효율적인 CCMP 코어 설계

성윤종*, 권성구*, 배두현*, 박세현*, 송오영*

*중앙대학교 전자전기공학부

An Efficient Design of CCMP for Robust Security Network

Yun-Jong Sung*, Sung-Gu Kwon*, SungDu-Hyun Bae*, Se-Hyun Park*, Oh-Young Song*

*School of Electrical & Electronic Engineering Chung Ang University.

요 약

IEEE 802.11e 과 IEEE 802.11n에서 data의 높은 전송률을 구현하기 위해 Block Ack와 frame agegation 과 같은 새로운 mechanism이 논의 되고 있다. 이러한 mechanism은 각각의 MPDU processing 마다 짧은 응답시간을 요구한다. 본 논문에서는 위의 새로운 MAC을 지원하는 IEEE 802.11i를 위한 효율적인 CCMP 설계를 제안한다. 제안된 설계에서는 한 AES-CCM core에서 MIC calculation 과 정보 암호화가 128bit씩 순차적으로 수행되어지는 mode toggling 접근을 채택했다. 본 설계에서는 응답시간이 44 clock cycle의 짧은 짧은 시간으로 줄었다. 또한 하나의 AES-CCM core를 사용하고 낮은 주파수에서 수용할만한 data throughput과 응답시간을 얻었기 때문에 하드웨어적인 복잡성과 전력 소모를 줄일수 있었다.

I. 서론

IEEE 802.11 standard가 발표 되었을때, WEP이라는 추가적인 보안 프로토콜을 포함하고 있었다. 하지만 IEEE 와 Wi-Fi는 WEP이 공격으로부터 안전하지 않다는 것을 알게 되고 IEEE 802.11 task group에서는 WEP (Wired Equivalent Privacy), TKIP (Temporal Key Integrity Protocol), 과 CCMP (Counter with CBC-MAC Protocol)을 사용하는 RSN (Robust Security Network) architecture을 발표 하였다.

CCMP에서는 data의 privacy를 제공하기위해 AES-CCM (Advanced Encryption Standard Counter with CBC-MAC) block cipher algorithm 을 사용한다. 암호화 가속과 MAC layer data throughput, secure operation과 interoperability 를 보장하기위해 CCMP operation은 WLAN device에 embedded화 되어야 한다.

IEEE 802.11e 과 IEEE 802.11n에서 data의 높은 전송률을 구현하기 위해 Block Ack와 frame agegation 과 같은 새로운 mechanism이 논의 되고 있다. 위 언급된 mechanism들은 MPDU간 time interval이 작기 때문에 cipher core로부터의 response time이 작아야 한다. 본 논문에서는 첫 번째 data의 입력 시점부터 처리되어 나오는 시간을 response time으로 정의 했으며 각각의 data는 128 bit으로 정의 했다. 주파수를 높임으로써 response time을 작게 할수 있지만 그만큼 전력 소비가 늘어난다. 무선환경에서 전력 소비가 중요한 요소임을 감안 하면 주파수를 높임으로써 성능을 향상시키는 것은 올바른 일이 아니라고 할 수 있다. 본 논문에서는 주파수를 높이지 않고 response time을 줄이는 CCMP 코어를 설계하고자 한다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(중앙대학교 홈네트워크 연구센터) 지원 사업의 연구결과로 수행되었음

본 논문에서는 순차적이고 병력적인 구조적인 접근 대신에, 차례로 MIC data를 계산하고 data를 암호화하는 CCMP core를 구현하였다. 제안된 설계에서는 병렬구조보다 가격면에서 우수하고 암호화, 복호화과정의 response time은 시간은 44 clock cycle 로 측정되었다

II. 본문

1. Efficient Architecture of CCMP

본 논문에서 제안한 design에서는 하나의 AES module이 MIC data를 계산하고 암호화한다. CCMP는 MIC data를 CBC-MAC 모드에서 계산하고 차례로 counter 모드에서 암호화를 수행한다. 다음의 Fig.1은 CCMP의 timing diagram을 나타내고 있다.

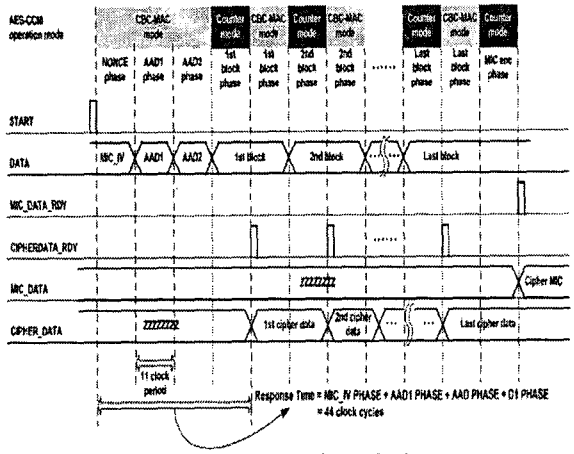

Fig.1 The encapsulation timing diagram of the CCMP

처음으로 CCMP core는 NONCE, Additional Authentication Data 1 (AAD1), AAD2를 계산하기 위해 CBC-MAC mode에서 동작한다. 두 번째로 data를 암호화 하기위해 counter mode에서 동작하며 차례로 MIC 계산을 하기 위해 CBC-MAC mode에서 동작한다. 각각의 phase는 11 clock cycle을 필요로 한다. 따라서 128 bit cipher data를 얻기 위해서 44 clock cycle이 걸린다. 본 논문에서 제안한 CCMP의 구조는 Fig.2에서 나타내고 있다.

CCMP는 AES module, Round Key Generator, Construction Block, Counter, Mode Controller, I/O Interface의 6개의 Block로 구성되어 있다. Construction Block는 PN과 MAC header로부터 NONCE와 ADD를 만들고 Round Key Generator는 seed key로부터 round key를 생성한다. Mode Controller는 AES module의 mode, 제어신호와 AES module의 입력 data를 control 한다. Counter는 간단한 16 bit counter로써 각각의 block에 적절한 counter value를 만들어 내는 역할을 한다.

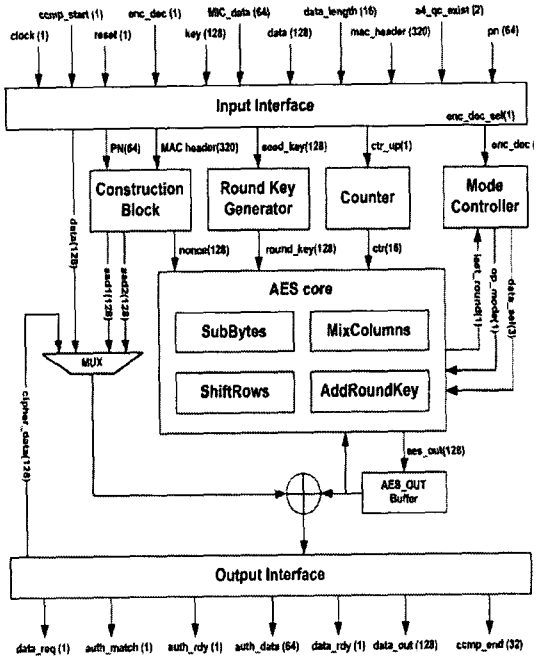

Fig.2 The architecture of the implemented CCMP

2. 구현 결과 및 비교

본 논문에서 구현한 CCMP 구조는 Quartus II compiler와 Altera Stratix FPGA (Field Programmable Gate Array) device를 사용했다. 표.1은 각각의 phase에 대한 clock cycle를 나타내고 있고 표.2는 다른 구조들과의 성능적인 비교를 보여주고 있다.

표.2에서 본 논문에서 구현한 구조가

Sequential 구조와 같은 data throughput을 나타내고 있고 응답시간은 확연히 나아진 것을 알 수 있다. 응답시간은 payload의 사이즈와 상관이 없고 clock 주파수와 관계가 있음을 알 수 있다.

Category	Cycles
CBC mode encryption	11 cycles
CBC mode MIC encryption	11 cycles
Counter mode encryption	11 cycles

표.1 Clock cycles for each phase in theimplemented CCMP

Category	Sequential Structure	Parallel Structure	Proposed Design
Data Throughput (Mbps)	285	562	285
Response Time (μs)	14.96	0.88	0.88

표.2 Performances for 1024 bytespayload at 50 MHz clock frequency

표.3은 다른 구조들과의 설계적인 차이를 보여주고 있다.주고 있다. 사용된 logic당 throughput은 다른 구조들과 거의 비슷하지만 50MHz의 주파수에서 1024 bytes의 프래임에 대한 응답시간에 대한 logic의 사용은 다른 구조와 비교해서 2배, 16배 정도 좋은 것으로 나타났다.

Category	Sequential Structure	Parallel Structure	Proposed Design
Logic Used (# : number of logic cells)	5437	9702	5605
Throughput / Logic usage (Kbps / #)	53.68	59.32	52.07
1/ Logic usage /ResponseTime (1 / # / sec)	12.29	117.13	202.74

표.3 Comparison with other implementation approaches

본 설계는 50MHz의 clock 주파수에서 285Mbps까지의 throughput을 낼 수 있고 이러한 결과는 모든 표준의 MAC data processing에 적용가능하다. IEEE 802.11b에서의 11Mbps, IEEE 802.11a와 802.11g에서의 54Mbps인 MAC Layer 의 data speed를 감안했을 때 충분한 성능을 낸다고 할 수 있다. 50MHz의 clock 주파수에서 0.88μs 의 response time은 802.11 표준의 새로운 MAC mechanism에 적용하기에 충분하다.

III.결론

새로운 MAC mechanism에 적용하기 위해서 chiper core는 충분이 작은 response time을 가져야 한다. 또한 낮은 전력 소비와 제조 비용을 위해 하드웨어의 복잡도도 고려 되어야 한다.

본 논문에서 제안한 효율적인 CCMP 구조는 802.11e의 Block Ack와 다른 802.11 표준의 frame aggregation과 같은 새로운 MAC mechanism에 mode toggling 접근 방식을 통해 적용 되어질 수 있다.

결과적으로 본 구조는 50MHz의 clock 주파수에서 285Mbps의 성능을 내고 응답시간은 44clock cycle이며 이러한 특징은 payload의 크기가 아닌 clock 주파수에 의존한다는 것이다.

본 구조는 낮은 주파수에서 짧은 응답시간과 높은 throughput을 낼 수 있기 때문에 전력 소비 측면에서 좋은 성능을 보여준다고 할 수 있고 새로운 MAC mechanism에 적용 될 수 있다.

[참고문헌]

[1] IEEE standard 802.11i, July 2004.

[2] IEEE standard 802.11e/D13.0 January 2005

[3] Duhyun Bae, Gwanyeon Kim, Jiho Kim, Sehyun Park, Ohyoung Song, "Design and Implementation of Efficient Cipher Engine for IEEE802.11i Compatible with IEEE802.11n and IEEE802.11e", LNAI 3802 Part, December 2005, pp.439-444, Springer-Verlag, Heidelberg 2005

[4] Duhyun Bae, Gwanyeon Kim, Jiho Kim, Sehyun Park, Ohyoung Song, "Design and Implementation of IEEE802.11i Architecture for Next Generation WLAN", LNCS 3822, December 2005, pp.246-357, Springer-Verlag, Heidelberg 2005