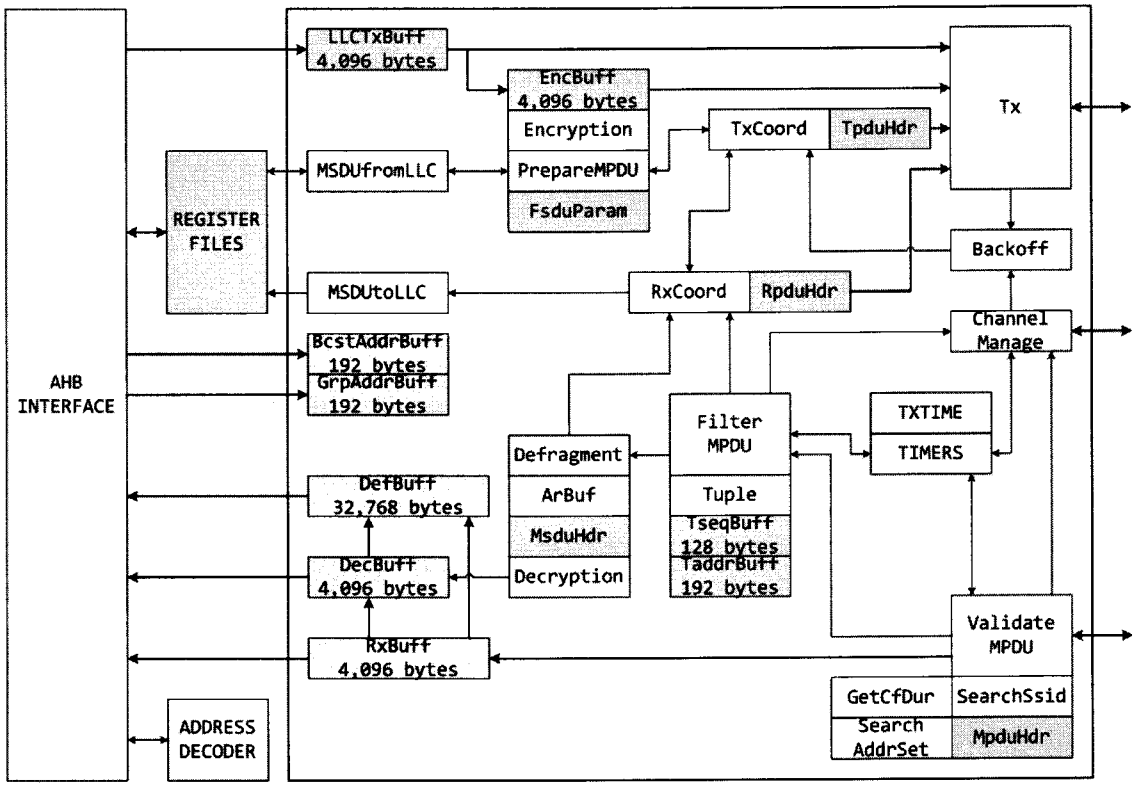

그림 6. 802.11 MAC layer 하드웨어 구조도
Fig. 6. block diagram for MAC layer hardware

로 되어 있다. TxCorrd 블록은 DCF를 제어하기 위한 신호와 SIFS 구간 타이머와 백오프를 제어한다. RxCoord 블록은 물리계층에서 데이터 수신이 완료된 후 ACK 응답과 CTS 응답 혹은 LLC계층과 MLME 블록으로 데이터의 수신확인을 요청하는 역할을 수행한다. 또한 하드웨어 블록들 사이의 복잡한 신호를 Queue구조를 이용하여 순차적으로 처리할 수 있게 하였다. 802.11i MAC layer 하드웨어는 소프트웨어와의 연결을 위하여 AHB 인터페이스를 사용하여 설계하였다.

Ⅵ. 802.11i MAC Layer 검증 및 성능

본 논문에서 제안하는 802.11i MAC layer 하드웨어의 구현 및 검증은 Xilinx사의 ISE 9.1버전을 이용하여 Virtex-5 LX330을 타켓 디바이스로 하여 합성하고 검증 하였다. 검증 플랫폼은 ARM926EJ-S 코어타일과 휴인스사의 RPS-3000보드를 이용하였다. 802.11i MAC layer간의 데이터 통신 검증은 타겟 FPGA에 2개의 MAC layer를 합성하였으며, 각각의 MAC layer 모듈들은 기본적인 기능을 가진 가상 PHY layer 하드웨어를 통해 연결하여 각각의 MAC layer가 데이터 전송이 가능하도록 구성하였다.

6.1 WEP 및 TKIP 검증 및 성능 평가

본 논문에서 설계한 WEP과 TKIP는 동일하게 RC4를 통해 데이터를 암,복호화를 한다. 그러므로 RC4 하드웨어를 공유하여 사용하며, Key 스트림을 생성하는 부분만 다르다. 그림 7은 클록에 따른 WEP과 TKIP의 동작 순서를 나타내고 있다. TKIP는 WEP과 비교해서 TK를 이용하여 KEY를 생성하는 Phase 연산이 추가되어 135클록이 더 소요가 된다. RC4는 S배열을 랜덤화 하기 위한 초기 동작에서 768클록이 소요되며, 이 지연 시간 후에 3클록마다 8비트의 데이터를 암호 및 복호화를 하는 구조로 되어 있다. 해당 구조에서의 암호화 데이터 스루풋(throughput)과 레이턴시(latency)는 다음 식 (1)에 의해 정의 되어질 수 있다[8].

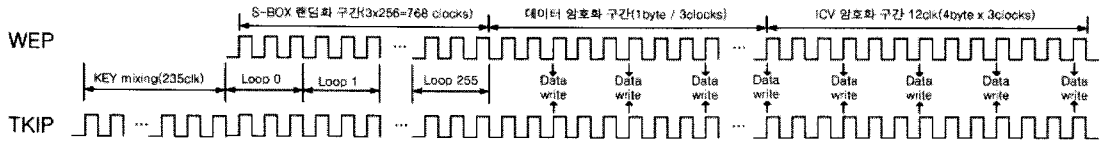

그림 7. WEP 및 TKIP 동작 타이밍도
Fig. 7. Processing timing diagram of WEP and TKIP

$$Throughput\ of\ RC4processor(bps) = \frac{8\times f}{3}$$
$$Latency(\ m\ of\ clock) = 3\times 256 \quad (1)$$
$$where\ f = clock frequency$$

설계된 RC4 모듈은 735개의 LUT와 456개의 레지스터, S-BOX에서 사용되는 256바이트의 듀얼포트 SRAM을 이용하고 있다. data path 지연 시간은 4.482ns (3.017ns logic, 1.465ns route)이고, 해당 타겟 FPGA에서 최대 동작 주파수는 186.7MHz이다. 그러므로 최대 동작 주파수와 식(1)에 의해 설계된 RC4의 스루풋은 497.8Mbps의 데이터 암호화 율을 가짐을 알 수 있다.

6.2 CCMP 검증 및 성능 평가

CCMP의 동작 검증은 802.11i 표준[2]에서 제시하고 있는 테스트 벡터를 이용하여 시뮬레이션을 통해 검증을 하였고, 설계된 802.11 MAC layer에 연동하여 FPGA를 통해 전체적인 동작 검증을 수행하였다.

표 1에서와 같이 설계된 CCMP 모듈은 3257개의 LUT와 1520개의 레지스터를 이용하고 있다. data path 지연 시간은 8.187ns (4.246ns logic, 3.941ns route)로 해당 타겟 FPGA에서 최대 동작 주파수는 134MHz이다. 설계된 CCMP에서 사용하고 있는 AES 코어의 성능은 다음의 식(2)에 의해서 정의 할 수 있다[10].

$$AES코어성능 = (128 \div (N_r + 1)) \times f \quad (2)$$

위의 식에서 f는 동작 클록 주파수를 나타내며, Nr은 AES의 동작 라운드 수를 나타낸다. 본 논문에서 설계된 AES 코어는 1라운드를 2클록에 수행하므로, 전체 동작 라운드 수는 21이 되며, 동작 주파수 134MHz를 식(2)에 대입하면 AES 코어 성능은 816.7Mbps가 된다. 이는 IEEE 802.11 a, g에서의 최대 전송 속도인 54Mbps를 충분히 만족시키며, IEEE 802.11n의 최대 전송 속도인 600MHz 또한 충분히 만족시킴을 알 수 있다.

표 2는 기존 논문과의 성능 비교를 나타내고 있다. 본 논문과 기존 논문에서의 데이터 처리 속도는 IEEE 802.11n의 최대 전송 속도인 600Mbps 이상을 보이고 있다. 논문 [13], [15], [16] 경우, 본 논문에서 제안하는 AES 코어 보다 빠른 데이터 처리 속도를 보이고 있다. 그러나 기존 논문에서의 AES 구조를 이용하여 CCMP를 구성할 경우 2개의 AES 코어가 필요하기 때문에 표에서 나와 있는 slice의 수의 2배가 필요할 뿐만 아니라 IEEE 802.11n의 최대 전송 속도인 600Mbps 보다 월등히 높아 필요 이상의 속도를 보인다고 볼 수 있다. 그러므로 본 논문에서 제안 하는 AES 구조는 IEEE 802.11n의 최대 전송 속도인 600Mbps를 만족하면서 하드웨어

표 1. 각 하드웨어 FPGA 합성 결과
Table 1. FPGA synthesis result of hardwares

Logic Utilization	RC4	CCMP	MAC LAYER
Number of Slice Registers	456	1,520	17,727
Number of Slice LUTs	735	3,257	27,203
Number of fully used Bit Slice	87	1,020	9,709
Number of bonded IOBs	174	396	157
Number of Block RAM/FIFO	1	0	24
Number of BUFG/BUFGCTRLs	1	1	2

표 2. AES 알고리즘의 FPGA 구현 성능 비교
Table 2. Comparisons of FPGA Implementations of the AES Algorithm

비교 논문	Slices	Clock (MHz)	Throughput (M bps)
[13]	4189	65	1190
[14]	4325	75	739
[15]	10992	141	1940
[16]	6766	194	2257
ours	2489	134	816

의 면적이 기존 논문에서 제안하는 구조보다 작아 CCMP에 사용하기에 가장 효율적인 설계라고 할 수 있다.

6.3 802.11i MAC layer 검증 및 성능 평가

802.11 MAC layer의 전체 검증 방법은 다음과 같다. 구동 프로그램은 MAC layer의 버퍼로 데이터를 쓰고, 레지스터 파일을 통해 MaUnitdata request 신호를 준다. 신호를 받은 MAC 하드웨어 모듈은 다른 MAC 하드웨어 모듈로 802.11i 프로토콜을 통해 데이터를 암호화 하여 전송한다. 데이터를 전송 받은 다른 MAC layer 하드웨어 모듈은 데이터를 복호화하고, 유효성 검사를 한다. 수신된 데이터가 유효하면 데이터를 버퍼에 저장한 후에 레지스터 파일에 MaUintdata indication 정보를 기록한다. 동작 프로그램은 레지스터 파일에서 수신된 데이터의 정보와 데이터를 읽어 온다.

설계된 IEEE 802.11i를 지원하는 MAC layer 하드웨어는 해당 타겟 FPGA에서 27,203개의 LUT와 17,727개의 레지스터를 이용하고 있다. 데이터를 저장하기 위한 SRAM은 274k bit의 Block RAM을 사용하였다.

본 논문에서 설계한 802.11i를 지원하는 MAC 하드웨어 설계는 삼성 0.18um CMOS 표준 라이브러리를 사용하여 MPW 공정으로 칩을 제작 중이다.

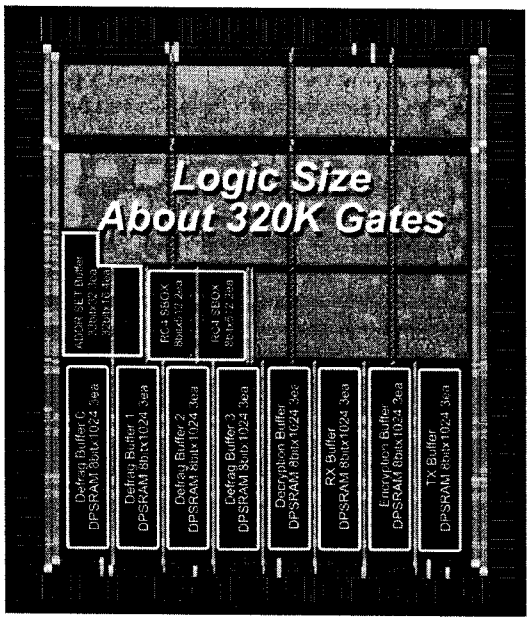

그림 8. IEEE 802.11i MAC 레이아웃
Fig. 8. 802.11i MAC hardware ASIC layout

Synopsys사의 Design Compiler를 이용한 MAC 하드웨어의 합성 결과는 314,820 gate count를 가지며, 189K bits의 메모리를 사용했다. 최대 동작 속도는 182MHz로 목표 동작 클록 속도인 100MHz를 만족한다. 이는 동작 클록 속도가 100MHz일 때, 수식 2를 통해 609Mbps의 AES 성능을 가짐을 알 수 있다. 그러므로 동작 클록 속도가 100MHz일 때, 본 설계는 IEEE 802.11n의 성능을 만족 시킬 수 있음을 나타낸다. 그림 8는 Synopsys사의 Astro 툴을 이용하여 백엔드 작업을 한 레이아웃을 보여주고 있다.

Ⅶ. 결 론

본 논문은 참고 논문 [12]에서 제안하는 IEEE 802.11 MAC layer 하드웨어 모델을 이용하여 IEEE 802.11a,g에서의 데이터 암,복호 메커니즘인 WEP 뿐만 아니라 IEEE802.11i에서 제안하는 TKIP와 CCMP를 포함한 IEEE 802.11i를 지원하는 MAC layer 하드웨어를 설계하였다. WEP 및 TKIP의 설계에서는 효율적인 RC4 설계를 통해 적은 면적을 가지도록 설계의 초점을 맞추어 설계를 하였으며, CCMP의 설계에서는 IEEE 802.11n에서도 적용이 가능하도록 최대 전송 속도인 600Mbps 이상의 스루풋을 가지도록 빠른 동작 속도에 초점을 맞추어 설계를 하였다. 또한 효율적인 하드웨어 면적을 위해 2단 파이프라인 구조의 AES 코어를 제안하여 CCMP 동작에 필요한 CBC 모드와 CTR 모드를 1개의 AES를 이용하여 처리하도록 하였다. MAC layer는 프로토콜의 제어와 데이터의 전송 부분을 하드웨어로 처리하여 IEEE 802.11n에서의 Aggregation 기능을 이용할 경우, 100MHz이상의 데이터 전송 속도를 가질 수 있도록 설계를 하였다. 이에 본 논문에서 제안하는 802.11i를 지원하는 MAC layer 하드웨어는 802.11n으로 확장 가능한 하드웨어 구조를 가진다는 것을 알 수 있다.

참 고 문 헌

[1] "한국 무선랜 장비 시장 분석 및 전망 보고서", *IDC* 2008-2012

[2] "Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," *IEEE,* IEEE standard P802.11-REVma, 2006.

[3] Matthew S. Gast, "*802.11 Wireless Networks : The Definitive Guide*", 2nd Edition, O'Reilly , April 2005.
[4] IEEE P802.11n/D2.00, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," Feb. 2007.
[5] S. Fluhrer, I. Mantin, and A. Shamir. "Weaknesses in the key scheduling algorithm of RC4" In Eighth Annual Workshop on Selected Areas in Cryptography, Toronto, Canada, Aug. 2001.
[6] 최병윤 외, "RC4 스트림 암호 알고리즘을 위한 고속 연산구조의 FPGA 구현 및 성능 분석", 정보보호학회논문지 vol.14 No.4, August 2004.
[7] 정병호 외, "공중 무선랜 망에서 인증 및 키관리 기술 동향" 전자통신동향분석 17권 제4호, August 2002.
[8] R. Housley, D. Whiting and N. Ferguson, "Counter with CBC-MAC (CCM) : AES Mode of Operation, Proposed to NIST, June 2002.
[9] Draft NIST Special Publicatin 800-38C, "Recom mendation for Block Cipher Modes of Operation : the CCM Mode for Authentication and confidentiality," U.S. Doc/NIST, May 2004
[10] 안하기 외, "AES Rijndael 블록 암호 알고리듬의 효율적인 하드웨어 구현", 한국 정보보호학회논문지, 제12권 2호, pp.53-64, 2002.
[11] V. Rijndael, "Eifficient implementation of the Rijndael S-box," http://www.esat. kuleuven.ac.be/~rijnmen/rijndael/sbox.pdf
[12] 이영곤 외, "차세대 무선랜 구현을 위한 MAC 엔진 설계 및 구현" 대한전자공학회논문지, 제 46권 6호, 2009
[13] Refik Sever A. Neslin Ismailoglu Yusuf Q. Tekmen Murat Askar Burak Okcan, A High Speed FPGA Implementation Of The Rijndael Algorithm. "Euromicro Symposium on Digital System Design, Architectures, Methods and Tools", (2004)
[14] Chitu, C. Chien, D. Chien, C. Verbauwhede, I. Chang "A Hardware Implementation in FPGA of the Rijndael algorithm" Dept. of Electr. Eng., Univ. of California, Los Angeles, CA, USA
[15] A.J. Elbirt, W. Yip, B. Chetwynd, and C. Paar, "An FPGA Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists," Proc. Third Advanced Encryption Standard (AES) Candidate Conf., Apr. 2000.
[16] C. SivakumarI and A .Velmurugan, "High Speed VLSI Design CCMP AES Cipher for WLAN (IEEE 802.11i)", IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. pp.398-403. Feb. 22-24, 2007.

홍 창 기 (Chang-ki Hong) 준회원

2007년 2월 광운대학교 전자공학과
2008년 3월~현재 광운대학교 전자통신공학과 석사과정
<관심분야> 무선통신, SoC설계, 신호처리,임베디드 시스템

정 용 진 (Yong-jin Jeung) 정회원

1983년 서울대학교 제어계측공학과 학사
1983년 3월~1989년 8월 한국전자통신연구원.
1995년 미국 UMASS 전자전산공학과 박사
1995년 4월~1999년 2월 삼성전자 반도체 수석 연구원.
1999년 3월~현재 광운대학교 전자통신공학과 교수
<관심분야> 무선통신, 정보보호, SoC 설계, 영상처리 및 인식, 임베디드 시스템