Covert Wireless Communications: Temporal Focusing and Information Theoretic Methods

Jon W. Wallace

Jacobs University Bremen
School of Engineering and Science
Campus Ring 1, 28759 Bremen, Germany
wall@ieee.org

1 Introduction

Temporal focusing of a signal by transmitting the time-revered channel response (equivalent to frequency domain phase conjugation) was first discovered in optical and acoustical treatments. Recent work demonstrates interest in applying this phenomenon to RF and microwave channels [1, 2]. With transmit and receive arrays, it is also well understood that gain is maximized by directing power along the transmit/receive singular vectors of the channel transfer matrix corresponding to the principal singular value, and this *spatial focusing* can further augment the focusing effect.

A possible advantage of temporal/spatial focusing is low probability of intercept, since a signal focused for an intended recipient is likely to be unfocused for others. This property is also useful in multiuser scenarios to avoid interference. However, to the author's knowledge, no work has yet appeared that analyzes focusing from an information theoretic standpoint. This paper derives two information theoretic transmission strategies and compares the resulting performance to focusing. This work mainly considers *temporal* focusing by interpreting subchannels as frequency bins. However, spatial focusing is easily accommodated by taking the SVD of the spatial subchannels and stacking singular values for different frequency bins and spatial indices together.

2 Transmission Strategies

Consider a wideband communications channel with N discrete subchannels. The complex baseband input/output relationship for the ith subchannel is

$$y_i = h_i x_i + n_i, \tag{1}$$

where h_i is the complex channel gain, x_i and y_i are the input and output signals, and n_i is noise for a single channel use. Noise is zero mean i.i.d. Gaussian with variance σ^2. Total transmit power is $\sum_i |x_i|^2 = \sum_i p_i = P_T$.

2.1 Temporal Focusing

In temporal focusing, the x_i are chosen to be proportional to the conjugate of the channel gain h_i, or $x_i = x(h_i^*/\alpha)$, where $\alpha = \sqrt{\sum_i g_i}$, $g_i = |h_i|^2$, and for an average transmit power of P_T, $\mathrm{E}\{|x|^2\} = P_T$.

Temporal focusing transforms the parallel subchannels into an effective SIMO channel $\mathbf{g}$, where a single input x leads to multiple outputs y_i, whose mutual information (MI) for complex Gaussian x is

$$I_{\mathrm{TF}} = \log\left(\frac{P_T\,\mathbf{g}\,\mathbf{g}^H}{\sigma^2\alpha^2} + \mathbf{I}\right) = \log\left(\frac{P_T\sum_i g_i^2}{\sigma^2\alpha^2} + 1\right), \tag{2}$$

where perfect channel state information (CSI) is assumed at transmit and receive.

We need to consider the MI of an unauthorized listener or *eavesdropper*. For a single channel realization, the MI to the eavesdropper is

$$\hat{I}_{\mathrm{TF}} = \log\left(\frac{\sum_i p_i \hat{g}_i}{\sigma^2\alpha^2} + 1\right), \tag{3}$$

1-4244-0878-4/07/$20.00 ©2007 IEEE

where $p_i = \mathrm{E}\{|x_i|^2\}$, and $(\hat{\cdot})$ refers to eavesdropper quantities. Obviously, the transmitter will not have detailed knowledge of the eavesdropper channel $\hat{h}_i$. Thus, we will concern ourselves mainly with the ergodic MI $\mathrm{E}\{\hat{I}\}$, which can be upper bounded with Jensen's inequality as

$$\hat{I}_{\mathrm{TF}} \leq \log\left(\frac{\sum_i p_i s_i}{\sigma^2 \alpha^2} + 1\right), \tag{4}$$

where $s_i = \mathrm{E}\{\hat{g}_i\}$. This will be referred to as the MI at the eavesdropper, recognizing that it is actually an upper bound.

2.2 Weighted Mutual Information (WMI)

One way of choosing x_i to communicate covertly is to seek to maximize

$$F = w_1 \underbrace{\sum_i \log\left(\frac{p_i g_i}{\sigma^2} + 1\right)}_{I_{\mathrm{WMI}}} - w_2 \underbrace{\sum_i \log\left(\frac{p_i s_i}{\sigma^2} + 1\right)}_{\hat{I}_{\mathrm{WMI}}}, \tag{5}$$

where the weights reflect the importance of transmitting information (I_{WMI}) to the intended user (w_1), while avoiding transmission to the eavesdropper (w_2), and the same noise is assumed for both receivers.

Although the optimization is involved for constrained transmit power, the solution is trivial when the power is left unconstrained. Taking the derivative of (5) with respect to p_k and setting to 0, we have

$$p_k = \left[\frac{\sigma_2}{w_2 - w_1}\left(\frac{w_1}{s_k} - \frac{w_2}{g_k}\right)\right]^+, \tag{6}$$

where $[\cdot]^+$ gives its argument when positive, and zero otherwise. This solution is only a maximum for the case $w_2 > w_1$. Otherwise, the eavesdropper is not very important, the solution is a minimum, and one should just transmit as much power as possible.

2.3 Constrained Capacity (CC)

An alternative criterion is to minimize MI to the eavesdropper while maintaining a given capacity to the intended user. In this case one minimizes

$$\hat{I}_{\mathrm{CC}} = \sum_i \log\left(\frac{p_i s_i}{\sigma^2} + 1\right) \quad \text{subject to} \quad C = \sum_i \log\left(\frac{p_i g_i}{\sigma^2} + 1\right). \tag{7}$$

Although the power level is technically not constrained, practice shows that power scales with C much like the water filling (WF) solution. Forming the Lagrangian of (7), taking the derivative with respect to p_k, and setting equal to 0,

$$p_k = \frac{\sigma^2(1 - \lambda g_k/s)}{g_k(\lambda - 1)}, \quad \lambda = \left(1 - \exp\left\{\frac{1}{N}\left[\sum_i \log\left(1 - g_i/s\right) - C\right]\right\}\right)^{-1}. \tag{8}$$

The sign of the second derivative of the Lagrangian with respect to p_k indicates whether this solution is a minimum, maximum, or saddle point, and the critical points are $c_k = [(p_k + \sigma^2/g_k)/(p_k + \sigma^2/s)]^2$. If $\lambda > c_k$ or $\lambda < c_k$ for all k, the solution is a minimum or maximum, respectively, otherwise the solution is a saddle point. Note that a saddle point means we should set the power to 0 for some of the subchannels, and a maximum (should it exist) would mean not transmitting is optimal. The solution procedure used in this work orders the subchannels in terms of decreasing quality and finds the subset that attains the optimal minimum solution, very similar to water-filling.

3 Performance Comparison

Channels are generated assuming the h_i are i.i.d. complex Gaussian with unit variance, $N = 40$, and an average SISO SNR of 10 dB ($\sigma^2 = 0.1$). The eavesdropper is assumed to have approximately the same channel quality, or $s = s_i = 1$. From a practical standpoint, these parameters are obtained for a noise level of -100 dBm per frequency bin, a path loss of 90 dB, and a transmit power of 0 dBm. If these figures are realistic, the transmit power in the following simulations can be considered to have units of dBm. For comparison, the capacity of a SISO channel with 10 dB SNR is 3.46 bits/s/Hz. Note that WMI and CC set the transmit power level for each channel realization, and this same level is then used for the WF and TF cases as well.

Figure 1 depicts the power distribution for WMI, WF, and TF for a typical channel for two different values of $w = w_2/w_1$. The channel coefficients are proportional to the p_i of the TF solution. For values of w slightly larger than 1, the power distribution for WMI and TF are very similar. However, the signaling strategy is quite different, since for TF, the signals x_i are perfectly correlated, and for WMI they are uncorrelated. As the relative importance of not being overheard increases (large w), WMI favors lower transmit power, with all power directed into a single frequency bin. For this low SNR case, the WF solution is nearly equivalent. Note that for larger w, sometimes all of the p_i in (6) are 0, meaning that the optimum is to not transmit at all.

Table 1a lists the numerical values for this same case. For low w, transmit power is high, and TF performs poorly, transmitting nearly equal MI to both the user and eavesdropper. The MI for WMI and WF is considerably higher than TF, since the subchannels are used independently. Also, the MI of the eavesdropper is significantly smaller than the user, as desired. For increasing w, the transmit power for WMI drops, and at this low SNR, WMI and WF are still better at avoiding transmission to the eavesdropper than TF. Figure 2b depicts the statistics of the ratio $(\hat{I}/I)$ for 1000 random channel realizations and $w = 4$, indicating that WMI is significantly better at avoiding unwanted reception than TF.

Next consider the CC strategy, where capacity to the desired user is held constant and MI to the eavesdropper is minimized. Figure 3 plots the power allocation for two levels of constrained capacity C. For a modest level of $C = 5$ bits/s/Hz, the power level is low, and only a few of the best frequency bins are selected in CC and WF, in contrast to TF that distributes power more evenly. For $C = 40$ bits/s/Hz, transmit power is higher, and the power distributions of CC and WF look more similar.

Table 1b lists the results for several values of C for this channel. For all levels of C, both CC and WF are able to create a larger information gap between the desired user and eavesdropper than the TF solution. Figure 2b plots CDFs of the ratio $(\hat{I}/I)$ for 1000 random realizations with $C = 20$ bits/s/Hz, indicating that the CC solution maintains a better ratio. Also note that the MI to the desired user is only about 5 bits/s/Hz for the TF case, compared to the constrained value of 20 bits/s/Hz for CC.

4 Conclusion

This paper has compared temporal focusing with information theoretic criteria for covert wireless communications. The two information theoretic methods considered provide a much larger information gap between the intended user and eavesdropper, demonstrating that temporal focusing methods can be very suboptimal for this simple scenario.

References

[1] H. T. Nguyen, J. B. Andersen, G. F. Pedersen, P. Kyritsi, and P. C. F. Eggers, "Time reversal in wireless communications: a measurement-based investigation," *IEEE Trans. Wireless Commun.*, vol. 5, pp. 2242–2252, Aug. 2006.

[2] C. Oestges, A. D. Kim, G. Papanicolaou, and A. J. Paulraj, “Characterization of space-time focusing in time-reversed random fields,” *IEEE Trans. Antennas Propag.*, vol. 53, pp. 283–293, Jan. 2005.

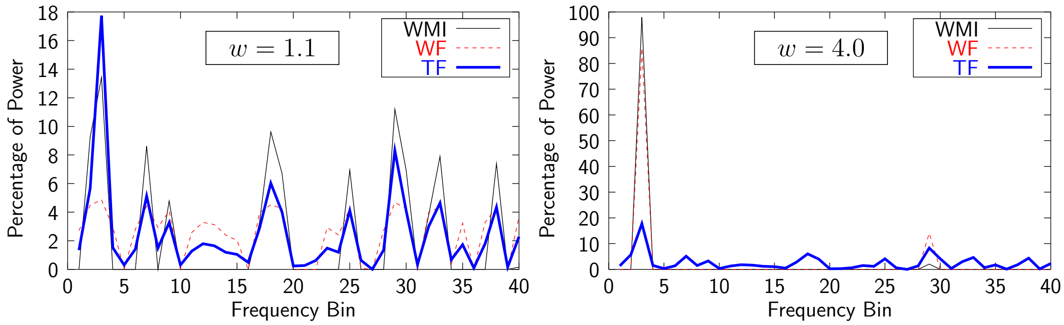

Figure 1: Power allocation for weighted MI and temporal focusing for a typical realization

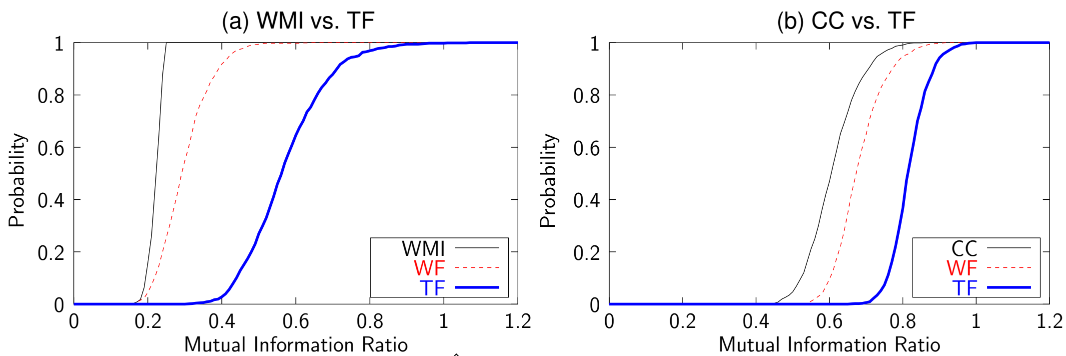

Figure 2: CDFs of the ratio $(\hat{I}/I)$ for the different transmission strategies

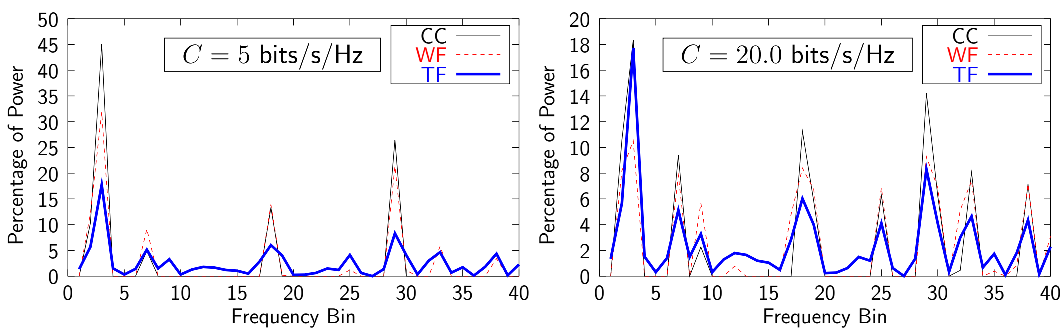

Figure 3: Power allocation for constrained capacity and temporal focusing for a typical realization

Table 1: Numerical performance for a typical channel realization. Units are dB for P_T and bits/s/Hz for C and I.

(a) WMI vs. TF

w	P_T	I_{WMI}	$\hat{I}_{\text{WMI}}$	I_{WF}	$\hat{I}_{\text{WF}}$	I_{TF}	$\hat{I}_{\text{TF}}$
1.1	8.1	47	33	57	48	7.7	6.0
2.0	-6.5	7.4	2.7	7.6	2.9	3.0	1.7
4.0	-17	1.4	0.24	1.4	0.25	0.65	0.24
8.0	-30	0.13	0.015	0.13	0.015	0.046	0.015

(b) CC vs. TF

C	P_T	I_{CC}	$\hat{I}_{\text{CC}}$	I_{WF}	$\hat{I}_{\text{WF}}$	I_{TF}	$\hat{I}_{\text{TF}}$
5	-9	5	1.5	5.1	1.6	2.3	1.2
10	-4.6	10	4	10	4.3	3.5	2.2
20	0.23	20	10	21	11	5.1	3.5
40	6.2	40	26	46	36	7	5.4