Increase Security in DS/CDMA UWB using Hybrid Method of CDMA

Bayan M. Sabbar
Information Technology Department
College of Information Engineering
Al-Nahrain University
Baghdad- Iraq

Ula Mohsen Taher
Network Engineering Department
College of Information Engineering
Al-Nahrain University
Baghdad-Iraq

ABSTRACT

ULTRA-WIDEBAND (UWB) is a new technology that provides high data rate and low power consumption. The physical layer built in of DS/CDMA UWB is provided by short pulses of nanosecond, the low output power and the absence of carrier signal. CDMA methods are considered as the main proposed method in this paper by integrating cryptographic techniques into the transceiver design. The two main methods that used in enhancement physical layer of CDMA are proposed to be used in DS/CDMA UWB in this paper. The first one is hidden direct sequence for encrypting spreading code. The second one is secure scrambling method at chip rate, which is based on Advanced Encryption Standard (AES) and Output Feedback Mode (OFB). The hybrid method is found much stronger than using anyone of the above method individually.

Keywords

Ultra-Wideband (UWB), Code Division Multiple Access (CDMA), Advanced Encryption Standard (AES), Output Feedback Mode (OFB), and Initialization vector (IV).

1. INTRODUCTION

Wireless networks plays important role in our daily life especially in civil and military application. Security of information is critical issue in wireless networks. It is very important to keep the data secret from the intruders and accessible only from intended users[1]. Wireless network is an un trustable environment [2] because the eavesdropper can obtain the signal in easy way by placing as antenna in the desired field. If messages are encrypted using strong encryption algorithm the Eavesdropper can not detect the signal and just the receiver can detect it [3].

Ultra Wideband (UWB) systems is one of possible solution that provides high data rate and low power for short ranges wireless networks [1]. This system is characterize by transmitting series of short pulses of sub nano seconds (monocycle) [2]. The Federal commission committee allows UWB devices to operate in a unlicensed band spectrum from 3.1 to 10.6 GHz with power of -41.3 dbm/MHz. The low power ensures the

UWB devices do not interfere with licensed services and other important operations (e.g. 802.11a devices). According to the DS/CDMA UWB proposal from Xtreme Spectrum company, the transmitted signal can lie in two bands: low band (LB, 3.1-5. I5 GHz) with chip rate 1368 Mc/s and high frequency band (HB, 5.825– 10.6 GHz) with chip rate 2736 Mc/s [4]. The single band can be implemented using impulse radio which based on base band pulses of very short duration in order of nano seconds. The advantage of these base band pulses that do not require up/down converter, this will reduce complexity and cost manufacturing [5].

UWB radios are inherently a built in security due to the low power of signal that is done by spreading one bit over multiple pulses. Also, short duration of pulses make the transmission appear to be like white noise[6]. These narrow pulses provides a measure of security because they allow little time for interception with other radio technologies. In a addition, the short pulses produce an ultra wide spectrum covering a bandwidth nominally in the range of hundreds of megahertz. These characteristics allow transmission of data in based band signal without need to carrier signal. The absence of a carrier signal provide secure transmission for UWB technology [7].

In spite of the built in security that provided in UWB devices, UWB signals could potentially be Penetrates by a attacker who is located close to the transmitter[6]. In this paper, the physical layer built-in security of DS/CDMA UWB is improved using hybrid method of CDMA security methods mentioned in section 3 to increase security in the system and prevent attacker from sniffing the signals.

2. DS/CDMA UWB SYSTEM MODEL

The direct-sequence CDMA that is powerful technique for achieving multi users in the system, it is very efficient when there are many users (>7 users). This system combines the power of two techniques: UWB and DS/CDMA techniques. In this application, the DS/CDMA is not used for spread spectrum but for multi-user access [8].

This system use single channel to accommodate more number of users at the same time. The transmitter uses first derivative Gaussian pulses which is called monocycle that are modulated using a bi-phase modulation technique [5]. The monocycle is mathematically defined as [5, 8, 9]:

$$p_{tx} = \left(\frac{t}{\tau}\right) e^{-\left(\frac{t}{\tau}\right)^2} \qquad (1)$$

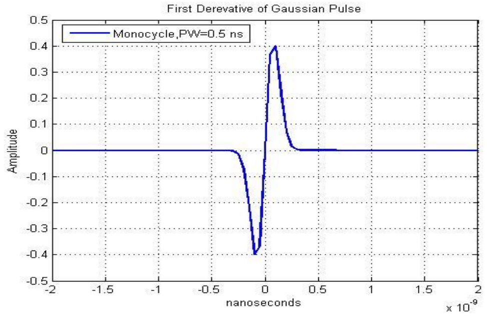

Figure 1. First derivative of a Gaussian pulse, low band of UWB. PW=0.5 ns

The bandwidth of the signal are determined by τ, where τ is the pulse width. The channel bandwidth of the system is defined by the bandwidth of the UWB pulse. The channel bandwidth is equal to 1/τ. In this case τ is equal to 0.5 ns [5].

The monocycle pulses are transmitted continuously. It is necessary to encode those pulses my multiplying then with pseudo random noise code of length SF= Tb/Tc which makes it possible for the receiver to separate the signals coming from different users [10]. At the receiver the signal is detected by a correlator receiver (matched filter), by multiplying the incoming signal with the template monocycle that generated at receiver. The Correlation results are integrated using int/dump over pulses to form the data bit Tb [11]. The result signal is then applying to the decision variable to decide the bits zero or one [10].

As a result of the above work mentioned in references [5,8,9,10,11], it is important to summarize their work in the block diagram in figure 2.

DS/CDMA UWB system with Nu users and N processing gain is N , that produces N chips per symbol. The resultant signal coming from users u can be given mathematically:

$$s^{(u)}(t)=\sum_{j=0}^{\infty}\alpha^{(u)}\left(\left|\frac{j}{N_s}\right|\right)\cdot\phi^{(u)}(t-jT_b) \qquad (2)$$

$$=\sum_{j=0}^{\infty}\alpha^{(u)}\left(\left|\frac{j}{N_s}\right|\right).\sum_{i=0}^{N-1}C_i^{(u)}\cdot p_{tx}(t-jT_b-iT_c)$$

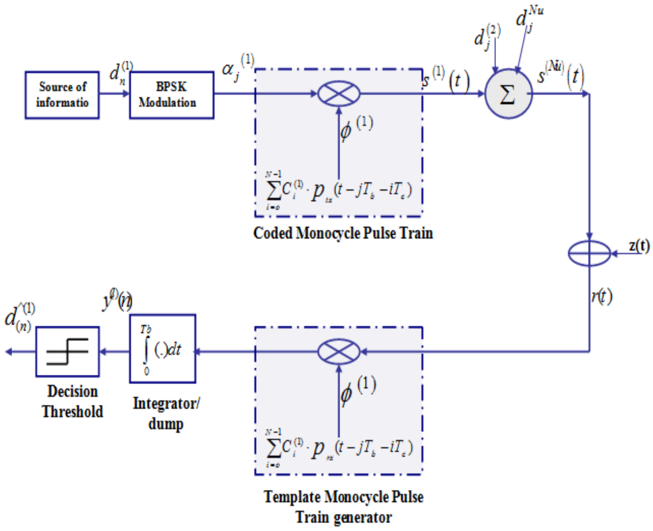

Figure 2. Block diagram DS/CDMA UWB system

Where, *Nu*: total number of users in the system, $p_{tx}(t)$:is the transmitted monocycle pulse located from 0 to chip duration T_c [10], pulse duration $Tp \le Tc$ [5,10], N_s: number of monocycle pulses per information bit, $\alpha^{(u)}\left(\left|\frac{j}{N_s}\right|\right)$: Carry information from user *u (u=1,•••,Nu)* denote the u^{th} user's j^{th} symbol, $d^{(u)}(n)\in\{0,1\}$: $n^{(th)}$ information bit from the $u^{(th)}$ user. The BPSK modulation variable is given by [5,10] :

$$DS-BPSK:\alpha^{(u)}\left(\left|\frac{j}{N_s}\right|\right)=\alpha^{(u)}(n)=2d^{(u)}(n)-1 \qquad (3)$$

The reason for inner summation in equation (2), each bit of the bipolar pseudo random noise code must multiply by the template monocycle pulse. For later use with matched filtering the template monocycle is multiplying by incoming signal, the template monocycle pulse of u^{th} user is termed $\phi^{(u)}(t)$, it defined by [10]:

$$\phi^{(u)}(t)=\sum_{i=0}^{N-1}C_i^{(u)}\cdot p_{tx}(t-iT_c) \qquad (4)$$

$C_j^{(u)}\in\{-1,+1\}$: Binary spreading code used to perform pseudo-random codes for each u^{th} user at the j^{th} pulse.

All users signals are transmitted together via AWGN Channel with zero mean and two-sided spectral density equal to N0/2 [10].

$$r(t)=\sum_{u=1}^{Nu}A_u s^{(u)}(t)+z(t) \qquad (5)$$

In the receiver to detect the data of user *l*, the incoming signal $r(t)$ is multiplied by the coded monocycles $\phi^{(l)}(t)$ of associated user *l* and integrated over Ns pulses to form sufficient statistics $y^{(l)}(n)$ for the l^{th} user [10].

$$y^{(l)}(n)=\int_{nT_b}^{(n+1)T_b}\phi^{(l)}(t-nT_b).r(t)dt \qquad (6)$$

$$=\int_{nT_b}^{(n+1)T_b}\phi^{(l)}(t-nT_b).\left(\sum_{u=1}^{Nu}A_u s^{(u)}(t)+z(t)\right)dt$$

Where $z(t)$: is white Gaussian noise with unit variance, and $A^{(u)}$: is the amplitude of u^{th} user.

The receiver monocycle $P_{rx}(t)$ is normalized [10]:

$$\int_0^{T_c}P_{rx}(t).P_{rx}(t)dt=1\Leftrightarrow\int_0^{Tb}\phi^{(l)}(t).\phi^{(l)}(t)dt=SF \qquad (7)$$

The correlation between the codes *l* and *u* in a completely synchronous system [10]:

$$\rho_{lu}=\int_0^{T_b}\phi^{(l)}.\phi^{(u)}(t)dt \qquad (8)$$

Can be used to yield:

$$y^{(l)}(n)=\sum_{u=1}^{Nu}\rho_{lu}A_u\alpha^{(u)}(n)+z^{(l)}(n) \qquad (9)$$

$$=\overbrace{SF\,A_l\alpha^{(l)}(n)}^{Desired}+\overbrace{\sum_{u\neq1}\rho_{lu}A_u\alpha^{(u)}(n)}^{Interference}+\overbrace{z^{(l)}(n)}^{Noise}$$

The correlation between any code and itself is $\rho_{ll}=SF$ and $\rho_{lu}=\rho_{ul}$, z(n) being noise samples.

The first part is the desired signal of user *l* and the next is the interference component coming from all other users in the system [10].

The signal now is applying the signal $y^{(l)}(n)$ to the decision variable which implemented by using the sgn function to decide the bit one or zero [10].

$$\hat{d}^{(l)}(n) = \operatorname{sgn}(y^{(l)}(n)) \qquad (10)$$

The decision variable will be [10]:

$$\hat{d}^{(l)}(n) = \operatorname{sgn}(SF.\alpha^{(l)} A_l + v) \qquad (11)$$

Where v is the sum of the noise and interference components [10].

The bit error probability of the coherent BPSK system matched filter reception is given by [8,11]:

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \qquad (12)$$

Where: $Q(x) = 0.5 * erfc(x / \sqrt{2})$ (13)

E_b is the bit energy, N_0 is the one-sided thermal noise power spectral density of the receiver.

3. SECURITY METHODS OF CDMA

In the current CDMA system, each user's signal is spread by multiplying it with the pseudo random noise code known as channelization code. The spreading signal is then scrambled using pseudo-random sequence to randomize the interference and make the signal appear like noise and can not detect and intercept by the intruders. To recover the desired user's signal, the intruder must knowing both the channelization code and scrambling code. The security of the CDMA system is depends on the long code generator from 42-bit Linear Feedback Shift Registers (LFSRs). The maximum complexity to recover the 42-bit long code mask is $O(2^{42})$. If the intruder can obtain the 42 bit plaintext-cipher text pairs, the long-code mask can be recovered after dropping the transmission on the traffic channel for about one second [12]. IS-95, CDMA uses the long-code to scramble the signal, and the security is set up in the physical layer. This available security is very low security and it is not suitable for data communication when compared with voice communications [3].

Secure scrambling sequence method at chip rate is used to enhance the physical layer built-in security of CDMA systems but with limited complexity load. This method use the advanced encryption standard (AES as known as Rijndael) with OFB (Out put feed back mode). The scrambling sequence can be generated from the initial vector and the AES secret key in output feedback mode (OFB). This method limit the block size and the key size to 128 bits, the scrambling sequence is produced by repeatedly encrypting the 128-bit initialization vector [2].

AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications [13]. AES cipher limit the plain text with block size 128 bits, or 16 bytes. The AES secret key can be 16, 24, or 32 bytes (128, 192, or 256 bits). The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length [13].

The Output Feedback (OFB) mode is a confidentiality mode that use the iteration of the forward cipher on an IV to generate a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. The OFB mode requires that the IV is a nonce. The IV must be unique for each execution of the mode under the given key [14]. The OFB encryption and decryption are done as follow:

OFB Encryption:

$$\begin{array}{ll} I_1 = IV; & \\ I_j = O_{j-1}; & forj = 2....n; \\ O_j = CIPH_K(I_j) & forj = 1,2....n; \\ C_j = P \oplus O_j & forj = 1,2....n-1; \\ C^*_n = P_n^* \oplus MSB_u(O_n). & \end{array}$$

OFB Decryption:

$$\begin{array}{ll} I_1 = IV; & \\ I_j = O_{j-1} & forj = 2....n; \\ O_j = CIPH_K(I_j) & forj = 1,2....n; \\ P_j = C_j \oplus O_j & forj = 1,2....n-1; \\ P_n^* = C^*_n \oplus MSB_u(O_n). & \end{array}$$

In OFB mode only encryption of AES is used. The input to the encryption algorithms is a single 128-bit block. This block must format as a 4X4 square matrix of bytes. Then it is copied into the State array, which is modified at each stage of encryption [13]. In both OFB encryption and decryption, each forward cipher function (except the first) depends on the results of the previous forward cipher function. As a result multiple forward cipher functions cannot be performed in parallel [14].

The secure scramble process has three steps [2]:

1. The base station and the mobile share a common initial vector and a common secret key which are generated using LFSR.

2. The secure scrambling sequence is generated using the initial vector and the secret key through AES operations.

3. The scrambling process is done by applying the secure scrambling sequence to the chip rate signal.

At the beginning of the cipher, The plain text breaks up in to multiple of 128 bits and the IV is encrypted using AES secret key. The encrypted IV is ox red with the first 128 bit of plaintext. Ay this stage, the first 128 bits of the secure scrambling sequence is obtained. This 128-bit segment of scrambling sequence obtain in the first step is then used as the initial vector of the above process to obtain the second 128-bit segment of the scrambling sequence. This process is repeated until the plaintext bits is finished , for the last block of the plaintext must be zero padded[2].

Hidden direct sequence method is used to enhance the built-in security of CDMA systems at the physical layer by encrypting the spreading code using cryptographic algorithm [12]. In this method every user encrypts its spreading code with his secret key. These encrypted codes are then used as the spreading code in the channelization section. At destination, the receiver that knows his secret key is able to regenerate the spreading code to despread the transmitted signal (decryption of his messages). By using the encrypted spreading code the amount of multi-user interference is increased and the performance of the system is degraded because the correlation between the encrypted codes is completely random and may become a large value. The large cross-correlation between codes will cause large interference among users at the receiving end [3]. To mitigate this problem and get good performance and proper security, a combined encrypted spreading code and the original un-encrypted spreading code can be employed [12]. With the increase in the joint un- encrypted and encrypted bits, the interference is reduced and the security is increased. The BER will increase if the number of encrypted bits is also increased [3].

4. THE NEW PROPOSED METHOD (HYBRID METHOD) FOR INCREASING SECURITY IN PHYSICAL LAYER OF DS/CDMA UWB

The built-in security of CDMA mentioned in section 3, has low security level and it is not suitable for data communication when compared with voice communications, this is due the big difference between the chip rate of long code of IS-95 CDMA (1.288 Mc/s) and chip rate of low and high bands of DS/CDMA UWB as mentioned in section 1.

Now, by incorporate the other two methods of CDMA discussed above, secure scrambling at chip rate which based on AES-OFB, and the joint between encrypt spreading code with un-encrypt spreading code, a high level of security added to the physical layer of DS/CDMA UWB devices is achieved. The first Advantage of this system is the high level of security (two levels of security) done from incorporating two methods of CDMA, this can be shown from the measured time of the simulation in Figure 6 in section 7. Second is with the increase of the number in the joint of encrypted and un-encrypted spreading code this guarantees security and the interference is reduced. The functional block diagram of this proposed system is shown in Figure 3.

The joint between encrypted spreading code with un-encrypted spreading code is done according to the steps below witch represents Spreader and despreader Blocks:

1. AES- Key is generated using LFSR at base station and mobile station with length 128.
2. The spreading code is a plaintext denoted to (P) which need to cyclic padding to be equal to 128 bit (the block size of AES).
3. The cyclic padding must be removed after encrypting spreading code to get just encrypted spreading code with the same length of un-encrypted spreading code.
4. The concatenation is done between encrypted spreading code with un-encrypted spreading code and this concatenation is used in spreading to spread user data.

Secure scrambling at chip rate use AES-OFB is done according to the steps below witch is represent secure scrambling block at TX in the diagram:

1. The initialization vector (IV) is essentially a nonce, which mean it must be unique for each execution of the mode under the same key, it is generated at base station and mobile station using LFSR or as random.
2. AES- Key is generated using LFSR at base station and mobile station with length 128.
3. IV is encrypted by AES Key.
4. Spreading data is a plaintext denoted to (P) which breaks up to multiple blocks of 128 bits.
5. M is a multiple of 128 bits (the block size of AES) of spreading data , no of 128 blocks of spreading data M= length (P)/128.
6. The encrypted IV results are XORed with the corresponding blocks (or partial block) of the spreading data.
7. Partial block must be padded with zeros to be oxred with corresponding encrypted IV, and xoring the padded zeros must be removed.

Secure descrambling is done according to the steps below witch is represent secure descrambling block at RX in the diagram:

1. Same steps from (1-3) in secure scrambling Block is done.
2. Cipher spreading data is denoted to (C) which breaks up to multiple blocks of 128 bits.
3. M is a multiple of 128 bits cipher spreading data, no of 128 blocks of cipher spreading data M= length (C)/128.
4. The encrypted IV results are XORed with the corresponding blocks (or partial block) of the cipher spreading data.
5. Partial block must be padded with zeros to be oxred with corresponding encrypted IV, and oxring the padded zeros must be removed.

5. SYSTEM MODEL OF HYBRID METHOD

Because secure scrambling at chip rate method is applied at chip rate as mentioned previously in section 3, therefore, the system model motioned in section 2 is need to modify in order to secure it. The problem is that DS/CDMA UWB system mentioned in section 2 used coded monocycle in transmitter as one unit and use one integrator at receiver to form one bit duration. This will mandate to modify the DS/CDMA UWB system to enable increase in security. The modification is done by splitting the coded monocycle at the transmitter and use two integrators at receiver one over chip duration Tc to integrate each pulse duration Tp and other integrator over one bit duration Tb to integrate N chips to form one data bit.

By incorporate two methods mentioned in section 4, and by using DS/CDMA UWB system model in section 2 with its modification in section 3. Figure 3 showing the Block diagram of Hybrid method of CDMA included in DS/CDMA UWB system.

Let

$$C^{u} = [C^{u}(0), C^{u}(1), ..., C^{u}(N-1)] \qquad (14)$$

Denote the $u^{(th)}$ user's spreading code and N is a processing gain, there are N chips per symbol and number of chips is equal to the number of pulses per symbol.

In the transmitter, every user encrypts its spreading code with his secret key K; these encrypted codes are then used as the spreading code.

$$C^{\backslash(u)} = E(K^{(u)}, C^{(u)}(t)) \qquad (15)$$

Where $E(K^{u}, C^{u}(t))$ is the symmetric encryption of plaintext $C^{u}(t)$ using secret key K^{u}, K^{u} is a 128 bit AES-Key associated for each user *u*.

The transmitter concatenate each encrypted spreading code with its un-encrypted spreading code for each user and then used it as spreading code to spread the user data.

$$C^{\backslash\backslash(u)}(t) = (C^{\backslash(u)}(t)\,||\,C^{(u)}(t)) \qquad (16)$$

The spreading chip rate signal can be express using equation (2) which can be modified:

$$x^{(u)}(t) = \sum_{j=0}^{\infty} \alpha_j^{(u)} (C^{\backslash\backslash(u)}(t - jT_b)) \qquad (17)$$

Secure scrambling at chip rate is done by encrypted the spreading chip rate using AES-OFB Encryption, which expressed in section 3 and by using the secure scrambling steps mentioned in section 4.

$$s^{(u)}(t) = E(K^{(u)}, x^{(u)}(t)) \qquad (18)$$

Where $x^{(u)}(t)$ is a plaintext for each user *u* need to encrypt by its intended users' symmetric secret key K. The cipher scrambled chip rate is multiplied by transmitted monocycle pulse train. Using equation (4) which must be modified, the resultant signal coming from users *u* is calculated using equation:

$$S^{(u)}(t) = \sum_{i=0}^{\infty} s_i^{(u)}(t) p_{tx}(t - iTc) \qquad (19)$$

All users are multiplexed together and send a signal via AWGN channel model using equation(5) which can be

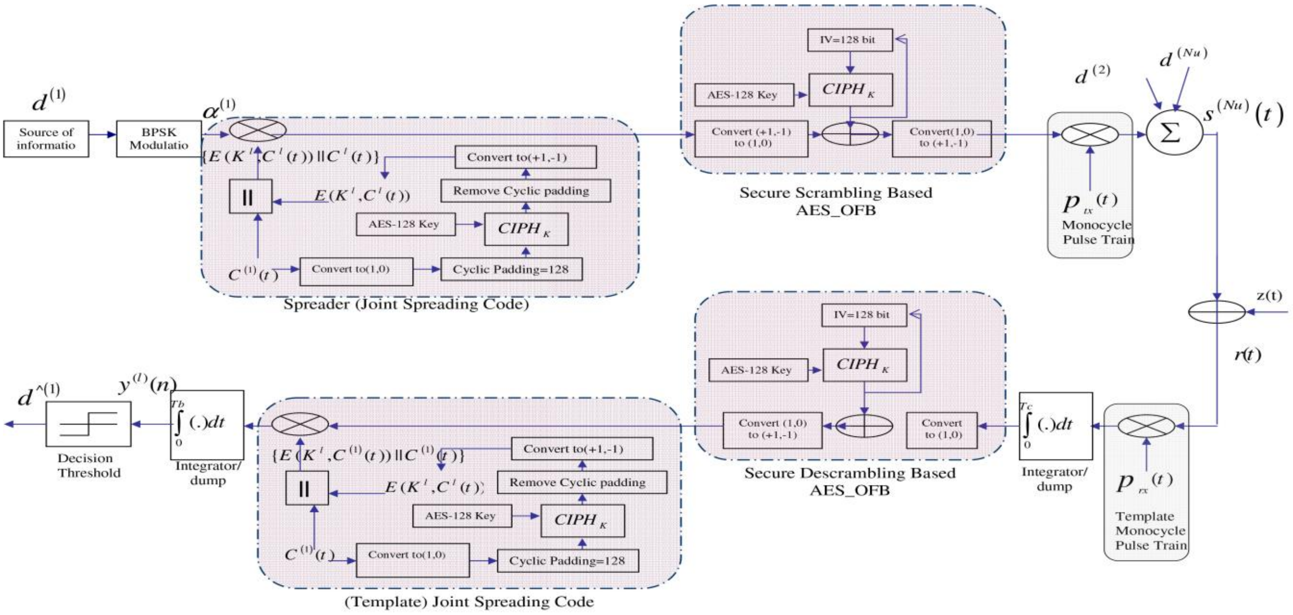

Figure 3. The Proposed system of DS/CDMA UWB with Hybrid method of CDMA

modified to be:

$$r(t) = \sum_{u=1}^{Nu} A_u S^{(u)}(t) + z(t) \qquad (20)$$

The sufficient statistics $y^{(1)}(n)$ for the l^{th} user is calculated using equation (6) which can be modified to be:

$$y^{(l)}(n) = \int_{nTc}^{(n+1)T_c} p_{rx}(t - nTc).r(t)dt \qquad (21)$$

$$= \int_{nTc}^{(n+1)T_c} p_{rx}(t - nTc).\left(\sum_{u=1}^{Nu} A_u S^{(u)}(t) + z(t)\right)dt$$

The receiver monocycle $P_{rx}(t)$ is normalized using equation (7).

$$y^{(l)}(n) = \int_{nTc}^{(n+1)Tc} p_{rx}(t - nTc).\left(\sum_{u=1}^{Nu} A_u s^{(u)}(t) p_{tx}(t - nTc) + z(t)\right)dt$$

$$= \sum_{u=1}^{Nu} A_u s^{(u)}(n) + z^{(l)}(n)$$

At destination, the receiver that knows the secret key of each user is able to regenerate the descrambling signal by decryption the signal by using AES-OFB decryption mentioned in section 3 and using the secure descrambling steps is mentioned in section 4.

The signal of user *l* is decrypt by using its secret key $K^{(l)}$ using equation below:

$$Y^{(l)}(n) = D(K^{(l)}, y^{(l)}(n)) \qquad (22)$$

$$= D(K^{(l)}, (A_l s^{(l)}(n) + \sum_{u \neq l}^{Nu} A_u s^{(u)}(n) + z^{(l)}(n)))$$

$$= A_l X^{(l)}(n) + \sum_{u \neq 1} A_{lu} s^{(lu)}(n) + z^{(ll)}(n)$$

$$= A_l X^{(l)}(n) + v(n)$$

Where $D(K^{(l)}, y^{(l)}(n))$ is the symmetric decryption of ciphertext $y^{(l)}(n)$ using intended user's secret key $K^{(l)}$, $A_l X^{(l)}(n)$ is decipher descrambling sequences of intended user *l*, and $v(n)$ is the cipher scrambling sequences of un-intended users with the noise.

$$v(n) = \sum_{u \neq l} A_{lu} s^{(lu)}(n) + z^{(ll)}(n) \qquad (23)$$

The receiver knows the secret key of each user is able to regenerate the spreading code of intended user *l* and encrypt its data by using its secret key $K^{(l)}$, the joint of encrypted spreading code with un-encrypted code is used to de-spread the transmitted signal (decryption of his messages). The de-spread transmitted signal (decryption of his messages):

$$YY^{(l)}(n) = \int_{nT_b}^{(n+1)T_b} C^{\backslash\backslash(l)}(t - nT_b)Y^{(l)}(n)dt \qquad (24)$$

$$= \int_{nT_b}^{(n+1)T_b} C^{\backslash\backslash(l)}(t - nT_b)\left[A_l X^{(l)}(n) + v(n)\right]dt$$

Using equation (9), it be modified to be:

$$YY^{(l)}(n) = \overbrace{A_l \alpha^{(l)}(n)}^{Desired} + \overbrace{\sum_{u \neq l} C^{lu}(n) A_u \alpha^{(u)}(n)}^{Interference} + \overbrace{v^{(l)}(n)}^{Noise} \qquad (25)$$

Where:

$$\int_0^{T_b} C^{\backslash\backslash(l)}(t) C^{\backslash\backslash(l)}(t)dt = 1 \Leftrightarrow \int_0^{T_b} C^{\backslash\backslash(l)}(t) C^{\backslash\backslash(u)}(t)dt = C^{(lu)}(t) \quad (26)$$

and , $$\int_{nTb}^{(n+1)T_b} C^{\backslash\backslash(l)}(t - nT_b)v(n) = v^{(l)}(n) \qquad (27)$$

Using equation (10)(11) the user data is detected using decision variable.

$$\hat{d}^{(l)}(n) = \text{sgn}(YY^{(l)}(n)) = \text{sgn}(A_l \alpha^{(l)}(n) + V) \quad (28)$$

With V being the sum of the noise and interference components.

6. SECURITY MEASUREMENTS

There are some of criteria to measure the security of the system:

1. System Performance: It is used to measure BER in the system; with the increasing of encrypted bits the BER will be increased.
2. Computational Complexity (Time): it is used to measure the security in the system. The system that required large time due to the encryption, it has strong security.
3. Number of security levels: The system with more than one level of security has the largest security.

7. SIMULATION RESULTS

In the simulation, we choose Walsh code with processing gain N = 16, it is assumed that BPSK signals are transmitted over AWGN Channel, and information sequence consists of 10000 BPSK symbols are generated randomly. Using a desktop computer equipped with Matlab simulator,8.00 GB RAM and 3.50 GHz CPU speed, the result is provided in Figure 4, 5 and 6.

Figure 4 shows the BER for each security method added to the DS/CDMA UWB system. we compare the input-output BER performance of DS/CDMA UWB with built

in security, Encrypt spreading code, joint between spreading code and un-encrypted spreading code, secure scrambling based AES-OFB and Hybrid method

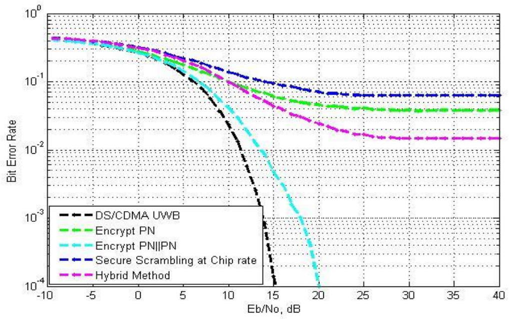

Figure 4. BER versus Eb/No of each security method applied to the CDMA/CDMA UWB system, Chip rate of UWB Low band =1368 Mc/s, Walsh code, processing gain N=16, AES- key length = 128, *Nu* =5.

Figure 5 shows the measurement of bit error rate in each security method applied to the DS/CDMA UWB system model using the results provided in Figure 4. It is observed secure scrambling at chip rate has larger BER because error is increased with the increasing of encrypted bits. Encrypt spreading code has large BER because the correlation between the encrypted codes may become a large value, this will cause large interference between users.

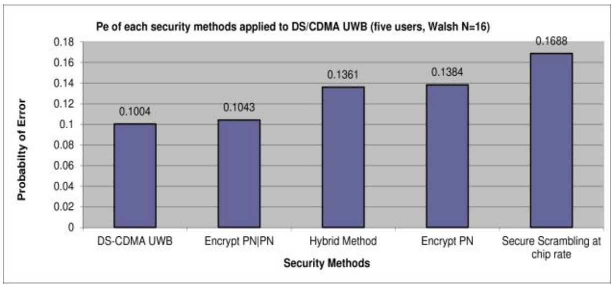

Figure 5. Probability of error of four security methods applied to the DS/CDMA UWB.

Hybrid method system enhance the larger BER in secure scrambling at chip rate and encrypt spreading code methods, because it use joint of the encrypted spreading code with un-encrypted spreading code, the spreading code after combination will be larger than before this guarantees BER is decreased with the increasing in spreading code length . In addition, security is increased in the system.

Figure 6 shows that the time of AES encryption required in the hybrid method system is the largest time among all methods, this mean this method has the largest security among them, the time is large because number of AES encryption to encrypt the bits is the very large. This method has two levels of security, one for encrypt PN with concatenation with un- encrypted spreading code and other for secure scrambling at chip rate based AES-OFB at chip rate.

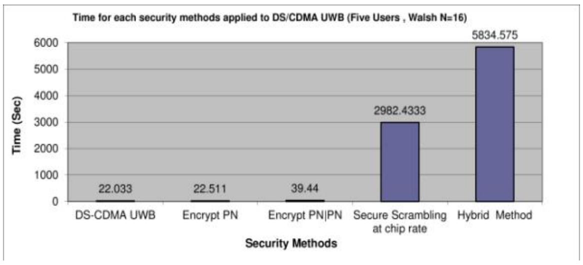

Figure 6. Computational complexity of four security methods applied to the to DS/CDMA system.

Without knowing the secret key no one can intercept the user signals, the complexity level is 2^128-1 of encrypting PN code and 2^128-1 of secure scrambling based AES-OFB at chip rate method.

By using security measurement criteria, and according to the curves and excel sheets, the hybrid method showing the highest security level with less error than using secure scrambling at chip rate and encrypt spreading code methods.

8. CONCLUSION

In this paper, three methods of CDMA are discussed. The security weakness of IS-95 CDMA is analyzed. Hidden direct sequence and secure scrambling at chip rate methods of CDMA are added to the physical layer to increase security in the DS/ CDMA UWB system. The simulation results ensure that the proposed Hybrid method produces much stronger security with less probability of error than that of existing two methods added individually to the DS/CDMA UWB system.

9. REFERENCES

[1] Yi-Sheng Shiu, Shih Yu Chang, Hsiao-Chun Wu, Scott C.-H. Huang, and Hsiao-Hwa Chen, Physical Layer Security in Wireless Networks - A Tutorial, IEEE Wireless Communications, Vol. 18, Issue 2, Page(s): 66-74, April 2011.

[2] Jian Ren, Tongtong Li, "CDMA physical layer built-in security enhancement", Vehicular Technology, IEEE Conference - VTC -Spring , vol. 3, pp. 2157-2161 Vol.3, 2003.

[3] M. Tafaroji and A. Falahati, “Improving Code Division Multiple Access Security by Applying Encryption Methods over the Spreading Codes,” IET Communication, Vol. 1, No. 3, 2007, pp. 398-404. doi:10.1049/iet-com:20060295.

[4] Ketan Mandke, Haewoon Nam, Lasya Yerramneni, and Christian Zuniga, " The Evolution of UWB and IEEE 802.15.3a for Very High Data Rate WPAN **",** EE 381K-11 Wireless Communications UWB Group, The University of Texas at Austin Prepared for Dr. T. S. Rappaport May 6, 2003.

[5] Saul Rodriguez Duenas, ”Design of a DS-UWB Transceiver” Master Thesis IMIT/LECS/ Stockholm, March 2005.

[6] Greg Hackmann, 802.15 Personal Area Networks, *[*Online].Available: http://www.cse.wustl.edu/~jain/cse574-06/ftp/wpans/index.html, *Last modified: March 21, 2006.*

[7] Conroy JT, LoCicero JL, Ucci DR, " Communication Techniques Using Monopulse Waveforms ", Proceedings of IEEE Military Communication Conference, vol.2, PP. 1181-1185, 1999.

[8] F. Elbahhar, A. Rivenq-Menhaj, J.M. Rouvaen, M. Heddebaut etT. Boukour, "Comparison between DS-CDMA and Modified Gegenbauer Functions for a multi-user communication Ultra Wide Band system", I.E.E. Proceedings-Communications ,vol. 152, pp. 1021-1027, December 2005.

[9] L. Sakkila, C. Tatkeu, Y. ElHillali, A. Rivenq, F. ElBahhar and J-M. Rouvaen (2010)"Short Range Radar Basedon UWB Technology", Radar Technology, Guy Kouemou (Ed.), ISBN: 978-953-307-029-2, InTech, Availablefrom: http://www.intechopen.com/books/radar-technology/short-range-radar-based-on-uwb-technology.

[10] L. P. B. Christensen, "Signal processing for ultra-wideband systems", M.S. thesis, Informatics and Mathematical Modelling, Technical University of Denmark, DTU, 2003.

[11] "On the UWB System Coexistence With GSM900, UMTS/WCDMA, and GPS", Matti Hamalain, et al., IEEE Journal On Selected Areas In Communications, vol. 20, No. 9, Dec. 2002, pp. 1712-1721.

[12] A. Falahati, M. Mashreghi, M. Tafaroji , "Security Enhancement in CDMA with a Hidden Direct Sequence Spread Spectrum System", in the 2nd Information and Communication Technologies (ICTTA 2006), 2006, pp. 2524 - 2529.

[13] William Stallings, "Cryptography and Network Security: Principles and Practice (5th Edition)", English | 2010 | ISBN: 0136097049 | 744 pages.

[14] M. Dworkin, "Recommendation for Block Cipher Modes of Operation", . No. NIST-SP-800-38A. National Inst of Standards and Technology Gaithersburg MD Computer Security DIV, 2001.