

# Derivation of artificial noise component, matched filtering at Eve

Sidney Golstein and François Rottenberg

November 25, 2020

## Hypothesis

- $Q$  subcarriers, back off rate =  $U$ ,  $N = Q/U$  symbols sent per OFDM block
- $\mathbf{H}_B = \mathbf{H}_{B,x} + j\mathbf{H}_{B,y} \sim \mathcal{CN}(0, 1) \sim \mathcal{N}(0, \frac{1}{2}) + j\mathcal{N}(0, \frac{1}{2})$
- $\mathbf{H}_E = \mathbf{H}_{E,x} + j\mathbf{H}_{E,y} \sim \mathcal{CN}(0, 1) \sim \mathcal{N}(0, \frac{1}{2}) + j\mathcal{N}(0, \frac{1}{2})$
- $h_{B,i} \perp h_{B,j}, \forall i \neq j$
- $h_{E,i} \perp h_{E,j}, \forall i \neq j$
- $h_{B,i} \perp h_{E,j}, \forall i, j$

## AN derivation

We want to compute the mean energy per symbol received at Eve for the artificial noise (AN) component when she performs a matched filtering. The AN term at Eve is given by:

$$\mathbf{v} = \mathbf{S}^H \mathbf{H}_B |\mathbf{H}_E|^2 \mathbf{w} \quad (1)$$

$$= \mathbf{A} |\mathbf{H}_E|^2 \mathbf{V}_2 \mathbf{w}' \quad (2)$$

$$= \mathbf{U} \begin{pmatrix} \mathbf{\Sigma} & \mathbf{0}_{N-Q \times N} \end{pmatrix} \begin{pmatrix} \mathbf{V}_1^H \\ \mathbf{V}_2^H \end{pmatrix} |\mathbf{H}_E|^2 \mathbf{V}_2 \mathbf{w}' \quad (3)$$

$$= \mathbf{U} \mathbf{\Sigma} \mathbf{V}_1^H |\mathbf{H}_E|^2 \mathbf{V}_2 \mathbf{w}' \quad (4)$$

where:

- $\mathbf{U}$  is a  $N \times N$  unitary matrix, i.e.,  $\mathbf{U}^H \mathbf{U} = \mathbf{I}_N$ , its columns form an orthonormal basis of  $\mathcal{C}^N$  and are the left singular vectors of each singular value of  $\mathbf{A}$ ;
- $\Sigma$  is a  $N \times N$  diagonal matrix containing the singular values of  $\mathbf{A}$  in the descending order, i.e.,  $\sigma_i = \Sigma_{i,i}$ ;
- $\mathbf{V}_1$  is a  $Q \times N$  complex matrix that contains the right singular vectors associated to the non-zero singular values;
- $\mathbf{V}_2$  is a  $Q \times Q - N$  complex matrix that contains the right singular vectors associated to the zeroes singular values, i.e., that span the right null-space of  $\mathbf{A}$ ;
- $\mathbf{V} = (\mathbf{V}_1 \ \mathbf{V}_2)$  is a  $Q \times Q$  unitary matrix, i.e.,  $\mathbf{V}^H \mathbf{V} = \mathbf{I}_Q$ , its columns form an orthonormal basis of  $\mathcal{C}^Q$  and are the right singular vectors of each singular value of  $\mathbf{A}$ ;
- $\mathbf{w}'$  is a  $Q - N \times 1$  complex normal random variable such that  $\mathbf{w}' \sim \mathcal{CN}(0, 1)$

Let us now look at the covariance matrix

$$\mathbb{E}(\mathbf{v}\mathbf{v}^H) = \mathbb{E}\left(\mathbf{U}\Sigma\mathbf{V}_1^H|\mathbf{H}_E|^2\mathbf{V}_2\mathbf{w}'\left(\mathbf{U}\Sigma\mathbf{V}_1^H|\mathbf{H}_E|^2\mathbf{V}_2\mathbf{w}'\right)^H\right) \quad (5)$$

$$= \mathbb{E}\left(\mathbf{U}\Sigma\mathbf{V}_1^H|\mathbf{H}_E|^2\mathbf{V}_2\mathbf{w}'\mathbf{w}'^H\mathbf{V}_2^H|\mathbf{H}_E|^2\mathbf{V}_1\Sigma^H\mathbf{U}^H\right) \quad (6)$$

Note that  $\mathbf{w}'$  is independent of other random variable and has a unit covariance matrix. We can thus put the expectation inside to get

$$\mathbb{E}(\mathbf{v}\mathbf{v}^H) = \mathbb{E}\left(\mathbf{U}\Sigma\mathbf{V}_1^H|\mathbf{H}_E|^2\mathbf{V}_2\mathbf{V}_2^H|\mathbf{H}_E|^2\mathbf{V}_1\Sigma^H\mathbf{U}^H\right) \quad (7)$$

We rewrite  $|\mathbf{H}_E|^2 = \sum_{q=1}^Q |H_{E,q}|^2 \mathbf{e}_q \mathbf{e}_q^T$  where  $\mathbf{e}_q$  is an all zero vector except a 1 at row  $q$  to isolate

the independent random variable  $H_E$

$$\mathbb{E}(\mathbf{v}\mathbf{v}^H) = \sum_{q=1}^Q \sum_{q'=1}^Q \mathbb{E}(|H_{E,q}|^2 |H_{E,q'}|^2) \mathbb{E}(\mathbf{U}\Sigma\mathbf{V}_1^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_{q'} \mathbf{e}_{q'}^T \mathbf{V}_1 \Sigma^H \mathbf{U}^H) \quad (8)$$

$$= \sum_{q=1}^Q \mathbb{E}(|H_{E,q}|^4) \mathbb{E}(\mathbf{U}\Sigma\mathbf{V}_1^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_1 \Sigma^H \mathbf{U}^H) \quad (9)$$

$$+ \sum_{q=1}^Q \sum_{q' \neq q}^Q \mathbb{E}(|H_{E,q}|^2 |H_{E,q'}|^2) \mathbb{E}(\mathbf{U}\Sigma\mathbf{V}_1^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_{q'} \mathbf{e}_{q'}^T \mathbf{V}_1 \Sigma^H \mathbf{U}^H) \quad (10)$$

$$= 2 \sum_{q=1}^Q \mathbb{E}(\mathbf{U}\Sigma\mathbf{V}_1^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_1 \Sigma^H \mathbf{U}^H) \quad (11)$$

$$+ \sum_{q=1}^Q \sum_{q' \neq q}^Q \mathbb{E}(\mathbf{U}\Sigma\mathbf{V}_1^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_{q'} \mathbf{e}_{q'}^T \mathbf{V}_1 \Sigma^H \mathbf{U}^H) \quad (12)$$

$$= \sum_{q=1}^Q \mathbb{E}(\mathbf{U}\Sigma\mathbf{V}_1^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_1 \Sigma^H \mathbf{U}^H) \quad (13)$$

$$+ \mathbb{E}\left(\mathbf{U}\Sigma\mathbf{V}_1^H \sum_{q=1}^Q \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \sum_{q'=1}^Q \mathbf{e}_{q'} \mathbf{e}_{q'}^T \mathbf{V}_1 \Sigma^H \mathbf{U}^H\right) \quad (14)$$

$$= \sum_{q=1}^Q \mathbb{E}(\mathbf{U}\Sigma\mathbf{V}_1^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_1 \Sigma^H \mathbf{U}^H) + \mathbb{E}(\mathbf{U}\Sigma\mathbf{V}_1^H \mathbf{V}_2 \mathbf{V}_2^H \mathbf{V}_1 \Sigma^H \mathbf{U}^H) \quad (15)$$

Using the fact that  $\mathbf{V}_2^H \mathbf{V}_1 = \mathbf{0}$ , the second term cancels and

$$\mathbb{E}(\mathbf{v}\mathbf{v}^H) = \mathbb{E}\left(\mathbf{U}\Sigma\mathbf{V}_1^H \sum_{q=1}^Q (\mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{e}_q^T) \mathbf{V}_1 \Sigma^H \mathbf{U}^H\right) \quad (16)$$

Since all elements of  $\mathbf{v}$  have same variance, we can compute it as

$$\frac{1}{N} \mathbb{E}(\|\mathbf{v}\|^2) = \frac{1}{N} \mathbb{E} \text{tr}(\mathbf{v}\mathbf{v}^H) \quad (17)$$

$$= \frac{1}{N} \mathbb{E} \text{tr}\left(\Sigma^2 \mathbf{V}_1^H \sum_{q=1}^Q (\mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{e}_q^T) \mathbf{V}_1\right) \quad (18)$$

Let us rewrite  $\mathbf{V}_1 = \sum_l \mathbf{e}_l \mathbf{v}_{1,l}^H$  where  $\mathbf{v}_{1,l}^H$  is the  $l$ -th row of  $\mathbf{V}_1$  (of dimension  $N \times 1$ ) with only one nonzero element.

$$\frac{1}{N} \mathbb{E}(\|\mathbf{v}\|^2) = \frac{1}{N} \sum_{q=1}^Q \sum_l \sum_{l'} \mathbb{E} \text{tr}(\Sigma^2 \mathbf{v}_{1,l} \mathbf{e}_{l'}^T \mathbf{e}_q \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{e}_q^T \mathbf{e}_l \mathbf{v}_{1,l}^H) \quad (19)$$

$$= \frac{1}{N} \sum_{q=1}^Q \sum_l \sum_{l'} \delta_{l'-q} \delta_{l-q} \mathbb{E} \text{tr}(\Sigma^2 \mathbf{v}_{1,l} \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{v}_{1,l}^H) \quad (20)$$

$$= \frac{1}{N} \sum_{q=1}^Q \mathbb{E} \text{tr}(\Sigma^2 \mathbf{v}_{1,q} \mathbf{e}_q^T \mathbf{V}_2 \mathbf{V}_2^H \mathbf{e}_q \mathbf{v}_{1,q}^H) \quad (21)$$

Let us rewrite  $\mathbf{V}_2 = \sum_l \mathbf{e}_l \mathbf{v}_{2,l}^H$  where  $\mathbf{v}_{2,l}^H$  is the  $l$ -th row of  $\mathbf{V}_2$  (of dimension  $Q - N \times 1$ ) with  $U - 1$  nonzero elements

$$\frac{1}{N} \mathbb{E} (\|\mathbf{v}\|^2) = \frac{1}{N} \sum_{q=1}^Q \sum_l \sum_{l'} \mathbb{E} \text{tr} \left( \Sigma^2 \mathbf{v}_{1,q} \mathbf{e}_q^T \mathbf{e}_l \mathbf{v}_{2,l}^H \mathbf{v}_{2,l'} \mathbf{e}_{l'}^T \mathbf{e}_q \mathbf{v}_{1,q}^H \right) \quad (22)$$

$$= \frac{1}{N} \sum_{q=1}^Q \mathbb{E} \text{tr} \left( \Sigma^2 \mathbf{v}_{1,q} \mathbf{v}_{2,q}^H \mathbf{v}_{2,q} \mathbf{v}_{1,q}^H \right) \quad (23)$$

$$= \frac{1}{N} \sum_{q=1}^Q \mathbb{E} \left( \|\mathbf{v}_{2,q}\|^2 \mathbf{v}_{1,q}^H \Sigma^2 \mathbf{v}_{1,q} \right) \quad (24)$$

where  $\mathbf{v}_{1,q}^H \Sigma^2 \mathbf{v}_{1,q} := \|\mathbf{v}_{1,q}\|^2 \sigma_n^2$  is a scalar. Therefore, we obtain:

$$\frac{1}{N} \mathbb{E} (\|\mathbf{v}\|^2) = \frac{1}{N} \sum_{q=1}^Q \mathbb{E} \left( \|\mathbf{v}_{2,q}\|^2 \|\mathbf{v}_{1,q}\|^2 \sigma_n^2 \right) \quad (25)$$

Since  $\mathbf{V}$  forms an orthonormal basis, i.e.,  $\mathbf{V}^H \mathbf{V} = \mathbf{I}_Q$ , we have  $\|\mathbf{v}_{1,q}\|^2 + \|\mathbf{v}_{2,q}\|^2 = 1$ . We then have:

$$\frac{1}{N} \mathbb{E} (\|\mathbf{v}\|^2) = \frac{1}{N} \sum_{q=1}^Q \mathbb{E} \left[ \left( \|\mathbf{v}_{1,q}\|^2 - \|\mathbf{v}_{1,q}\|^4 \right) \sigma_n^2 \right] \quad (26)$$

To determine eq.26, we need to know the transformations performed by the singular value decomposition on the input matrix  $\mathbf{A}$  to obtain  $\mathbf{v}_{1,q}$  and  $\sigma_n^2$ , i.e., we have to find an analytic expression of  $\mathbf{v}_{1,q}$  and  $\sigma_n^2$ . We know that:

$$\mathbf{A} = \mathbf{S}^H \mathbf{H}_B = \begin{bmatrix} z_1 & 0 & \dots & 0 & z_2 & 0 & \dots & 0 & \dots & z_U & 0 & \dots & 0 \\ 0 & z_{U+1} & \dots & 0 & 0 & z_{U+2} & \dots & 0 & \dots & 0 & z_{2U} & \dots & 0 \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots & \dots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & z_{(N-1)U+1} & 0 & 0 & \dots & z_{(N-1)U+2} & \dots & 0 & 0 & \dots & z_Q \end{bmatrix} \quad (27)$$

where  $\mathbf{A} \in \mathcal{C}^{N \times Q}$  and  $z_i = z_{i,x} + j z_{i,y} \sim \mathcal{CN}(0, \frac{1}{U}) \sim \mathcal{N}(0, \frac{1}{2U}) + j \mathcal{N}(0, \frac{1}{2U})$ . After singular value decomposition, we obtain:

$$\Sigma = \begin{bmatrix} \sigma_1 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_N \end{bmatrix} \quad (28)$$

where  $\sigma_n = \sqrt{\sum_{i=1}^U |z_{(n-1)U+i}|^2}$ ,  $n = 1 \dots N$

$$\mathbf{V}_1 = \begin{bmatrix} v_1 & 0 & \dots & 0 \\ 0 & v_{U+1} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & v_{(U-1)N+1} \\ v_2 & 0 & \dots & 0 \\ 0 & v_{U+2} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & v_{(U-1)N+2} \\ \vdots & \vdots & & \vdots \\ v_U & 0 & \dots & 0 \\ 0 & v_{2U} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & v_Q \end{bmatrix} \quad (29)$$

where  $v_i = \frac{z_i^*}{\sigma_k}$ ,  $i = 1 \dots Q$ ,  $k = 1 \dots N$  represents the column of  $\mathbf{V}_1$  where  $v_i$  belongs.

From that, we obtain:

$$\mathbb{E} [\sigma_n^2] = \mathbb{E} \left[ \sum_{i=1}^U |z_{(n-1)U+i}|^2 \right] \quad (30)$$

$$= U \mathbb{E} \left[ |z_{(n-1)U+i}|^2 \right] \quad (31)$$

$$= U \frac{1}{U} \quad (32)$$

$$= 1 \quad (33)$$

Without loss of generality, we compute  $\mathbb{E} [\|v_1\|^2]$  and  $\mathbb{E} [\|v_1\|^4]$  since all components of  $\mathbf{V}_1$  are

identically distributed:

$$\mathbb{E} [\|v_1\|^2] = \mathbb{E} \left[ \left| \frac{z_1^*}{\sigma_1} \right|^2 \right] \quad (34)$$

$$= \mathbb{E} \left[ \frac{|z_1|^2}{\sigma_1^2} \right] \quad (35)$$

$$= \mathbb{E} \left[ \frac{|z_1|^2}{\sum_{i=1}^U |z_i|^2} \right] \quad (36)$$

$$= \mathbb{E} \left[ \frac{|z_1|^2}{U |z_1|^2} \right] \quad (37)$$

$$= \frac{1}{U} \quad (38)$$

For the moment of order 4, we note that  $\mathbb{E} [|z_i|^4] = \frac{2}{U^2}$ , cfr "*Momentum of complex normal random variables*" pdf.

$$\mathbb{E} [\|v_1\|^4] = \mathbb{E} \left[ \left| \frac{z_1^*}{\sigma_1} \right|^4 \right] \quad (39)$$

$$= \mathbb{E} \left[ \frac{|z_1|^4}{\sigma_1^4} \right] \quad (40)$$

$$= \mathbb{E} \left[ \frac{|z_1|^4}{\left( \sum_{i=1}^U |z_i|^2 \right)^2} \right] \quad (41)$$

$$= \mathbb{E} \left[ \frac{|z_1|^4}{\sum_{i=1}^U |z_i|^4 + 2 \sum_{i=1}^U \sum_{j<i} |z_i|^2 |z_j|^2} \right] \quad (42)$$

$$= \mathbb{E} \left[ \frac{|z_1|^4}{U |z_1|^4 + 2 \frac{(U-1)U}{2} |z_i|^2 |z_j|^2} \right] \quad (43)$$

$$= \frac{\frac{2}{U^2}}{U \frac{2}{U^2} + 2 \frac{(U-1)U}{2} \frac{1}{U} \frac{1}{U}} \quad (44)$$

$$= \frac{\frac{2}{U^2}}{\frac{U+1}{U}} \quad (45)$$

$$= \frac{2}{U(U+1)} \quad (46)$$

The double sum on the denominator of eq.42 contains  $\frac{(U-1)U}{2}$  double products.

Finally, we can compute eq.26 as:

$$\frac{1}{N}\mathbb{E}(\|\mathbf{v}\|^2) = \frac{1}{N} \sum_{q=1}^Q \left[ \left( \frac{1}{U} - \frac{2}{U(U+1)} \right) 1 \right] \quad (47)$$

$$= \frac{1}{N} Q \frac{U-1}{U(U+1)} \quad (48)$$

$$= \frac{U-1}{U+1} \quad (49)$$

which is the mean energy per symbol of the AN component when Eve implements a matched filtering.

It is exactly what we observe in the simulations.

$$\mathbb{E}[\gamma_{E,n}] = \frac{\alpha(U+1)(U+3)}{U[(U+1)\sigma_E^2 + (1-\alpha)]} \quad (50)$$

$$C_s = \log_2 \left( 1 + \frac{\alpha(U+1)}{U\sigma_B^2} \right) - \log_2 \left( 1 + \frac{\alpha(U+1)(U+3)}{U[(U+1)\sigma_E^2 + (1-\alpha)]} \right) \quad (51)$$