國立交通大學

電信工程研究所

碩士論文

一個802.11n通訊協定以WPA2加密之有效結構及其實現

Design and Implementation of an Efficient Structure of 802.11n with WPA2

研究生：邱鐙標

指導教授：李程輝　教授

中華民國　一零二年七月

一個 802.11n 通訊協定以 WPA2 加密之有效結構及其實現

Design and Implementation of an Efficient Structure of 802.11n with WPA2

研 究 生：邱鐙標　　Student：Teng -Piao Chiu
指導教授：李程輝　　Advisor：Tsern-Huei Lee

國 立 交 通 大 學
電機學院電信工程研究所碩士班
碩 士 論 文

A Thesis
Submitted to College of Electrical and Computer Engineering
National Chiao Tung University
for the Degree of
Master
in
Institute of Communication Engineering

June 2013

Hsinchu, Taiwan, Republic of China

中華民國 一零二 年七月

一個 802.11n 通訊協定以 WPA2 加密之有效結構及其實現

學生：邱鐙標　　指導教授：李程輝

國立交通大學電信工程研究所

摘　　要

隨著無線通訊的普及化，通訊品質及資訊安全變成一個重要的課題。802.11n 是一種現今被普遍使用的 **WLAN**(Wireless Local Area Network) 技術，其中包含了封包聚合技術(Frame Aggregation)及其他技術來提升傳輸速度。另外也包含 **WPA2**(Wi-Fi Protected Access 2) 這種安全機制以保護傳輸過程中資料不被竊取或竄改。但是這兩個機制卻沒有被同時考慮，因此當使用者開起 **WPA2** 來進行保護時，傳輸的速率會急速下降。

在本篇論文中，我們提出運用分割式計數器模式密碼塊鏈消息完整碼協議的複合結合式自動回覆請求 (Aggregated Hybrid Automatic Repeat Request Mechanism with Fragmentation Counter Mode with CBC-MAC Protocol, AH-FCCMP)使得用戶在保證安全傳輸的情況下，也能有良好的傳輸品質。這個機制利用改變 CCMP 的運算方式，使得資料傳輸與加解密運算可以同步運算，以達到整體運算時間的減少。模擬結果顯示我們提出的 AH-FCCMP 機制能達到比傳統機制高的系統傳輸量，並保證資訊安全上的需求。

關鍵字：Wi-Fi, 802.11n, 自動回覆請求, WPA2

Design and Implementation of an Efficient Structure of 802.11n with WPA2

Student：Teng-Piao Chiu　　Advisors：Prof. Tsern-Huei Lee

Institute of Communication Engineering
National Chiao Tung University

ABSTRACT

Since the spread of wireless communication, it is more and more important about transmission rate and information safety. 802.11n is one of the famous technology in **WLAN** (Wireless Local Area Network), which boosts its own transmission speed by frame aggregation (**FA**) and other core technologies. Furthermore, it also contains **WPA2**(Wi-Fi Protected Access 2), which provides secure mechanism for preventing data eavesdropped or stolen during transmission. However, these two features are not taken into consideration together. If users switch on **WPA2** for secure purpose during **802.11n** transmission, the system throughput will nosedive.

In this thesis, we propose **AH-FCCMP** (Aggregated Hybrid Automatic Repeat Request Mechanism with Fragmentation Counter Mode with **CBC-MAC** Protocol), which provides high transmission speed under data transfer safety. This mechanism change the architecture of **CCMP** for computing encryption/decryption and receiving data in parallel, so the total service time can be reduced. The simulation result shows that **AH-FCCMP** provides higher system throughput than the original one and the requirement of information security.

Keywords: Wi-Fi, 802.11n, ARQ, WPA2

誌　　謝

在完成這篇論文的過程中，我接受了許多人的幫忙與協助，在此我想向他們致上最高的敬意。首先要感謝我的指導教授－李程輝教授。他總是能點出問題的所在並不辭辛勞地教導著我許多作研究的方法以及該有的態度，在這兩年的研究生活中，我學習到許多專業領域的知識和獨立研究的能力，更重要的是，老師也教導了我許多對研究以及做事的正確態度。相信這段經歷在未來的道路上，會是一股強大的助力。

也感謝我的父母及大哥－邱國濱先生、陳燕子女士與邱榮標先生。感謝父母對我的養育之恩，並且在我的求學生涯裡，一路上對我的支持與鼓勵。

再來也要感謝交大電信所 NTL 實驗室的各位同伴，在這兩年的研究生涯裡，學長姐的熱心指導、同窗好友的互助合作及學弟妹們帶給實驗室的活力與歡笑，都是支持我完成學業的最大推力。謝謝你們給我適時的鼓勵與陪伴，讓我能夠順利的完成這兩年的學業。

最後也感謝我的好友們，在我煩惱焦慮時，陪我舒壓解悶，一直以來給我精神上的支持與鼓勵。

最後謹將此論文獻給身邊所有愛我的人及我愛的人。

2013/08　邱鐙標

Contents

List of Figures

List of Tables

Chapter 1.

Introduction

IEEE 802.11 Wireless Local Area Network(**WLAN**) provides wireless communication over short distances. Many users have switched from using wired networks to using **802.11 WLAN** as their primary network connection media because it is easily deployed and can be used without the wire connection. Nevertheless, the open media in **WLAN** leads lots of security vulnerabilities, the security requirement is more and more important nowadays.

The traditional **802.11 a/b/g WLAN**s use the **DCF**(Distributed Coordination Function) for accessing the shared wireless medium, which employs the **CSMA/CA**(Carrier Sense Multiple Accesses with Collision Avoidance) algorithm. However, researches have shown that the **MAC** layer overhead is the main reason for their inefficiency. For increasing the demand of data-intensive applications over **WLAN**, the **IEEE 802.11n WLAN** is being standardized with new medium access control (**MAC**) and physical layer (**PHY**) specifications[3]. This new design increases the **WLAN** throughput above 100Mbps, comparable to 100Mbps Fast Ethernet. The backward compatibility with **802.11 a/b/g** devices is also a critical design requirement. These goals are aided by improvements in radio technology, such as the **OFDM**(Orthogonal Frequency Division Multiplexing) modulation method and the **MIMO** (Multiple Input Multiple Output) antenna, and the enhanced **PHY** mode also works for the same purpose. **802.11n** can provide a network with longer range and higher speed data transmission and theoretically reaches a maximum raw **PHY** data rate of

600Mbps, compared to the 54Mbps data rate in the previous **802.11 a/b/g** standards.

For reliable data transmission, we need to design lots of error-free methods. We use strong and reliable error correction code in those services with strict delay requirements, such as voice and video stream, and we apply **ARQ**(Automatic Repeat Request) protocol usually for delay-tolerant wireless data transmission. Frame aggregation and block acknowledgement are defined in **802.11n** for reducing **MAC** layer overhead and boosting the total channel utilities. Furthermore, Aggregated Selective Repeat ARQ (**ASR-ARQ**) and Aggregated Hybrid ARQ(**AH-ARQ**)[7][8] are proposed to increase the tolerance of error occurrence.

However, those modification improves the throughput but not take account into security issues. **802.11i**[2] is an amendment which is raised for secure **WLAN**, and the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol(**CCMP**)[12] is the main replacement for **WEP** and **WPA**, which are raised for **WLAN** security in 1997 and 2003 respectively. **CCMP** contains two parts, **MIC**(Message Integer Checksum) computation and **CTR**-mode encryption, for different purposes of security. The cascade of **AH-ARQ** and **CCMP** limits the speed of total throughput. But the transmitting/receiving chip and the encrypt/decrypt chip usually work in different parts in one device, we propose a new structure of **CCMP, FCCMP**(Fragmentation **CCMP**), which can reduce the processing time by using both chips simultaneous.**AH-FCCMP** is an architecture that consider not only retransmission mechanism but also security algorithm for less efficiency waste.

The reminder of this thesis is organized as follows. **Chapter 2** describes the system model and some related work. And **Chapter 3** formulates the **AH-ARQ** and **FCCMP** algorithms and the hybrid architecture, **AH-FCCMP**. Simulation results and discussions are provided in **Chapter 4**, and the conclusion of our work is in **Chapter 5**.

Chapter 2.

Related work

2.1 IEEE 802.11 family

In 1997, the **IEEE**(Institute of Electrical and Electronics Engineers) created the first WLAN standard which is called it 802.11 after the name of the group formed to oversee its development. The 802.11 family consist of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The original version, **802.11-1997**, was released in 1997 but it was widely accepted by new amendment, **802.11b**, which is applied **OFDM**(orthogonal frequency-division multiplexing) technology until 1999. The following amendment such as **802.11a** and **802.11g** were raised for higher throughput in 1999 and 2003 respectively.

Because these three protocol utilize different frequencies, 2.4 GHz band for **802.11b/g** and 5 GHz band for 802.11a, the **802.11a** is incompatible with the other two. **802.11n** is developed in order to improve the data transmission rate to 600**Mbps** by **MIMO**(Multiple-Input-Multiple-Output), a new multi-streaming modulation technique, and is incompatible with **802.11a/b/g** because of operating on both the 2.4 GHz and the 5 GHz bands. Other standards in the family, such c, e, i, are service amendments and extensions or corrections to the previous specifications.

2.1.1 IEEE 802.11n

IEEE 802.11n is an amendment to the **IEEE 802.11-2007** wireless networking standard[1][10].The main purpose is to improve network throughput over those two previous standards, **802.11a** and **802.11g**. The significant incensement in the maximum data rate from 54 Mbps to 600 Mbps in 4x4 **MIMO** configuration and 40 MHz bandwidth.

In **PHY** layer, there are several modification for improvement. First, the **OFDM**'s subcarriers is increased from 48 to 52 which improves the maximum throughput from 54 Mbps to 58.5 Mbps. Second, the highly efficient **FEC**(Forward Error Correction) code, **LDPC**(low-density-parity-check), is applied and this new puncturing mode makes the coding rate rise from 3/4 to 5/6 boosting the data rate to 65Mbps. Third, the **GI**(guard-interval), which is the interval between **OFDM** symbols, is reduced from 800ns to 400ns and the throughput increased to 72.2Mbps. Forth, doubling bandwidth from 20MHz to 40 MHz gains slightly more than double the rate from 72.2Mbps to 150Mbps. The last, the use of **MIMO SDM**(Spatial Division Multiplexing), which spatially multiplexes multiple independent data streams, can significantly increase data throughput as the number of resolved spatial data streams is increased. **802.11n** supports four spatial streams at most and the data rate grows up to 600Mbps. Various modulation schemes and coding rates are represented by **MCS**(Modulation Coding Scheme) index value and the configurations between the different values show in **Table. 1**.

MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbps)				MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbps)			
				20 MHz channel		40 MHz channel						20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI					800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15	16	3	BPSK	1/2	19.5	21.7	40.5	45
1	1	QPSK	1/2	13	14.4	27	30	17	3	QPSK	1/2	39	43.3	81	90
2	1	QPSK	3/4	19.5	21.7	40.5	45	18	3	QPSK	3/4	58.5	65	121.5	135
3	1	16-QAM	1/2	26	28.9	54	60	19	3	16-QAM	1/2	78	86.7	162	180
4	1	16-QAM	3/4	39	43.3	81	90	20	3	16-QAM	3/4	117	130	243	270
5	1	64-QAM	2/3	52	57.8	108	120	21	3	64-QAM	2/3	156	173.3	324	360
6	1	64-QAM	3/4	58.5	65	121.5	135	22	3	64-QAM	3/4	175.5	195	364.5	405
7	1	64-QAM	5/6	65	72.2	135	150	23	3	64-QAM	5/6	195	216.7	405	450
8	2	BPSK	1/2	13	14.4	27	30	24	4	BPSK	1/2	26	28.8	54	60
9	2	QPSK	1/2	26	28.9	54	60	25	4	QPSK	1/2	52	57.6	108	120
10	2	QPSK	3/4	39	43.3	81	90	26	4	QPSK	3/4	78	86.8	162	180
11	2	16-QAM	1/2	52	57.8	108	120	27	4	16-QAM	1/2	104	115.6	216	240
12	2	16-QAM	3/4	78	86.7	162	180	28	4	16-QAM	3/4	156	173.2	324	360
13	2	64-QAM	2/3	104	115.6	216	240	29	4	64-QAM	2/3	208	231.2	432	480
14	2	64-QAM	3/4	117	130	243	270	30	4	64-QAM	3/4	234	260	486	540
15	2	64-QAM	5/6	130	144.4	270	300	31	4	64-QAM	5/6	260	288.8	540	600

Table. 1 Relationship between MCS index and other configuration

In **MAC** layer, frame aggregation(**FA**) and block acknowledgement(**BA**) are applied for reducing the cost due to the large amount of overhead compared to wired network protocol, especially in the inter-frame spaces and control frames such as acknowledgements. Each **802.11** frame has fixed overhead in the radio preamble and **MAC** frame fields. Even that **802.11n** supports high data rate, the fixed overhead restricts actual throughput. Frame aggregation, in simple terms, puts more than one frame together into a single transmission with the same header and declines the collision probability for less time loss to back-off. **802.11n** includes two methods for frame aggregation: **MAC** Service Data Units aggregation(**A-MSDU**) and Message Protocol Data Unit aggregation (**A-MPDU**). Both aggregation methods reduce the overhead to only a single radio preamble and **MAC** headers for each frame transmission. To compensate for the larger aggregated frame size, **802.11n** also has augmented the maximum frame size from 4KB to 64KB.

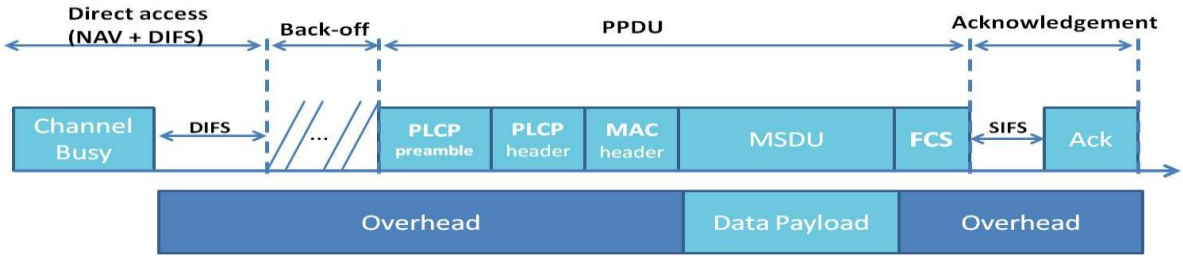

Fig. 1 DCF basic Operation

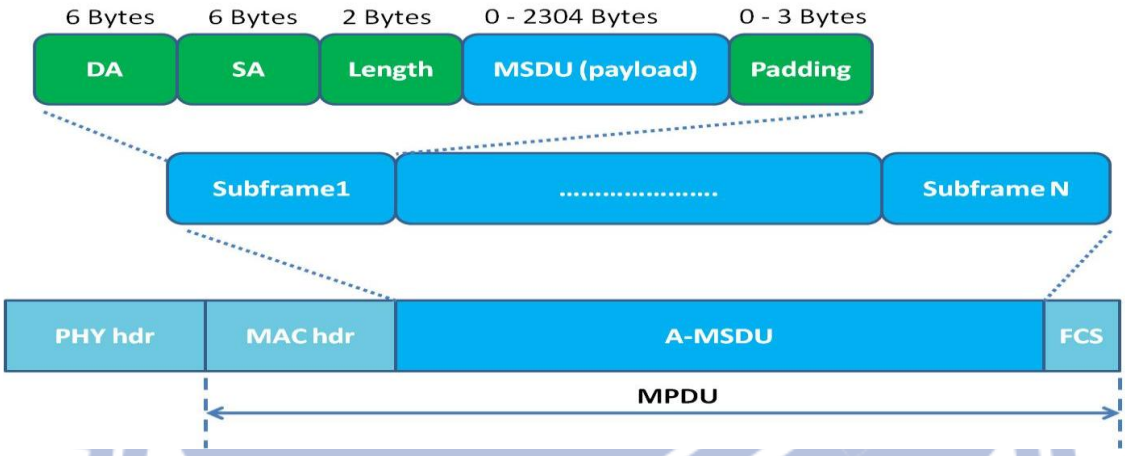

Fig. 2 A-MSDU frame format

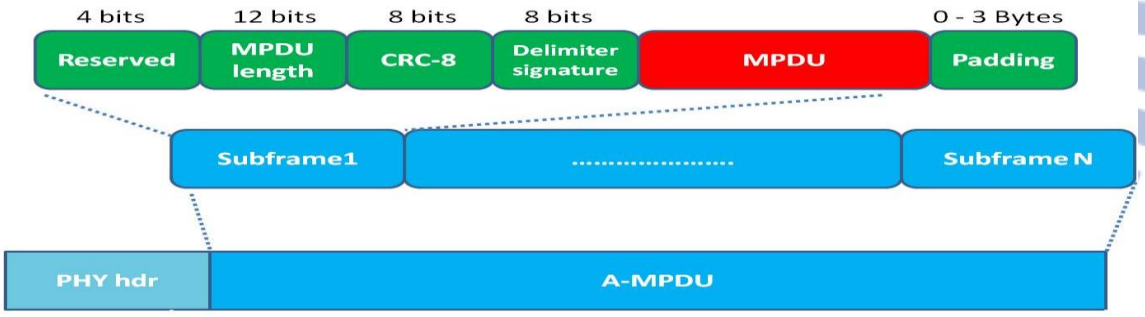

Fig. 3 A-MPDU frame format

BA is designed within the same idea, which makes the overhead in **Ack** reduce. Rather than sending an individual **Ack** following each data frame, **802.11n** introduces the technique of confirming a burst of up to 64 frames with a single **BA** frame. The Block ACK even contains a bitmap to selectively acknowledge individual frames of a burst.

2.1.2 802.11i

802.11i is one of service amendments which is raised in 2004 for security propose. **WEP**(Wired Equivalent Privacy) is the original security algorithm in **802.11-1997** standard and ratified in September 1999. However, **WEP** has been demonstrated to have numerous flaws and then the **Wi-Fi Alliance** announced that **WEP** had been superseded by **WPA**(Wi-Fi Protected Access) in 2003. The **Wi-Fi Alliance** refers to their approved, interoperable implementation of the full **802.11i** as **WPA2** in 2007, which is also called **RSN**(Robust Security Network). **802.11i** makes use of the **AES**(Advanced Encryption Standard) block cipher, whereas **WEP** and **WPA** use the **RC4** stream cipher.

RSN proposes the secure architecture with two new protocols, the **4-Way Handshake** and the **Group Key Handshake.** The authentication services and port access control described in **IEEE 802.1X** are utilized to generate and exchange the cryptographic keys. The **RSN** only allows the creation of **RSNA**s(robust security network associations), which are a type of association used by a pair of **STA**s(stations) if the procedure to establish authentication or association between them includes the **4-Way Handshake**, to access this secure network. **RSN** also provides two **RSNA**(Robust Security Network Association) protocols, **TKIP**(Temporal Key Integrity Protocol) and **CCMP**(Counter Cipher Mode with Block Chaining Message Authentication Code Protocol), for ensuring data confidentiality and integrity respectively.

2.2 Cryptography and Data Encryption

Cryptography is the practice and study of techniques for secure communication in the presence of the malicious third parties. In other words, it is about constructing and

analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security, such as data confidentiality, data integrity, authentication, and non-repudiation. Cryptography was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique or the secret which is needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same.

Modern cryptography is heavily based on mathematical theory and computer science practice. The modern data encryption methods can be classified as two types, **symmetric-key** cryptography and **public-key** cryptography. **Symmetric-key** cryptography refers to encryption methods in which both the sender and receiver share the same key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher. And stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In practical implement, block cipher algorithms can be treated as stream cipher ones by applying different block cipher mode.

2.2.1 Block Cipher Mode

A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block. Most modes require a unique binary sequence, often called an initialization vector (**IV**), for each encryption operation. The **IV** has to be

non-repeating and for some modes random as well. The initialization vector is used to ensure distinct ciphertexts are produced even when the same plaintext is encrypted multiple times independently with the same key. Block ciphers have one or more block size(s), but during transformation the block size is always fixed. Block cipher modes operate on whole blocks and require that the last part of the data be padded to a full block if it is smaller than the current block size. There are, however, modes that do not require padding because they effectively use a block cipher as a stream cipher.

2.2.2 Advanced Encryption Standard

The Advanced Encryption Standard (**AES**) is a specification for the encryption of electronic data in 2001[11]. It is based on the Rijndael[6] cipher developed by two Belgian cryptographers, **Joan Daemen** and **Vincent Rijmen**, who submitted a proposal which was evaluated by the **NIST** during the **AES** selection process. In other words, the **AES** standard is a variant of Rijndael under the restriction that the block size is 128 bits using cipher key with lengths of 128,192,256 bits. **AES** now is available in many different encryption packages, and is the first publicly accessible and open cipher approved by the National Security Agency (**NSA**) for top secret information when used in an **NSA** approved cryptographic module.

AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of **Rijndael** have a larger block size and have additional columns in the state. Most AES calculations are done in a special Galois field, **GF**(2^8). Different key sizes used for an **AES** cipher lead different numbers of repetitions of transformation rounds that convert the plaintext into the ciphertext. For **128-AES**, **192-AES**, and **256-AES** need 10, 12, 14 cycles of repetitions respectively and each cycle contains several processing stages, each consisting of

four steps, such as ***SubBytes***, ***ShiftRows***, ***MixColumns***, and ***AddRoundKey***.

2.2.3 CCMP

The **CCMP** is an encryption protocol designed for **WLAN** products that implement the standards of the **IEEE 802.11i** amendment to the original **IEEE 802.11** standard[12]. **CCMP** is based on **AES** encryption algorithm using the Counter(**CTR**) Mode with **CBC–MAC** mode of operation to enhance data cryptographic encapsulation mechanism designed for data confidentiality. It was created to address the flaws shown in **WEP**.

CCM also requires a unique nonce value for each frame protected by a given temporal key(**TK**), and **CCMP** uses a 48-bit packet number(**PN**) for the same purpose. Reuse of a **PN** with the same **TK** will make the mechanism insecure. **CCMP** contains two major parts: **MIC** computation and **CTR**-mode encryption for authentication and data confidentiality respectively. Therefore, each message block requires two block cipher encryption operations. In hardware, for large packets, the speed achievable for **CCM** is roughly the same as that achievable with the **CBC** encryption mode. Both the **CCM** encryption and **CCM** decryption operations require only the block cipher encryption function. In **AES**, the encryption and decryption algorithms have some significant differences. Thus, using only the encrypt operation can lead to a significant savings in code size or hardware size.

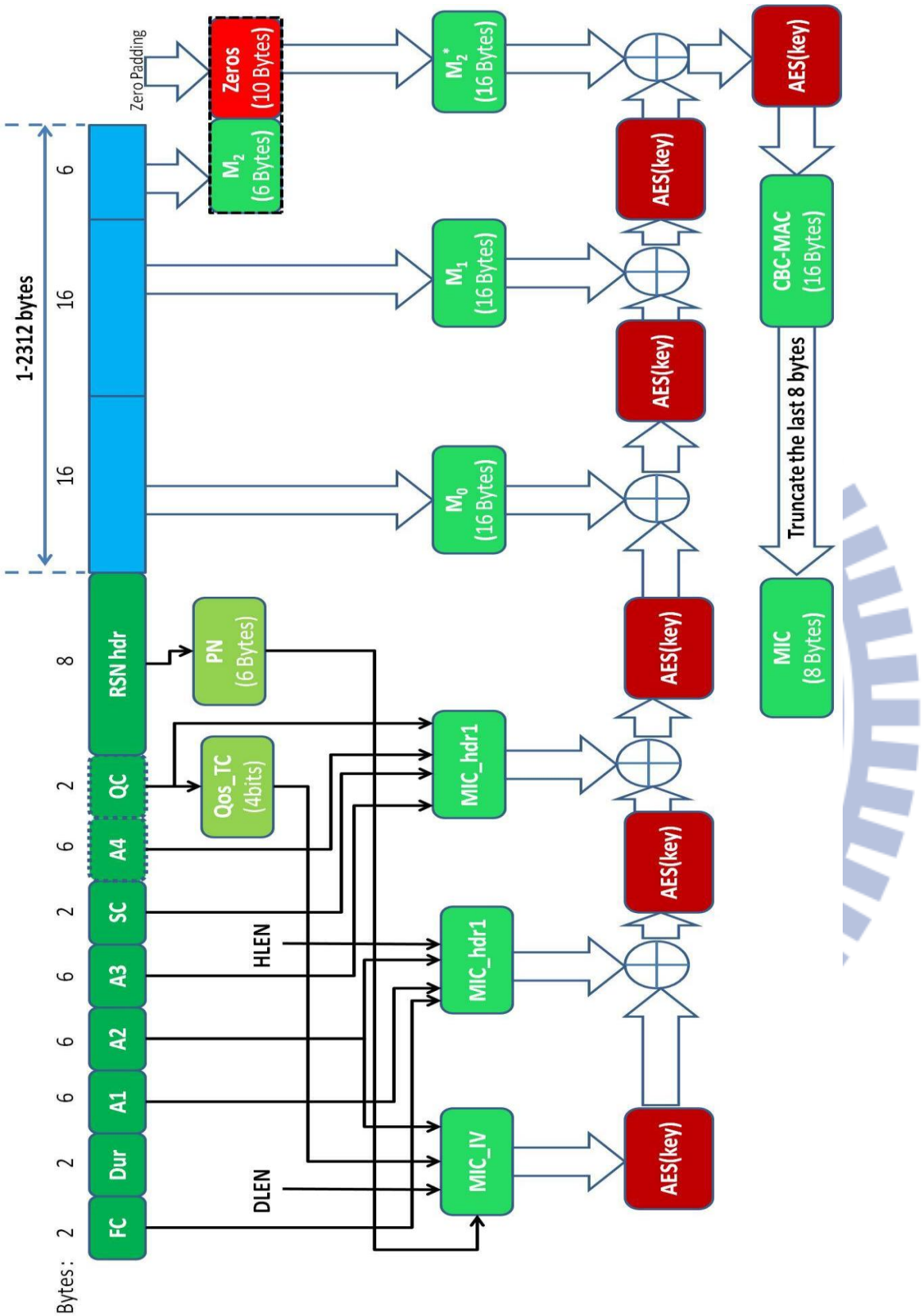

Fig. 4 CCMP MIC Calculation

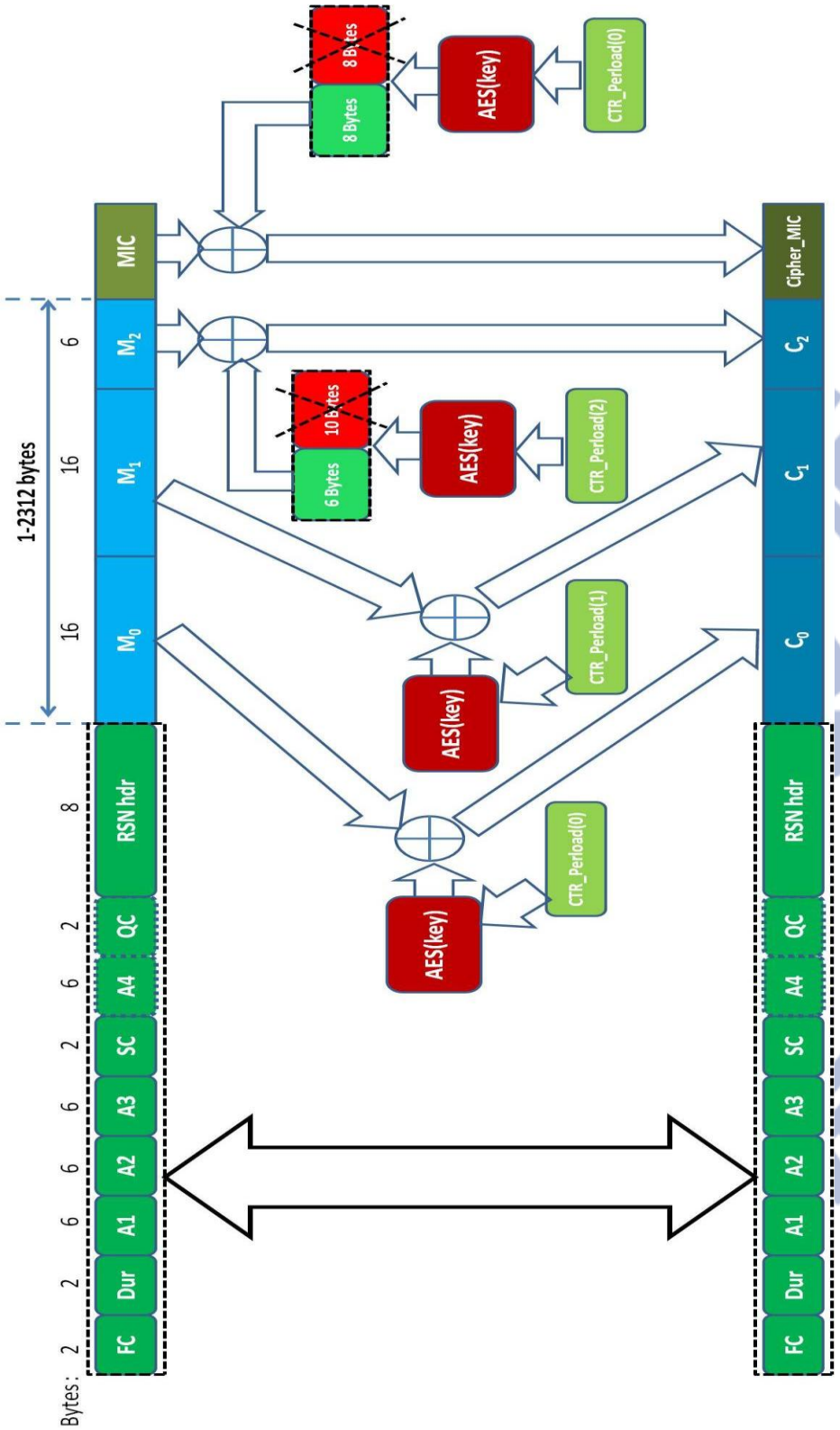

Fig. 5 CCMP CTR-mode Encryption

Chapter 3.

Proposed Algorithm

3.1 Aggregated Hybrid-ARQ

Compared with the causal **ARQ** protocol, **Stop-and-Wait(SW)**, **Go-back-N(GBN)** and **Selective Repeat(SR)**, the most efficiency protocol is **SR**. **SR** avoid unnecessary retransmissions by having the sender retransmit only those packets that it suspects were received in error, however, some factors in telecommunication such as burst-error due to fading and huge latency do not be taken into account.

For **SR-ARQ**, we need to retransmit whole the packet which can't be recover by channel code (such as **Hamming**, **Reed-Solomon** or turbo code). It waste lots of efficacious information we have sent before. **Aggregated Hybrid-ARQ** (**AH-ARQ**) divide the packet into several blocks with light overhead h_b, which contains **Forward Error Correction code** (**FEC**) , **Cyclic Redundancy Check** (**CRC**) and some identical patterns (**ID**), and an addressing overhead, h_o(such as **IP** header, **PLCP**), for whole packet.

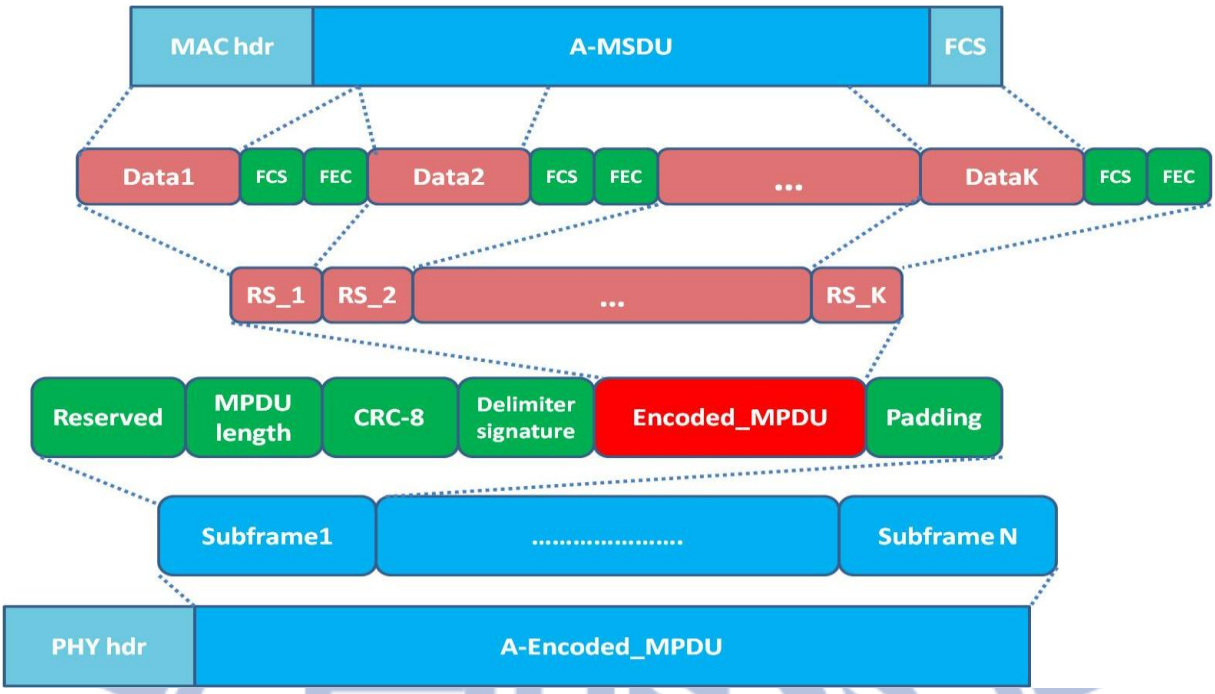

Fig. 6 AH-ARQ packet format

Over a noisy fading channel, some blocks may be corrupted more severely than others. More corruption leads to higher probability of having error bits. When a packet which is recovered by correction code does not pass the **CRC** check , only those blocks which can't be recovered are selected for retransmission instead of whole packet.

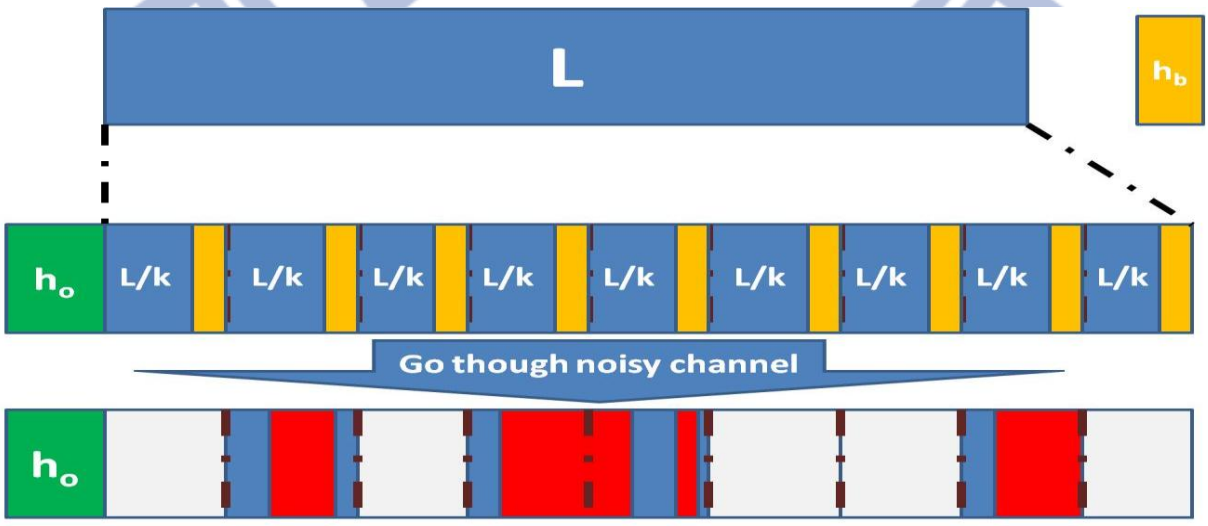

Fig. 7 Block corruption with AH-ARQ in noisy channel

Based on **RS** code, those blocks corrupted contain more than **θ** error symbols and ***SER*** represents the symbol error rate of a **RS** symbol defined in **GF(2^n)**, i.e., ***SER*** = 1-(1-***Pe***)^n where the ***Pe*** is the bit error rate. Therefore, Be_k , the block error probability after decoding with block length, can be illustrated as following :

$$Be_k = \sum_{i=\theta+1}^{k} C_i^k SER^i (1-SER)^{k-i} \quad (3.1)$$

Assume that we divide a data frame with length ***L*** into ***K*** blocks. ***R*** and T_{CSMA} are the transmitting rate and the expected time of latency for **CSMA**. The expected transmitting time of **AH-ARQ** is:

$$T_{AH} = \frac{\sum_{i=1}^{\infty} P_K(i) \cdot [R \cdot T_{CSMA} + h_o] + [K \cdot Be_{L/K}^{i-1}](\frac{L}{K} + h_b)}{R} \quad (3.2)$$

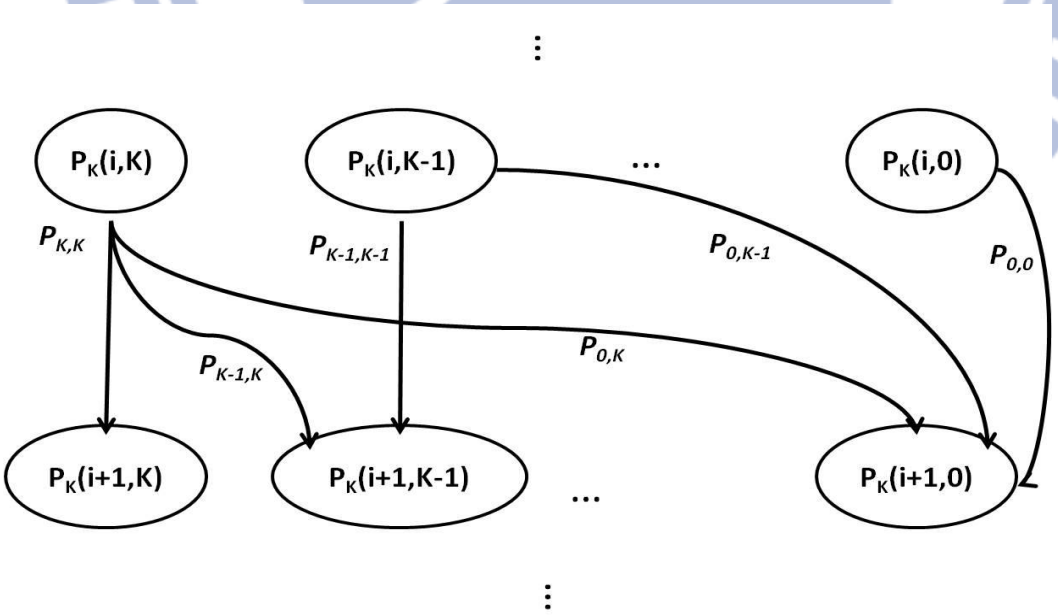

Fig. 8 State diagram for AH-ARQ scheme

where $P_K(i)$ represents the probability that the ***i-th*** retransmission contains at least one error block science there are K blocks needed to be transmitted in the beginning, and $P_K(0) = 1$ as the boundary condition. $P_K(i)$ can be considered as the summation of $P_K(i,j)$, the probability that the ***i-th*** retransmission contains j error block(s) for transmitting K blocks as $0<j\leqq K$, and can be formulated as :

$$P_K(i) = \sum_{j=1}^{K} P_K(i,j) = \sum_{j=1}^{K}\sum_{t=j}^{K} P_{jt} \cdot P_K(i-1,t) \tag{3.3}$$

where P_{jt} is the state probability that there is j error block(s) left after transmitting t block(s). The two-dimensional Markov chain model can be adopted as the baseline model to analyze this model.

$$\begin{bmatrix} P_{00} & P_{01} & \cdots & \cdots & P_{0K} \\ P_{10} & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & \vdots \\ P_{K0} & \cdots & \cdots & \cdots & P_{KK} \end{bmatrix}^i \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} P_K(i,0) \\ P_K(i,1) \\ \vdots \\ \vdots \\ P_K(i,K) \end{bmatrix}, i = 0,1,2\ldots \tag{3.4}$$

and the transition probability P_{jt} can be calculated as

$$P_{jt} = \begin{cases} C_j^t \cdot Be_K{}^j \cdot (1-Be_K)^{t-j} & ,t \geq j \\ 0 & ,t < j \end{cases} \tag{3.5}$$

Now, we can estimate E_K, where E_K is the expected number of the transmitted packet which contains K **RS** blocks.

$$E_K = \sum_{i=0}^{\infty} P_K(i)$$
$$= \sum_{j=0}^{K} (1 + E_j) \cdot P_{jK} \qquad , where\ E_0 = 0 \tag{3.6}$$

Combining (3.2) and (3.6), the expected transmitting time with ***K*** blocks can be obtained as

$$T_{AH} = \frac{E_K \cdot [R \cdot T_{CSMA} + h_o] + (L + K \cdot h_b) \Big/ 1 - Be_{\frac{L}{K}}}{R} \tag{3.7}$$

Therefore, the efficiency for **AH-ARQ** is shown below:

$$\eta_{AH} = \frac{T_L}{T_{AH}} = \frac{\frac{L}{R}}{T_{AH}} = \frac{L}{\frac{L + K \cdot h_b}{1 - Be_{L/K}} + (R \cdot T_{CSMA} + h_o) \cdot E_K} \tag{3.8}$$

Moreover, we can find out that **SR-ARQ** is a special case with ***K*** = 1, $\boldsymbol{h_b}$ = 0, and ***Be*** = ***PER*** (**Packet Error rate**) :

$$\eta_{SR} = \frac{L}{\frac{L + 1 \cdot 0}{1 - PER} + (R \cdot T_{CSMA} + h_o) \cdot E_1} = \frac{L \cdot (1 - PER)}{L + R \cdot T_{CSMA} + h_o} \tag{3.9}$$

3.2 Fragmentation CCMP

CCMP is the replacement encryption protocol for the **WPA2** for providing much more

secure than the **WEP** protocol and **TKIP** protocol of **WPA**. This protocol supports two main secure service: **data confidentiality** and **authentication**.

Data confidentiality is guaranteed by using the encryption part of **AES** and **XOR** operator. All data blocks can be decrypted respectively because all the cipher blocks are constructed within **CTR(Counter-Mode)**. But on the other hand, **CBC-MAC** is applied for authentication in **CCMP**. Any data block which is needed for generating the **MIC(Message Integrity Check)** depends on all block(s) in the past of this packet. Therefore, it is impossible that calculating part of information in **MIC** before all data blocks are received.

In order to decrease the time consumption, we have modified some parts of the **CBC-MAC** into **FCBC-MAC(Fragment-CBC-MAC)**. The main difference is that we divide a long **CBC** chain into several shorter ones. Each chain C_i operates the **CBC-MAC** protocol and compute the result, MIC_i, and the final checksum, **MIC**, will be the XOR result of all MIC_i.

Assume that the **MIC** is used to authenticate L_B data blocks, we divide the chain into several groups, $G_1 \ldots G_p$, which are disjoint sets and whose union is the whole L_B blocks. The formula can be illustrated below:

$$MIC_{i,j} = AES(MIC_{i,j-1}, M_{t_i+j}), t_i = \sum_{p=1}^{i-1} NG_p, \ and \ \ \mathrm{MIC}_{i,0} = IV_i \tag{3.10}$$

$$MIC_i = MIC_{i,NG_i} \quad \text{and} \quad MIC = \bigoplus_{i=1}^{p} MIC_i \tag{3.11}$$

where NG_i is the number of elements in G_i, and the IV_i (initial vector) is used for secure

propose and will be stated in the next two sections.

The best benefit is that we can compute some of the information of **MIC** before all the messages are received or decoded successfully. But the penalty of this architecture is security because of the shorter **CBC** block chain length. We replace some **AES** operations with faster and exchangeable **XOR** operator for higher efficiency. Because of the using of **XOR** operator, the calculation of MIC_i can be executed out of sequence. Therefore, we can calculate those MIC_i , whose required elements are all received, first even if there are some groups are not completely received.

In **Chapter 3.3**, each group is defined as all the encrypted block in a **RS** block, so we use this configuration to explain the cases of replay attack scenario and its corresponding solution in **Chapter 3.2.1** and **3.2.1** .

3.2.1 Replay Attack in different packets in FCCMP

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it. The common solutions are one-time key/password or timestamp. In **CCMP** architecture, ***PN* (packet number)**, which is a 6-byte field, incorporated into the encryption and **MIC** calculations, provides replay protection.

Because we separate the **CBC-MAC** into several fragments, the MIC_i must be generated including the ***PN*** information. Otherwise, there will be a security vulnerability with simple replacement of some **RS** blocks which is obtained from those packet transmitted before. For

example, if there is a packet which contains ***N*** **RS** blocks, $\boldsymbol{RS_1}$... $\boldsymbol{RS_N}$, the adversary can insert even block, $\boldsymbol{RS_K^*}$, from another packet. Therefore, the new **MIC** value will be the same as the original one.

$$MIC = MIC_1 \oplus ... \oplus MIC_{K^*} ... \oplus MIC_2 \oplus .... \oplus MIC_N$$
$$= \left\{ \bigoplus_{i=1}^{p} MIC_i \right\} \oplus \left\{ MIC_{K^*} \oplus MIC_{K^*} \right\} = \bigoplus_{i=1}^{p} MIC_i \quad (3.12)$$

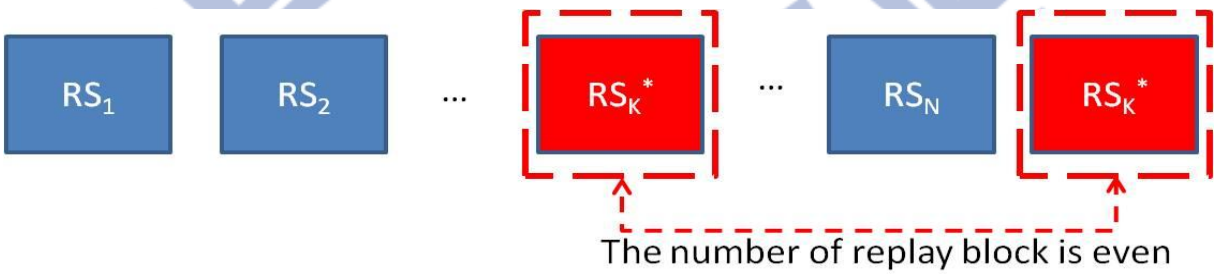

Fig. 9 Replay Attack in Different Packets

Therefore, we can construct the ***IV*** with the ***PN***:

$$IV = AES(AES(AES(MIC\_IV) \oplus MIC\_HEADER1) \oplus MIC\_HEADER2) \quad (3.13)$$

where **MIC_IV** includes the ***PN*** information (**Fig. 4 CCMP MIC Calculation**).

3.2.2 Replay Attack in the same packets in FCCMP

Because of the retransmission due to error occurrence, replay attack can be applied. The adversary can transmit the packet with **RS** blocks within incorrect sequence or more than one time.

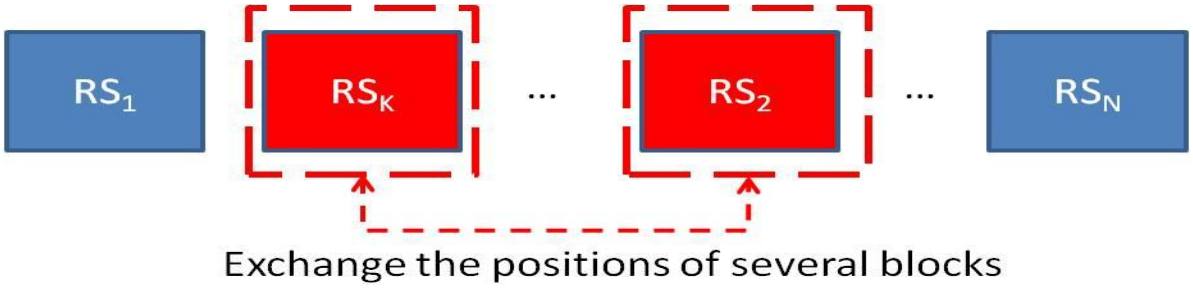

Fig. 10 Replay Attack in the Same Packet - Type(A)

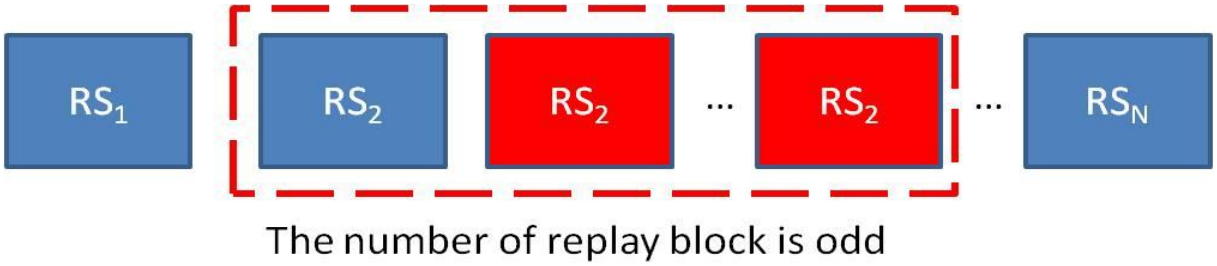

Fig. 11 Replay Attack in the Same Packet - Type(B)

For the situation stated in **Fig. 10**, the adversary swaps the position of two **RS** blocks, ***RS*$_2$** and ***RS*$_K$**, and the **MIC** is identical to the primitive result.

$$MIC = MIC_1 \oplus MIC_K \ldots \oplus MIC_2 \oplus \ldots \oplus MIC_N$$
$$= MIC_1 \oplus MIC_2 \ldots \oplus MIC_K \oplus \ldots \oplus MIC_N = \bigoplus_{i=1}^{p} MIC_i \quad (3.14)$$

And for the second case in **Fig. 11**, it is similar to the condition illustrated in **Section 3.2.1**. The adversary retransmits one of the RS block within ***X*** more times, where ***X*** is even, and then the information is different but the **MIC** is exactly the same.

$$MIC = MIC_1 \oplus \left\{ \bigoplus_{i=1}^{X+1} MIC_i MIC_2 \right\} \oplus \ldots \oplus MIC_N$$
$$= \left\{ \bigoplus_{i=1}^{p} MIC_i \right\} \oplus \left\{ \bigoplus_{i=1}^{X/2} \{ MIC_2 \oplus MIC_2 \} \right\} = \bigoplus_{i=1}^{p} MIC_i \quad (3.15)$$

To prevent this two problems, we should make every **RS** block's checksum, ***MIC$_i$***, depends on its own sequence number.

$$IV_i = AES(IV \oplus i) \tag{3.16}$$

3.2.3 FCCMP Algorithm

From what has been mentioned above, we can depict the **MIC** calculation process in the next three figures and the encryption process is the same as original **CCMP** process.

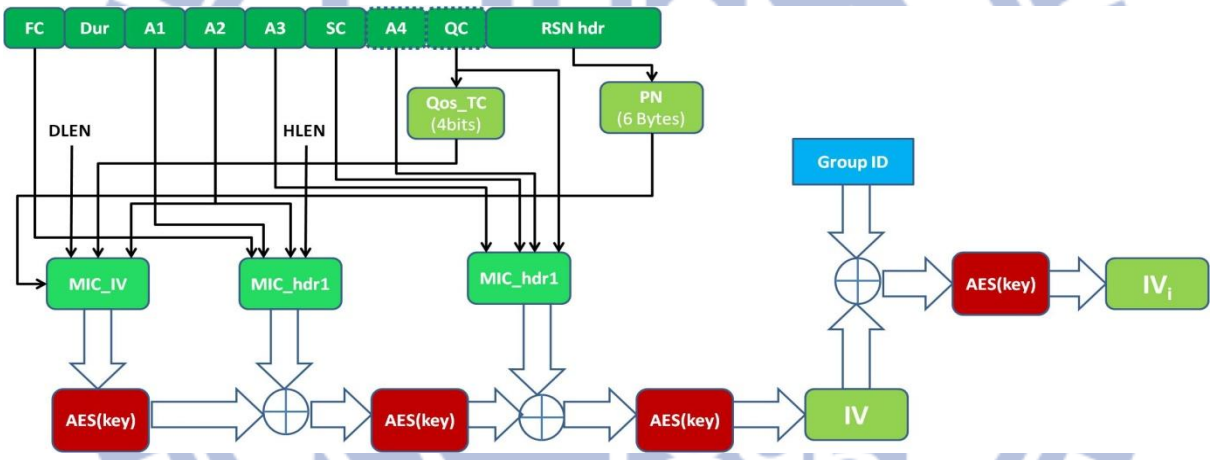

Fig. 12 IV$_i$ calculation

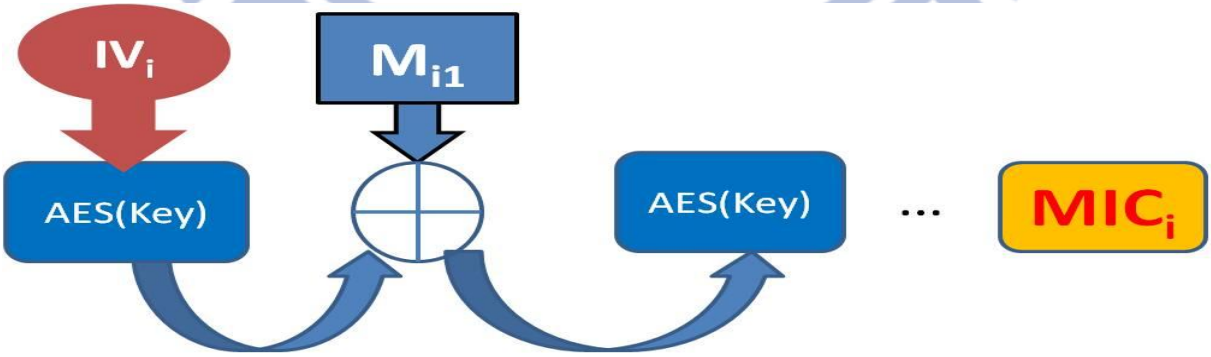

Fig. 13 MIC$_i$ calculation

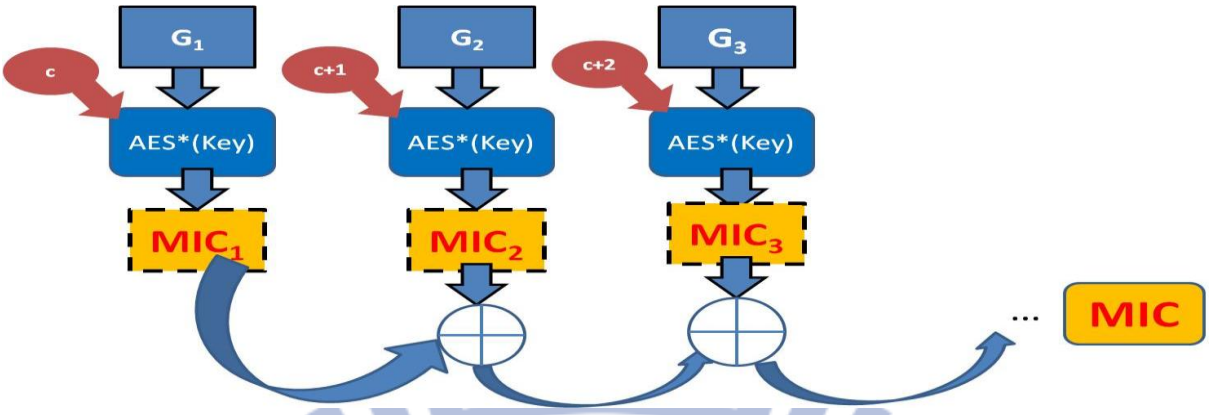

Fig. 14 Fragment-CBC-MAC

3.3 AH-ARQ with FCCMP

Typically, we obtain whole packet which is encrypted in plaintext within the following two phases: First, receive all the packet(s) and ensure that there is no errors after error correcting. Second, decrypt the ciphertext into plaintext and check if this packet is authenticated or not. Therefore, the time that the receiver obtains a packet successfully is:

$$T_{total} = T_{AH} + K \cdot T_{dec} \tag{3.17}$$

where K is the number of RS block in a packet, T_{dec} is the decryption time of a **RS** block, and T_{AH} is the expected time of **AH-ARQ**.

But we can reduce the total service time to almost T_{AH} by applying **AH-FCCMP**. The main idea of this structure is that we want to decrypt the packet not until whole bytes are received correctly. And the group, G_i, defined in **FCCMP** is RS_i here in the **MPDUs**.

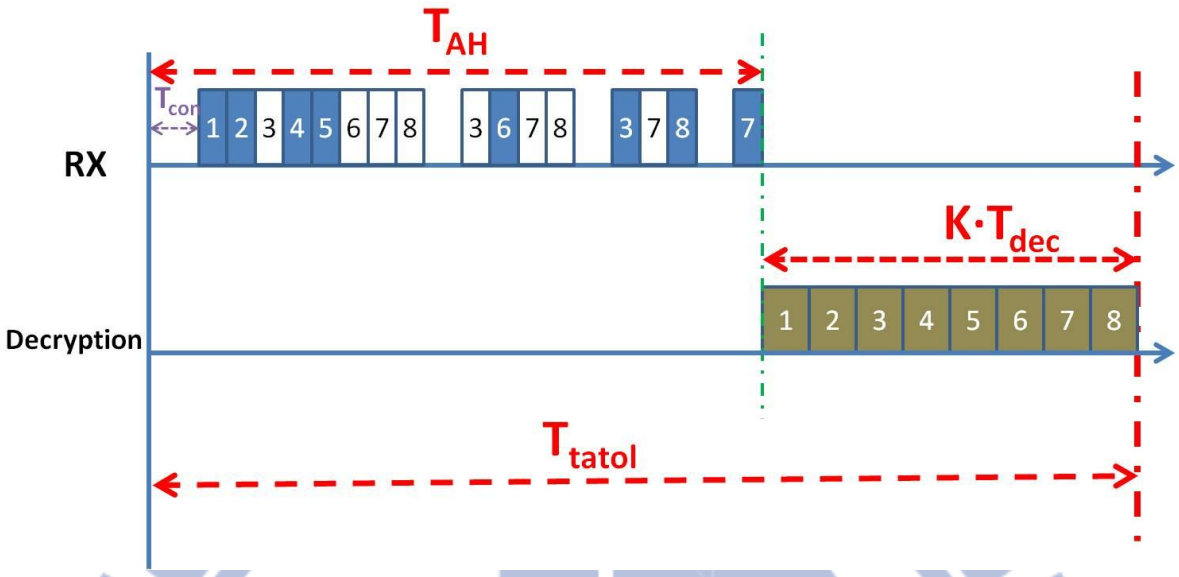

Fig. 15 AH-CCMP example

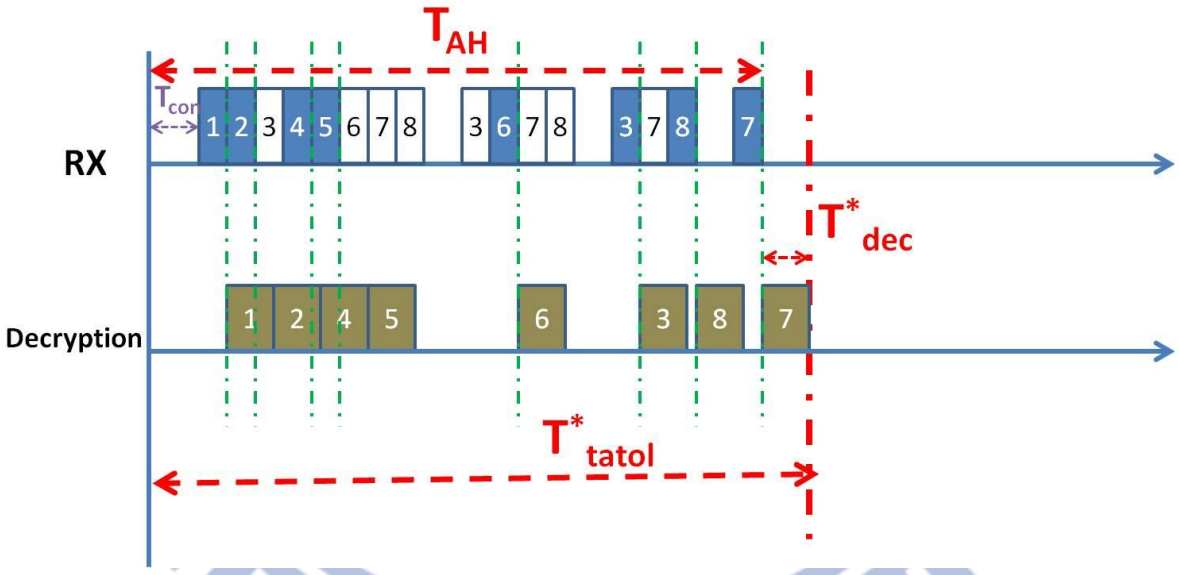

Fig. 16 AH-FCCMP example

Now we can calculate the service time, T_{total}^{*}, with the following formulation:

$$
\begin{aligned}
T^{*}_{tatol} &= T_{AH} + T_{dec}^{*} \\
&= T_{AH} + T_{RS} + \sum_{i=1}^{K} \Pr ob\{the\ last\ packet\ contains\ i\ blocks\} \cdot i \cdot (T_{dec} - T_{RS}) \\
&= T_{AH} + T_{RS} + L_{num} \cdot (T_{dec} - T_{RS}) \\
&\le T_{AH} + T_{RS} + K \cdot (T_{dec} - T_{RS}) \le T_{AH} + K \cdot T_{dec} = T_{tatol}
\end{aligned}
\qquad (3.18)
$$

where L_{num} is the expected block number of the last retransmitted packet. Obviously, T_{total}^{*} is less than or equal to T_{total} and there is a high positive correlation between T_{dec}^{*} and L_{num}.

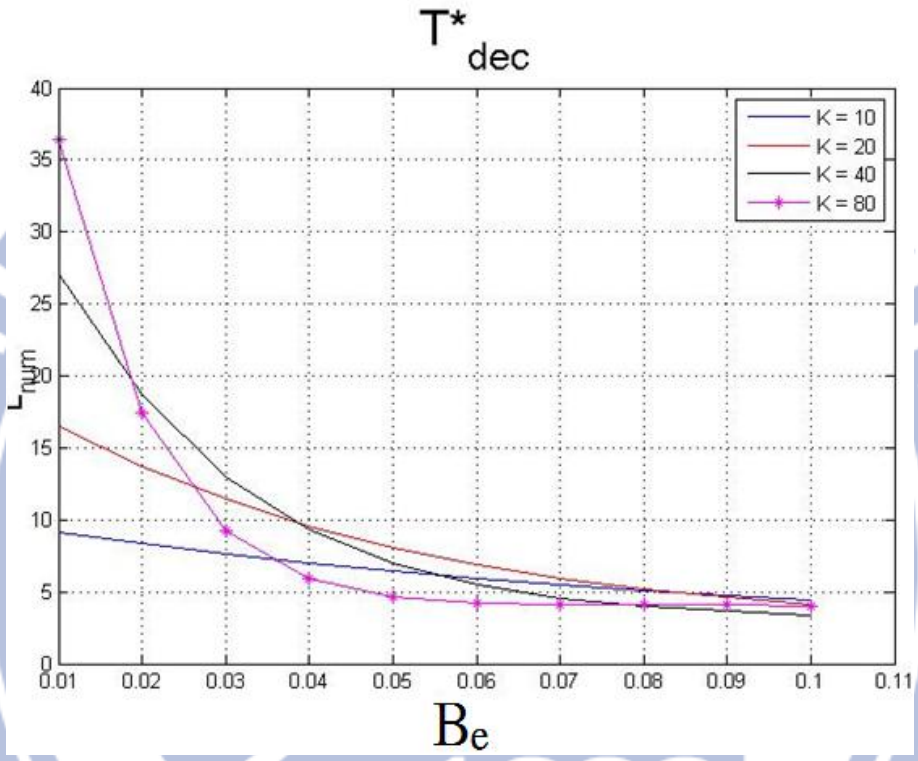

Fig. 17 L_{num} under different B_e

As the result shows above, we notice that T_{dec}^{*} increases when the B_e is low, but T_{AH} decreases in the same condition. On the contrary, T_{AH} rises but T_{dec}^{*} descends under high B_e circumstance. Therefore, the growing rate of T_{tatol}^{*} decreases as B_e declines, and T_{tatol}^{*} is close to T_{AH} when **SNR** is small.

As the structure we illustrate above, we can decrypt some blocks earlier after the first successful block and make the service time shorten if all **RS** blocks satisfies those two features below. First, all the information payload in each **RS** block contains D encryption

blocks at most and ***D*** must be an positive integer. Therefore, every **RS** block can be decrypted independently. Second, redundancy in **RS** block has better include **FCS**. Otherwise, we need to know if this block is cracked or not until it is been decrypted.

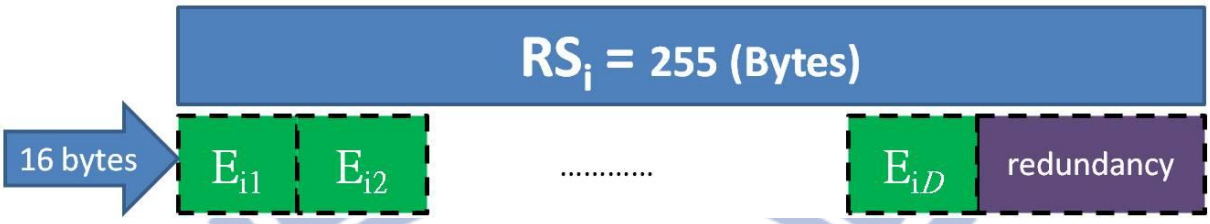

Fig. 18 RS block format in AH-FCCMP

The original **RS** block in **AH-ARQ** contains n_i bytes information and (4+2θ) bytes redundancy, including **CRC-32** and **FEC**. But because of the first feature stated above, ***D*** must be $\left\lfloor \frac{255-(4+2\theta)}{16} \right\rfloor$ bytes. For ***RS(255,239)*** codec, there will be 11 bytes waste in each RS block. The solution of this situation is reduce **θ** from 8 bytes into 4 bytes, ***RS(255,247)***, enlarge the **RS** block length. These two cases will be simulated in next section.

Chapter 4.

Simulation

4.1 System configurations

In this section, the performance of the original **AH-ARQ**, **AH-ARQ** with **CCMP**, and **AH-ARQ** with **FCCMP** schemes will be validated and compared via simulations. For simulating the performance, we apply this system with **Multi-mode RS-codec chip**[5] for **RS**-codec, **Motorola PowerPC G4 7410**, referenced by [15], for **(F)CCMP**, respectively, and other **MAC**-defined parameters, which are described in **802.11n** standard, are showing in **Table. 2**.

Parameter	Value
Min / Max window size (W_{min} / W_{Max})	7/31
Maximum back-off stage (M)	5
Maximum Retransmission (RT)	25
# of RS blocks in one MPDU (R)	16
Slot time (σ)	20 (μs)
Basic rate	7.2Mbps
T_{SIFS} / T_{DIFS}	10 / 50 (μs)
PHY header / MAC header	24 / 28 (Byte)
RTS / CTS / BA	20 / 14 / 56 (Byte)
Delimiter	4 (Byte)
Propagation Delay	1(μs)

Table. 2 Simulation System Parameters

4.2 Performance comparison under different numbers of MPDUs

In this section, we demonstrate the performance evaluation under different number of aggregated **MPDU**s within an **A-MPDU**, i.e., ***J*** = 1,10,20. The special case, ***J*** = 1, is shown for comparison purpose because it is also the same as the **SR-ARQ**, which transmits only one **MPDU** within each transmission. The rest configurations, **RS**-codec and **MCS**, are set by ***RS(255,239)*** and ***MCS(16QAM,3/4,180Mbps)*** respectively.

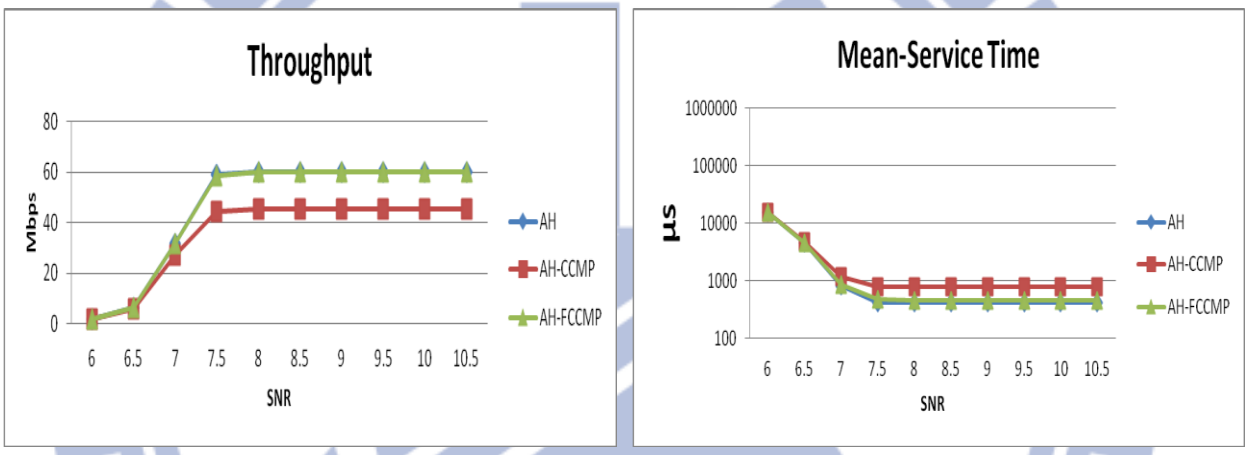

Fig. 19 Performance comparison among three architectures when *J* = 1

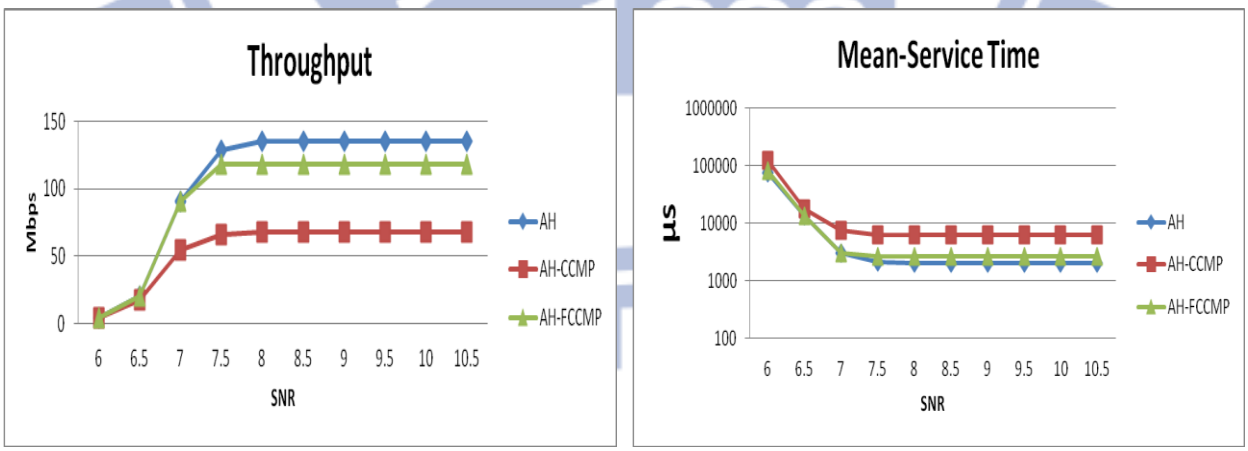

Fig. 20 Performance comparison among three architectures when *J* = 10

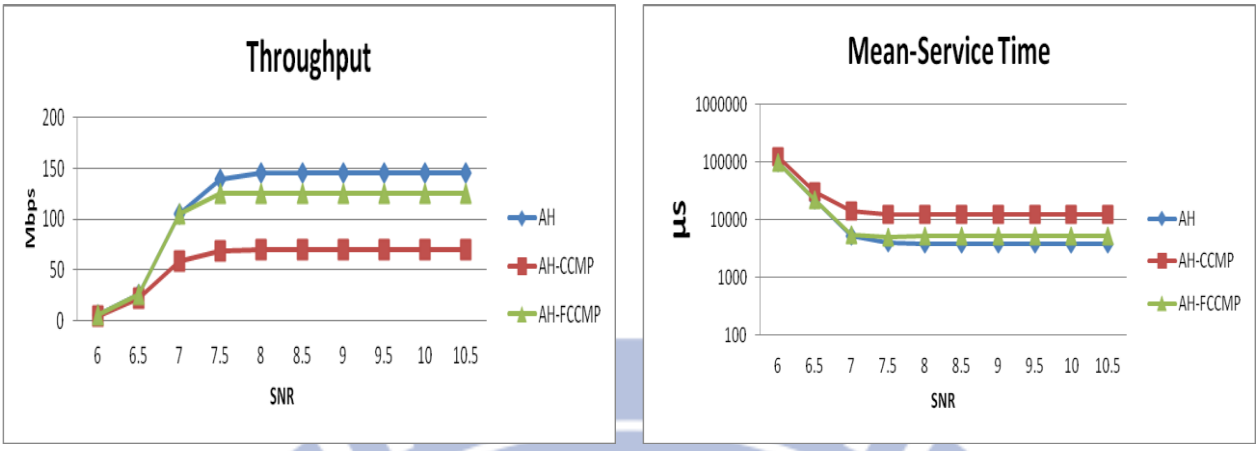

Fig. 21 Performance comparison among three architectures when J = 20

Fig. 19, **Fig. 20**, and **Fig. 21** show the performance comparison for both throughput and mean service time under different ***J***s consideration. As the result of these three figures, we notice that the throughput performance declines as the **SNR** is lower than 8 and eventually reaches the retransmission threshold when **SNR** is 6 due to high B_e. The maximum throughput ratio of **AH-ARQ** to **AH-FCCMP** are 99.8%, 87.89%, and 86.096% respectively, and the ratio of **AH-ARQ** to **AH-CCMP** are 75.79%, 50.13%, and 47.99% respectively. The difference of output rate between **AH-ARQ** and **AH-FCCMP** are extremely close especially when the **SNR** is low and the reason is shown in **Fig. 17** and **Eq.(3.17)** in **Chapter 3**. The mean service time of **AH-CCMP** is the highest one in these three figures due to the time wasting in the **CCMP** procedure. In **AH-FCCMP** scheme, the mean service time ratio of **AH-ARQ** decreases from 1.894 to 1.1105, 3.0812 to 1.3153, and 3.2195 to 1.3447 respectively.

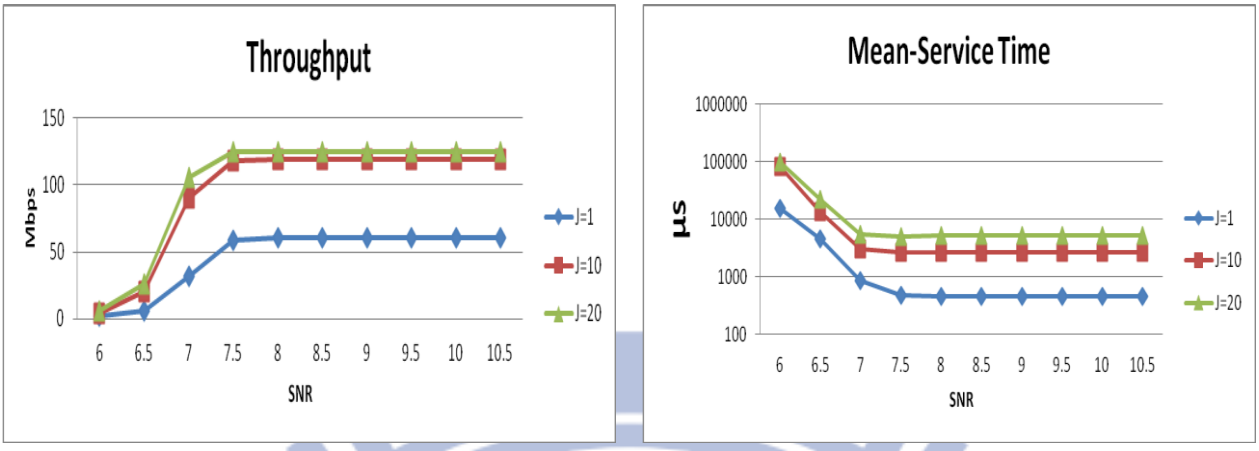

Fig. 22 Performance comparison under different value of *J* with AH-FCCMP scheme

Fig. 22 provide performance compared to the **SR-ARQ** scheme, whose number of **MPDU** per packet is one, since frame aggregation can improve channel utilization effectively. More **MPDU**s in one packet reduces the time consumptions by shared contention phase and **PHY** header. The maximum throughput enhancement to **SR-FCCMP** are 97.55% and 107.9% for ***J*** = 10 and 20 respectively. However, the mean service time increments are not the multiple of the number of **MPDU**s. In **AH-FCCMP** scheme, the mean service time ratio of ***J***=1 to ***J*** = 10 and 20 are 5.896 and 11.382 respectively in high **SNR** circumstance. Based on the simulation result, we notice that the performances are close in ***J***=10 and 20's schemes, so the configuration of ***J*** in the next two cases is set with 10.

4.3 Performance comparison under different RS-codec schemes

In this section, we demonstrate the performance evaluation under different **RS** coding rate. While the number of **AES** encrypted payloads must be an integer and the total payload should be lower than **RS**'s information data, the payloads in a **MPDU** with **AH-ARQ** scheme with ***RS(255,223)***, ***RS(255,239)***, and ***RS(255,247)*** are 3300, 3556, and 3812 bytes respectively as the number of **RS** blocks in one **MPDU**, ***R***, is 16. Note that the 3556-byte **MPDU** is computed from $(D \times Block_{AES}) \times R - MAC\_Header = 3556\ bytes$, where

$D = \left\lfloor \frac{239-4}{16} \right\rfloor = 14$, ***Block***$_{AES}$ = 16 bytes, and ***MAC_Header*** = 28 bytes. The rest configurations, ***J*** and **MCS**, are set by 10 and ***MCS(16QAM,3/4,180Mbps)*** respectively.

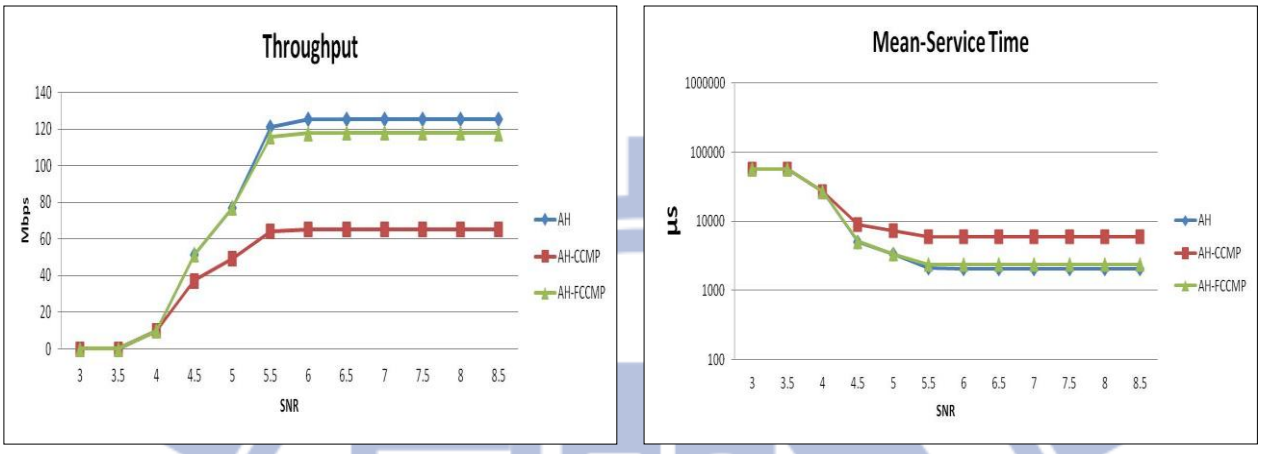

Fig. 23 Performance comparison among three architectures under *RS(255,223)*

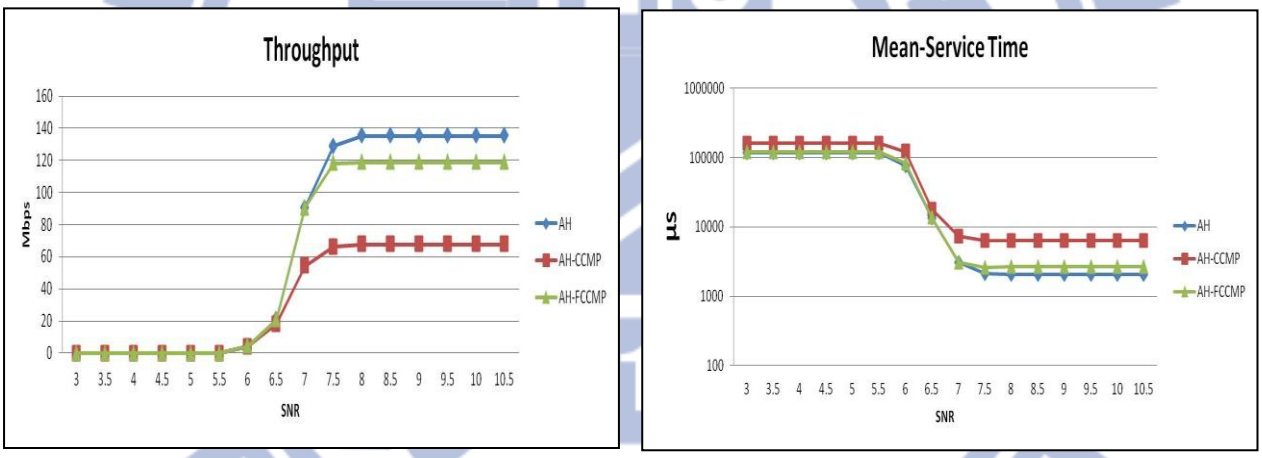

Fig. 24 Performance comparison among three architectures under *RS(255,239)*

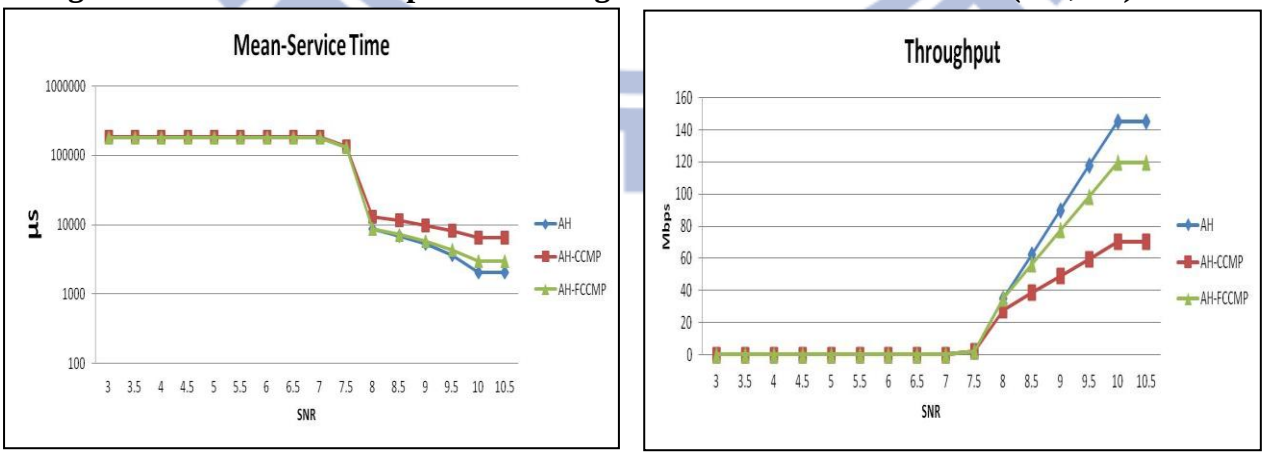

Fig. 25 Performance comparison among three architectures under *RS(255,247)*

Fig. 23, **Fig. 24**, and **Fig. 25** show the performance comparison for both throughput and mean service time under different **RS**-codec consideration. As the result of these three figures, we notice that the throughput performance under ***RS(255,223)***, ***RS(255,239)***, and ***RS(255,247)*** **FEC** code declines as the **SNR** are lower than 6, 8, 10 and eventually reaches the retransmission threshold when **SNR** are 4, 6, 8 due to high B_e. The maximum throughput ratio of **AH-ARQ** to **AH-FCCMP** are 93.89%, 87.89%, and 85.53% respectively, and the ratio of **AH-ARQ** to **AH-CCMP** are 52.061%, 50.13%, and 48.35% respectively. In **AH-FCCMP** scheme, the mean service time ratio of **AH-ARQ** decreases from 2.928 to 1.165, 3.0812 to 1.3153, and 3.233 to 1.467 respectively in high **SNR** circumstance.

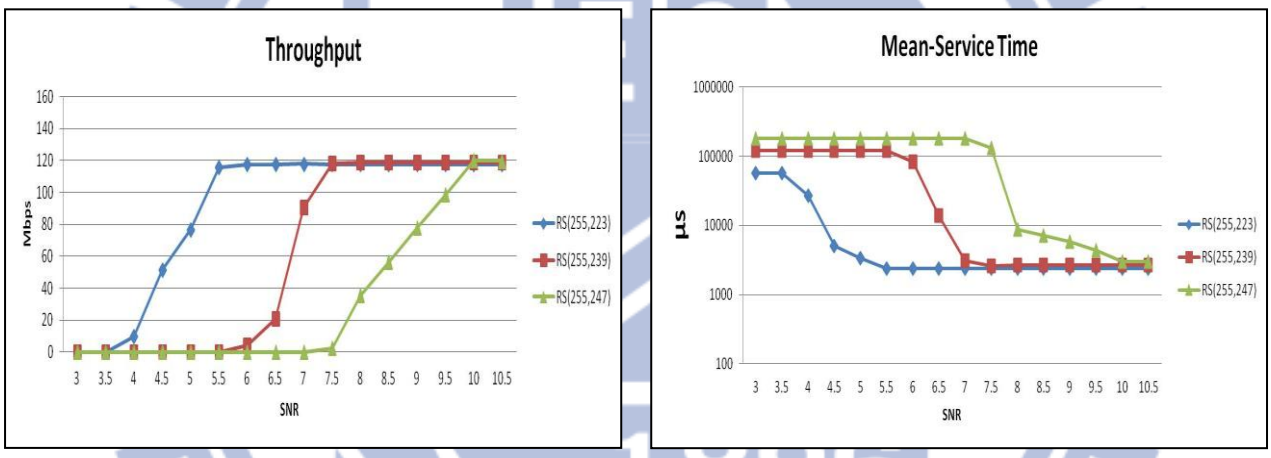

Fig. 26 Performance comparison under different RS-codec with AH-FCCMP scheme

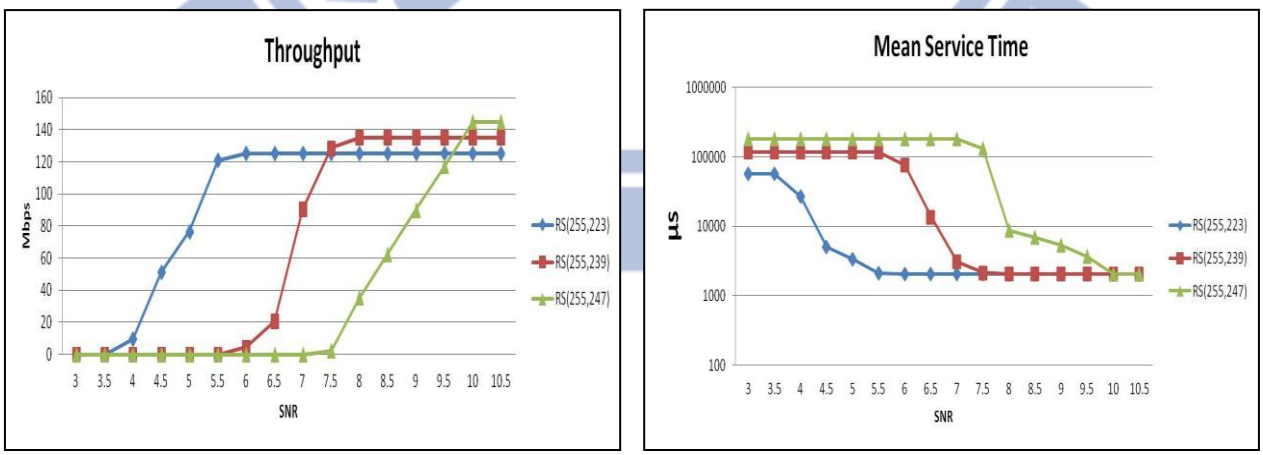

Fig. 27 Performance comparison under different RS-codec with AH-ARQ scheme

Fig. 26, and **Fig. 27** provide performance comparison within different **RS**-codec in **AH-ARQ** and **AH-FCCMP** scheme. The maximum throughput of **AH-ARQ** are 125.36, 135.148, and 144.958 Mbps and throughput of **AH-FCCMP** are 117.69, 118.78, and 119.64 Mbps in three schemes. In **AH-FCCMP** scheme, the mean service time ratio of ***RS(255,239)*** are 0.886 and 1.115 in high **SNR** condition and 0.47 and 1.498 in low **SNR** condition for ***RS(255,223)*** and ***RS(255,247)*** respectively. In addition, In addition, the values shown in **AH-ARQ** scheme are 1.0001 and 0.9994 in high **SNR** condition and 0.4889 and 1.5596 in low **SNR** condition for **RS(255,223)** and **RS(255,247)** respectively in **AH-ARQ** scheme.

The result shows that larger latency used for error correction leads to higher error tolerance under noisy channel quality but less efficiency when channel quality is good. But there is a special case showed in **Fig. 26** when the **SNR** is high but the throughputs are all close to 118Mbps. It is because of the limitation of **Motorola PowerPC G4 7410**'s computational speed. Each **AES** received encrypted block needs two **AES** calculation, which are used for data confidentiality and authentication respectively, to recover the original information. This chip computational speed for **AES** and **CCMP** calculation are approximated as 265Mbps and 120Mbps respectively. When the throughput of **AH**'s is over 120Mbps, the system output rate will be saturated by cipher chip's speed. Upgrading the cipher chip is one of the solution, but the cost of each device will raise. It can be a consideration for trade-off between throughput and cost.

4.4 Performance comparison under different MCSs

In this section, we demonstrate the performance evaluation under different **MCS** configuration. Under the number of spatial streams is 2, the **MCS** for simulation are ***MCS(QPSK,1/2,60Mbps)***, ***MCS(16QAM,3/4,180Mbps)***, and ***MCS(16QAM,3/4,180Mbps)***

respectively. The rest configurations, ***J*** and **RS**-codec, are set by 10 and ***RS(255,239)*** respectively.

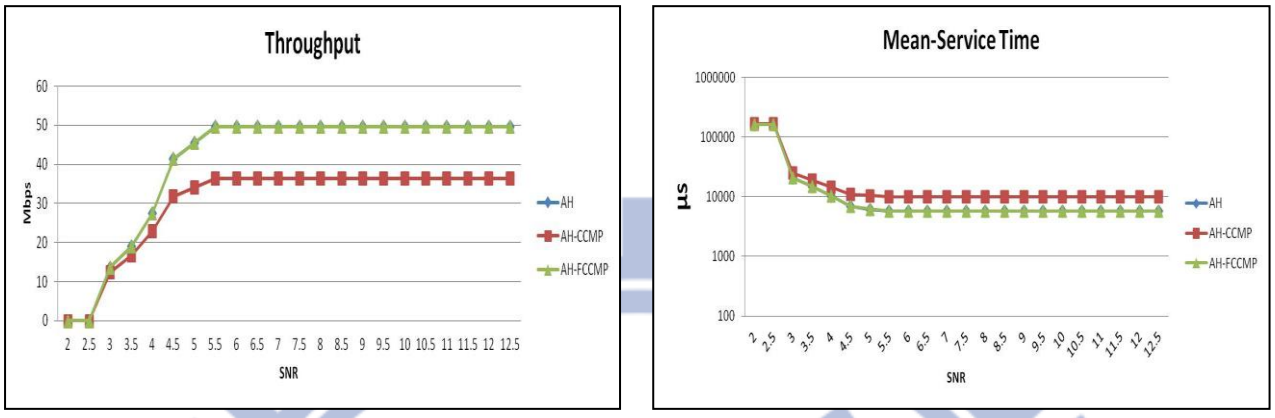

Fig. 28 Performance comparison among three architectures under MCS(QPSK,1/2,60Mbps)

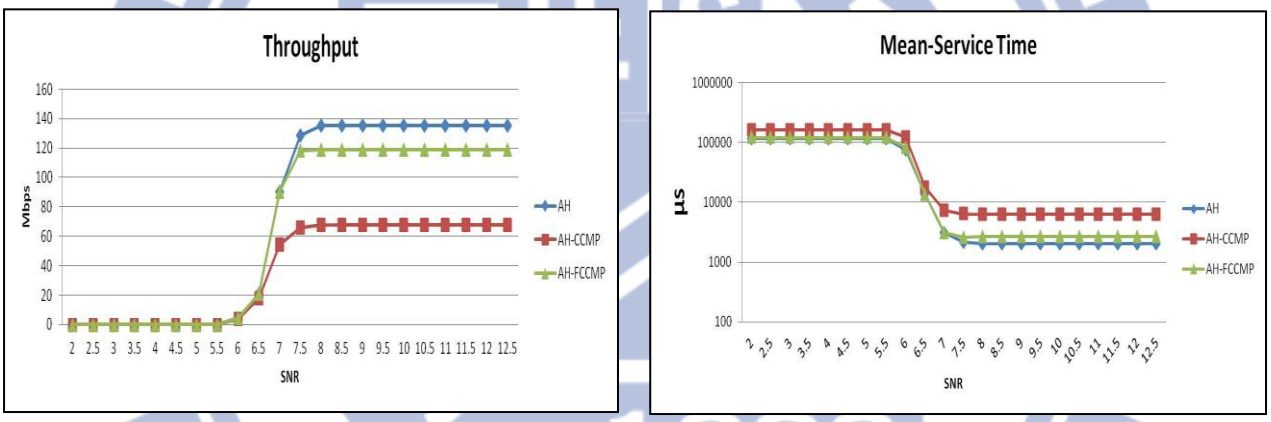

Fig. 29 Performance comparison among three architectures under MCS(16QAM,3/4,180Mbps)

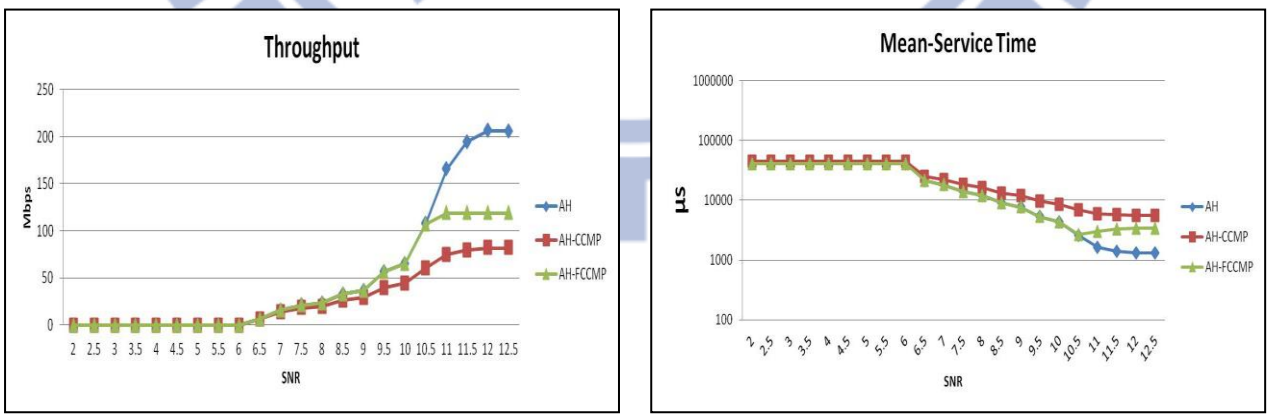

Fig. 30 Performance comparison among three architectures under MCS(64QAM,5/6,300Mbps)

Fig. 28,

Fig. 29, and **Fig. 30** show the performance comparison for both throughput and mean service time under different **MCS** consideration. As the result of these three figures, we notice that the throughput performance under ***MCS(QPSK,1/2,60Mbps)***, ***MCS(16QAM,3/4,180Mbps)***, and ***MCS(16QAM,3/4,180Mbps)*** declines as the **SNR** are lower than 5.5, 8, 12 and eventually reaches the retransmission threshold when **SNR** are 2.5, 6, 6.5 due to high B_e. The maximum throughput ratio of **AH-ARQ** to **AH-FCCMP** are 99.98%, 87.89%, and 57.73% respectively, and the ratio of **AH-ARQ** to **AH-CCMP** are 73.26%, 50.13%, and 39.74% respectively. In **AH-FCCMP** scheme, the mean service time ratio of **AH-ARQ** decreases from 1.749 to 1.0025, 3.0812 to 1.3153, and 4.225 to 2.5834 respectively in high **SNR** circumstance.

We notice that the mean service time increases as long as the **SNR** raises after the **SNR** is 10.5, and it is unusual from the other figures shown before. The reason of this rebound is the limitation of cipher chip's computational speed, and the detail is stated in **Chapter 4.3**. The sender's strategy in simulation program is that transmitting a new packet as long as the previous packet is all received correctly within **AH-ARQ** but not take into account whether it is fully decrypted by **CCMP** or not. Therefore, higher input rate leads early initial time, but the ending time of each packet is bounded by **AES**. On the other hand, the difference increases as the **AH-ARQ** throughput raises.

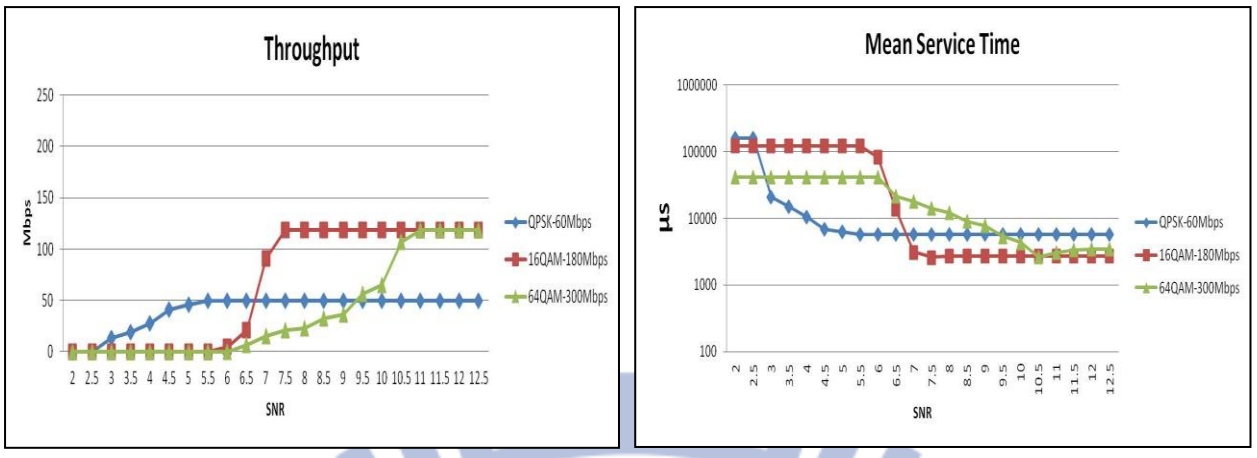

Fig. 31 Performance comparison under different MCS with AH-FCCMP scheme

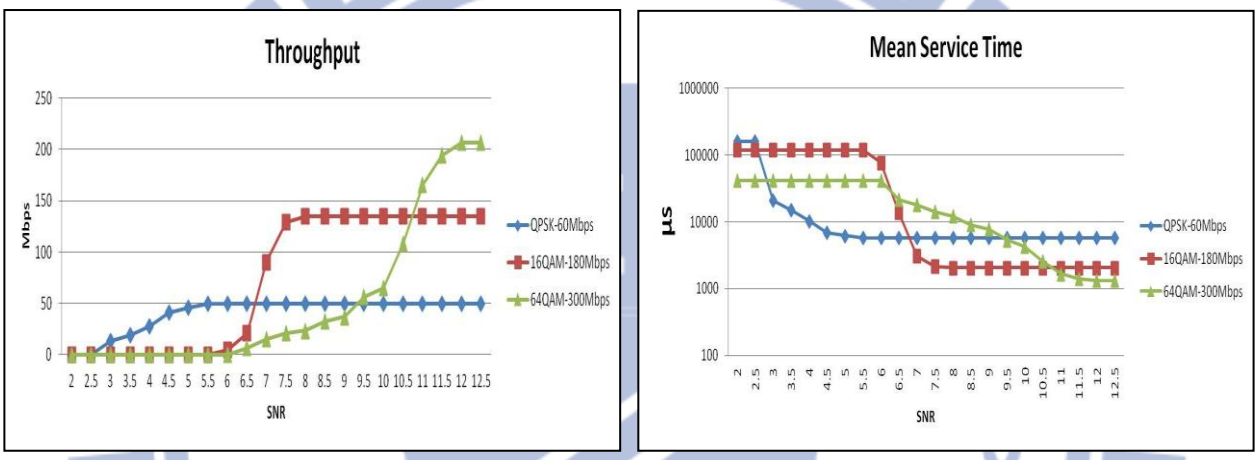

Fig. 32 Performance comparison under different MCS with AH-ARQ scheme

Fig. 31, and **Fig. 32** provide performance comparison within different **MCS** configuration in **AH-ARQ** and **AH-FCCMP** scheme. The ratio of data rate to maximum throughput are 82.73%, 75.08% and 68.73% in three setting respectively in **AH-ARQ** scheme, and 82.72%, 65.99% and 39.67% in **AH-FCCMP** scheme. In **AH-FCCMP** scheme, the mean service time ratio of ***MCS(16QAM,3/4,180Mbps)*** are 2.12 and 1.266 in high **SNR** condition and 1.326 and 0.3413 in low **SNR** condition for ***MCS(QPSK,1/2,60Mbps)*** and ***MCS(16QAM,3/4,180Mbps)*** respectively. In addition, the values shown in **AH-ARQ** scheme are 2.78 and 0.645 in high **SNR** condition and 1.38 and 0.355 in low **SNR** condition.

Chapter 5.

Conclusion

In this thesis, we propose the efficient structure of **802.11n** with **WPA2** protocol, Aggregated Hybrid Automatic Repeat Request Mechanism with Fragmentation Counter Mode with CBC-MAC Protocol (**AH-FCCMP**), while we consider different parameters in **802.11n** configuration so as to analyze the performance of the **AH-FCCMP** scheme in practice. The **AH-FCCMP** scheme is composed of two algorithms: **AH-ARQ** protocol and **FCCMP** protocol.

AH-ARQ is designed with the consideration of frame aggregation and block acknowledgement, which are proposed in **802.11n**, for boosting the throughput under low **SNR** channel quality by using **Reed-Solomon** block code as the forward error correction code (**FEC**). Based on the feature of **AH-ARQ**, we modify the **CCMP** to **FCCMP** so that we can compute in parallel not only the **AES** decryption but the **CBC-MAC** calculation. The modification of **CCMP** may raise some flaws such as replay attack, but we demonstrate the solution for preventing replay attack in **Chapter 3.2.2** and **3.2.3**. As long as **AES** is not cracked, **FCCMP** should be as safe as **CCMP**.

From the simulation results in **Chapter 4**, we can conclude that the throughput of **AH-FCCMP** is close to the one without security requirement. **AH-FCCMP** makes the cost of security operation decrease and provides the same security level. Moreover, we find that the total throughput is bounded by either data rate or cipher chip operation capability. So that high data rate does not necessarily lead to high system throughput since low level cipher chip.

References

[1] Cisco PSE, Inside 802.11n Technical details about the new WLAN standard, Mar. 2009.

[2] J.-C. C. e. al., "WIRELESS LAN SECURITY AND IEEE 802.11i," *IEEE Wireless Communications,* pp. 24 - 36, Feb. 2005.

[3] Committee, LAN/MAN Standards, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Computer Society, 2012.

[4] C.-X. W. e. al., "A Novel Generative Model for Burst Error Characterization in Rayleigh Fading Channels," *IEEE PIMRC Proceedings Vol.1,* pp. 960 - 964, Sept. 2003.

[5] H.-Y. Hsu, *Reconfigurable Multi-mode Reed-Solomon Codec for High-Speed Communication Systems,* National Central University,, 2001.

[6] J.-S. L. e. al., "Novel Design and Analysis of Aggregated ARQ Protocols for IEEE 802.11n Networks," *IEEE Trans. Mobile Computing vol.12, no.3,* pp. 556-570, Mar. 2013.

[7] Y. Wu, "Novel Burst Error Correction Algorithms for Reed-Solomon Codes," *nformation Theory, IEEE Trans. on , vol.58, no.2,* pp. 519 - 529, Feb. 2012.

[8] D. e. a. Skordoulis, "IEEE 802.11n MAC frame aggregation mechanisms for next-generation high-throughput WLANs," *Wireless Communications, IEEE , vol.15, no.1,* pp. 40 - 47, Feb. 2008.

[9] *Advanced Encryption Standard (AES),* NIST, 2001.

[10] V. Technologies, *Counter CBC-MAC Protocol (CCMP) Encryption Algorithm,* 2003.

[11] L. C. T. Shi, "Combining techniques and segment selective repeat on turbo coded hybrid ARQ," *WCNC. 2004 IEEE , vol.4,* pp. 21-25, Mar. 2004.

[12] S. C. Tinnirello I., "Efficiency analysis of burst transmissions with block ACK in contention-based 802.11e WLANs," *ICC 2005. on , vol.5,* pp. 16 - 20, May 2005.

[13] D. J. Bernstein, "AES speed," Sept. 2008. [Online]. Available: http://cr.yp.to/aes-speed.html.

[14] V. R. Joan Daemen, "AES Proposal: Rijndael," http://www.esat. kuleuven.ac.be/~rijmen/rijndael, 2001.

[15] Y.-T. H. e.al, "Performance analysis for aggregated selective repeat ARQ scheme in IEEE 802.11n networks," *IEEE PIMRC,* pp. 37,41, 13-16, Sept. 2009.

102

碩士論文

一個802.11n通訊協定以WPA2加密之有效結構及其實現

交通大學

電信工程研究所

邱鐙標