International Journal on Advanced Science Engineering Information Technology

Vol.8 (2018) No. 2
ISSN: 2088-5334

Confidential Data Transmission Using Subcarrier Randomization with RSA Algorithm for Synchronization on MIMO-OFDM System

Nihayatus Sa'adah[#], I Gede Puja Astawa[#], Amang Sudarsono[*]

[#] *Department of Electrical Engineering, Politeknik Elektronika Negeri Surabaya, Indonesia*
E-mail: nihayatussaadah28@gmail.com
E-mail: puja@pens.ac.id

**Department of Informatic and Computer Engineering, Politeknik Elektronika Negeri Surabaya, Indonesia*
E-mail: amang@pens.ac.id

***Abstract*— In wireless communication, the transmitted information data is often intercepted by eavesdropper through fading channels. Since the signal is transmitted by the transmitter through a wireless channel, it is not only the authorized receiver but also the attacker or the eavesdropper can easily capture and store the information signal. This research examines the security methods in wireless communication, where the security method used is subcarrier randomization. In the receiver, the subcarrier position must be restored to its original position. To restore the subcarrier position to its original position there needs to be a synchronization between transmitter and receiver. We use RSA algorithm as synchronization between transmitter and receiver. Subcarrier randomization security method is implemented on Multiple Input Multiple Output - Orthogonal Frequency Division Multiplexing (MIMO-OFDM) system. We perform QoS measurements including delay, throughput and packet loss on MIMO-OFDM systems using security and MIMO-OFDM systems without security. From the results obtained, we can prove that the proposed security method does not degrade the performance of the MIMO-OFDM system. MIMO-OFDM system with security can result in smaller packet loss than the MIMO-OFDM system without security. MIMO-OFDM system with security has the average packet loss 0.145%.**

***Keywords*— MIMO-OFDM; Subcarrier Randomization; Security; RSA; Synchronization.**

I. INTRODUCTION

Currently, wireless communication is a technology development that is in great demand by most people in the global era. The transformation of most media to support voice telephony into the media to support other services, such as video, image, text and data transmission encourages the development of wireless communications technology [1]. Wireless communications have shaded various applications. MIMO-OFDM is one of the techniques used in wireless communication technology. MIMO-OFDM technology can work very well on multipath components. MIMO is a technique used to raise the transmission rate of bits without expanding the frequency bandwidth [2]. This MIMO system uses more than one antenna on the transmitter and receiver [3]. It aims to make the reflected signal as the main signal amplifier so that mutual support or not mutual interrupt. There has been a lot of interest in applying orthogonal frequency-division multiplexing (OFDM) in wireless and mobile communication systems because of its sundry advantages in reducing the severe effects of frequency selective fading. OFDM has been proposed to transmit information entirely in the channel without interference [4]. A wireless communication system has much scattering that causes the signal to suffer from multipath fading so that the transmitted signal is disturbed by frequency selective fading channels known as Inter-Symbol Interferences (ISI). With OFDM, the signal fading across the bandwidth of each subcarrier is equally distributed, and OFDM is said to have converted the nature of frequency selective fading channels to flat fading channel by multicarrier transmission. This feature causes OFDM to become enticing multiple-access scheme for future wireless communication systems.

Assuring security is an essential role to avoid eavesdropper [5]. In wireless communication, eavesdropping is a well-known security susceptibility due to their broadcast nature [6]. This happens when unauthorized recipients hear a secret conversation between two wireless nodes in communication. In this research, the security techniques is implemented in the MIMO-OFDM system utilize the subcarrier on OFDM technology. The subcarrier position will be randomized to the transmitter, and in the receiver, the subcarrier position will be restored as before. This security technique can avoid attacks from eavesdropper due to the

random subcarrier. Subcarrier randomization methods are classified as physical layer security.

Billions of more users already use wireless communication technology. Along with the growing wireless communication, it will require increased security as well. Wireless communication using the security is usually applied to government, financial services, health services, and the military [7]. For the transmitted data to be safe, the data must be encrypted first using cryptographic technology. There are two cryptographic techniques for data encryption namely symmetric and asymmetric cryptography. The symmetric algorithm or commonly called a conventional cryptographic algorithm is an algorithm that uses the same key for the encryption and description process. Symmetric cryptographic algorithms are divided into two categories: stream algorithms (Stream Ciphers) and block algorithms (Block Ciphers). Where in the streaming algorithm, the encoding process will orientate to one bit/byte of data. While in the block algorithm, the encoding process is oriented to a set of bits/bytes of data (per block). The examples of symmetric key algorithms are DES (Data Encryption Standard), Blowfish, Twofish, MARS, IDEA, 3DES (DES applied three times), AES (Advanced Encryption Standard) named Rijndael. Asymmetric cryptography is an algorithm that uses different keys for encryption and description processes [8]. The encryption key can be distributed to the public and named as a public key, while the description key is stored for its use and is called a private key. Therefore, cryptography is also known as public key cryptography. The examples of algorithms that use asymmetric keys are RSA (Riverst Shamir Adleman) and ECC (Elliptic Curve Cryptography). As for asymmetric cryptography, where each perpetrator of the information system will have a pair of keys, namely the public key and private key, where the public key is used for data encryption, while the private key for decryption.

Symmetric cryptography requires a private channel to send a secret key because the key used for encryption and decryption is the same. In contrast to symmetric cryptography, asymmetric cryptography uses different keys when encryption and decryption [9]. So asymmetric cryptography does not need more channels to share a key. That is why in this research, we use asymmetric cryptography. Cryptography is usually used to encrypt information data, but in this research asymmetric cryptography is used for synchronization between transmitter and receiver.

In this research, we particularize on physical layer security using RSA algorithm for synchronization in the MIMO-OFDM system. Subcarrier's location is randomized by using change the location of the ciphertext bit with plaintext bit. Subcarrier randomization uses synchronization between the transmitter and the receiver. RSA algorithm for synchronization is expected to create the system more efficient. This research exhibits the influence of private data transmission on the attacker. The bit error rate (BER) of an attacker without knowing subcarrier's location is exceptionally degenerated. Besides the above output, we also measure QoS in the MIMO-OFDM system. From QoS results, can be compared between systems that use security and systems without security. This research is organized as follows; firstly we describe the introduction about this research. Secondly, we discuss related works and explain the proposed security scheme on a MIMO-OFDM system using synchronization. Thirdly, we discuss the experimental result. Finally, we draw the conclusion of this study in Section IV.

II. Material and Method

In this section, we describe the security technique which is used in wireless communication. The security technique is used to protect data information. It utilizes subcarrier on OFDM technology, where the subcarrier is randomized to avoid eavesdropper in fading channels. Transmitter and receiver synchronization is required to know the position of random subcarriers. We use RSA algorithm for synchronization. Synchronization using RSA algorithm is more secure than manual synchronization.

A. Related Works

In general, data information is secured using cryptographic technology that is encryption. Several studies have investigated secure communications using cryptography. Based on the key used, cryptographic algorithm there are two types of symmetric cryptography and symmetric cryptography. Nidhi Singhal and Raina [10] provide a comparison of AES algorithm and RC4 algorithm. Both of them are symmetric cryptography. In this paper, AES algorithm is compared with the RC4 algorithm, where the result is a time of encryption, time of CPU process, memory utilization, throughput in a different setting for each algorithm such as the size of key and size of data packet.

Asymmetric cryptography is proved more secure than symmetric cryptography because it has two keys used for encryption (public key) and decryption (private key). Asymmetric cryptography is also named as public key cryptography. In their work on information security, Vincent, PM Durai Raj, and E. Sathiyamoorthy presented security technique which can reduce encryption time [11]. This security technique is an improvement of RSA algorithm. RSA is a type of public key cryptography. The power of the RSA algorithm lies in the factorization of prime numbers. Exponent operation on encryption and decryption causes longer computation time.

Also, there was research by Xiaozhong Zhang et al. [12] where attractive features of chaos sequence and OFDM transmission is combined; this work proposes a secure communication scheme with subcarrier mapping and phase rotation based on chaos sequences. This scheme harness the characteristics of pseudorandom and sensitivity to beginning conditions of chaos sequences. Both the system performance and complexity are considered. We randomly altered the phases of constellation mapping and chose the subcarrier index to bring out the data symbols, where the beginning conditions of chaos sequence work as keys at the baseband processing of transmitter. In the receiver, authorized receivers would demodulate the info with keys from the inverse procedure. The scheme is proved to work efficiently against eavesdropper.

Previously, Rizky et al. [13] subcarrier randomization is proposed to secure data transmission. In this research, they proved that security schemes do not degrade the performance of the system. However, the proposed security

technique is less efficient because it uses manual synchronization. We propose a method for synchronization between transmitter and receiver. This synchronization uses RSA algorithm to know the location of randomized subcarrier position and restore the subcarrier position to its original position.

B. MIMO-OFDM Wireless Communication

MIMO technology is a system which uses many antennas on the transmitter and receiver. The use of many antennas can serve to ameliorate the superiority of links using the method of diversity transmission and raise data rate using spatial diversity transmission method.

Each antenna will transmit different information independently and simultaneously in the same frequency band. The MIMO system is supposed to diminish fading and interference from other users, ameliorate reliability, raise throughput without raising bandwidth, diminish transmit power [14].

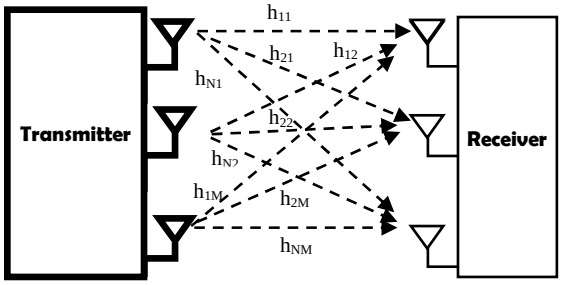

Fig. 1 MIMO Channel

If the transmitted information signal by the antenna is s_1, s_2, s_3, ..., s_M, then the received information signal by the receiver antenna such as equation

$$\begin{aligned} y_1 &= h_{11}s_1 + h_{12}s_2 + \ldots + h_{1M}\, s_M \\ y_2 &= h_{21}s_1 + h_{22}s_2 + \ldots + h_{2M}\, s_M \\ &\vdots \\ y_N &= h_{N1}s_1 + h_{N2}s_2 + \ldots + h_{NM}s_M \end{aligned} \tag{1}$$

With M is the number of antennas at the transmitter side and N is the number of antennas at the receiver side.

Equation (1) above, can be expressed in the form of matrix in equation (3) with the basic equation (2) as follows:

$$\boldsymbol{y} = \mathbf{H}\, \boldsymbol{s} + \boldsymbol{z} \tag{2}$$

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_N \end{bmatrix} = \begin{bmatrix} h_{11}\, h_{12} \cdots h_{1M} \\ h_{21}\, h_{22} \cdots h_{2M} \\ \vdots \quad \vdots \quad \vdots \\ h_{N1}\, h_{N2} \cdots h_{NM} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_M \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_M \end{bmatrix} \tag{3}$$

h_{ZM} expresses the channel gain between the transmitter antenna M to the receiver antenna N, $\boldsymbol{s}$ represents the transmitted signal matrix, $\boldsymbol{y}$ represents the received signal matrix, and $\boldsymbol{z}$ is the AWGN matrix experienced by the receiver antenna N.

MIMO can provide multiplexing gain and diversity gain. Multiplexing gain is obtained by applying spatial multiplexing and diversity gain techniques obtained by applying spatial diversity technique to the wireless communication system.

In the spatial multiplexing technique, the sequence of transmitted symbols is split into several parallel rows of symbols which are then transmitted simultaneously with the same bandwidth on each antenna so that this technique can provide an increase in data rate. Fig 2. illustrates spatial multiplexing technique.

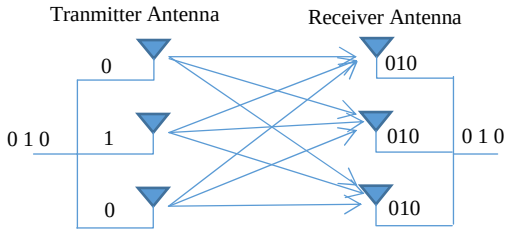

Fig. 2 MIMO with Spatial Multiplexing

The primary purpose of spatial multiplexing technique is to increase channel capacity, by splitting the high-speed data stream into some parallel data streams according to the number of transmitter antennas. With independent fading channels between transmitter and receiver pairs under multipath conditions, MIMO provides a linear capacity increase with the number of antennas used without increasing bandwidth and transmitting power.

The principle of spatial diversity is each transmitter antenna sends the same information signal in parallel by using different coding on an independent fading channel so that at the receiver there is at least one signal that does not undergo deep fade. The spatial diversity technique is illustrated by Fig. 3. Spatial diversity techniques can cope with fading and can significantly increase link quality and improve the signal-to-noise ratio (SNR) [15].

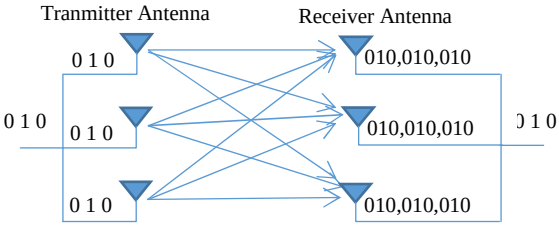

Fig. 3 MIMO with Spatial Diversity

OFDM modulation technique is one that uses multichannel scheme. This technique utilizes several subcarriers which are orthogonal. The orthogonal subcarrier can make bandwidth efficient. OFDM signals are generated using DFT (Discrete Fourier Transform) in receiver and IDFT (Inverse Discrete Fourier Transform) in the transmitter. To make low cost computation able to use fast fourier transform (FFT) for the transmitter and inverse fast fourier transform (IFFT) for the receiver. Applying the N-point IFFT for transmitted signals Isis transformed $\{s[n]\}_{n=0}^{N-1}$. $s[n]$ are OFDM signals, which is transmitted to the wireless channel. For example the received signals are $s[n]$ and the additive gaussian noise $z[n]$, so as $y[n] = s[n] + z[n]$. In the receiver, N-point FFT is

applied to transform $\{y[n]\}_{n=0}^{N-1}$ into $\{Y_1[m]\}_{m=0}^{N-1}$, transformed signals in the receiver.

Orthogonal signals are illustrated in Fig. 4. The subcarrier is considered to be orthogonal when one of the signals is at its maximum, and the other is at its lowest point.

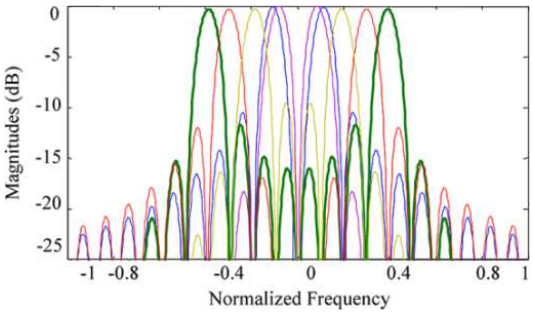

Fig. 4 Orthogonal Subcarrier Spectrum

In the OFDM signal, exponential signals $\{e^{j2\pi f_m t}\}_{m=0}^{N-1}$ indicate another subcarrier at $f_m = m/T_{sym}$ where time range is $0 \le t \le T_{sym}$. The subcarrier signals are interpreted as orthogonal if the integral of subcarrier signals multiplication for their general period is zero, as

$$\frac{1}{T_{sym}}\int_0^{T_{sym}} e^{j2\pi f_m t} e^{-j2\pi f_j t}\,dt = \frac{1}{T_{sym}}\int_0^{T_{sym}} e^{j2\pi \frac{m}{T_{sym}} t} e^{-j2\pi \frac{j}{T_{sym}} t}\,dt$$

$$= \frac{1}{T_{sym}}\int_0^{T_{sym}} e^{j2\pi \frac{(m-j)}{T_{sym}} t}\,dt$$

$$= \begin{cases} 1, & \forall \text{ integer } m = j \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

The discrete signals in time domain can be represented in equation (5), where $t = nT_s = n\,T_{sym}/N$, $n = 0,1,2,..,N\text{-}1$.

$$\frac{1}{N}\sum_{n=0}^{N-1} e^{j2\pi \frac{m}{T_{sym}} nT_s} e^{-j2\pi \frac{j}{T} nT_s} = \frac{1}{N}\sum_{n=0}^{N-1} e^{j2\pi \frac{m}{T_{sym}} \frac{nT}{N}} e^{-j2\pi \frac{j}{T_{sym}} \frac{nT_{sym}}{N}}$$

$$= \frac{1}{N}\sum_{n=0}^{N-1} e^{j2\pi \frac{(m-j)}{T_{sym}} nT_s}$$

$$= \begin{cases} 1, & \forall \text{ integer } m = j \\ 0, & \text{otherwise} \end{cases} \quad (5)$$

MIMO-OFDM is an alternative system which utilizes multiple antenna and multicarrier. This system can raise data rate without growing bandwidth. Fig. 5 and Fig.6 illustrate the design of the MIMO-OFDM system.

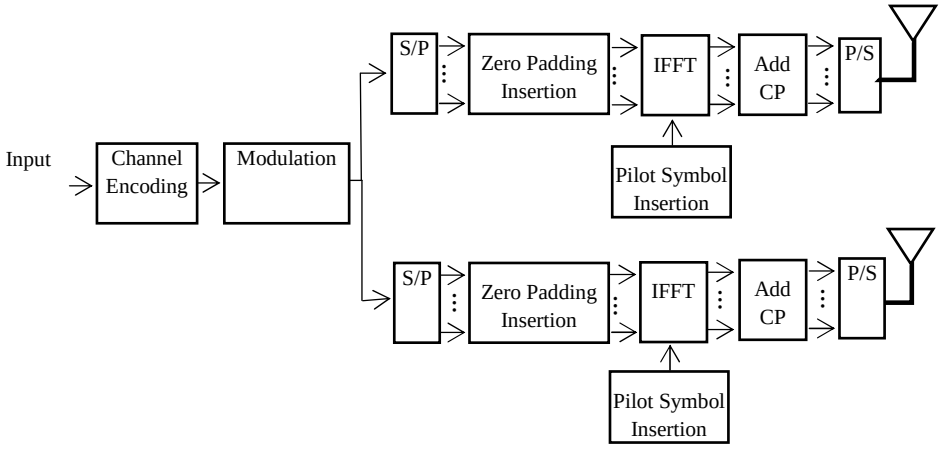

Fig. 5 Design of Transmitter on MIMO-OFDM System

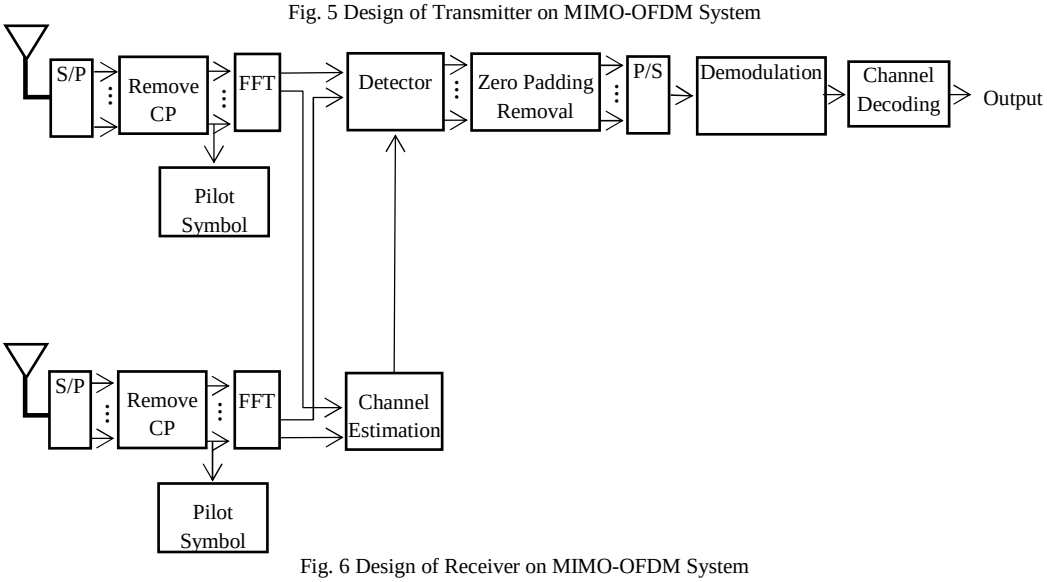

Fig. 6 Design of Receiver on MIMO-OFDM System

In this system, input data is encoded using convolutional channel coding. The function of channel coding is escalating performance of communication by modifying the number of the transmitted signal. Considered the convolution code has a code rate 1/2 is represented by Fig. 7.

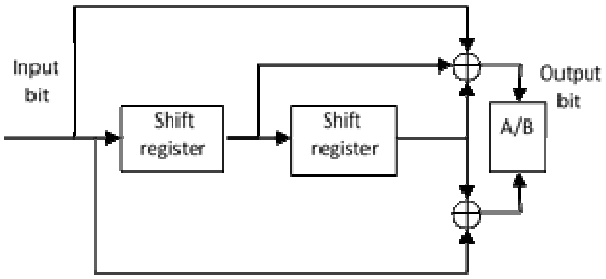

Fig. 7 Generator of Convolutional Code Rate ½

Code rate ½, it means one input will produce two outputs. Encoded information signals are modulated using digital modulation. The encoded signal form using M-ary QAM modulation is denoted by equation (6).

$$s_i(t) = \sqrt{\frac{2E_i(t)}{T}}\, a_i \cos 2\pi fct + \sqrt{\frac{2E_i(t)}{T}}\, b_i \sin 2\pi fct \quad (6)$$

Where, $0 \le t \le T$, i=1,2,...16. E_i is the energy signal and a_i b_i is the amplitude level to place each symbol into its constellation diagram.

OFDM process in transmitter converts a serial sequence of modulated signal into *N*-parallel bit sequence. Each N symbol results from serial to parallel will have an FFT with a different subcarrier. $s_i(n)$ represents *i*-th transmitted symbol with *n*-th subcarrier, $i = 0,1,2,..,\infty$, $n = 0,1,2,...,N\text{-}1$. For IFFT equations can be expressed by equation (7).

$$s_i(t) = \sum_{n=0}^{N-1} s_i(n) \sin\left(\frac{2\pi tn}{N}\right) - j \sum_{n=0}^{N-1} s_i(n) \cos\left(\frac{2\pi tn}{N}\right) \quad (7)$$

Adding CP (Cyclic Prefix) is one of the ways to minimize the occurrence of ISI (Inter-Symbol Interference). CP is copying of the last OFDM symbol which is placed in front of the symbol. ISI will affect the symbol in the form of CP, while the OFDM payload data are not distorted due to ISI. Length of CP can be configured 1/32, 1/16, 1/8 or 1/4 of OFDM symbol length. So the addition of CP period of OFDM symbol can be written in equation (8).

$$T = T_{CP} + T_{sym} \quad (8)$$

In Rayleigh fading channel, the obtained information signals will have noise and multipath fading. The equation of obtained signals can be seen in equation (2) dan (3). OFDM receiver has IFFT process to change the signal's domain into the time domain. The equation FFT is represented by equation (9) as follows :

$$s_i(n) = \sum_{t=0}^{N-1} s_i(t) \sin\left(\frac{2\pi tn}{N}\right) + j \sum_{t=0}^{N-1} s_i(t) \cos\left(\frac{2\pi tn}{N}\right) \quad (9)$$

The V-BLAST/ZF Detection algorithm is one type of V-BLAST algorithm combined with the ZF concept. Systematically can be implemented by following equation (10) to (17) [16]:

Initialization :

$$W_1 = H^+ \quad (10)$$

$$i = 1 \quad (11)$$

Recursion :

$$k_i = \underset{j \notin \{k_1, \ldots, k_{i-1}\}}{\arg\min} \left\| (W_i)_j \right\|^2 \quad (12)$$

$$y_{k_i} = (W_i)_{k_i} r_i \quad (13)$$

$$\hat{a}_{k_i} = Q(y_{k_i}) \quad (14)$$

$$r_{i+1} = r_i - \hat{a}_{k_i} (H)_{k_i} \quad (15)$$

$$W_{i+1} = H_{\bar{k}i}^{+} \quad (16)$$

$$i = i + 1 \quad (17)$$

The purpose of the MMSE estimation is to obtain a better estimation value, in this case, is the appropriate load selection (W), so the above equation must be minimized. By utilizing the orthogonality properties of the estimation error vector $e = H - \hat{H}$ to be orthogonal to can be written by the equation:

$$\begin{aligned} \{e\hat{H}^H\} &= E\{(H - \hat{H})\hat{H}^H\} \\ &= E\{(H - W\hat{H})\hat{H}^H\} \\ &= E\{HH^H\} - WE\{HH^H\} \\ &= R_{H\hat{H}} - WR_{\hat{H}\hat{H}} \\ &= 0 \end{aligned} \quad (18)$$

In this case $\hat{H}$ is the least square (LS) channel estimation given in the equation (19).

$$\hat{H} = X^{-1}Y = H + X^{-1}Z \quad (19)$$

Then, W is obtained as in the equation (20) :

$$W = R_{H\hat{H}} R_{\hat{H}\hat{H}}^{-1} \quad (20)$$

Where $R_{H\hat{H}}$ is the autocorrelation matrix of H and given the equation

$$\begin{aligned} E\{e\hat{H}^H\} &= E\{\hat{H}\hat{H}^H\} \\ &= E\{X^{-1}Y(X^{-1}Y)^H\} \\ &= E\{(H + X^{-1}Z)(H + X^{-1}Y)^H\} \end{aligned}$$

$$= E\{HH^H\} + E\{X^{-1}ZZ^H(X^{-1})^H\}$$

$$= E\{HH^H\} + \frac{\sigma_z^2}{\sigma_x^2} I \quad (21)$$

Isis the cross-matrix correlation between the real channel vector with the temporary channel vector in the frequency domain. Furthermore, MMSE channel estimation can be given as in the equation (22) :

$$\begin{aligned} \hat{H} &= W\hat{H} \\ &= R_{H\hat{H}} R_{\hat{H}\hat{H}}^{-1} \hat{H} \\ &= R_{H\hat{H}} \left(R_{HH} + \frac{\sigma_z^2}{\sigma_x^2} I \right)^{-1} \hat{H} \end{aligned} \quad (22)$$

Then the signal is demodulated by M-QAM demodulator. The output of the demodulator to be decoded using Viterbi algorithm to obtain back row of transmitted bits by the transmitter.

A. RSA Algorithm for Synchronization

RSA is a cryptographic algorithm which applies the concept of public key cryptography. This algorithm was first evolved by; Rivest, Adi Shamir, and Leonardo Adleman were developers of RSA (Rivest Shamir Adleman) cryptography from MIT. RSA is an easy-to-implement and understandable algorithm. RSA algorithm is an application of many theories such as extended Euclid algorithm, Euler's function to format theorem. The key is applied to encode called the public key, and which is applied to decode is called the private key or secret key. RSA requires three steps in the process, namely crucial generation, encrypt messages, and messages decryption. Encryption and decryption process is almost the same process. On the RSA algorithm, to know the secret key is robust because of the factoring of significant numbers *x* into two prime numbers.

There are the parameters or quantities used in RSA cryptography:

a. p and q primes (secret)
b. x = pq (not secret)
c. φ (x) = (p-1) (q-1) (secret)
d. e (encryption key) (no secret)
e. d (decryption key) (secret)
f. m (plaintexts) (secret)
g. c (chipertexts) (not secret)

Based on the theory, RSA algorithm is based on Euler's theorem expressed as follows:

$$a^{\varphi(x)} \equiv 1 \ (mod\ x) \quad (23)$$

Where the value of a must be relatively prime to the value of *x*, and the value of $\varphi(x)$ is

$$\varphi(x) = x\left(1 - {}^1/_{y_1}\right)\left(1 - {}^1/_{y_2}\right) \ldots\ldots\ldots \left(1 - {}^1/_{y_r}\right) \quad (24)$$

which in this case $y_1, y_2, \ldots\ldots y_r$ is the prime factor of $\varphi(x)$ is a function that determines how many of the numbers 1, 2, 3, ..., *x* is relatively primed to *x*.

Based on the properties of $a^z \equiv b^z \ (mod\ x)$ for integers z ≥ 1, then equation (23) becomes

$$a^{z\varphi(x)} \equiv 1^z \ (mod\ x) \quad (25)$$

Alternatively, it can be written with :

$$a^{z\varphi(x)} \equiv 1 \ (mod\ x) \quad (26)$$

If a is replaced by M, then equation (26) turns into the following :

$$M^{z\varphi(x)} \equiv 1 \ (mod\ x) \quad (27)$$

Based on the nature of $ac \equiv bc \ (mod\ n)$, then if M multiplies equation (27) then the equation changes to :

$$M^{z\varphi(x)+1} \equiv M \ (mod\ x) \quad (28)$$

The next step is to select the value of E (encryption key) and D (decryption key). suppose the values of E and D are chosen such that

$$E.D \equiv 1 \left(mod\ \varphi(x)\right) \quad (29)$$

Or

$$E.D = z\varphi(x) + 1 \quad (30)$$

The sequence of plaintext encryption and decryption processes using RSA algorithm is illustrated in Fig. 8

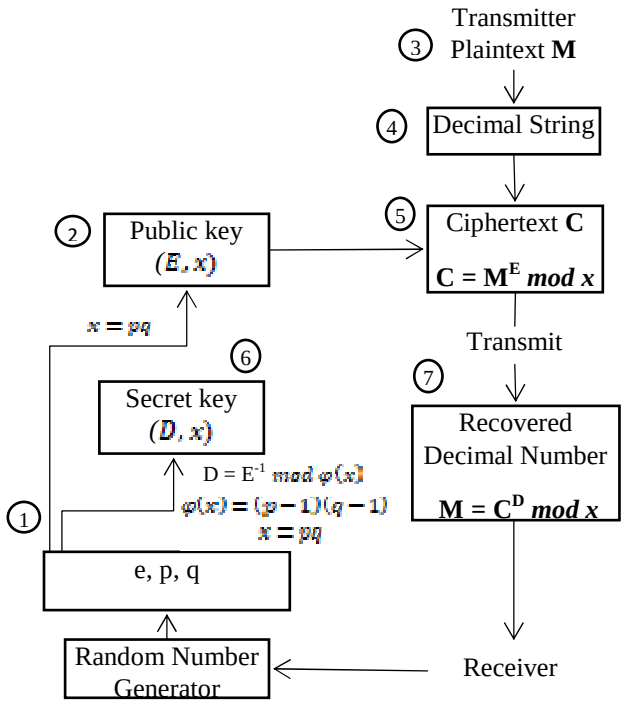

Fig. 8 The Sequence of cryptanalysis Using RSA

In this research, plaintext will be encrypted is not information data, but it is a random number. Cryptanalysis

process is used for synchronization between transmitter and receiver. RSA algorithm for synchronization uses 64 bits because subcarriers which used on OFDM system are 64 subcarriers.

B. The Proposed Security Method

The 802.11n Wireless LAN Standard has pledged that the OFDM technology has been used and adapted to meet its various requirements. The 802.11n works on bandwidth 20 MHz using 56 subcarriers. 56 subcarriers consisting of 52 data transmission subcarriers and four pilot subcarriers. Subcarrier 0 is the center of the carrier. Subcarrier -29 until -32 and +29 until +32 is filled zero padding. The proposed security method which used on the MIMO-OFDM system is subcarrier randomization. This physical layer security utilizes subcarrier on OFDM technology. The goal of security method is securing data without the decreased performance of the system when eavesdroppers try to retrieve sent data. Fig. 9 is shown a MIMO-OFDM system using subcarrier randomization security method.

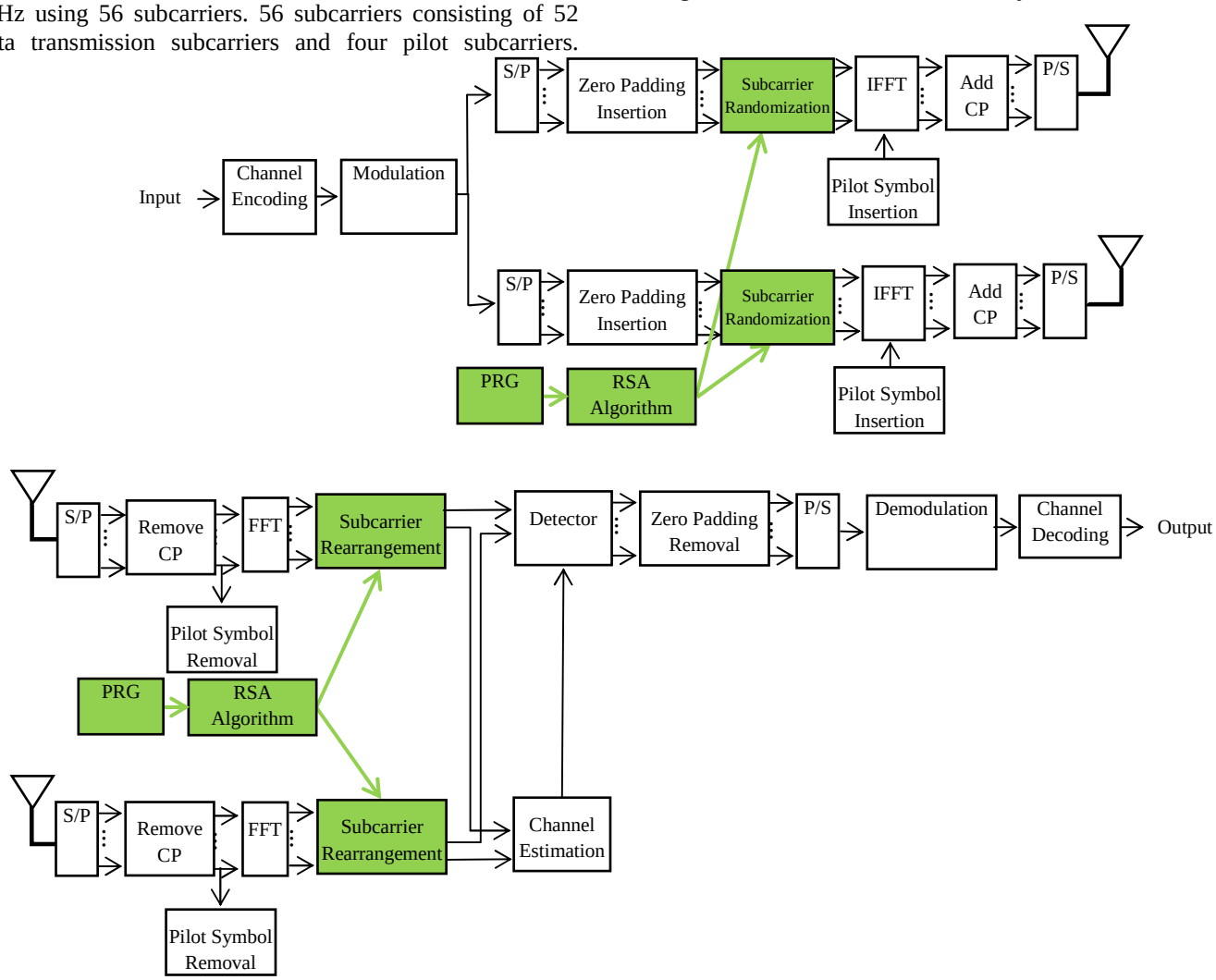

Fig 9. The proposed Block Diagram System

Subcarrier randomization is the change of bits of plaintext generated using pseudo-random generator and its ciphertext. n order for the receiver to know perfectly the location of the subcarrier randomization then it needs a synchronization. One of synchronization technique is using RSA algorithm. For more details, the complete subcarrier randomization algorithm is as follows :

Step 1 : Create a sequence of bits according to the length of the subcarrier using pseudo-random generator.
Step 2 : Change the sequence of bits into decimal numbers
Step 3 : Specify the value of p, q. p and q are prime numbers.
Step 4 : Choose the value of E (public key), where E < x, E is relative prime with $\varphi(x)$.
Step 5 : Compute secret key (D,x).

$$D = \frac{z\varphi(x) + 1}{E}$$

Step 6 : Create ciphertext by encrypting the decimal number using RSA cryptography.

$$E_E(M) = C = M^E \bmod x$$

Step 7 : Convert ciphertext into a sequence of bits.

Step 8 : Location of the subcarrier is randomized based on the change of initial bit with the ciphertext bit.

Step 9 : Decrypt the ciphertext on the receiver using a secret key of the authorized receiver.

$$D_p(C) = M = C^D \bmod x$$

Step 10:Change the ciphertext into sequence bits.

Step 11:Position the subcarrier in its original location according to the change of ciphertext bit with the decrypted bit.

Step 12:Subcarrier position back as early.

Fig 10. is a flow diagram of randomization on transmitter, we let the data length is 8 bits (Example: 1000011), which is converted to decimal = 134 (M), then searched the ciphertext to the equation $C = M^E \bmod x$, in this case E = 61 and x = 187.

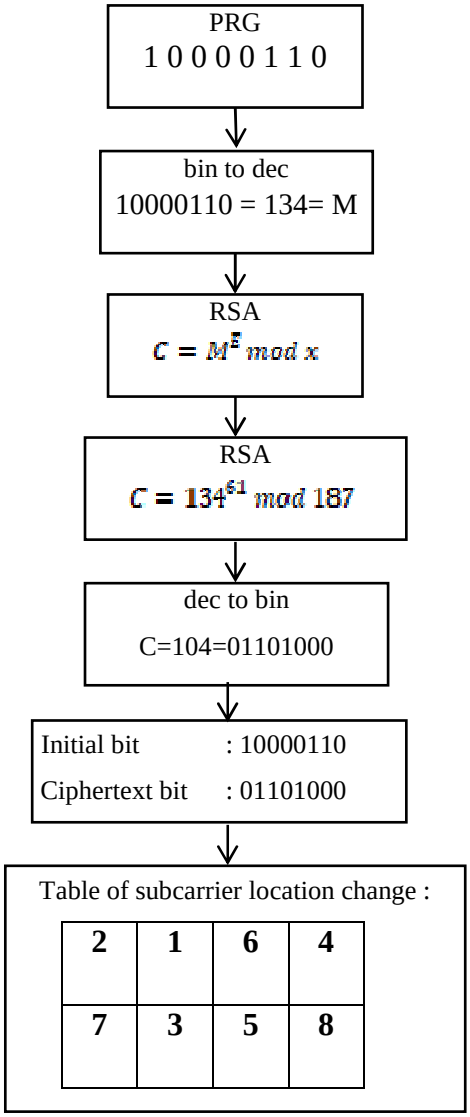

Fig. 10 Flow Diagram of Randomization on Transmitter

The subcarrier position is rearranged as before at the receiving end. For more details, it is explained by the Fig. 11 :

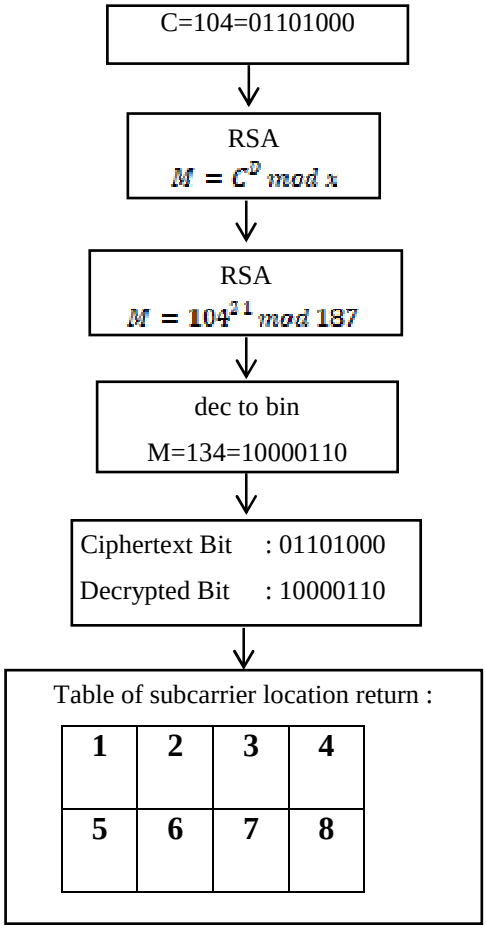

Fig. 11 Flow Diagram of Randomization on Receiver

III. Results and Discussion

In the simulation of the MIMO-OFDM system, the carrier frequency is 2.4 GHz with bandwidth 20 MHz. The simulation of system use parameters in Table 1.

TABLE I
SYSYEM'S PARAMETER

Section	Parameters	Value
Transmitter	Channel Coding	Convolution Code
	Code Rate	½
	Modulation	4QAM
	Sequence of Pilot	HTLTF
	Amount of Subcarrier	56 subcarrier
	Size of FFT	64
	Number of Antenna	2x2
	Size of CP	25% size of FFT
Channel	Channel model	Rayleigh Fading
	Noise	AWGN
Receiver	Channel Estimation	MMSE
	Detection	V-BLAST/ZF

This system needs adding zero padding because the number of subcarriers is 56 while the FFT size is 64. We will contrast performance of the system when it uses security method and without security method. According to 802.11n standard, we use high throughput (HT) mode for data

transmission on a channel with 20 MHz bandwidth. Subcarrier number -28 until -1 to and 1 until 28 are used for data transmission, while subcarrier number -32 until -29 and 29 until 32 are interjected zero padding.

On section result and discussion, we exhibit performance of MIMO-OFDM wireless communication using subcarrier randomization through Bit Error Rate (BER) and Quality of Service (QoS) measurement.

A. Bit Error Rate (BER)

Bit Error Rate or BER is one of digital communication parameter which indicates the level of system performance when sending data information, where BER is the ratio between the number of bits received incorrectly and the total number of bits received. Fig. 12 is a comparison of MIMO-OFDM system performance when using security and without security.

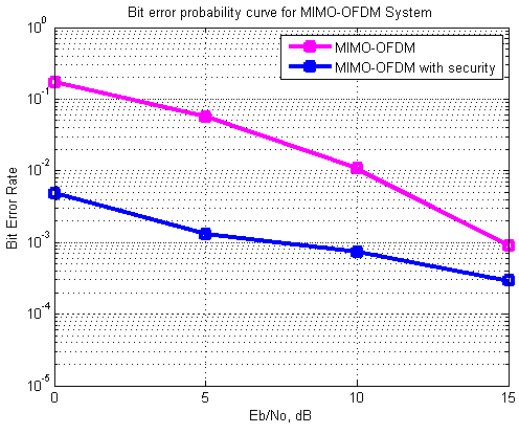

Fig. 12 Comparison of System with Security and without Security

Fig. 12 shows the performance of MIMO-OFDM with subcarrier randomization is better than MIMO-OFDM without security. This proves that the subcarrier randomization security method does not bring down or worsen the performance of the MIMO-OFDM system. The bit error rate of the MIMO-OFDM system with subcarrier randomization security method is 2.92×10^{-4} whereas MIMO-OFDM without its BER security is 1.2×10^{-1} when SNR is 15 dB. MIMO-OFDM system uses subcarrier randomization security technique without RSA algorithm synchronization have bit error rate which is almost the same as MIMO-OFDM without security [13]. In this research, we use RSA algorithm for synchronization between transmitter and receiver. Synchronization uses RSA algorithm not only to synchronize positions of the randomized subcarrier but also to reduce the number of transmitted bit errors. MIMO-OFDM performance improvement when using RSA algorithm for synchronization occurs because the synchronization can overcome the phenomenon of CFO (Carrier Frequency Offset) and STO (Symbol Time Offset) in the MIMO-OFDM system. CFO and STO resulted in decreasing system performance. Jitter causes CFO on the carrier wave and also to the Doppler effect caused by the device by both the transmitter station and the receiver station whereas delay or leading signal cause STO.

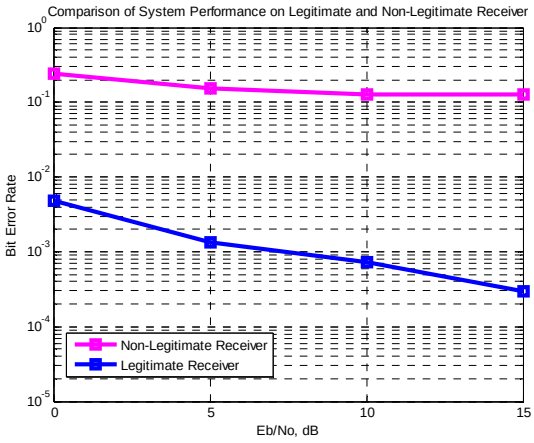

Fig. 13 Comparison of Performance on Legitimate and Non-Legitimate Receiver

Performance of MIMO-OFDM system on the non-legitimate receiver is shown in Fig. 13. Non-legitimate receivers have higher bit error rate than legitimate receivers. It proves the subcarrier randomization security method can protect the transmitted information data from eavesdroppers.

B. Quality of Service (QoS) Measurement

Quality of Service (QoS) is a method of measuring how good network and an attempt to define the characteristics of service. QoS is used to measure a set of performance attributes which have been specified and associated with a service. The parameters of Quality of Service (QoS) measured in this research are throughput, packet loss, and delay.

Throughput is the speed (rate) of information data transfer, measured in bps (bits per second). To calculate throughput using the formula in equation (31) :

$$\text{Throughput} = \frac{rp}{t} \tag{31}$$

rp is received packets and *t* is the delivery time.

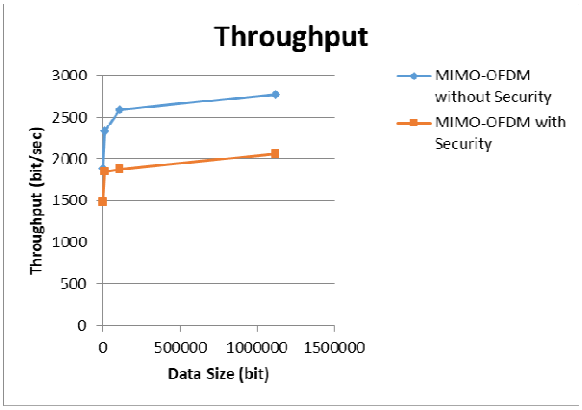

Fig. 14 Comparison of Throughput Values

From the Fig. 14, the throughput value of the MIMO-OFDM without a security system is higher than the MIMO-OFDM system using the security method. For more details, details of the throughput value can be seen in Table 2.

TABLE II
THROUGHPUT ON MIMO-OFDM SYSTEM

Data Size (bit)	Throughput (bits/sec)	
	Without Security	With Security
1,120	1,888.78	1,480.77
11,200	2,328.23	1,848.48
112,000	2,592.71	1,881.53
1,120,000	2,778.04	2,056.02

When the data sent by 11.2 K bits, throughput generated on the system using security is 1,848.48 bits/sec while the system without security can reach 2,323.23 bits/sec.

Packet loss is defined as data transmission failure reaching its destination. Some interference can cause failure of the package to reach the destination. Calculating of packet loss is follow as :

$$pc = \frac{(tp - rp)}{tp} x\ 100\% \quad (32)$$

Where tp is transmitted, packet and rp have received the packet. As in Fig. 15, during the data transmission, takes place the packet loss generated on MIMO-OFDM with security is less than MIMO-OFDM without security. This happens because in the proposed security method there is a synchronization process between transmitter and receiver. OFDM is very sensitive to STO and CFO. CFO caused by jitter on a carrier wave and also to Doppler effect caused by the device either by transmitter or receiver. CFO resulted in a phase shift. The STO is caused due to delay or leading signal first. CFO and STO can be solved by synchronization using RSA algorithm. From the above packet loss result can be analyzed that subcarrier randomization security method by using RSA synchronization algorithm in the MIMO-OFDM system can improve data delivery performance.

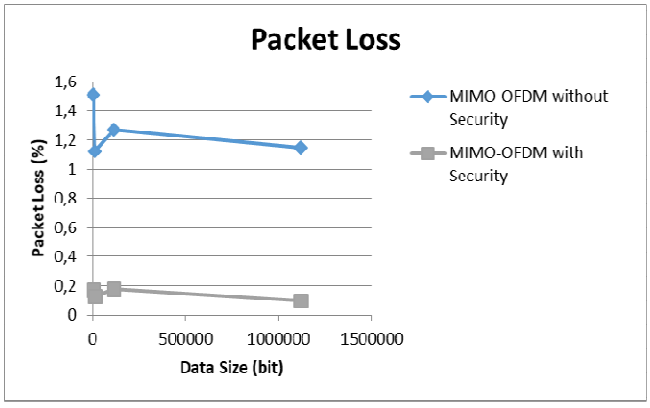

Fig. 15 Comparison of Packet Loss Values

We can see the comparison of packet loss values in a MIMO-OFDM system using subcarrier randomization and MIMO-OFDM without security system on Fig. 15. From Table 3, it is shown that in MIMO-OFDM without security when data sent of 112000 bits has a packet loss of 1.27% while using subcarrier randomization security method has packet loss equal to 0.18%.

TABLE III
PACKET LOSS ON MIMO-OFDM SYSTEM

Data Size (bit)	Packet Loss (%)	
	Without Security	With Security
1,120	1.51	0.17
11,200	1.125	0.13
112,000	1.27	0.18
1,120,000	1.15	0.10

Delay is the time delay of a packet caused by the transmission process from one point to another point of its purpose. On Fig. 16, the delay of MIMO-OFDM with security is higher than MIMO-OFDM without security because of the computation of subcarrier randomization for data security and RSA algorithms for synchronization between the transmitter and receiver.

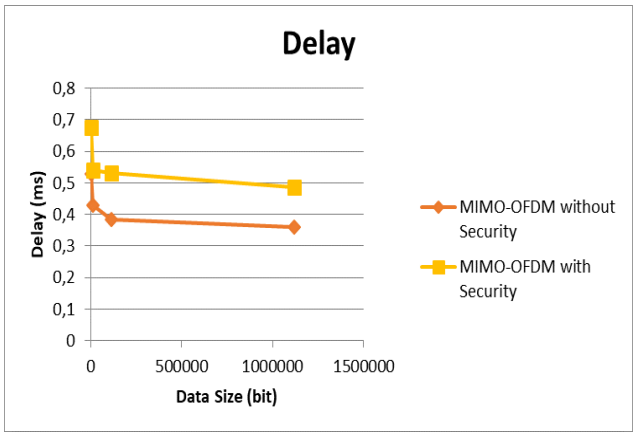

Fig. 16 Comparison of Delay Values

The delay value can be seen more detail in Table 4. Delay calculation formula at equation (33) :

$$dl = \frac{td}{trp} \quad (33)$$

td is a total delay when data is transmitted and *trp* is a total received packet.

TABLE IV
DELAY ON MIMO-OFDM SYSTEM

Data Size (bit)	Delay (ms)	
	Without Security	With Security
1,120	0.529	0.675
11,200	0.429	0.540
112,000	0.385	0.531
1,120,000	0.359	0.486

Delay generated when sending data 1120000bits on a MIMO-OFDM system using security is 0.486 ms while in the system without subcarrier randomization security method its delay is 0.359 ms. This happens because the system takes more time to compute subcarrier randomization with synchronization using the RSA algorithm.

IV. CONCLUSIONS

Subcarrier randomization is one of security method which applied on MIMO-OFDM wireless communication. This security method can secure information data from an eavesdropper. Subcarrier randomization needs synchronization to know the position of the randomized subcarrier. We use RSA algorithm for synchronization. Synchronization using the RSA algorithm not only helps to know the randomized subcarrier position on the receiver but also overcomes the phenomenon of CFO and STO. This is proven because the average packet loss is minimal in a MIMO-OFDM system with security is 0.145%.

ACKNOWLEDGMENT

This research was partially supported by the Penelitian Terapan Unggulan Perguruan Tinggi (PTUPT) Grant 2018 Program of Ristek-Dikti Indonesian Government.

REFERENCES

[1] S. Aramvith and R. D. Cajote,"Handbook of Research on Secure Multimedia Distribution", ISBN-13: 978-1605662626 ,Pp. 211-240, Information Science Reference ,2009

[2] I. G. P. Astawa, Y. Moegiharto, A. Zainudin, I. D. A. Salim, & N. A. Anggraeni, "Performance of MIMO-OFDM using convolution codes with QAM modulation", Proc. SPIE 9159, Sixth International Conference on Digital Image Processing (ICDIP), 2014.

[3] L. Kansal, A. Kansal, K. Singh, "Performance Analysis of MIMO-OFDM System Using QOSTBC Code Structure for M-PSK", *Canadian Journal on Signal Processing*, vol.5, no. 2, May 2011.

[4] Pathak, Neha. "OFDM (Orthogonal Frequency Division Multiplexing) Simulation Using MatLab." *International Journal of Engineering Research and Technology*. Vol. 1. No. 6 (August-2012). ESRSA Publications, 2012.

[5] W.Stalling, "Network Security Essentials: Applications and Standards", Fourth edition, Prentice-Hall, Inc., 2011.

[6] S.Gupta and C.Kumar, "Shared Information Based Security Solution for Mobile Ad Hoc Networks", international Journal of wireless & mobile networks(IJWMN), Vol.2, No.1, February 2010, pp.176-187, 2010.

[7] B.A. Forouzan, "Data Communications and Networking", McGraw-Hill, 4 th Edition.

[8] W. Stallings, "Cryptography and etwork Security: Principles and Practice", Pearson Education/Prentice Hall, 5 th Edition.

[9] Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." *International Journal of Computer Applications* 67.19 (2013).

[10] Singhal, Nidhi, and J. P. S. Raina. "Comparative analysis of AES and RC4 algorithms for better utilization." *International Journal of Computer Trends and Technology* 2.6 (2011): 177-181.

[11] Vincent, PM Durai Raj, and E. Sathiyamoorthy. "A novel and efficient public key encryption algorithm." *International Journal of Information and communication technology* 9.2 (2016): 199-211.

[12] Zhang, Xiaozhong, et al. "A secure OFDM transmission scheme based on chaos mapping." *Computing and Communications Conference (IPCCC), 2015 IEEE 34th International Performance*. IEEE, 2015.

[13] R.P. Hudhajanto, I.G.P. Astawa, and A. Sudarsono. "Covert Communication in MIMO-OFDM System Using Pseudo Random Location of Fake Subcarriers." *EMITTER International Journal of Engineering Technology* 4.1 (2016): 150-163.

[14] I. Hen, "MIMO Architecture for Wireless Communication", in Intel Technology Journal, vol.10, issue02, May 2006.

[15] Rohde and Schwarz, *"Introduction to MIMO Systems"*, Munchen, 2006.

[16] Y. S. Cho etc, "MIMO-OFDM Wireless Communication with Matlab," WILLEY, 2010.