



## §8.4 Why should CDMA codes Be Pseudo-Random Noise?

Small autocorrelation values  $|R_{a_i, a_i}(d)|$  for  $d \neq 0$

⇒ Flat Spectrum of  $a_{i,k}$  for a fixed  $i$ .

⇒ The components of  $\underline{a}_i$  are close to be independent.

Small crosscorrelation values  $|R_{a_i, a_j}(d)|$  for  $i \neq j$

⇒  $a_{i,k_1}, a_{j,k_2}$  are uncorrelated for  $i \neq j$  and any  $k_1$  and  $k_2$

⇒ All components of all CDMA codes  $\underline{a}_i, i=1, \dots, K$ , are i.i.d. with mean 0 and variance 1.

$$\frac{\sum_{l=0}^{G-1} a_{i,l} a_{j,l+d}^*}{\sqrt{G}} \rightarrow \text{Normal, central limit theorem}$$

$$\Rightarrow \sum_{l=0}^{G-1} a_{i,l} a_{j,l+d}^* \rightarrow O(\sqrt{G})$$

⇒ Pure random codes  $\underline{a}_i$  reaches the lower bound. i.e., they are already optimal.



# What Good CDMA Codes Should Be?

## Four conditions for a good CDMA code

- ① Easy to generate
- ② Good randomness property
- ③ Difficult to reconstruct from a short segment  
(defense purpose, or privacy)
- ④ Large size of a family

To generate a pure random sequence  
flipping coins

head  $\rightarrow$  1

tail  $\rightarrow$  -1

Bernoulli sequence

pure random!

## Is it good?



## §8.5 CDMA Code Design

### 1. Randomness

Good randomness can be interpreted as (for a binary sequence)

R1: Relative frequencies of "1" and "-1" are each  $\frac{1}{2}$

(Not enough, such as, 1 - 1 1 - 1 1 - 1 ...)

R2: Run length (of 1 or -1) are as expected in a coin-flipping experiments: half of all run length are unity; one-quarter are of length two; one-eighth are of length 3, ...

$$\begin{array}{ccc} \textcircled{\frac{1}{2}} \begin{array}{c} | \\ -1 \end{array} & \textcircled{\frac{1}{4}} \begin{array}{c} | \quad | \\ -1 \quad -1 \end{array} & \textcircled{\frac{1}{8}} \begin{array}{c} | \quad | \quad | \\ -1 \quad -1 \quad -1 \end{array} \dots \\ \left(\frac{1}{2}\right)^1, & \left(\frac{1}{2}\right)^2, & \left(\frac{1}{2}\right)^3 \end{array}$$

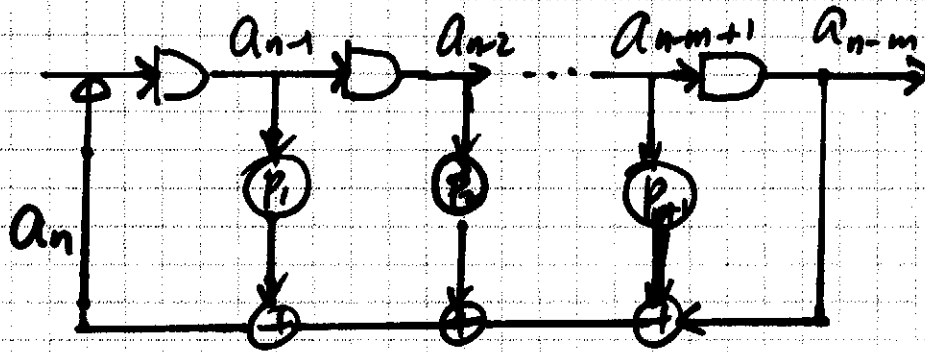
R3: If the random sequences shifted by any nonzero number of elements, the resulting sequences will have an equal number of agreements and disagreements with the original sequence.

$\begin{array}{cccccccc} \checkmark & & & \checkmark & & & \checkmark & \\ x & x & x & x & x & x & x & x \\ 0 & 0 & x & 0 & 0 & x & 0 & 0 & x \end{array}$   
 3 agreements

→ after a shift  
 there are still  
 3 agreements



## 2. Linear feedback shift register (LFSR) of length $m$



1 and 0 sequence

$$p_i \in \{0, 1\}$$

$m$  is called the order of the above LFSR

The question is how to select the constants  $p_1, p_2, \dots, p_{m-1}$

## 3. $m$ -sequences (length $2^m - 1$ ) (maximum length sequences)

For coefficients  $p_1, \dots, p_{m-1}$  in an LFSR, let

$$p(x) = 1 + p_1 x + \dots + p_{m-1} x^{m-1} + x^m, \text{ a polynomial of degree } m$$

If  $p(x)$  can not be factorized in two lower degree polynomials with all coefficients 1 or 0, then  $p(x)$  is called primitive. Given  $m$ , primitive polynomials are listed in many text books.

For example,  $p(x) = 1 + x + x^3$  is primitive.

When the polynomials with coefficients  $p_i$  in an LFSR are primitive, the binary sequences are called m-sequences.



The autocorrelation of a length  $G$   $m$ -sequence is

$$\phi_{aa}(l) = \begin{cases} G, & l=0 \\ -1, & l \neq 0 \end{cases}$$

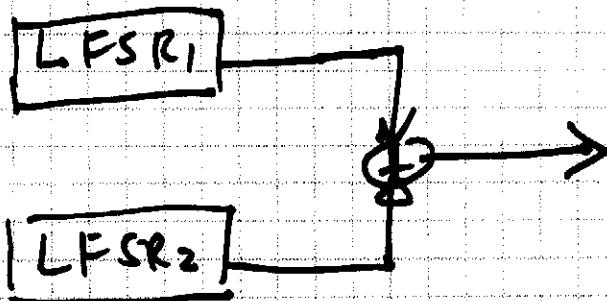
the best you can do  
for binary sequences

$$\approx G\delta(n)$$

In general,  $m$ -sequences don't have good cross correlations properties

#### 4. Gold sequences

A set of Gold sequences has  $2^m+1$  sequences each with a period of  $G=2^m-1$  (length). Gold sequences are generated by a pair of  $m$ -sequences.



The pair is not arbitrary but called "preferred" pairs.



Their crosscorrelation has only three values  
 $\{-1, -t(m), t(m), -2\}$

$$\text{Where } t(m) = \begin{cases} 2^{(m+1)/2} + 1, & m \text{ odd} \\ 2^{(m+2)/2} + 1, & m \text{ even} \end{cases}$$

(Notice  $\sqrt{G}$  is about the optimal).

Examples  $p_1(x) = 1 + x^2 + x^5$

$$p_2(x) = 1 + x + x^2 + x^4 + x^5$$

$$m=5$$

$$2^m + 1 = 33 \text{ sequences with length } 2^m - 1 = 31$$

5. Randomness for  $m$ -sequences

$$R_1: P_1(0) = \frac{1}{2} \left( 1 - \frac{1}{p} \right)$$

$$P_1(1) = \frac{1}{2} \left( 1 + \frac{1}{p} \right)$$

$$p = 2^m - 1$$

$$\text{When } m=10, \frac{1}{p} \approx 10^{-3}$$

$$=30, \frac{1}{p} \approx 10^{-9}$$

$$=50, \frac{1}{p} \approx 10^{-15}$$

$m=42$  is used for IS-95

$m=128$  is used for NSA



$R_2$ : Relative frequency of run lengths  $n$

is  $\frac{1}{2^n}$  for all  $n \leq m-1$

$\frac{1}{2^{m-1}}$  for  $n = m$ .

No run lengths possible for  $n > m$ .

$R_3$ : OK

$\Rightarrow$   $m$ -sequences ① have good randomness

② easy to generate

③ large size of family

④ security is not good

Since they are generated from a linear device, as long as  $2m+2$  consecutive symbols are known, the code can be detected by solving linear systems due to the linearity of an LFSR.

The bottom line for generating CDMA codes is to have a good random number generator.



## 6. Walsh-Hadamard sequences

When the transmission is synchronized, the orthogonality is the most important property. Walsh-Hadamard sequences are binary orthogonal sequences:

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix}$$

$$H_{2M} = \begin{bmatrix} H_M & H_M \\ H_M & -H_M \end{bmatrix}$$

## § 8. 6. Demodulation at the Receiver: RAKE

### Receiver in multipath Environment

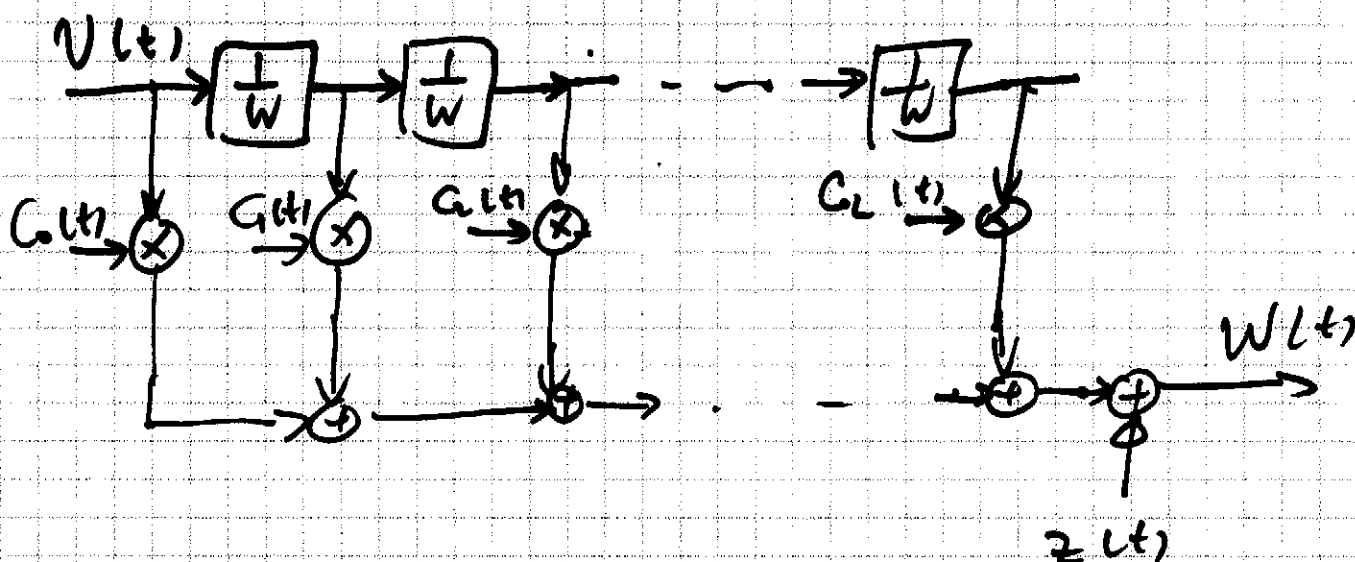
RAKE receiver is to use the autocorrelation properties of spreading sequences by involving and combining the multipath components to obtain multipath diversity

RAKE comes from its similarity to an ordinary garden rake.

Consider first single user case with signal model:

$$W(t) = \sum_{n=0}^L c_n(t) v(t - \frac{n}{W}) + \underbrace{Q(t)}_{\text{additive noise}}$$

↑ multipaths



Received signal model (single user)

In practice,  $C_l(t)$ ,  $0 \leq l \leq L$ , are estimated using pilot signals. So, in the RAKE receiver, they are assumed known.

For simplicity, we assume BPSK is used, i.e., either  $V_l(t)$  or  $-V_l(t)$  is transmitted.

$$V_l(t) = \sum_{k=1}^G A_{nG+k} h_{al}(t - (nG+k)T_c), \quad nT \leq t \leq (n+1)T$$

Also, for simplicity, assume  $T \gg L T_c$ .

$\Rightarrow$  No ISI between data bits/symbols

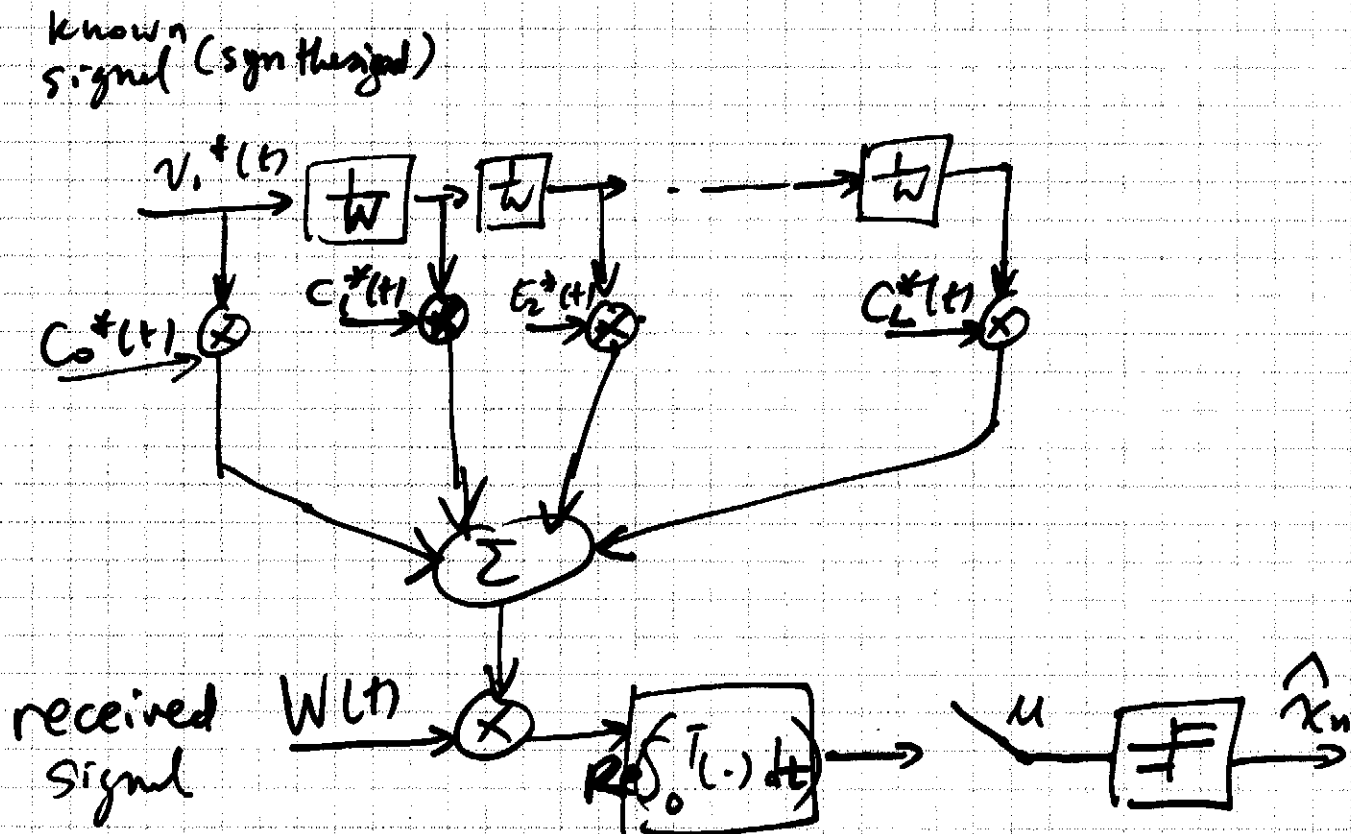
When  $V_l(t)$  is transmitted, then  $(\pm V_l(t))$  are transmitted with data  $\pm 1$ .

$$W(t) = \sum_{l=0}^L C_l(t) V_l(t - \frac{t}{W}) + z(t).$$

The receiver knows  $V_l(t)$  (don't know the sign)



## The RAKE Receiver



$$u = \text{Re} \left\{ \int_{nT}^{(n+1)T} W(t) \sum_{l=0}^L C_l^*(t) v_l^* \left( t - \frac{l}{W} \right) dt \right\}$$

We next derive  $u$  (the output of the RAKE)

For simplicity we assume  $n=0$ .

$$\begin{aligned} u &= \text{Re} \left\{ \int_0^T \left[ \sum_{l=0}^L C_l(t) v_l \left( t - \frac{l}{W} \right) + z(t) \right] \sum_{l=0}^L C_l^*(t) v_l^* \left( t - \frac{l}{W} \right) dt \right\} \\ &= \text{Re} \left\{ \int_0^T \sum_{l=0}^L \sum_{k=0}^L C_l(t) C_k^*(t) v_l \left( t - \frac{l}{W} \right) v_k^* \left( t - \frac{k}{W} \right) dt \right\} \\ &\quad + \text{Re} \left\{ \int_0^T \sum_{l=0}^L z(t) C_l^*(t) v_l^* \left( t - \frac{l}{W} \right) dt \right\} \end{aligned}$$



Note  $\frac{1}{W} = T_c$

$$N = \sum_{l=0}^L \sum_{k=0}^{L-l} R_e \left\{ \int_{-T_c}^T a_k(t) a_k^*(t-l, T_c) v_l^*(t-l, T_c) dt \right\}$$
$$+ \sum_{l=0}^L R_e \left\{ \int_{-T_c}^T a_l(t) a_l^*(t-l, T_c) v_l^*(t-l, T_c) dt \right\}$$

In the slow fading case,  $a_k(t) \approx c_k$  constant for  $t \in [0, T]$  or  $[nT, (n+1)T]$ .

$$N \approx \sum_{l=0}^L \sum_{k=0}^{L-l} R_e \{ a_k c_k^* R_{a, a}(l-l) \}$$

$$+ \sum_{l=0}^L R_e \{ c_l^* \int_{-T_c}^T a_l(t) c_l^*(t-l, T_c) dt \}$$

$$\approx \sum_{l=0}^L |c_l|^2 G + \sum_{l \neq l_0}^{L-l_0} R_e \{ a_{l_0} c_{l_0}^* R_{a, a}(l-l_0) \}$$

Spreading gain  
Multipath diversity gain.  
Small by the small autocorrelation

The random variable  $\eta_c$  is Gaussian and has mean zero and variance

$$\sigma_{\eta_c}^2 = 2 E N_0 \sum_{l=0}^L |c_l|^2$$



$$\Rightarrow \mu = G \varepsilon \sum_{l=0}^L |c_l|^2 + \varepsilon \sum_{l \neq l'} \operatorname{Re}\{c_l c_{l'}^*\} R_{a,a}(l-l') + \eta_c$$

In the ideal case, i.e.,  $R_{a,a}(l) = \delta(l) G$ ,

$$\mu = \varepsilon G \sum_{l=0}^L |c_l|^2 + \eta_c$$

$$\text{BER: } P_b(\gamma_b) = Q(\sqrt{2\gamma_b}),$$

where  $\gamma_b$  is the received bit energy-to-noise ratio

$$\gamma_b = \frac{1}{\sigma_{\eta_c}^2} \left( \varepsilon G \sum_{l=0}^L |c_l|^2 \right)$$

### Multiple Users No Multipath Case:

For the  $i$ th user, CDMA code waveform

$$v_i(t) = \sum_{k=0}^G a_{i,nG+k} h_a(t - (nG+k)T_c), \quad nT \leq t < (n+1)T,$$

$b_{i,n}$  is the information  $\pm 1$  (data)

The received signal

$$\begin{aligned} W(t) &= \sum_{i=1}^K b_{i,n} v_i(t) = \\ &= \sum_{i=1}^K b_{i,n} \sum_{k=0}^G a_{i,nG+k} h_a(t - \tau_i - (nG+k)T_c) + Z(t) \end{aligned}$$

$\uparrow$   $i$ th user information sequence



The receiver knows  $N_i(t)$ ,  $1 \leq i \leq K$ , but not  $b_{i,n}$ .

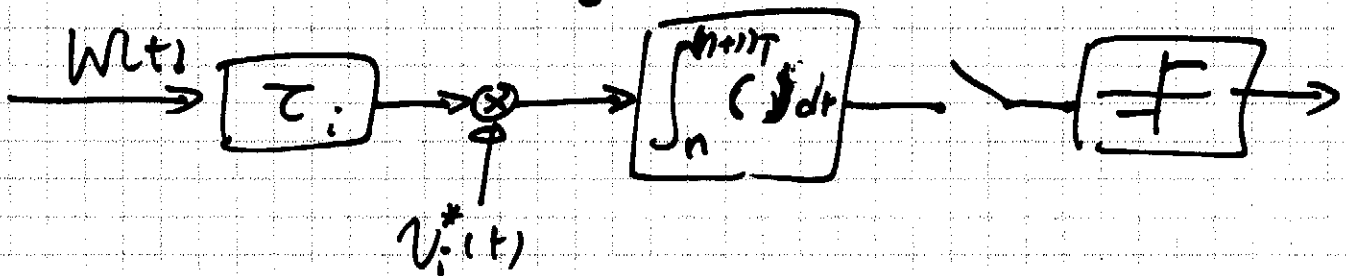
Assume all the delays  $\tau_i$  are known.

The detection of the  $i$ th information sequence  $b_{i,n}$

$$U_i = \operatorname{Re} \left\{ \int_{nT}^{(n+1)T} W(t + \tau_i) U_i^*(t) dt \right\}$$

$$= \operatorname{Re} \left\{ b_{i,n} \int_0^T v_i(t) v_i^*(t) dt + \sum_{j \neq i}^K b_{j,n} \int_0^T v_j(t + \tau_i - \tau_j) v_i^*(t) dt \right\}$$

$$= \operatorname{Re} \left\{ b_{i,n} \zeta + \sum_{j \neq i}^K b_{j,n} \rho_{a_j, a_i}^{(2)}(\tau_i - \tau_j) \right\}$$



Single user detection

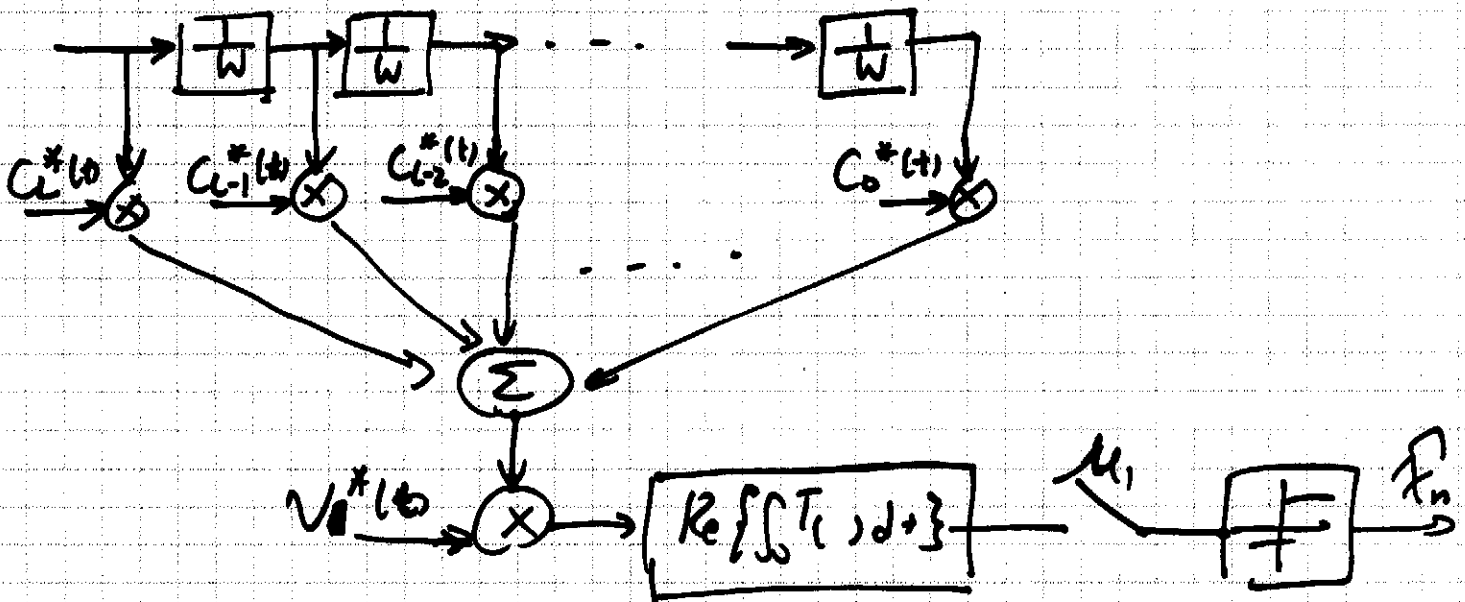


## Multi User Multipath Case:

Assume synchronization (such as down link) forward

Consider two user case for simplicity.

$$W(t) = \sum_{i=1}^2 \sum_{\ell=0}^L c_{i,\ell}(t) b_{i,\ell} v_i(t - \ell T_c) + Z(t)$$



Consider two path case

$$\mu_1 = \text{Re} \left\{ \int_0^T (W(t) c_{i,1}^*(t) + W(t - \beta T_c) c_{i,1}^*(t)) v_i^*(t - \beta T_c) dt \right\}$$

Note that

$$W(t) = c_{0,1}(t) b_{1,1} v_1(t) + c_{1,1}(t) b_{1,1} v_1(t - \beta T_c) \\ + c_{0,2}(t) b_{2,1} v_2(t) + c_{1,2}(t) b_{2,1} v_2(t - \beta T_c) + Z(t)$$



$$\begin{aligned}
 & \int_0^T W(t) c_0^*(t) v_1^*(t - \beta T_c) dt \\
 &= \int_0^T C_0(t) b_{1,n} v_1(t) c_0^*(t) v_1^*(t - \beta T_c) dt \\
 &\quad + \int_0^T C_1(t) b_{1,n} v_1(t - \beta T_c) c_0^*(t) v_1^*(t - \beta T_c) dt \\
 &\quad + \int_0^T C_0(t) b_{2,n} v_2(t) c_1^*(t) v_1^*(t - \beta T_c) dt \\
 &\quad + \int_0^T C_1(t) b_{2,n} v_2(t - \beta T_c) c_1^*(t) v_1^*(t - \beta T_c) dt \\
 &\quad + \int_0^T z(t) c_1^*(t) v_1^*(t - \beta T_c) dt \\
 &= b_{1,n} \int_0^T |C_0(t)|^2 |v_1(t - \beta T_c)|^2 dt + \eta_1 \\
 &= b_{1,n} |C_0|^2 G + \eta_1
 \end{aligned}$$

$$\begin{aligned}
 & \int_0^T W(t - \beta T_c) c_0^*(t) v_1^*(t - \beta T_c) dt \\
 &= \dots = b_{1,n} |C_0|^2 G + \eta_2
 \end{aligned}$$

$$\Rightarrow \mu_1 = b_{1,n} G (|C_0|^2 + |C_1|^2) + \text{Re} \{ \eta_1 + \eta_2 \}$$

spreading  
gain

multipath diversity  
under synchronization assumption