A Performance of Complementary Code Keying Codes

Yusung Lee* and Hyuncheol Park*
* School of Engineering, Information and Communications University, Daejeon, 305-714, Korea
Tel : +82-042-866-6808 Fax : +82-042-866-6228 E-mail: {diotima and hpark}@icu.ac.kr

Abstract: In this paper, we drive a theoretical performance of complementary code keying (CCK) codes on additive white Gaussian noise (AWGN) channel. The CCK codes can be demodulated by the optimal maximum likelihood decoding method and sub-optimal correlation magnitude decoding algorithm. We calculate the bit error rate (BER) and symbol or codeword error rate (SER) of the CCK codes using the above mentioned two decoding algorithms. To derive the error performance, we use the weigh distributions and cross-correlation distributions of CCK codes.

Key words: CCK, BER, IEEE 802.11b, WLAN.

1. INTRODUCTION

Complementary code keying (CCK) code is a variation of complementary codes originally proposed by M. J. E. Golay in 1951 [1]. CCK codes are chosen as a modulation method to support the high data rate of IEEE 802.11b wireless local area networks (wireless LANs) [2]. As the CCK easily provides a path for inter-operability with existing systems by maintaining the same bandwidth as the 1Mbps and 2Mbps data rates operating in the 2.4GHz Industrial, Scientific and Medical (ISM) band [3], it is chosen as a modulation method for the high data rates of 5.5Mbps and 11Mbps.

The CCK codes can be decoded by following methods: first, there is an optimal maximum likelihood method that needs a bank of 256 correlators in the receiver. However this optimal method may be considered too complex for implementation. In order to solve this problem, R. van Nee proposed sub-optimum decoding method that is less complex to implement [4]. In this algorithm, the transmitted data are decoded by using the phase information of the CCK chips. Another algorithm is the correlation magnitude decoding method. It can be constructed by using 64 correlators in the receiver [5].

In this paper, to compare the optimal maximum likelihood decoding algorithm with sub-optimal decoding algorithm, we derive the error performance using the correlation property and Euclidean distance of the CCK codes.

This paper is organized as follows: in section 2, we introduce the CCK codes used in IEEE 802.11b standard and the CCK decoding methods. In section 3, we derive the theoretical error performance for the CCK decoding algorithms. In section 4, we evaluate the bit error rate (BER) and symbol error rate (SER) performance of the CCK codes on each decoding algorithm by comparing analytic results with simulated. Finally, in section 5, we summarize and conclude this paper.

2. COMPLEMENTARY CODE KEYING CODES

The CCK code is a subset of complementary codes based on generalized Walsh/Hadamard codes. Complementary codes are defined by the property that the sum of their aperiodic autocorrelation functions is zero everywhere except at the zero shift [6]. That is,

$$\frac{1}{M}\sum_{k=1}^{M}\phi_{k,k}^{a}(n)=\delta(n) \tag{1}$$

where

$$\phi_{k,k}^{a}(n)=\begin{cases}\frac{1}{N}\sum_{i=1}^{N-n}a_{k,i+n}a_{k,i}^{*} & \text{if } 0\le n\le N-1\\ \frac{1}{N}\sum_{i=1}^{N+n}a_{k,i}a_{k,i-n}^{*} & \text{if } -N+1\le n\le 0\\ 0 & \text{otherwise } |n|\ge N\end{cases} \tag{2}$$

where N is the length the spreading sequences and M is the number of sequences. Therefore, the CCK code is also characterized by the auto-correlation property called complementary property.

CCK is a form of M-ary orthogonal keying modulation where one of set of M unique signal codewords is chosen for transmission and is based on an in-phase (I) and quadrature (Q) architecture using complex symbols. CCK uses 8 complex chips in each spreading codeword. Each chip consists of one of four phases (QPSK). CCK uses one vector from a set of M almost orthogonal vectors for the symbol. CCK codewords composed 256 possible 8 chips codes, **c**, can be constructed as the following formula [2]:

$$\mathbf{c}=\{e^{j(\phi_1+\phi_2+\phi_3+\phi_4)},e^{j(\phi_1+\phi_3+\phi_4)},e^{j(\phi_1+\phi_2+\phi_4)},\\ -e^{j(\phi_1+\phi_4)},e^{j(\phi_1+\phi_2+\phi_3)},e^{j(\phi_1+\phi_3)},-e^{j(\phi_1+\phi_2)},e^{j\phi_1}\} \tag{3}$$

where the phases $\{\phi_1,\phi_2,\phi_3,\phi_4\}$ are QPSK phases. One of the phases ϕ_1, is differentially encoded across successive codewords. The others modulate every odd chip, every odd pair of chips, and every odd quad of chips, respectively. To minimize DC offsets, the 4-th and 7-th terms in the equation are rotated by 180 degrees with a cover sequence. Since each of the phases represents 2 bits of information, 8 bits are transmitted per codeword.

The CCK modulated signals can be demodulated by several methods. The correlator is a straightforward implementation of the structure described in [5]. Since the maximum correlation is the value which is closest to 0 radian, only the real part of the complex result is required to search for the maximum. This optimal maximum likelihood method as shown in Fig. 1 needs a bank of 256 correlators in the receiver. Although optimum, this method may be considered too complex for implementations.

There are also less complex sub-optimum algorithms. Among them, the sub-optimum algorithm proposed in [4] is to multiply the complex odd samples with the complex conjugate of the even samples. By summing the results, a vector is obtained which has the desired phase value. It is less complex to implement.

The other sub-optimum algorithm is the correlation magnitude decoding method as shown in Fig. 2. In (3), ϕ_1 is present in all chips. Therefore, CCK codes can be decoded by using only 64 correlators for the three phases $\{\phi_2, \phi_3, \phi_4\}$, plus an additional phase detection of the code that has the largest correlation output. The correlation for the 64 vectors can be significantly simplified by using technique like the fast Walsh transform (FWT) because CCK codes use a complex set of Walsh/Hadamard functions and have an inherent Walsh type structure that allows a simple butterfly implementation of the decoder.

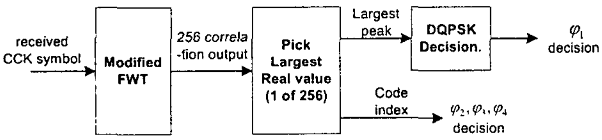

Fig. 1. Optimal CCK decoder.

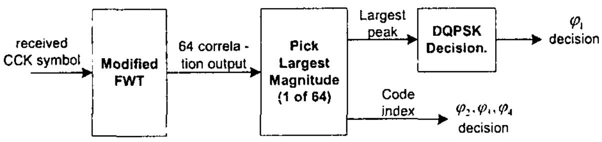

Fig. 2. Sub-optimal CCK decoder using correlation method.

3. PERFORMANCE OF CCK CODES

3.1. Optimal Decoding

The m-th CCK waveform is represented by the signal vectors

$$\mathbf{s}_m = [s_{m1}\ s_{m2}\ s_{m3} \cdots s_{mN}] \qquad m = 1, 2, ..., M \qquad (4)$$

where s_{mj} is the j-th CCK chip of the m-th CCK codeword, M is the number of CCK codes, and N is the number of CCK chips. In the IEEE 802.11b standard, M and N are equal to 256 and 8, respectively. The received signal vector, $\mathbf{r}$, consisting of the transmitted signal vector and an additive complex Gaussian noise vector is given by

$$\mathbf{r} = \mathbf{s}_m + \mathbf{n} \qquad (5)$$

where $\mathbf{r} = [r_1\ r_2\ r_3 \cdots r_N]$ is the received signal, $\mathbf{s}_m$ is the m-th transmitted signal vector, and $\mathbf{n} = [n_1\ n_1\ n_1 \cdots n_N]$ is a vector of noise samples.

To determine the performance of CCK codes, we use the minimum distance receiver. For the AWGN channel, the decision rule based on the maximum likelihood criterion can be reduced to finding the signal $\mathbf{s}_m$ that is closest in distance to the receiver signal vector $\mathbf{r}$. The Euclidean distance is given by

$$\begin{aligned} D(r, \mathbf{s}_m) &= \|\mathbf{r} - \mathbf{s}_m\|^2 \\ &= \|\mathbf{r}\|^2 + \|\mathbf{s}_m\|^2 - 2\operatorname{Re}\{\langle \mathbf{r}, \mathbf{s}_m \rangle\} \end{aligned} \qquad (6)$$

Table 1. The distance squared of the CCK codes.

Weight (w_d)	0	4	6	8	10	12	16
Number of codewords (A_d)	1	24	16	174	16	24	1
Number of bit error per codeword (B_d)	0	2.75	5.25	4	5.75	3.75	2

where $D(r, \mathbf{s}_m)$, m=1,2,...,M is called the distance metrics and $\langle \mathbf{r}, \mathbf{s}_m \rangle = \mathbf{r}^* \cdot \mathbf{s}_m$, which represents an inner product of two vectors. Therefore, we can decode as picking the codeword that has the minimum value of distance metric, or the maximum real value of the cross-correlation.

We will determine the pairwise error probability $P(\mathbf{s}_i \to \mathbf{s}_j)$, defined as the probability that the received signal is closer to $\mathbf{s}_j$ than it is to $\mathbf{s}_i$, given that $\mathbf{s}_i$ was transmitted, for some $i \neq j$ [7].

$$P(\mathbf{s}_i \to \mathbf{s}_j) = \Pr\lfloor D(\mathbf{r}, \mathbf{s}_j) < D(\mathbf{r}, \mathbf{s}_i) \mid s_i \text{ transmitted} \rfloor \quad (7)$$

Substituting $\mathbf{s}_i + \mathbf{n}$ for $\mathbf{r}$,

$$\begin{aligned} P(\mathbf{s}_i \to \mathbf{s}_j) &= \Pr\left[\|\mathbf{s}_j - \mathbf{s}_i\| - 2\operatorname{Re}\{\langle \mathbf{n}, \mathbf{s}_i - \mathbf{s}_j \rangle\} + \|\mathbf{n}\|^2 < \|\mathbf{n}\|^2\right] \\ &= \Pr\left[\operatorname{Re}\{\langle \mathbf{n}, (\mathbf{s}_i - \mathbf{s}_j)/\|\mathbf{s}_i - \mathbf{s}_j\| \rangle\} > \|\mathbf{s}_i - \mathbf{s}_j\|/2\right] \end{aligned} \quad (8)$$

where the $\operatorname{Re}\{*\}$ term above is a Gaussian random variable with variance $\sigma^2 = N_0/2$. Therefore, the pairwise error probability is

$$P(\mathbf{s}_i \to \mathbf{s}_j) = Q\left(\frac{d_{i,j}}{\sqrt{2N_0}}\right), \qquad (9)$$

where $d_{i,j} = \|s_i - s_j\| = \sqrt{2(N - \operatorname{Re}\{\langle s_i, s_j \rangle\})}$, which is the distance between $\mathbf{s}_i$ and $\mathbf{s}_j$, and the weight factor $w_{i,j}$ represents the squared distance between codewords. Table I shows the weight factor for CCK codes and also represents the number of CCK codewords that are each distance away from the specific codeword [8].

By using Table I and (9), we can get the SER (or codeword error rate) and BER performance of CCK codes in AWGN channel based on union bound,

$$P_s \leq \sum_{d=d_{min}} A_d P(\mathbf{s}_1 \to \mathbf{s}_d) = \sum_{d=d_{min}} A_d Q\left(\sqrt{\frac{w_d E_b}{N_0}}\right) \qquad (10)$$

$$P_b \leq \sum_{d=d_{min}} \frac{A_d B_d}{N} Q\left(\sqrt{\frac{w_d E_b}{N_0}}\right) \qquad (11)$$

where w_d is the weight factor, A_d is the number of codewords, and B_d is the number of bit error occurred in codewords that are distance d away from $\mathbf{s}_1$.

3.2. Sub-optimal Decoding

The CCK codes can be decoded using the index, which contains the absolute maximum value at the correlator outputs. Since ϕ_1 is present in all chips, CCK codes can be decoded by using only 64 correlators for the three phases $\{\phi_2, \phi_3, \phi_4\}$, plus an additional phase detector for the phase ϕ_1. This is another sub-optimal decoding method. When the two signals are correlated, the input to the detector is the complex-valued random variable given as follows. Suppose that the transmitted codeword is $\mathbf{s}_1$, the outputs of the 64 correlators, the inputs to the detector, may be expressed as

$$r_m = \rho_m e^{j\phi_1}\sqrt{E_s} + n_m, \qquad m = 1, 2, ..., 64 \qquad (12)$$

where ρ_m is the cross-correlation coefficient between $\tilde{\mathbf{s}}_1$ and $\tilde{\mathbf{s}}_m$ which represent the codeword $\mathbf{s}_1$ and $\mathbf{s}_m$ except ϕ_1, E_s is the codeword energy, and n_m is the complex Gaussian random noise component.

As the detector bases its decision on the envelopes $|r_m|$, the PDFs of $R_m = |r_m|$ is Ricean distributed random variable and may be expressed as

$$p(R_m) = \frac{R_m}{\sigma^2}\exp\left(-\frac{R_m^{\ 2} + \beta_m^{\ 2}}{2\sigma^2}\right) I_0\left(\frac{R_m \beta_m}{\sigma^2}\right), \quad m = 1, 2, ..., 64 \qquad (13)$$

where $\beta_1 = \sqrt{E_s}$ and $\beta_m = \rho_m\sqrt{E_s}$, $m \neq 1$, $\sigma^2 = N \cdot N_0/2$, and $I_0(x)$ is the modified Bessel function of order zero.

Since R_1 and R_m are statistically dependent as a consequence of the non-orthogonality of the signals, the probability of error may be obtained by evaluating the double integral. The pairwise error probability is

$$P(\tilde{\mathbf{s}}_1 \to \tilde{\mathbf{s}}_m) = P(R_m > R_1) = \int_0^{\infty}\int_{x_1}^{\infty} p(x_1, x_2)\, dx_2 dx_1, \qquad (14)$$

where $p(x_1, x_2)$ is the joint PDF of the envelopes R_1 and R_m.

In (14), the probability of error may also be expressed as

$$P(R_m > R_1) = P(R_m^{\ 2} > R_1^{\ 2}) = P(R_m^{\ 2} - R_1^{\ 2} > 0). \qquad (15)$$

But $R_m^2 - R_1^2$ is a special case of a general quadratic form in complex-valued Gaussian random variables. The derivation yields the pairwise error probability in the form [9]

$$P(\tilde{\mathbf{s}}_1 \to \tilde{\mathbf{s}}_m) = Q_1(a_m, b_m) - \frac{1}{2}\exp\left(-\frac{a_m^{\ 2} + b_m^{\ 2}}{2}\right) I_0(a_m b_m), \qquad (16)$$

where $Q_1(a,b)$ is the Marcum Q function and the parameters a and b are defined as

$$a_m = \sqrt{\frac{4E_b}{N_0}\left(1 - \sqrt{1 - |\rho_m|^2}\right)},$$

$$b_m = \sqrt{\frac{4E_b}{N_0}\left(1 + \sqrt{1 - |\rho_m|^2}\right)}. \qquad (17)$$

Table II displays the cross-correlation statistics among 64 CCK codewords except ϕ_1. BER and SER for CCK codes except ϕ_1 can be calculated by applying correlation coefficients in Table II to (16). Therefore, the symbol error probability using pairwise error probability can be expressed by

$$P_{\tilde{s}} \leq \frac{1}{64}\sum_i \sum_{j \neq i} P(\tilde{\mathbf{s}}_i \to \tilde{\mathbf{s}}_j). \qquad (18)$$

As explained before, differentially decoded PSK signal,

Table 2. *Cross-correlation distributions of CCK codes except* ϕ_1

Cross-correlation coefficient	Number of codewords
1	1
$\sqrt{2}/2$	6
1/2	12
$\sqrt{2}/4$	8
0	37

ϕ_1, can be decoded by detecting the phase of the largest correlation output in DQPSK decision block in Fig. 2. The probability of symbol error for DQPSK can be expressed by using (16) as follows [9]:

$$P_{\phi_1} = 2Q_1(a,b) - \exp\left(-\frac{a^2 + b^2}{2}\right) I_0(ab) \qquad (19)$$

where a and b are obtained by substituting $\rho = \sqrt{1/2}$ for cross-correlation coefficient of (17). Thus, the probability of a correct decision is

$$P_c = (1 - P_{\tilde{s}})(1 - P_{\phi_1}). \qquad (20)$$

Therefore, the symbol error probability of CCK codes is

$$P_s = 1 - P_c = P_{\tilde{s}} + P_{\phi_1} - P_{\tilde{s}}P_{\phi_1}. \qquad (21)$$

4. PERFORMANCE RESULTS

In this section, we compare analytic results to simulated BER and SER for the two decoding algorithms, the optimal decoding algorithm and sub-optimal correlation magnitude-decoding algorithm.

Fig. 3 shows the BER performance of the two decoding algorithms for the CCK 11Mbps in AWGN channel. The optimum maximum likelihood technique has a better performance than correlation magnitude decoding algorithm by 1.7dB when BER is equal to 10^{-4}.

In Fig. 4, the theoretical and simulated BER and SER performance of the two decoding algorithms as a function of the energy per bit noise ratio E_b/N_0 are shown. As SNR is increased, the theoretical and simulated error rates are almost identical.

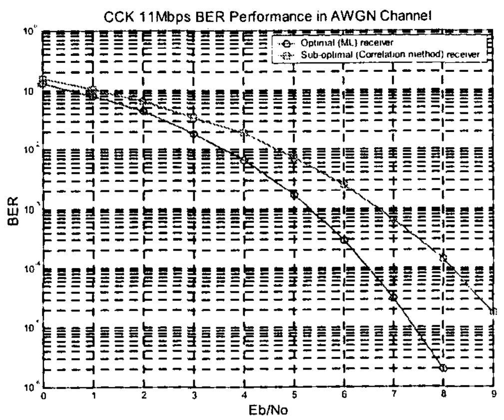

Fig. 3. CCK BER simulated performance of the two decoding algorithms in AWGN channel.

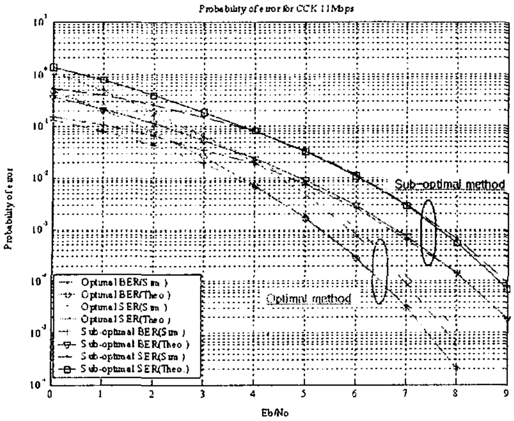

Fig. 5. The performance comparison between theoretical and simulated results of the two decoding algorithms.

5. SUMMARY AND CONCLUSIONS

In this paper, we analyzed the performance of CCK receiver in AWGN channel and derived the pairwise error probability for the two decoding schemes of the CCK codes using the weight distributions and cross-correlation distributions of CCK codes. We also verified theoretical BER and SER by comparing them with simulation results. For example, when E_b / N_0 is more than 6dB, the theoretical and the simulated BER of the optimal decoder and sub-optimal decoder have nearly the same values.

References

[1] M. J. E. Golay, "Complementary series," *IRE Transactions on Information Theory*, pp. 82-87, Apr. 1961.

[2] IEEE Std 802.11b, *Part 11: Wireless LAN medium access contròl (MAC) and physical layer (PHY) specifications: High-speed physical layer extension in the 2.4 GHz band*, 1999.

[3] B. O'Hara and A. Petrick, *IEEE 802.11 Handbook: Designer's Companion*, IEEE Press, Dec. 1999.

[4] R. van Nee, "OFDM codes for peak-to-average power reduction and error correction," *Proc. IEEE Global Telecommun. Conference*, vol. 1, pp. 740- 744, Nov. 1996.

[5] C. Andren and M. Webster, "CCK modulation delivers 11Mbps for high rate 802.11 extension," *Wireless Symposium/Portable By Design Conference Proceedings*, Spr. 1999.

[6] G. L. Stuber, *Principles of Mobile Communication*, Second edition, Boston, MA: Kluwer Academic Publishers, 2001.

[7] J. R. Barry, E. A. Lee, and D. G. Messerschmitt, *Digital Communication*, Third edition, Boston, MA: Kluwer Academic Publishers, 2003.

[8] C. Heegard, J. T. Coffey, S, Gummadi, P. A. Murphy, R. Provencio, E. J. Rossin, S. Schrum, and M. B. Shoemake, "High-performance wireless ethernet," *IEEE Communications Magazine*, pp. 64-73, Nov. 2001.

[9] John G. Proakis, *Digital Communications*, Fourth edition, McGrow-Hill, 2001.

[10] Yusung Lee, *A Thesis for the Degree of Master: A RAKE Receiver with ICI/ISI Equalizer for CCK Wireless LAN Modem*, Information and Communications University (ICU) Press, Korea, Feb. 2004.