SAPIENZA
UNIVERSITÀ DI ROMA

MASTER THESIS

OPTIMAL POWER ALLOCATION IN MIMO WIRE-TAP CHANNELS

Inés Marqués Durán
July, 2011

Thesis advisor: Mauro Biagi
Dipartamento di Scienza e Tecnica dell'Informazione e della Comunicazione INFOCOM
Università La Sapienza di Roma
Via Eudossiana, 18 -00184 Rome- Italy
http://www.uniroma1.it/

OPTIMAL POWER ALLOCATION IN MIMO WIRE-TAP CHANNELS

Inés MarquésDurán

July, 2011

I would like to thank my advisor Mauro Biagi for providing the motivation and resources for this research to be done, as well as my familyand friends for their unwavering support during this work and in all my academic pursuits.

Contents

Chapter 1: Introduction

Today, with the advent of the Information Age, the need to protect the integrity of communications and maintain an adequate level of privacy is more important than ever.

Aside from traditional cryptographic security mechanisms, information-theoric-based security techniques have gained increasing attention in recent years.

Especially in wireless communications security and privacy protection is one of the most important issues. Wireless transmission can be received by multiple receivers with different signal strengths and this broadcast naturein particular makes this transmission susceptible to eavesdropping. Anyone within communication range can listen to the transmission in the air and extract the information.

In the following it's shown how solving secrecy issues at Physical Layer could try to provide a background foot confidentially to the upper layers without the substitution of cryptography.

The present work is structured in 3 chapters. The first one is an introduction of MIMO Systems, which is the model we are going to follow in the whole thesis. The second one is a summary of classic cryptography. Finally in the third chapter we present our scenario and a novel way to keep confidence paying attention to the secrecy level. This secrecy level is measured by the information rate of the eavesdropper and corresponds to the level of ignorance of the eavesdropper with respect to the confidential message. We are going to consider waterfilling-based approaches with additional constraint on the secrecy level that is compromised by a passive eavesdropper and the introduction of a new element (a matrix) that is going to introduce randomness and hence increase secrecy.

Chapter 2: MIMO Systems

2.1 Definition of SISO Channels

Let $\mathrm{h}(\tau,\mathrm{t})$ be the time-varying channel impulse response from the input of the pulse-shaping filter $\mathrm{g}(\mathrm{t})$ at the transmitter, through the propagation channel $\mathrm{p}(\tau,\mathrm{t})$ to the output of the receiver matched-filter. We define $\mathrm{h}(\tau,\mathrm{t})$as the response at time t to an impulse at time $\mathrm{t}-\tau$. The combination of the pulse shaping filter and the matched-filtermakes the $\mathrm{h}(\tau,\mathrm{t})$ a narrowband channel. For convenience we normally refer to $\mathrm{h}(\tau,\mathrm{t})$ as the channel from the transmit antenna to the receiver antenna, but it is strictly defined as above. Note that $\mathrm{h}(\tau,\mathrm{t})$is the complex envelope of thebandpassimpulse response function.

If a signal $s(t)$ is transmitted, the received signal $y(t)$ is given by:

$$y(t) = \int_0^{T_{total}} h(\tau,t)s(t-\tau) \qquad (2.1)$$

2.2 Definition of MIMO Channels

Consider a MIMO system with M_T transmits antennas and $M_R$receives antennas. Denoting the impulse response between the $jth\,(j = 1,2,\dots,M_T)$ transmit antenna and the $jth\,(j = 1,2,\dots,M_R)$ receive antenna by $h_{i,j}(\tau,t)$, the MIMO channel is given

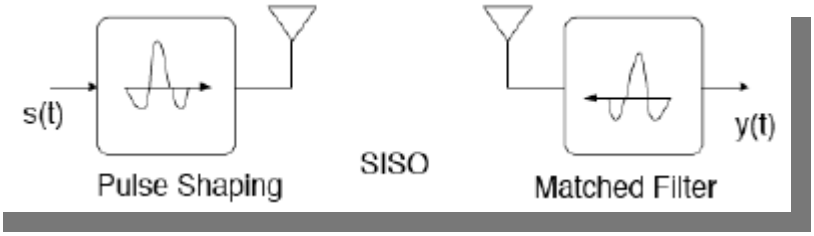

Figure 2.1: a schematic for a SISO system

by the $MR\ xMT$ matrix $\mathbf{H}(\tau,\mathrm{t})$with

$$\mathbf{H}(\tau,t) = \begin{bmatrix} h_{1,1}(\tau,t) & \cdots & h_{1,M_T}(\tau,t) \\ \vdots & \ddots & \vdots \\ h_{M_R,1}(\tau,t) & \cdots & h_{M_R M_T}(\tau,t) \end{bmatrix} \quad (2.2)$$

The vector $\left[h_{i,j}(\tau,t)h_{2,j}(\tau,t) \;\cdots\; h_{M_R,j}(\tau,t)\right]^T$is the spatio-temporal signature or channel induces by the jth transmit antenna across the receive antenna array. Further, given that the signal $s_j(t)$ is launched from the jth transmit antenna, the signal received at the ith receive antenna, $y_i(t)$ is given by

$$y_i(t) = \sum_{j=1}^{M_T} h_{i,j}(\tau, t) \ * s_j(t) \quad i = 1,2, \dots, M_R \quad (2.3)$$

The input output relation for the MIMO channel may be expressed in matrix notation as

$$\mathbf{y}(\mathbf{t}) = \mathbf{H}(\tau, \mathbf{t}) * \mathbf{s}(\mathbf{t}) (2.4)$$

where $\mathbf{s}(\mathbf{t}) = [s_1(t) s_2(t) \quad \cdots \quad s_{M_T}(t)]^T$ is an $M_T \times 1$ vector and $\mathbf{y}(\mathbf{t}) = [y_1(t) y_2(t) \ \cdots \ y_{M_R}(t)]^T$ is a vector of dimension $M_R \times 1$.

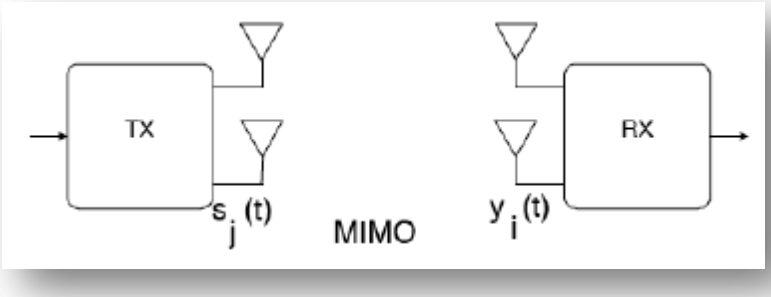

Figure 2.2: schematic for a MIMO system

2.3 Physical Scattering Model for ST Channels

In this section we relate the multiple antenna wireless channels to a physical scattering model. For convenience, we neglect the time-varying nature of the channel.

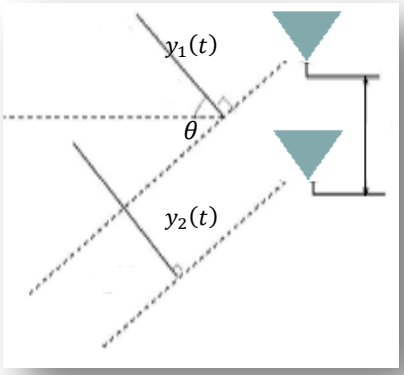

Figure 2.3: incomingwavefront

Narrowband Array: Consider a signal wavefront$z(t)$ impinging on an antenna array composed of two antennas spaced d apart at angle θ(see Fig.2.3).

We assume that the wavefront has a bandwidth B and is represented as

$$z(t) = \beta(t)e^{j2\pi\vartheta_c t}, \qquad (2.5)$$

where$\beta(t)$is the complex envelope representation of the signal (with bandwidth B) and ϑ_c is the carrier frequency. Under the narrowband assumption, we take the bandwidth B to be much smaller than the reciprocal of the transit time of the wavefront across the antenna array T_Z; i.e.,$B \ll 1/T_Z$. Under this assumption, if the signal received at the first antenna($y_1(t)$)is$z(t)$,then the signal received at the second antenna ($y_2(t)$) is given by

$$y_2(t) = z(t - T_z) = \beta(t - T_Z)e^{j2\pi\vartheta_c(t-T_z)} \qquad (2.6)$$

where we have assumed identical elements patterns. Under the narrowband assumption, further (reminding that $T_z = d\sin\theta$ and that $\vartheta_c = \frac{1}{\lambda_c}$)

$$e^{j2\pi\vartheta_c(t-T_z)} = e^{j2\pi\vartheta_c t}e^{-j2\pi\sin\theta\frac{d}{\lambda_c}} \quad (2.7)$$

whereλ_c is the wavelength of the signal wavefront. Hence, the output at the second antenna can be written as

$$y_2(t) = \beta(t)e^{j2\pi\vartheta_c t}e^{-j2\pi\sin\theta\frac{d}{\lambda_c}} = \ y_1(t)e^{-j2\pi\sin\theta\frac{d}{\lambda_c}} \qquad (2.8)$$

from the former equation we can see that the signal received at the two antennas are identical, except for a phase shift that depends on the array geometry and the AOA of the wavefront. The results can be extended to arrays with more than two antennas. Note that the narrowband assumption does not imply that the channel is frequency flat.

Array Manifold: Consider an antenna array comprising M antennas in a free field environment, the spatial signature induced across the antenna array from a planar CW wave arriving from angle $\theta$is modelled ad and$M \times 1$ complex array response vector.

$$\mathbf{a}(\theta) = [\mathrm{a}_1(\theta)\mathrm{a}_2(\theta) \quad \cdots \quad \mathrm{a}_\mathrm{M}(\theta)]^\mathrm{T} \quad (2.9)$$

2.3.1 MIMO Channel

Consider a MIMO channel with $M_T$transmit antennas and $M_R$receive antennas. For underlying scatters at transmit angle $\emptyset$and receive angleθ, the scattering amplitude$S(\theta,\tau) = S(\emptyset,\tau)$.So the MIMO channel $\mathbf{H}(\tau)$ can be constructedas

$$\mathbf{H}(\tau) = \int_{-\pi}^{\pi}\int_{0}^{\tau_{max}} S(\theta,\tau')\ \mathbf{a}(\theta)\boldsymbol{b}(\emptyset)^T g(\tau-\tau')d\tau' d\theta \qquad (2.10)$$

The single scattering model in Eq. 2.10has a lot of limitations and cannot adequately model all observed channel effects. A more general model is to assume multiple scattering, i.e., energy from transmitter uses more than one scatter to reach the receiver. If we use a multiple scattering model, the parameters$\emptyset$, $\theta$and τ are not related.

The scatter location, antenna element patterns and geometry and the scattering model together determine the correlation between the elements of$\mathbf{H}$, the channel between the receiver and the transmitting antenna. Under suitable conditions of the above parameters, we can show that the elements of $\mathbf{H}$ are independent zero meancircularly symmetric complex Gaussian random variables (ZMCSCG). A complexGaussian random variable $Z = X + jY$ is ZMCSCG if X and Y are independent realGaussian random variables with zero mean and equal variance.

IDD (Independent Identically Distributed) Channel Model

Assuming that the delay spread in the channel is negligible, i.e., $\tau_{RMS} = 0$ Eq 2.10 can be rewritten as

$$\mathbf{H}(\tau) = \mathbf{H}g(\tau)(2.11)$$

Dropping $g(\tau)$ and considering the assumption discussed above, the elements of $\mathbf{H}$ can be modelled to be ZMCSCG with unit variance. Then we get $\mathbf{H} = \mathbf{H}_{\boldsymbol{w}}$ the IID (spatially white) channel. Some properties of $\mathbf{H}_{\boldsymbol{w}}$include:

$$E\{[H_W]_{i,j}\} = 0$$
$$E\{[H_W]_{i,j}\}^2 = 1$$
$$E\{[H_W]_{i,j}[H_W]^*_{m,n}\} = 0 \quad if\ i \neq m\ or\ j \neq n$$

$\mathbf{H}_{\boldsymbol{w}}$is known as non-physical model since it do not incorporate the physical path structure.

Frequency Flat vs. Frequency Selective Fading

The channel is said to be frequency selective if the bandwidth-delay spread productis$B \times \tau_{RMS} \geq 0.1$. Otherwise the channel is frequency flat. The channel$\mathbf{H}(\tau)$may be expressed in the frequency domain by its Fourier transform as

$$\widetilde{\mathbf{H}}(\mathrm{f}) = \int_{0}^{\infty} \mathbf{H}(\tau)\mathrm{e}^{-\mathrm{j}2\pi\mathrm{f}\tau}\, d\tau \qquad (2.12)$$

The variation of $\widetilde{\mathbf{H}}(\mathrm{f})$ with f will depend on the delay spread and hence on the coherence bandwidth B_C . If f_1 and f_2 are two frequencies such that $|f_1 - f_2| \gg B_c$, we should expect that $E\{vec(\widetilde{\mathbf{H}}(\mathrm{f}_1))vec(\widetilde{\mathbf{H}}(\mathrm{f}_2))^H\} = 0_{M_T M_R}$, i.e. f_1 and f_2 are independent and uncorrelated. The spatial statistic of $\widetilde{\mathbf{H}}(\mathrm{f})$depend on the scattering environment and array geometry at both the transmitter and receiver, under appropriate scattering and antenna conditions we get$\widetilde{\mathbf{H}}(\mathrm{f}) = \widetilde{\mathbf{H}}_{\boldsymbol{w}}(f)$, . This implies that the channel is$\mathbf{H}w$at any given frequency and that it varies with frequency depending on coherence bandwidth B_c.

Spatial Fading Correlation

Correlated Channels imply that elements of **H** are correlated and may be modelled by

$$\mathbf{H} = \mathbf{R}_{\mathrm{r}}^{1/2}\mathbf{H}_{\mathrm{w}}\mathbf{R}_{\mathrm{t}}^{1/2} \qquad (2.13)$$

where$\mathbf{R}_{\mathrm{t}}$ is the $MT \times MT$ transmit covariance matrix and $\mathbf{R}_{\mathrm{r}}$ is the $MR \times MR$receive covariance matrix. Both $\mathbf{R}_{\mathrm{t}}$and $\mathbf{R}_{\mathrm{r}}$ are positive semi-definite Hermitian matrices. This model is valid if all the transmit antennas are closely located and have identical radiation patterns.

LOS Component

We have considered only Rayleigh fading in describing the MIMO channel. In the presence of a LOS component between the transmitter and the receiver, the MIMO channel may be modelled as the sum of a fixed component and a variable component, as follows

$$\mathbf{H} = \sqrt{\frac{\mathrm{K}}{1+\mathrm{K}}}\widetilde{\mathbf{H}} + \sqrt{\frac{1}{1+\mathrm{K}}}\mathbf{H}_{\mathrm{W}} \qquad (2.14)$$

where the first term represents the LOS component of the channel and the second term is the fading component that assumes uncorrelated fading. K is the Ricean factor of the system and is essentially the ratio of the power in the LOS component of the channel to the power in fading component. K = 0 correspond to a pure Rayleigh fading while K =∞correspond to a non-fading channel.

2.4 Singular Values of H

The $MR \times MT$ channel matrix **H**, with rank r, has a Singular Value Decomposition(SVD)

$$\mathbf{H} = \mathbf{U}\sum\mathbf{V}^{\mathbf{H}} \qquad (2.15)$$

where**U** and **V** are $MR \times r$ and $MT \times r$ matrices respectively, and satisfy $\mathbf{UU^H} = \mathbf{VV^H} = \mathbf{I_r}$ and $\sum = diag\{\sigma_1, \sigma_2, \cdots \sigma_r\}$with$\sigma_i \geq 0$ and$\sigma_i \geq \sigma_{i+1}$, where$\sigma_i$is the ith singular value of the channel. The columns of **V** and **U** are also known as the input and output singular vectors, respectively.

$\mathbf{HH}^{\mathrm{H}}$is an $MR \times MR$ semi-definite Hermitian matrix and its Eigen decomposition is

$$\mathbf{HH}^{\mathrm{H}} = \mathbf{Q\Lambda Q^H} (2.16)$$

where**Q** is an $MR \times MR$ matrix satisying the relation $\mathbf{Q}^{\mathrm{H}}\mathbf{Q} = \mathbf{QQ}^{\mathrm{H}} = \mathbf{I}_{\mathrm{M_R}}$ and $\mathbf{\Lambda} = \mathrm{diag}\{\lambda_1, \lambda_2, \cdots, \lambda_{M_R}\}$with $\lambda_i \geq 0$ and $\lambda_i \geq \lambda_{i+1}$. Then

$$\lambda_i = \begin{cases} {\sigma_i}^2, & if \quad i = 1,2, \dots, r \\ 0, & if \quad i = r, r+1, \dots, M_R \end{cases} \qquad (2.17)$$

Since H is random, $\lambda_i$is also a random variable.

2.5 MIMO sampled Signal Model

2.5.1 Normalization

For Single Carrier modulation, we assume the channel bandwidth is 1 Hz and the symbol period is 1 second. We assume all signal and noise are modelled as the complex envelope of the underlying passband channel.We assume that in frequency flat channels the average channel element energy is normalized i.e., $E\left\{\left|h_{i,j}\right|^2\right\} = 1$.Further we assume that delay spread channels have a multitap channel response and that the total average energy of all taps for a given channel element is normalized, i.e., the multipath effects do not change average channel power transfer efficiency. We also assume that the fading component of the channel is ZMCSCG.

For the MIMO channel we assume the average transmit energy per symbol period is constant and therefore the symbol energy per antenna is reduced by the number of antennas, i.e., the energy per symbol per antenna is E_S/M_T. We also assume that data symbol prior to coding are IID and are drawn from scalar constellation with zero mean and unit average energy.

The noise on each antenna is assumed to be Additive White Gaussian Noise (AWGN) and that the noise is independent across receive antennas. The noise have got the following features

$$\mathbf{z}(\mathrm{t}) = \mathbf{y}(\mathrm{t}) + \mathbf{n}(\mathrm{t});$$

$$\mathrm{E}\{\mathrm{n_i^* n_j}\} = \delta_{\mathrm{i,j}}\sigma_{\mathrm{n}}^2;$$

$$\mathrm{E}\{\mathrm{Re}(\mathrm{n_i})^*\mathrm{Im}(\mathrm{n_j})\} = 0;$$

$\mathrm{E}\{\mathrm{Re}(\mathrm{n}_\mathrm{i}^2)\} = \mathrm{E}\{\mathrm{Im}(\mathrm{n}_\mathrm{j}^2)\}$.

2.5.2 Frequency Flat Channel

The channel is modelled by the $MR \times MT$ matrix **H**. The signal model is

$$\mathbf{y}[k] = \sqrt{\frac{E_s}{M_T}}\mathbf{H}\mathbf{s}[k] + \mathbf{n}[k], \qquad (2.18)$$

where$\mathbf{y}[k]$ is the received signal vector with dimension $MR \times 1$, $\mathbf{s}[k]$ is the transmit signal vector of dimension $MT \times 1$ and $\mathbf{n}[k]$ is the $MR \times 1$ spatio-temporally white ZMCSCG noise vector with variance$\mathcal{N}_0$in each dimension. Since the output at any instant of time is independent of inputs at previous time, we can drop the time index k.

2.5.3 Frequency Selective Channel

We represent the channel by the $MR \times MT$ matrix $\mathbf{H}[l](l = 0,1,2, \dots, L-1)$where L is the maximum channel length of all component $M_R M_T$ SISO link. The channel between the ith receives and jth transmitter antenna is given by $h_{i,j}[l]$ $(i = 0,1,2, \dots, M_R\ j = 0,1,2, \dots, M_T$. The received signal vector at time k, $\mathbf{y}[k]$, of dimension $MR \times 1$ may be expressed as

$$\mathbf{y}[k] = \sqrt{\frac{E_S}{M_T}}\begin{bmatrix} \mathbf{h}_{1,1} & \cdots & \mathbf{h}_{1,M_T} \\ \vdots & \ddots & \vdots \\ \mathbf{h}_{M_R,1} & \cdots & \mathbf{h}_{M_R M_T} \end{bmatrix}\begin{bmatrix} \mathrm{s}_1[k] \\ \vdots \\ \mathrm{s}_{M_R}[k] \end{bmatrix} + \mathbf{n}[k] \qquad (2.19)$$

where

$$\mathbf{h}_{\mathrm{i,j}} = \left[\mathrm{h}_{\mathrm{i,j}}[\mathrm{L}-1] \ \cdots \ \mathrm{h}_{\mathrm{i,j}}[0]\right], \qquad \mathrm{s}_\mathrm{j}[\mathrm{k}] = \begin{bmatrix} s_j[k-L+1] \\ \vdots \\ s_j[k] \end{bmatrix} \qquad (2.20)$$

2.6 ST Channel Estimation

In this section we briefly review ST channel estimation at the receiver and transmitter.We begin by considering channel estimation at the receiver, which is commonlyneededin communication systems.

2.6.1 Estimating the ST Channel at the Receiver

In SISO systems, the channel is estimated by the receiver using training signalemitted by the transmitter. A number of training techniques have been developer and are specific to each modulation scheme. The receiver know the trainingsequence F[k] (k = 0, 1, 2,J - 1) in advance. Denoting the channel by$\mathbf{h} = \left[\, \mathrm{h}[\mathrm{L}-1] \quad \cdots \quad \mathrm{h}[0] \right]$the received signal is

$$\left[\mathrm{y}[k] \quad \cdots \quad \mathrm{y}[k+\mathrm{T}-1]\right] = \mathbf{h}\mathcal{F} + \left[\mathrm{n}[k] \quad \cdots \quad \mathrm{n}[k+\mathrm{T}-1]\right] (2.21)$$

where$\mathcal{F}$ is appropriately constructed from $\mathrm{F}[\mathrm{k}]$ $(\mathrm{k} = 0,1,2,\ldots.,\mathrm{J}-1)$The channel estimate, $\hat{\mathbf{h}}$, is obtained using a least squares approach.

$$\hat{\mathbf{h}} = \left[y[k] \quad \cdots \quad y[k+T-1]\right]\mathcal{F}^{\dagger} \qquad (2.22)$$

F[k] is typically chosen to have good autocorrelation properties. Depending on the SNR at the receiver and the desired channel estimation accuracy, the duration (or energy) of the training signal has to be selected. The desired channel estimation accuracy depends on the modulation order used, a useful rule of thumb being that the channel estimation error should be 10 dB below the additive noise power. If the channel has delay spread, more channel parameters have to be estimated and additional training signal energy has to be expected to estimate the channel. Further, the frequency of channel estimation depends on the Doppler spread, i.e., the more rapidly the channel change, the more frequently we need to estimate.

Channel estimation often use interpolation techniques, where the channel is estimated at discrete points in time or frequency (spaced well below TC or BC respectively) and the channel at the other points is interpolated through some suitable scheme.

In blind techniques for channel estimation no explicit training signal are used, instead the receiver estimates the channel from the signal received during normal data (information) transmission.

Training with Multiple Transmit Antennas. All the above comments on training apply. In addition, the multiple transmit antennas will need additional training effort, since more parameters (proportional to the number of transmit antennas) have to be estimated. We try to ensure that the training signals from the multiple antennas are mutually orthogonal in some dimension, for example in time (different time slot), frequency (different tones in OFDM) or code (in orthogonal codes).

Orthogonal signals provide the best estimation accuracy for a given transmit power under most circumstances. The same channel estimation technique expressed inEq. 2.21applies, except that **h**and $\mathcal{F}$are suitably structured to reflect multiple antenna training structure as per Eq. 2.19.Typically the training sequence should have good auto and cross-correlation properties.

The number of the samples collected during training (per receive antenna) must now be $T \geq MT \times L$. If we assume a block fading model (i.e. the channel is constant during a coherenceperiod T_C and changes abruptly to a new value at T_C intervals), the maximum number of symbols per coherent period is $T_c \times B$. Thus T can be at most $T_c \times B$.Therefore if$M_T \times L > T_C \times B,$ we can never get perfect channel estimation at the receiver even in the absence of noise.

Channel estimation for frequency and time selective ST channels has been studied. Usually the receiver estimate the channel at adequately (Nyquist) spaced frequencies or time (sampling). The full channel is the determined through interpolation.

2.6.2 Estimating the ST Channel at the Transmitter

In SISO wireless link, knowledge of the channel at the transmitter is typically used for adapting the modulation rate or for power control. This only needs the magnitude (or gain) of the forward channel. In MIMO channels, knowledge of the channel can be leveraged in additional ways, such as beamforming or pre-filtering, to provide significant value. Therefore, there is significant motivation for channel knowledge at the transmitter at the ST channels. In MIMO-MU (Multi User) channel knowledge is necessary to steer signal selectively at user. Depending on the application, differing levels of accuracy in channel information are needed.

We assume a two-way communication link. For convenience, we assume that we are interesting in estimating the forward channel at the base-station. Forward channel estimation at the base is not directly possible as the signal travels through only after leaving the base transmitter. Two general techniques are used in channel estimation at the transmitter. In the first approach the forward channel is estimated at terminal receiver after the signal has travelled through the channel and then sent back (feedback) to the transmitter on the reverse link. In the second approach, we leverage the reciprocity principle in duplex transmission. The transmitter first estimate the reverse link channel, and uses this estimate for the forward link channel.

In the following we describe the two techniques mentioned before.

Channel Estimation at Transmitter Using Feedback. In this approach the forward link ST channel is estimated at the terminal (the channel of interest to the base station transmitter) and is sent to the base station on the reverse link. This feedback will involve some delay, δ_{lag}.Since wireless channel are time varying we need.

$$\delta_{lag} \ll T_C \qquad (2.23)$$

where T_C is the coherence time. Therefore δ_{lag}=T_C determines channel accuracy at the transmitter. In a fast changing channel, we need more frequent estimation and feedback. The resulting overhead on the reverse channel can be prohibitive.

One approach to reducing the feedback overhead is to send a slow changing statistic of the channel such as the correlation matrices Rt or Rr. Another option can be to feedback only partial channel information such as channel condition number.

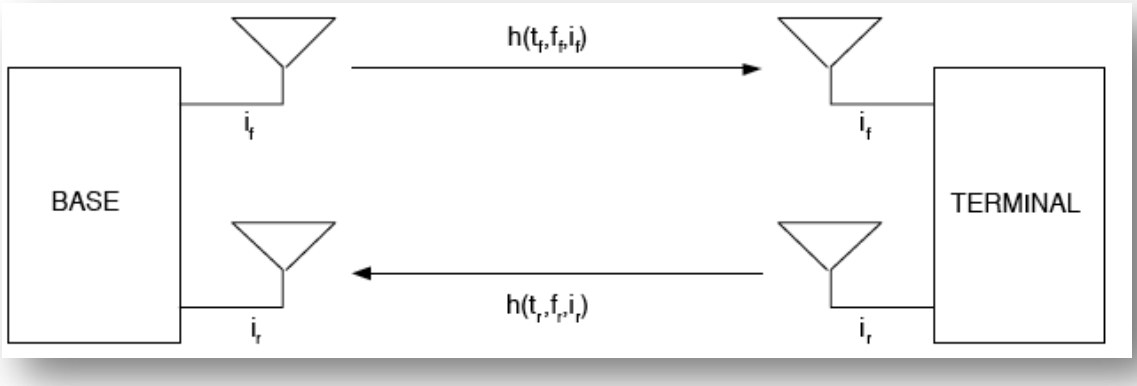

Figure2.5: Channel between Tx-Rx

Channel Estimation at Transmitter Using Reciprocity. Let us first consider a SISO case. Let $h_f(t_f,\ f_f,\ i_f)$ be the forward SISO channel from the base-station transmitter antenna to the terminal and $h_r(t_r,\ f_r,\ i_r)$ be the reverse SISO channel (see figure 2.5).$t_f,\ f_f$andi_f refer to the time, frequency and antenna index used on the forward link. $t_r,\ f_r$and$i_r$are similarly defined for the reverse link. The antenna index specifies the antenna used at the base and the terminal.

The reciprocity principle states that if the time, frequency and antenna for channel use are the same $(t_f = t_r,\ f_f =\ f_r, i_f = i_r)$then the channels in the forward and reverse links are identical, i.e.,

$$h_f(t_f,\ f_f, i_f) = h_r(t_r,\ f_r, i_r) \qquad (2.24)$$

However duplexing schemes support simultaneous two-way links and need to isolate these links to prevent interference. Therefore we need to force some difference in time, or frequency and/or spatial parameters. In turn this causes errors in estimating the base-station transmit (forward) channel from the base station receive (reverse) channel. A few approaches are discussed below. In Time Division Duplexing (TDD), the forward and reverse channels use the frequency and antennas for the duplex links, but use different time slots to communicate. Let $\delta_t = t_f - t_r$ be the duplexing time delay. It follows that the forward and revers channels can be equated only if

$$\delta_t \ll T_C \qquad (2.25)$$

Clearly, the more stringent the requirements of accuracy in channel estimates, the smaller δ_t/T_Cwill need to be.

In Frequency Division Duplexing (FDD), the forward and the reverse channels use the same time and antennas to communicate, but use different frequencies on the links. Let $\delta_f = f_f - f_r$ be the duplexing frequency difference. It follows that the forward and the reverse channel can be equates if

$$\delta_f \ll B_C \qquad (2.26)$$

There will still be a face difference given by $2\pi\delta_f T_{f-r}$, where t is the total travel time. In practice, due to physical limits of duplexing filters that isolate the reverse and forward links, $\delta_f$is about 5% of the operating frequency v_c. This usually means that$\delta_f \gg B_c$.Therefore, the reciprocity principle in general cannot be exploited in FDD for transmit estimation. In Antenna Division Duplexing, the forward and the reverse channel use the same frequency and time, but use different antennas (or beams) on each link to communicate. Let δ_d be the separation (also called duplexing location difference) between the antenna indexed by $i_f$and i_r: It follows that the forward and the reverse channel can be equates if

$$\delta_d \ll D_C \qquad (2.27)$$

where D_C is the coherence distance of the channel. This may be impossible to meet physically when D_C is itself as small as $\lambda_c/2$. When ADD can be applied, a correction will still need to cover array antenna element and geometry differences. Another disadvantage is that ADD does not provide sufficient isolation between the two links and is almost never used directly as duplexing scheme.

Many communication systems use a combination of time/frequency/antenna separation in the duplex links, making the reciprocity infeasible. Only pure TDD offers a realistic opportunity for exploiting reciprocity for channel estimation at the transmitter.However even here there are a number of complications, including lack of reciprocity in thetransmitand receive electronics and so great care must be exercised to arrive ata reliable transmit channel estimates.

If reciprocity is truly applicable, the reverse SIMO channel will be the same as the forward MISO channel. Likewise, the reverse MIMO channel will be the same as the MIMO forward channel.

Reciprocity is a very poor leverage to obtain the transmit channel estimation.

2.7 Capacity of a Deterministic Channel

2.7.1 Capacity of the Frequency Flat Deterministic MIMOChannel

We assume here that the channel has a bandwidth of 1 Hz and is flat in frequencyover this band. Consider a MIMO channel with M_T transmitting antennas and $M_R$receiving antennas. Denoting the $MR \times MT$ channel matrix by **H**, the input-outputrelation for the MIMO channel is, as seen before

$$\mathbf{y} = \sqrt{\frac{E_S}{M_T}}\mathbf{Hs} + \mathbf{n} \qquad (2.28)$$

where **y** is the received signal vector with dimension $M_R \times 1$, **s** is the transmit signal vector of dimension $M_T \times 1$ and **n** is the $MR \times 1$ spatio-temporally white ZMCSCG noise vector with covariance matrix $\mathcal{E}\{\mathbf{nn}^H\} = \mathcal{N}_0\mathbf{I}_{M_R}$and E_S is the total average energy available at the transmitter over a symbol period (T = 1 s).The covariance matrix of **s**,$\boldsymbol{R_{SS}} = \mathcal{E}\{\mathbf{ss}^H\}$must satisfy Tr($\boldsymbol{R_{SS}}$) = M_T in order toconstrain the total average energy transmitted over a symbol period.

In the following, we assume that the channel **H** is known to the receiver, andwe assume that the channel is deterministic. The capacity of the MIMO channel isdefined as

$$C = \max_{f(s)} I(\mathbf{s};\mathbf{y}) \qquad (2.29)$$

where$f(s)$ is the probability distribution of the vector **s** and $I(\mathbf{s};\mathbf{y})$is the mutual information between vector **s** and **y**. Note that

$$I(\mathbf{s};\mathbf{y}) = H(\mathbf{y}) - H(\mathbf{y}\backslash\mathbf{s}) \qquad (2.30)$$

where$H(\mathbf{y})$ is the differential entropy of the vector $\mathbf{y}$, while $H(\mathbf{y}\backslash\mathbf{s})$is the conditional differential entropy of the vector $\mathbf{y}$, given the knowledge of the vector **s**. Since the vector **s** and **n** are independent, $H(\mathbf{y}\backslash\mathbf{s}) = H(\mathbf{n})$and equation 2.30 simplifies to

$$I(\mathbf{s};\mathbf{y}) = H(\mathbf{y}) - H(\mathbf{n}) \qquad (2.31)$$

Maximizing the mutual information $I(\mathbf{s};\mathbf{y})$ reduces to maximizing$H(\mathbf{y})$. The covariance matrix of **y**, $\boldsymbol{R_{yy}} = \mathcal{E}\{\mathbf{yy}^H\}$satisfies

$$\mathbf{R_{yy}} = \frac{E_S}{M_T}\mathbf{HR_{SS}H^H} + \mathcal{N}_0\mathbf{I}_{\mathrm{M_R}}, \qquad (2.32)$$

where$\mathbf{R_{SS}}$is the covariance matrix of **s**. We know that amongst all vectors **y** with a given matrix $\mathbf{R_{yy}}$, the differential entropy $H(\mathbf{y})$is maximized when **y** is ZMCSCG. This in turn implies that **s** must be a ZMCSCG vector, the distribution of which is completely characterized by $\mathbf{R_{SS}}$. The differential entropies of the vector **y** and **n** are given by

$$H(\mathbf{y}) = \log_2\left(det\left(\pi e\mathbf{R_{yy}}\right)\right) bps/Hz \qquad (2.33)$$

$$H(\mathbf{n}) = \log_2\left(det\left(\pi e \mathcal{N}_0 \mathbf{I}_{\mathrm{M_R}}\right)\right) bps/Hz \qquad (2.34)$$

Therefore, $I(\mathbf{s};\mathbf{y})$in Eq. 2.31 reduces to

$$I(\mathbf{s};\mathbf{y}) = \log_2 det\left(\mathbf{I}_{\mathrm{M_R}} + \frac{E_s}{M_T \mathcal{N}_0}\mathbf{H}\mathbf{R}_{\mathbf{SS}}\mathbf{H}^{\mathbf{H}}\right) bps/Hz \qquad (2.35)$$

and it follows from Eq. 2.29 that the capacity of the MIMO channel is given by

$$C = \max_{Tr(\mathbf{R}_{\mathbf{SS}})=M_T} \log_2 det\left(\mathbf{I}_{\mathrm{M_R}} + \frac{E_s}{M_T \mathcal{N}_0}\mathbf{H}\mathbf{R}_{\mathbf{SS}}\mathbf{H}^{\mathbf{H}}\right) bps/Hz \qquad (2.36)$$

The capacity C in Eq. 2.36 is often referred to as the error-free spectral efficiency, or the data rate per unit bandwidth that can be sustained reliably over the MIMO link. Thus given a bandwidth of W Hz, the maximum achievable data rate over this bandwidth using the MIMO channel is WC bps.

2.7.2 Channel Unknown to the Transmitter

If the channel is completely unknown to the transmitter, the vector **s** may be chosen to be statistically non-preferential, i.e., $\mathbf{R}_{\mathbf{SS}} = \mathbf{I}_{\mathrm{M_T}}$**.** This implies that the signal are independent and equi-powered at the transmit antennas. The capacity of the MIMO channel in absence of channel knowledge at the transmitter is given by

$$C = \log_2 det\left(\mathbf{I}_{\mathrm{M_R}} + \frac{E_s}{M_T \mathcal{N}_0}\mathbf{H}\mathbf{H}^{\mathbf{H}}\right) bps/Hz \qquad (2.37)$$

This is not the Shannon capacity in the true sense, since a genie with channel knowledge can choose a signal covariance matrix that outperforms$\mathbf{R}_{\mathbf{SS}} = \mathbf{I}_{\mathrm{M_T}}$. Nevertheless, we shall refer to the expression in Eq. 2.37as the capacity. Given that$\mathbf{H}\mathbf{H}^{\mathbf{H}} = \mathbf{Q}\boldsymbol{\Lambda}\mathbf{Q}^{\mathbf{H}}$ the capacity of the MIMO channel can be expressed as

$$C = \log_2 det\left(\mathbf{I}_{\mathrm{M_R}} + \frac{E_s}{M_T \mathcal{N}_0}\mathbf{Q}\boldsymbol{\Lambda}\mathbf{Q}^{\mathbf{H}}\right) \qquad (2.38)$$

Using the identity $det(\boldsymbol{I}_m + \mathbf{AB}) = det(\boldsymbol{I}_{\boldsymbol{n}} + \mathbf{BA})$and $\mathbf{Q}^{\mathbf{H}}\mathbf{Q} = \mathbf{I}_{M_R}$Eq. 2.38simplifies to

$$C = \log_2 det\left(\mathbf{I}_{\mathrm{M_R}} + \frac{E_s}{M_T \mathcal{N}_0}\boldsymbol{\Lambda}\right) \qquad (2.39)$$

orequivalently

$$C = \sum_{i=1}^{r} \log_2\left(1 + \frac{E_S}{M_T \mathcal{N}_0}\lambda_i\right) \qquad (2.40)$$

where r is the rank of the channel and λ_i(i = 1, 2, …, r) are the positive eigenvalues of $\mathbf{HH^H}$. Equation 2.40 expresses the capacity of the MIMO channel as the sum of the capacities of r SISO channels, each having power gain λ_i(i = 1, 2, …, r) and transmit power Es/M_T .

Hence, the use of multiple antennas at the transmitter and receiver in a wireless link opens multiple scalar spatial data pipes (also known as modes) between transmitter and receiver. We note that in the absence of channel knowledge the individual channel modes are not accessible and that equal transmit energy is allocated to each spatial data pipe.

Orthogonal Channels Maximize Capacity

Given a fixed total channel power transfer, i.e., $\|\boldsymbol{H}\|_F^2 = \sum_{i=1}^{r} \lambda_i = \xi$, what is the nature of the channel **H** that maximizes capacity?

Consider a full rank MIMO channel with $M_T = M_R = M$; so that r = M: The capacity C in Eq. 2.40is concave in the variables λ_i(i = 1, 2, …,r) and is maximized subject to the constraint$\sum_{i=1}^{r} \lambda_i = \xi$, when $\lambda_i = \lambda_j = \xi/M \ (i,j = 1,2,\dots,M)$. Therefore, for the maximum capacity, **H** must be an orthogonal matrix,i.e., $\mathbf{HH^H} = \mathbf{H^H H} = (\xi/\mathrm{M})\mathbf{I}_\mathrm{M}$and the resulting capacity is

$$C = M \log_2\left(1 + \frac{\xi E_S}{\mathcal{N}_0 M^2}\right) \qquad (2.41)$$

Further, if the elements of **H**satisfy $\|H_{i,j}\|^2 = 1$, then $\|\boldsymbol{H}\|_F^2 = M^2$ and

$$C = M \log_2\left(1 + \frac{E_S}{\mathcal{N}_0}\right) \qquad (2.42)$$

The capacity of an orthogonal MIMO channel is therefore M times the scalar channelcapacity.

2.7.3 Channel Known to the Transmitter

So far we have studied the capacity of MIMO channels when the channel is knownperfectly to the receiver and is unknown to the transmitter. As we have seen, equal power allocation across the transmit antenna array is logical under this scenario.We now ask if we can increase channel capacity if the channel is also known to thetransmitter.

Channel knowledge at the transmitter can be maintained via feedback from thereceiver or through the reciprocity principle in a duplex system.

From Eq. 2.40 we conclude that in absence of channel knowledge at the transmitter,

the capacity of the $M_R \times M_T$MIMO channel is equivalent to the capacity of *r* parallelspatial sub-channels, with equal power allocated to each sub-channel. When thechannel is known at both the transmitter and receiver, the individual channel modesmay be accessed through linear processing at the transmitter and receiver.

Consider a ZMCSCG signal vector $\tilde{\mathbf{s}}$of dimension $r \times 1$ where r is the rank of thechannel **H** to be transmitted. The vector is multiplied (see Fig 2.6) by the matrix**V**prior to transmission (recall that$\mathbf{H} = \mathbf{U}\sum\mathbf{V}^{\mathbf{H}}$).

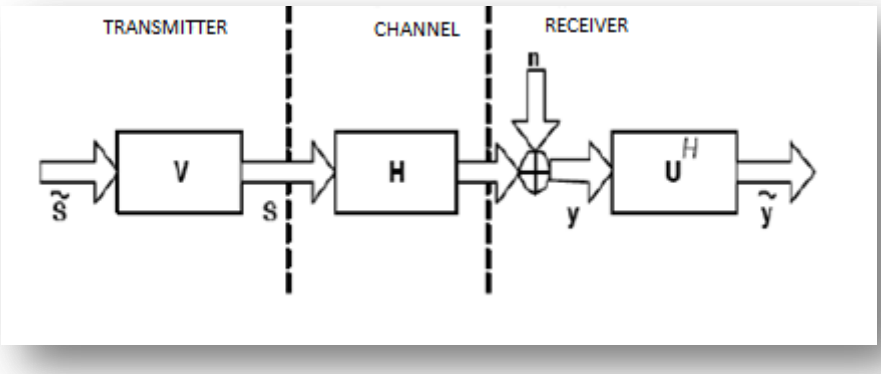

Figure 2.6: Scheme

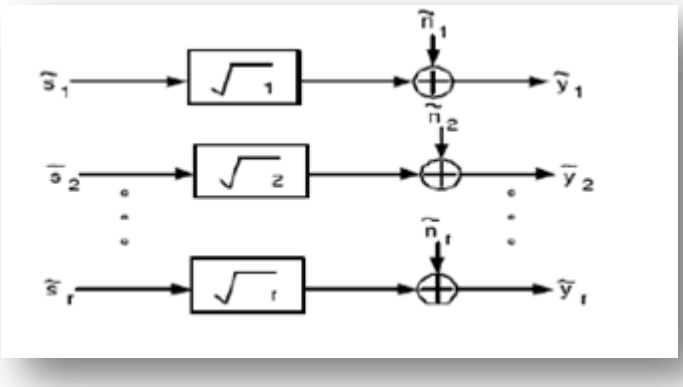

Figure 2.7: Scheme 2

At the receiver, the received signal vector **y** is multiplied by the matrix $\mathbf{U}^{\mathbf{H}}$.the effective input-output relation for this system is given by

$$\tilde{\mathbf{y}} = \sqrt{\frac{E_S}{M_T}}\mathbf{U}^{\mathbf{H}}\mathbf{H}\mathbf{V}\tilde{\mathbf{s}} + \mathbf{U}^{\mathbf{H}}\mathbf{n} = \sqrt{\frac{E_S}{M_T}}\sum\tilde{\mathbf{s}} + \tilde{\mathbf{n}} \quad (2.43)$$

where$\tilde{\mathbf{y}}$ is the transformed received signal vector of dimension $r \times 1$ and $\tilde{\mathbf{n}}$ is theZMCSCG $r \times 1$ transformed noise vector with covariance matrix$\varepsilon\{\tilde{\mathbf{n}}\tilde{\mathbf{n}}^{\mathrm{H}}\} = \mathcal{N}_0\mathbf{I}_{\mathrm{r}}$.The vector$\tilde{\mathbf{s}}$ must satisfy $\varepsilon\{\tilde{\mathbf{s}}^{\mathrm{H}}\tilde{\mathbf{s}}\} = \mathrm{M}_{\mathrm{T}}$to constrain the total transmit energy. Equation 2.43 shows that with channel knowledge at the transmitter, **H** can be explicitly decomposed (see figure 2.7) into r parallel SISO channels satisfying

$$\tilde{y}_i = \sqrt{\frac{E_s}{M_t}}\sqrt{\lambda_i}s_i + n_i, \quad i = 1,2,\dots,r. \qquad (2.44)$$

The capacity of the MIMO channel is the sum of the individual parallel SISO channel capacities given by

$$C = \sum_{i=1}^{r}\log_2(1 + \frac{E_s\gamma_i}{M_T\mathcal{N}_0}\lambda_i) \qquad (2.45)$$

where$\gamma_i = \varepsilon\{|\tilde{s}_i|^2\}$ $(i = 1,2,\dots,r)$reflects the transmit energy in the ithsubchanneland satisfies $\sum_{i=1}^{r}\gamma_i = M_{T.}$

Since the transmitter can access the spatial sub-channel, it can allocate variableenergy across the sub-channel to maximize the mutual information. The mutualinformation maximization problem now becomes

$$c = \max_{\sum_{i=1}^{r}\gamma_i = M_{T.}} \sum_{I=1}^{R}\log_2\left(1 + \frac{E_s\gamma_i}{M_T\mathcal{N}_0}\lambda_i\right) \qquad (2.46)$$

The objective for the maximization is concave in the variables$\gamma_i(i = 1,\dots,r)$and can be maximized using Lagrangian methods. The optimal energy allocationpolicy, ${\gamma_i}^{opt}$, satisfies

$${\gamma_i}^{opt} = \left(\mu - \frac{M_T\mathcal{N}_0}{E_s\gamma_i}\right)_+, i = 1,\dots,r \qquad (2.47)$$

$$\sum_{i=1}^{r}{\gamma_i}^{opt} = M_{T.} \qquad (2.48)$$

whereμ is a constant value and $(x)_+$implies

$$(x)_+ = \begin{cases} x & if \quad x \geq 0 \\ 0 & if \quad x < 0 \end{cases} \qquad (2.49)$$

The optimal energy is found iteratively through the “waterfilling algorithm”, briefly described below.

Waterfilling Algorithm

Setting the iteration count p to 1, we first calculate the constant μin Eq. 2.48:

$$\mu = \frac{M_T}{(r-p+1)}\left[1 + \frac{\mathcal{N}_0}{E_s}\sum_{i=1}^{r-p+1}\frac{1}{\lambda_i}\right] \qquad (2.50)$$

Using the value of μ found above, the power allocated to the ith sub-channel can be calculating using

$$\gamma_i = \left(\mu - \frac{M_T\mathcal{N}_0}{E_s\lambda_i}\right), \quad i = 1,2,\dots,r-p+1 \qquad (2.51)$$

If the energy allocated to the channel with the lowest gain is negative, i.e.,$\gamma_{r-p+1} < 0$, we discard this channel by setting$\gamma^{opt}{}_{r-p+1} = 0$ and return the algorithmwith the iteration count p increased by 1. The optimal waterfilling power allocationstrategy is found when power allocated to each spatial sub-channel is non-negative.Fig. 2.8 illustrates the described algorithm.

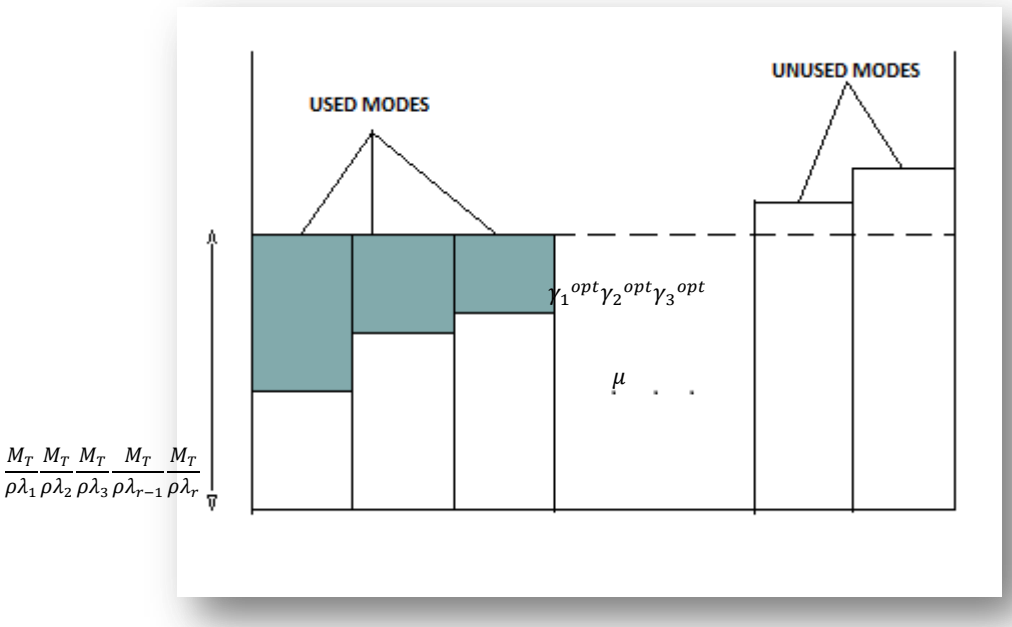

Figure 2.8: Waterfilling power allocation

The capacity of the MIMO channel when the channel is known to the transmitter is necessarily great than (or equal to) the capacity when the channel is unknown tothe transmitter.

Optimal Rss

Once the optimal power allocation across the spatial sub-channel isdetermined, we can determinate the optimal $\mathbf{Rss}$ sought in Eq. 2.36. Noting fromFig. 2.6 that

$$\mathbf{s} = \mathbf{V}\tilde{\mathbf{s}} (2.52)$$

the optimal covariance matrix Rss opt is given by

$$\mathbf{R}_{\mathbf{ss}}^{\mathrm{opt}} = \mathbf{V}\mathbf{R}_{\tilde{\mathbf{s}}\tilde{\mathbf{s}}}^{\mathrm{opt}}\mathbf{V}^{\mathbf{H}} (2.53)$$

where$\mathbf{R}_{\tilde{\mathbf{s}}\tilde{\mathbf{s}}}^{\mathrm{opt}}$ is an $r \times r$ diagonal matrix (since the elements$\tilde{\mathbf{s}}$ are independent) given by

$$\mathbf{R}_{\tilde{\mathbf{s}}\tilde{\mathbf{s}}}^{\mathrm{opt}} = diag\{\gamma_1^{opt}, \gamma_2^{opt}, \dots, \gamma_r^{opt}\} \qquad (2.54)$$

Referring back to Fig. 2.7, we can maximize capacity when we allocate power in each mode according to $\mathbf{R}_{\tilde{\mathbf{s}}\tilde{\mathbf{s}}}^{\mathrm{opt}}$**.**

2.8 Influence of Fading on MIMO Capacity

In the following we assume that the channel is perfectly known to the receiver andis unknown to the transmitter.

2.8.1 Effect of the Spatial Fading Correlation

As seen before, the effect of spatial fading correlation for a Rayleigh flat fadingchannel is to makes The MIMO channel matrix **H** as

$$\mathbf{H} = \mathbf{R}_{\mathrm{r}}^{1/2}\mathbf{H}_{\mathrm{w}}\mathbf{R}_{\mathrm{t}}^{1/2} \quad (2.55)$$

where the matrices $\boldsymbol{R}_r$ and $\boldsymbol{R}_t$ are positive definite Hermitian matrices that specitythe receive and transmit correlations respectively. Furthermore, $\boldsymbol{R}_r$ and $\boldsymbol{R}_t$ are normalized so that $[\boldsymbol{R}_r]_{i,i} = 1 \quad (i = 1,2, \dots, M_R)$ and t $[\boldsymbol{R}_t]_{j,j} = 1 \quad (j = 1,2, \dots, M_T)$ resulting in $\varepsilon\left\{\left|h_{i,j}\right|^2\right\} = 1$. The capacity of the MIMO

channel in the presence ofthe spatial fading correlation without channel knowledge at the transmitter followsthe simple substitution.

$$C = \log_2 det\left(\mathbf{I}_{M_R} + \frac{\rho}{M_T}\right)\mathbf{R}_{\mathrm{r}}^{1/2}\mathbf{H}_{\mathrm{w}}\boldsymbol{R_t}\mathbf{H}_{\mathrm{w}}{}^{\boldsymbol{H}}\mathbf{R}_{\mathrm{r}}^{1/2}(2.56)$$

Assume that $M_R = M_T = M$ and the receive and transmit correlation matrices, $\boldsymbol{R_r}$and $\boldsymbol{R_t}$, are full rank. At high SNR the capacity of the MIMO channel can bewritten as

$$C \approx \log_2 det\left(\frac{\rho}{M_T}\mathbf{H}_{\mathrm{w}}\mathbf{H}_{\mathrm{w}}{}^{\boldsymbol{H}}\right) + \log_2 det(\boldsymbol{R_r}) + \log_2 det(\boldsymbol{R_t}) \qquad (2.57)$$

From Eq. 2.57 it is clear that $\boldsymbol{R}_r$ and $\boldsymbol{R}_t$have the same impact on the capacityof the MIMO channel. We now examine the conditions on $\boldsymbol{R}_r$($\boldsymbol{R}_t$ will be similar)that maximize the capacity. The eigenvalues of $\boldsymbol{R}_{r,}$ $\lambda_i(\boldsymbol{R}_r)(i = 1,2, \dots, M)$ are constrained such that $\sum_{i=1}^{M}\lambda_i(\boldsymbol{R}_r) = M$. The arithmetic mean-geometric meaninequality implies

$$\prod_{i=1}^{M}\lambda_i(\boldsymbol{R}_r) \leq \mathbf{1}\ (2.58)$$

However,$\det(\boldsymbol{R}_r) = \prod_{i=1}^{M}\lambda_i(\boldsymbol{R}_r)$.This implies that $\log_2 \det(\boldsymbol{R}_r) \leq 0$, and is zeroonly if all eigenvalues of $\boldsymbol{R}_r$ are equal, i.e.,$\boldsymbol{R}_r = \mathbf{I}_M$. Hence, we can conclude thatfading signal correlation is detrimental to MIMO capacity and that the loss in ergodicor outage capacity at high SNR is given by$(\log_2 \det(\boldsymbol{R}_r) + \log_2 \det(\boldsymbol{R}_t))\ bps/Hz$.

2.8.2 Effect of the LOS Component

As we seen before, the MIMO channel in presence of Ricean fading component canbe modelled as the sum of a fixed (LOS) matrix and a fading matrix as follows:

$$\mathbf{H} = \sqrt{\frac{K}{1+K}}\bar{\mathbf{H}} + \sqrt{\frac{1}{1+K}}\mathbf{H}_w, \qquad (2.59)$$

where$\sqrt{\frac{K}{1+K}}\bar{\mathbf{H}} = \varepsilon\{\mathbf{H}\}$ is the fixed component of the channel and$\sqrt{\frac{1}{1+K}}\mathbf{H}_w$is the fading component of the channel. $K$is the Ricean factor of the channel. $\mathbf{H}_w$dominates channel behaviour for low values of K, while $\mathbf{H}$ dominates system behaviorwith an increase degree of Ricean fading, in the presence of the Ricean fading, theergodic capacity became a function of the K-factor.

2.9 MIMO Multiuser

2.9.1 Introduction

Another approach in ST wireless is to deploy multiple antennas at the base to supportmultiple users with one or more antennas per user terminal (see Fig. 2.9). Assuminga single antenna per user, the forward link from a base to the users is a vectorbroadcast channel and the reverse link is a vector multiple access channel. Withmultiple antenna terminals, we get the corresponding matrix channels. We refer tothis class of channel as MIMO-MU. The single user case is referred to as MIMO-SU (single user) to differentiate it from the multiuser case.

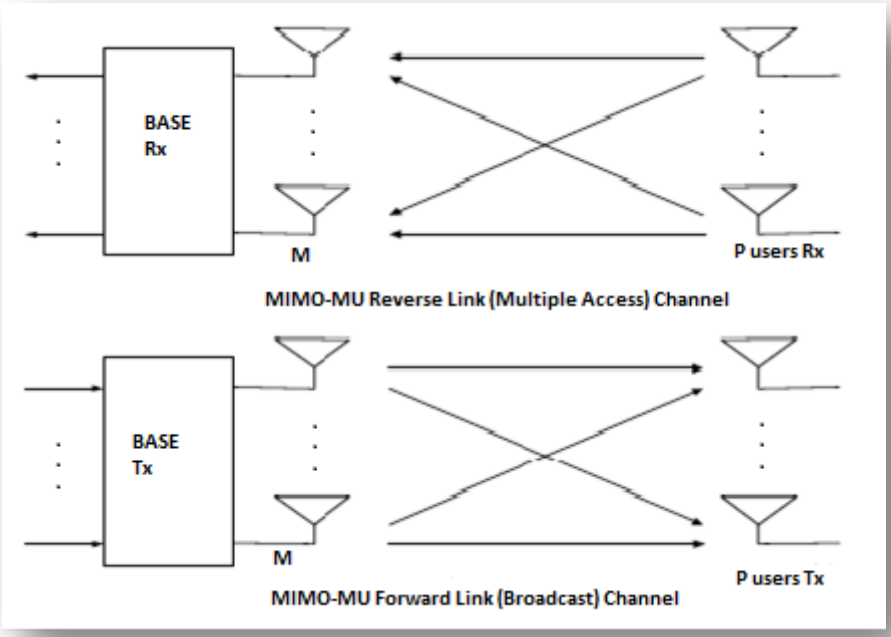

Figure 2.9: MIMO multiuser scheme

The base-station communicates with the multiple users simultaneously in the samefrequency channel by exploiting differences in spatial signatures at the base-antennaarray induced by spatially dispersed users. This technique is also known as SDMA. The value of SDMA in wireless is not much because of its multiple access capability,but rather that it allows channel reuse within a cell to increase spectral efficiency.Another view of MIMO-MU is that it extends the usual scalar (SISO) multiuserchannel to vector (SIMO, MISO) or matrix (MIMO) multiuser channels.

MIMO-MU has been used in satellite communication, where a frequency channelis reused in angle at the satellite using beamforming. The users located in the groundhave LOS paths to the satellite that are completely free of scattering and hence havezero angle spread. The satellite employs beams

instead of cells in a cluster formatwith frequency reuse between clusters. Cluster size and side lobe levels determineco-channel interference.

In the terrestrial cellular system MIMO-MU implies reuse within the sector (orcell). This is more complicated due to scattering in such environments. Wavefrontsmay have large angle spreads and therefore random channels or signatures. Thereforeeven well-separated users nay have potentially overlapping channels. Also, usersmay have identical spatial channels at the base-station if their signal are scatteredby the same dominant scatter making separability hard to guarantee. With SSmodulation (CDMA), the problem of guaranteeing spatial channel separability isgreatly mitigated since users have quasi or fully orthogonal temporal spreading codes.

Here we assume only single antenna terminals and that the full channel is known tothe base and to all users. Because there are distributed users, obtaining completechannel knowledge at the transmitters is even more complicated than that describedfor the single user case. We refer to the forward link MIMO-MU channel as theMIMO broadcast channel (MIMO-BC) and the reverse link MIMO-MU channel asthe MIMO multiple access channel (MIMO-MAC)

2.9.2 MIMO MAC

2.9.2.1 Signal Model

Consider a system with M antennas at the base-station and P users, each equippedwith one antenna. The model can be extended to multiple antennas at each user,but that is not attempted here. Assuming a frequency flat channel, the channelbetween the ith$(i = 1,2, \dots, P)$ user and the base-station is given by a complexGaussian M _1 vector, $\mathbf{h}_\mathrm{i}$. Assume s_i is a complex data symbol transmitted by theith user with average energy$\varepsilon\{|s_i|^2\} = E_{s,i}$ $(i = 1,2, \dots, P)$. Note that $E_{s,i}$ ingeneral will not be the same for each user since each user will employ power controlto compensate for differences in path loss.

The signal received at the base-station is an$M \times 1$ vector, **y**, given by

$$\mathbf{y} = \sum_{i=1}^{P} \mathbf{h}_\mathrm{i} s_i + \mathbf{n} = \mathbf{H}s + \mathbf{n}, \qquad (2.60)$$

where$s$is a $P \times 1$ vector, $\mathbf{H}$is an$M \times P$ matrix and **n** is the $M \times 1$ ZMCSCG spatially white noise vector with covariancematrix $\mathcal{N}_0 \mathbf{I}_m$. Note that the element of **H** has unit power. Further, we observe that$M$ must be equal to or greater than P to obtain acceptable spatial separability ofthe users. Assuming that the user signals are uncorrelated, the covariance matrix of the vector $\mathbf{s}$, $\mathbf{R_{ss}}$becomes

$$\mathbf{R_{ss}} = diag\{E_{s,1}, E_{s,2}, \dots, E_{s.P}\} \qquad (2.61),$$

The reverse link channel is a multiple access channel. The data rate than can bereliably maintained by all users simultaneously is characterized by a capacity region.In the following, we

consider a deterministic problem and consider a sample realizationof the channel **H** and assume that it is perfectly known to the receiver (i.e., atthe base-station). What makes this problem different from that in MIMO-SU is thatco-ordinated encoding is not allowed at the transmitters which are geographicallydispersed.

2.9.2.2 Capacity Region

We study the capacity region for two different receiver decoding strategies at the base-station, joint decoding and independent decoding. Joint decoding impliesthat the signals are decoded in a co-operative fashion, while independent decodingassumes that the signals are decoded independently in parallel.

Joint Decoding

Joint decoding implies that the signals are detected optimally atthe receiver via ML detection. Let $\mathcal{T}$ be a sub-set of the set $\{1,2,\ldots,P\}$and$\mathcal{T}'$ represent its complement. We denote the covariance matrix of the signals transmittedfrom the terminals indexed by $\mathcal{T}$ by $\mathbf{R_{ss}}$ and the corresponding $M \times c(\mathcal{T})$ channelmatrix by $\mathbf{H}_{\mathcal{T}}(c(\mathcal{T})$is the cardinality of the set$\mathcal{T}$). Representing the rate thatcan be reliably (error free) maintained for the ith user by $R_i(i = 1,2,\ldots,P)$(inbps/Hz) and assuming Gaussian signalling for each user, the capacity region has beenshown to satisfy

$$\sum_{k\in\mathcal{T}} R_k \leq \log_2 \det\left(\mathbf{I}_M + \frac{1}{\mathcal{N}_0}\boldsymbol{H}_{\mathcal{T}}\boldsymbol{R}_{\boldsymbol{ss},\mathcal{T}}\boldsymbol{H}_{\mathcal{T}}{}^H\right) bps/Hz \qquad (2.62)$$

for all 2^P –1 possible non-empty sub-test $\mathcal{T}$ of the set$\{1,2,\ldots,P\}$. For example,the capacity region for a two-user system (P = 2) satisfies the following inequalities:

$$R_1 \leq \log_2\left(1 + \frac{E_{s,1}}{\mathcal{N}_0}\|\mathbf{h}_1\|_F^2\right) \qquad (2.63)$$

$$R_2 \leq \log_2\left(1 + \frac{E_{s,2}}{\mathcal{N}_0}\|\mathbf{h}_2\|_F^2\right) \qquad (2.64)$$

$$R_1 + R_2 \leq \log_2\left(\mathbf{I}_2 + \frac{E_{s,1}}{\mathcal{N}_0}\mathbf{h}_1\mathbf{h}_1^H + \frac{E_{s,2}}{\mathcal{N}_0}\mathbf{h}_2\mathbf{h}_2^H\right) \qquad (2.65)$$

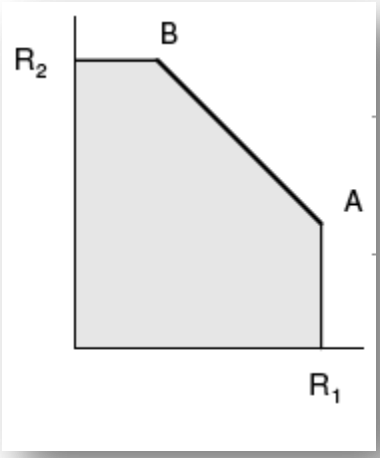

Figure 2.10: Capacity Region

The rate region is shown in Fig. 2.10. Along the bold line the sum-rate R1 + R2 isconstant and is the maximum achievable sum-rate, C_{MC}.Every point along this line is achieved by each user transmitting at the maximumavailable power. To achieve the lower corner point A, user 1 builds Gaussian codewordsat full rate $R_1 = \log_2\left(1 + \left(E_{s,1}/\mathcal{N}_0\right)\|\mathbf{h}_1\|_F^2\right)$, thus assuming no interference.User 2 builds codewords assuming that the signal from user 1 is additional noise. The upper corner point B may be achieved in a similar fashion, with user 1 designingcodewords treating user 2 as additional noise and user 2 designing codewords withfull rate $R_2 = \log_2\left(1 + \left(E_{s,2}/\mathcal{N}_0\right)\|\mathbf{h}_2\|_F^2\right)$. All other points along the bold line canbe achieved by time-sharing between the two schemes. The capacity region for morethan two users will, in general, be polyhedral.

We note that while ML decoding is optional, the multiuser reverse link sum-ratecapacity, C_{MC}, given by Eq. 2.62 can also be achieved via a MMSE receiver withsuccessive cancellation. We summarize the proof below.

For clarity assume that all users have the same average energy at the transmitter.Then the sum rate may be expressed as

$$\sum_{k=1}^{P} R_k = \log_2 det\left(\mathbf{I}_M + \frac{E_{s,i}}{\mathcal{N}_0}\mathbf{H}\mathbf{H}^H\right) = \sum_{k=1}^{P} \log_2\left(1 + \frac{E_{s,i}}{\mathcal{N}_0}\mathbf{h}_k^H\left(\mathbf{I}_M + \frac{E_{s,i}}{\mathcal{N}_0}\mathbf{H}_{(k)}\mathbf{H}_{(k)}^H\right)^{-1}\mathbf{h}_k\right) \quad (2.66)$$

$\mathbf{H}_{(k)}$is the channel matrix obtained by removing users (columns) with indices k,k+1,…,P. Consider the term corresponding tok = P. It is easily verified that thisterm corresponds to a capacity obtained by extracting the Pth user through MMSEfiltering. If the user signal at a rate, R_P, less than or equal to this capacity, thesignal can be decoded without any error and then subtracted from the receivedsignal. The effective channel reduces to an $M \times (P-1)$ matrix, $\mathbf{H}_{(p)}$, correspondingto the remaining $P-1$ users. The $(P-1)$th user (with a capacity corresponding tothe term indexed by= $P-1$) may now be similarly decoded and subtracted fromthe received signal. This procedure is repeated until all users' signals are extractedwithout error. Note that for this procedure to work,

first a decoding order has to bedecided upon and then the users must signal with the correct rate assignments specificto that order. Each such ordering corresponds to one maximum sum-rate achievingvertex of the polyhedral capacity region. Since there are $P!$ possible orderings of theusers, there are a corresponding number of vertices. Other rate assignments may beobtained through a convex combination (time-sharing) of these vertices.

Independent Decoding

Recall that independent decoding attempts to recovereach user's signal treating all other signal as interfering noise. The received signalcovariance matrix, $\mathbf{R}_{yy}$, is given by

$$\mathbf{R}_{yy} = \mathbf{H}\mathbf{R}_{yy}\mathbf{H}^H + \mathcal{N}_0\mathbf{I}_M \qquad (2.67)$$

The capacity region for independent decoding is the set of all rates satisfying

$$R_i \leq \log_2\left(\frac{det(\mathbf{R}_{yy})}{det(\mathbf{R}_{yy} - E_{s,i}\boldsymbol{h}_i\mathbf{h}_i^H)}\right), \quad i = 1,2,..,P \qquad (2.68)$$

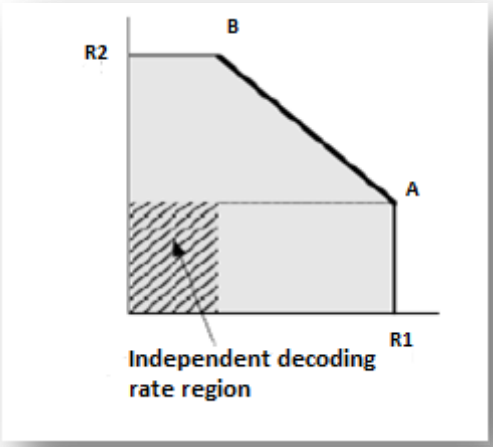

Figure 2.11: Independent decoding rate region

The maximum rate for each user is achieved via MMSE reception for each user. Thecapacity region for independent decoding relative to the joint decoding region fortwo users is shown in Fig. 2.11. Note that the MMSE decoding maximum rates arefound by projecting the corner points A and B back on to the axes. For more thantwo users the capacity region will, in general, be a cuboid.

Discussion

Focusing on the two-user scenario, we see that the capacity regiondepends strongly on the geometry of $\mathbf{h}_1$ relative to $\mathbf{h}_2$and the power available to the individual users. Note that when $\mathbf{h}_1$ is orthogonal to $\mathbf{h}_2$, the two decoding schemes (joint and independent) have equal and square capacity regions. This is so since thesignals transmitted by the users can be perfectly separated and do not appear asinterference to each other. At the other extreme, the smallest capacity region

occurswhen $\mathbf{h}_1$ is parallel to $\mathbf{h}_2$, as the two users cannot be spatially separated. Typically,with random channels the spatial separability of the users will improve as the numberof base-station antennas M increases.

In a random fading channel, the capacity region is also random and given sum-rate can be sustained only with a certain level of reliability. Even in this case, jointdecoding outperforms independent decoding at all outage levels. Also, the maximumsum-rate achieved at any outage level increases with as increase in the number ofbase-station antennas. Further, we note that the difference in maximum sum-rateachieved by the two schemes decreases in the number of base-station antennas. Thiscan be attributed to better separability (orthogonally) of the spatial signatures withincreasing M.

So far, we have discussed the sum-rate that can be achieved when the channel isknown perfectly to the transmitter. In order to achieve a certain point in the capacityregion, coordination between the users is necessary. This can be accomplished if allusers are aware of the channel H and transmit at rates according to a pre-determinedstrategy. Alternatively, the base-station can determine and notify each user of thecorrect transmission rate.

The capacity region of MIMO-MAC for the case when the number of antenna at the users is greater than 1 is a convex hull of the pentagonal regions obtained bychoosing different transmit signal covariance matrices $\mathbf{R}_{s_i s_i}$ with power constraints$Tr\left[\mathbf{R}_{s_i s_i}\right] = E_{s,i}$. The boundary of the region is generally curved, except at the sumpoint where it is a straight line. Each point on the boundary is achievable witha different set of optional covariance matrices $\mathbf{R}_{s_i s_i}^{opt}$ and is the corner point of thecorresponding pentagonal region.

Like in the single antenna discussion, we need to decode users in an ordered mannercorresponding to the operating point on the rate region. The optimal covariancefor the sum rate is obtained by solving a convex optimization problem. Thisleads to a solution in which each user waterfills to his own channel with an effectivenoise equal to the additive noise and the interference from the other $P-1$ users.

2.9.3 MIMO-BC

2.9.3.1 Signal Model

Once again, we assume a frequency flat channel. Let signals si$(i = 1,2, \dots, P)$with average energy $E_{s,i}$be the signals transmitted from the base-station to the$P$ users. The total average power (energy per symbol period) is constrained by$\sum_{i=1}^{P} E_{s,i} = E_s$. We assume the base-station has perfect knowledge of the forwardlink channel $\mathbf{H}$. The signals travel over different vector channels to each of the P users. This is clearly a broadcast channel. Denoting the signal received at the ithterminal by y_i, the forward link signal model is given by

$$\mathbf{y} = \mathbf{Hs} + \mathbf{n} \quad (2.69)$$

where $\mathbf{y} = [y_1 y_2 \cdots y_P]^T$ is a $P \times 1$ vector, $\mathbf{H}$ is the $P \times P$ forward link channel(including prefiltering) matrix, $\mathbf{s} = [s_1 s_2 \cdots s_P]^T$ is a $P \times 1$ vector containing thesignals transmitted at the antennas and $\mathbf{n} = [n_1 n_2 \cdots n_P]^T$is the $P \times 1$ additiveZMCSCG noise vector with variance $\mathcal{N}_0$ in each dimension. Again, the elements of$\mathbf{H}$ are not normalized to unit average power since they include a different path lossand shadow loss for each user. What differentiates this problem from MIMO-SU isthat co-ordinated decoding is not allowed at the receivers whish are geographicallydispersed.

2.9.3.2 Forward Link Capacity

The MIMO-BC channel in general belongs to the class of non-degraded Gaussianbroadcast channels. The capacity region for such a channel remains an unsolvedproblem.

Furthermore, a duality between the achievable rate region and the multiple accesscapacity region that simplifies computation of the achievable rate region has beendemonstrated.

2.9.4 Outage Performance of MIMO-MU

MIMO-MU is in theory an attractive approach to increasing spectral efficiency inwireless links, particularly since the users need to have only one antenna each. However,MIMO-MU with non-spread modulation has a number of problems that canmake its implementation difficult. First, in random fading channels, user separabilitycannot be guaranteed since two user channels may become close and this will becomea source of outage or link failure beyond the usual problems in wireless system causedby fading and interference. Another problem is the near-far problem. Perhaps themost difficult issue is the need for accurate channel knowledge at the transmitter inthe forward link. This fundamental requirement is hard to satisfy, as pointed outbefore. The above problems have so far blocked the deployment of MIMO-MU inpractical system for non-spread modulation.

The performance of MIMO-BC degrades rapidly with the channel estimationerror.

Chapter 3: Information Secrecy and Cryptography

As introduced in the second chapter, wireless ad-hoc networks are at risk, from a security point of view. The wireless links between nodes are highly susceptible to passive eavesdropping, active interfering, leaking secret information, message distortion, denial of service and so on. We saw that the key requirements for the networks are confidentiality, authentication, integrity, non-repudiation and availability.

Ad hoc networks do not have a centralized controller such as a base station, which could lead to a single point of failure and, thus, make the network that much more vulnerable. On the flipside, however, the lack of support infrastructure leads to prevention of application of standard techniques to secure the network. This gives rise to the need for new schemes to ensure the network security.

3.1 Cryptography Basis

A security mechanism follows three steps — identification, authentication, and authorization — to control access to resources. Identification names entities. Authentication checks that an entity is who or what it claims to be. Authorization Esther grants or refuses access rights based on some security policies, which are a part of an organization policy. Policies define access control rules and translate the trust that we place on entities into access control decisions.

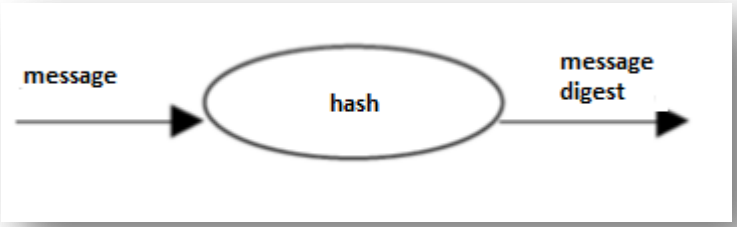

Figure 3.1: Hash function uses no key

Security systems for information processing are used to protect information against unauthorized access, passive access like eavesdropping, or active access like modification of the information. Protocols and cryptographic systems are among the main components of such security systems. Protocols define how system components are to be used; cryptographic systems achieve information hiding.

Preventive security controls are often protocols that utilize cryptography. Cryptographic algorithms are functions that transform information to conceal it. There are three types of cryptographic algorithms:

hash, secret-key cryptography, and public-key cryptography. Hash algorithms do not use keys. Secret-key cryptography uses one key. Public-key cryptography uses two keys.

A hash algorithm is a one-way function that maps a message of any size into afixed size digest (see Fig. 3.1).

Message digests are fingerprints of messages. A hash function is considered secure if it is computationally infeasible to find a corresponding message given a fingerprint, or to find one message that has the same fingerprint as a given message, or to find two arbitrary messages that have the same fingerprint.

Secret-key cryptography makes use of a pair of functions: encryption and decryption (see Fig. 3.2). The encryption function uses a key to mangle a message.

The message before encryption is called plaintext. The encrypted message is called cipher text. The decryption function uses the same key to unmangle the cipher text. The key is a shared secret between communicating entities. Secret-key encryption provides confidentiality, as only those entities knowing the secret can uncover the plaintext messages.

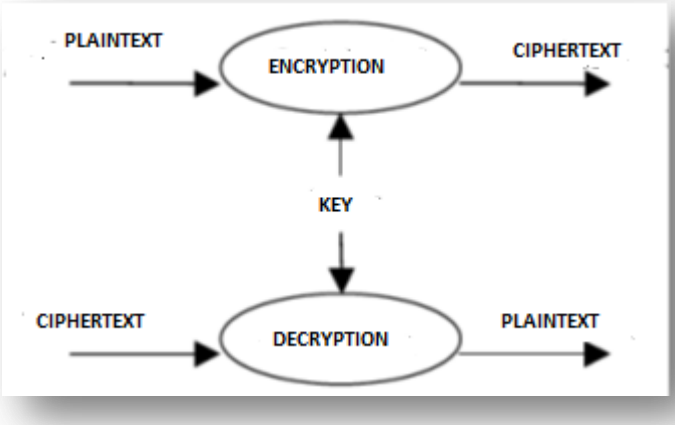

Figure 3.2: Secret-key cryptography uses one key

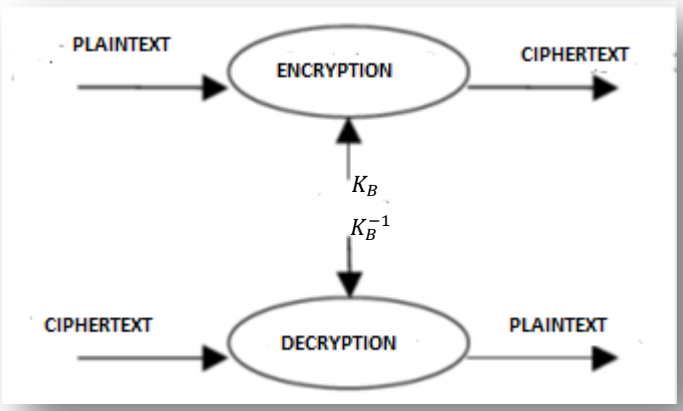

Figure 3.3: Public-key encryption uses a key pair K_B andK_B^{-1}.

Public-key cryptography uses a pair of keys, a public key and a private key, whichare uniquely associated with each other (see Fig. 3.3). Each entity has a key pair,$\langle K_E, K_E^{-1}\rangle$, where K_E is the public key of entity E, and $K_E^{-1}$is E's private key. The private key is only known to the owner, while the public key is widely publicized. Public key encryption uses a public key for encryption and a private key for decryption. To send Bob a message that only Bob can read, Alice uses Bob's public key,K_B, to encrypt the message. Bob uses his private key, K_B^{-1}, to decrypt the cipher text.

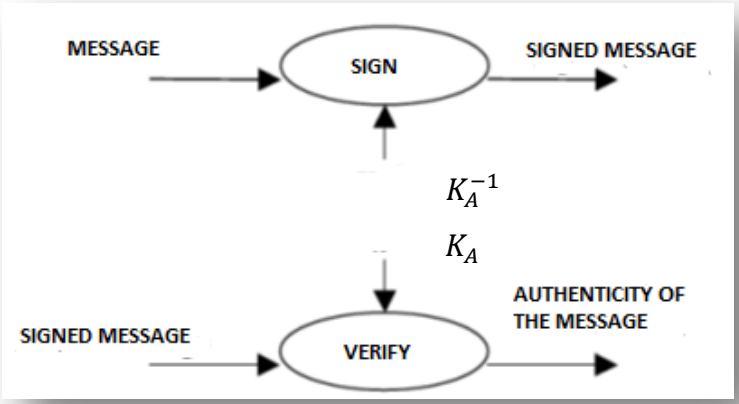

Figure 3.4: Public-key digital signature

Public-key cryptography can also generate digital signatures that can be verified by an arbitrator (see Fig. 3.4). A digital signature binds a signature with an entity and a message. Alice signs a message using her private key, K_A^{-1}. An arbitrator can verify the signature using Alice's public key K_A,.

Public-key encryption provides confidentiality because a private key is only knownto the key owner. Public-key signature provides authentication, integrity, and non-repudiation because of the binding of a

message, a signature, and the private key that was used to generate the signature. In practice, we sign a digest of a message instead of the message itself, which takes less processing time because of the reduced size.

A comprehensive solution to communication security includes protocols, algorithms, and key management. The breakdown of any of these components compromises security.

After a briefly description of the cryptography it follows a mathematical definitionof it.

3.2 Cryptography: Mathematical Definition

The first general formal analysis of cryptographic systems was developed by Shannon [38]. Shannon's model is based on probability theoretic and information theoretic considerations. The present discussion is intended to be a continuation of this very basic work towards a rigorous mathematical foundation of cryptography.

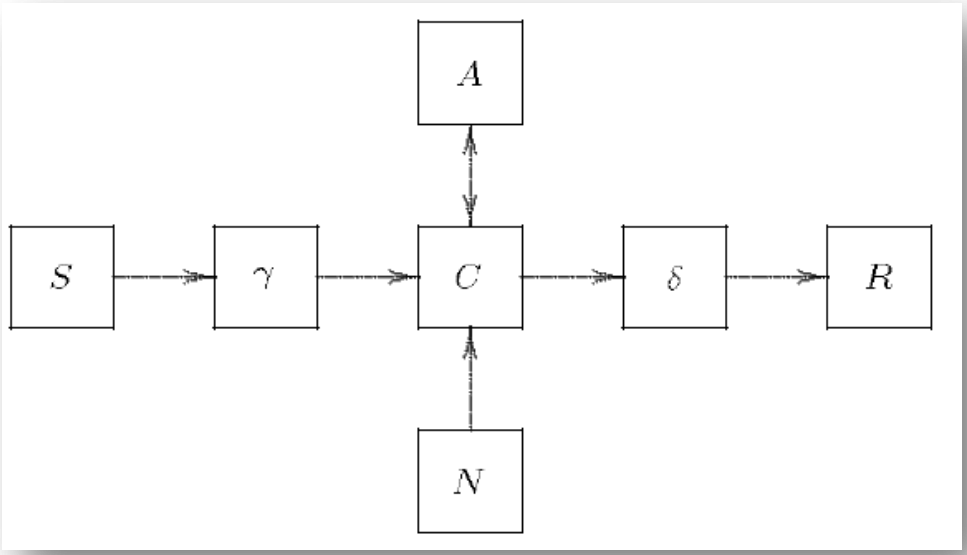

Figure 3.5: The information processing and transmission scheme

3.2.1 System Model

In the following discussion we assume the well-known model of information transmission consisting of a source Ssending information to a receiver R via a channel C as illustrated in Fig. 3.5.

Before actual transmission, the information is encoded using an encoder and, before reception, it is decoded using adecoder δ. During transmission, the encoged information may undergo changes due to

faults in the channel or environmental conditions; such faults are modelled by a source N of noise. Moreover, the information may be overheard or even altered during transmission by a hostile participant, the adversary A. In this model, S and R may be distinct physical entities, and C may represent any kind of physical channel. We consider only discrete channels which operate in discrete time steps and which use discrete signals.

The purposes of the encoding γ and the decoding δinclude the following:

• translation between the alphabets used by $S, C,$ and R;
• reduction of the effect of noise on C;
• adaptation of the information rates at which S, C, and R operate;
• information compression;
• information security.

Here only the aspect of information security is considered, especially that of secrecy.

3.2.2 Perfect Secrecy

Intuitively, a system should be deemed to achieve perfect secrecy if it is impossible for the adversary to gain unauthorized access to the information being transmitted.

This is the motivation for Shannon's definition of perfect secrecy: a system achieves perfect secrecy if the a posteriori message probabilities are the same as the a priori message probabilities, that is, if by receiving the encoded message, the cryptogram, the adversary learns nothing about the message.

It seems natural to require that any definition S of perfect secrecy should have to satisfy the following two conditions:

1. No system with any cryptographic weaknesses should be said to achieve perfect secrecy according to S.
2. If a system is cryptographically unbreakable then it should be said to achieve perfect secrecy according to S.

There is a problem with the Shannon's definition of perfect secrecy and the two conditions expressed above. There are some cryptographic systems, which makes use of the key to encrypt the message that does not exclude the usage of so-called weak keys. A key is weak, if cryptograms obtained with it can be read by the adversary comparatively easily. For example, a key that happens to leave messages largely unchanged should be considered weak. These systems satisfy the Shannon's definition so they achieve perfect secrecy in that sense, but they violate the two conditions expressed above. So the problem with Shannon's definition of perfect secrecy is that cryptographic systems with weaknesses can be proven to achieve perfect secrecy in that sense.

As a consequence of these considerations, we examine whether it is possible at all to arrive at a cryptographically acceptable rigorous definition of perfect secrecy.We show evidence that allows us to argue that such a definition may not be possible.

3.3 Security Issues in Ad Hoc Networks

Security requirements in ad hoc networks do not differ dramatically from their wired network counterparts. Traditional security mechanisms still play a role in achieving ad hoc networks security. However, the context to achieve security goals is different. Changes in network topology and membership occur rapidly in this new context.

Consequently, some issues that are only of concern to high-assurance applications in wired networks are now essential to general ad hoc network applications. In wired networks we assume the following are in place:

1.Availability of routing service, which implies knowledge of network topology and membership;

2. Availability of supporting services, such as naming and key distribution, through central, static system control;

3. Security policy for networks and systems.

Security policies (i.e., access control policies) are embedded in the networked nodes and protocols as prevention and detection mechanisms. Prevention mechanisms include identification,authentication, authorization and firewall.

We can say that traditionally the security is a higher network layer service, but encryption can be complex and difficult without infrastructure. From this point was born the need to implement another way to perform security, directly in the cover layer of the structure. Information theoretic security characterizes the fundamental ability of the physical layer to provide security.

Chapter 4: Numerical Results

4.1 Introduction

Security and privacy protection is one of the most important issues in wireless communications due to the broadcast nature of wireless channels; anyone is able to listen to the transmission in the air and could possibly extract information. Apart from traditional cryptography, security mechanisms, information-theoretic-based security techniques have gained increasing attention in recent years.

[2]Wyner, who developed the concept of “wire-tap channel”, shown in fig.4.1, introduced information-theoretic approach. It is a form of degraded broadcast channel, with the novel difference that one information rate is to be maximized and the other minimized. The objective is to maximize the rate of reliable communication from the source to the legitimate receiver, subject to the constraint that the wire-tapper learns as little as possible about the source output. The objective is the same as in classic cryptography but the technique used to archived privacy is very different. Wyner showed that if a wire-tap channel satisfies certain degradedness conditions, perfectly secure communication with non-zero rate between the transmitter and the intended receiver is achievable. Meanwhile the eavesdropper learns nothing about secret messages from its observations. The maximum rate of secrecy information from the transmitter to the intended receiver is called secrecy capacity.

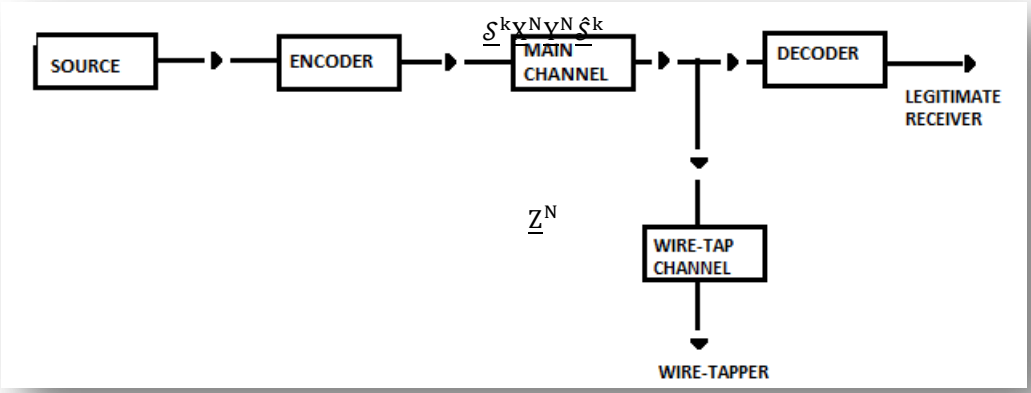

Fig. 4.1: General wire-tap channel

The cooperation between transmitter and receiver put in a disadvantage position to the eavesdropper, the most common is to use a cipher to encrypt each data stream transmitted and later deciphered at the receiver using a private shared key, this kind of transmission based on traditional cryptography it’s shown on the previous chapter.

Spread-spectrum Information hiding is another common way of cooperation between transmitter and receiver it consist to encode private messages in a background signal or noise process in such a way that the presence of the messages is hidden from those without access to the private key. An example of this kind of cooperation is Spread-spectrum modulation for wireless channels, which hides the spectral signature of the signal in the broad-band noise background using a pseudorandom convolution sequence as a private key.

But, as we said there are many other ways to increase secrecy attending to the wire-tap channel. Adding artificial noise [6] in the null spaces of the channel and transmit information along the directions corresponding to non-zero singular values is one example. Another interesting example could be the channel enhancement[4], it is shown in [8] that the optimal transmission strategy is to transmit only to the subchannels for which the receiver signal by the legitimate receiver is stronger than that by the eavesdropper. Therefore, an enhanced channel can be constructed by reducing the noise variance for the legitimate receiver in each of those subchannels to the noise variance level of the eavesdropper.

In the former chapter we focus our attention to the problem of secret communication in the wireless environment using MIMO systems, and especially on the eavesdropping. The central idea is that the transmitter uses stochastic encoding to introduce randomness, and hence increase secrecy. The ultimate goal is not to substitute cryptography by solving secrecy issues at Physical Layer, but, only to show this last could try to provide a background for confidentially to the upper layers.

4.2 System modelling

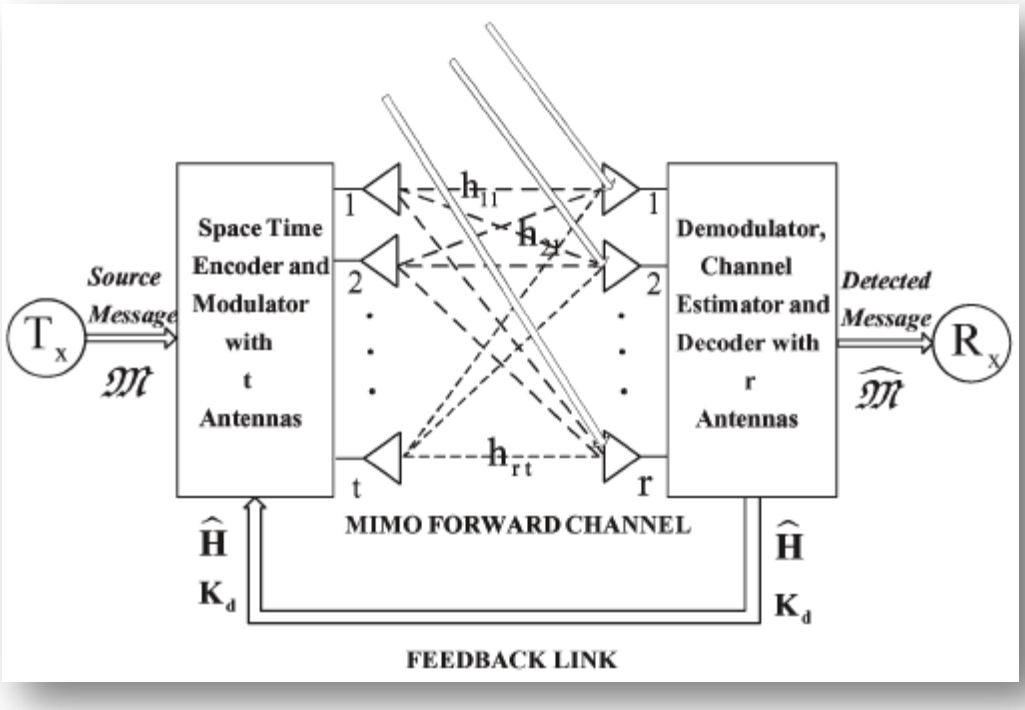

Fig: 4.2: Multiantenna system equipped with imperfect (forward) channel estimates and impaired by MAI with spatial covariance matrix.

The scenario that is considered refers to a local wireless ad-hoc networks, where transmission are affected by MAI [X], considering that the multiple autonomous transmit-receive nodes are simultaneously active over a limited-size hot-spot cell.

Transmit and receive units are equipped with t and r antennas, respectively. Slow-variant Rayleigh flat fading and multiple access interference should affect the MIMO radio channel. Path gains hjifrom theith transmit antenna to the jthreceive one may be modelled as complex zero-mean unit-variance random variables, and they may be assumed to be mutually uncorrelated when the antennas are properly spaced. Furthermore, when low-mobility applications are considered, all path gains may be assumed to change (at least) everyT ≥ 1 signalling period at new statistically independent values. The resulting block fading model may be used to properly describe the main features of interleaved frequency hopping or interleaved packet-based systems. MAI, affecting the link in Fig. 4.2, is supposed

to be at least constant over a packed period and it depends on the network topology. Despite this,hjiand MAI statistics may be different over temporally adjacent packets, so that the Tx and Rx nodes in Fig. 4.2 do not exactly know them at the beginning of any transmission period. Therefore, according to Fig. 4.3, the packet structure is composed of T ≥1slots: the first TL ≥ 0 ones are used by Rx for learning the MAI statistics, the second Ttr ≥ 0 ones are employed for estimating the (forward) MIMO channel path gains hji, and finally, the last Tpay =T - Ttr - TL ones are adopted to carry out payload data.

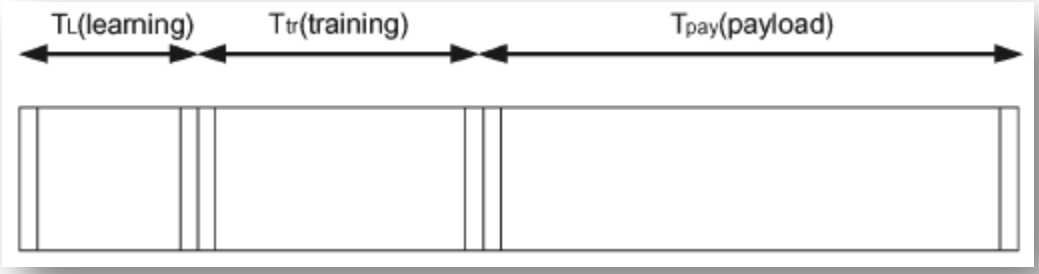

Figure 4.3: Packet structure

As a result of this, after denoting the space-time information rate as Rc(in nats per slot), the resulting system spectral efficiency η (in nats per second per hertz) is equal to

$$\eta = \frac{T_{pay}}{T}\frac{R_c}{\Delta_s B_w}, \quad (4.1)$$

whereΔs(in seconds) and Bw(in hertz) denote the slot duration and RF bandwidth of the radiated signals, respectively.

4.2.1 Learning Phase

During the learning phase, Tx in Fig. 4.2 is off, and Rx attempts to learn the MAI statistics. Thus, all receive antennas are now used to capture the interfering signals that are emitted by the interfering transmit nodes. Denoting the r-dimensional column vector of the (sampled) signals that were received at the nth learning slot as $\underline{\dot{y}}(n) \triangleq [\dot{y}_1(n), \dots, \dot{y}_r(n)]$ the latter equates to

$$\underline{\dot{y}}(n) \equiv \underline{\dot{d}}(n) \triangleq \underline{\dot{w}}(n) + \underline{\dot{v}}(n), \qquad 1 \le n \le T. \quad (4.2)$$

The overall disturbance vector $\underline{\dot{d}}(n) \triangleq [\underline{\dot{d}}_1(n), \dots, \underline{\dot{d}}_r(n)]^T$ in 4.2 is composed of two mutually independent components, which are denoted by$\underline{\dot{w}}(n) \triangleq [\underline{\dot{w}}_1(n), \dots, \underline{\dot{w}}_r(n)]^T$and $\underline{\dot{v}}(n) \triangleq [\underline{\dot{v}}_1(n), \dots, \underline{\dot{v}}_r(n)]^T$, respectively. The first component represent the receiver thermal noise, and then, it is modelled as a zero-mean spatially and temporally white Gaussian complex r -variant sequence, with covariance matrix

$$E\{\underline{\dot{w}}(n)\, \underline{\dot{w}}(m)\} = \mathcal{N}_0 I_r \delta(m,n), \quad (4.3)$$

where$\mathcal{N}_0$(in watt per hertz) is the power spectral density of the thermal noise. The second component in 4.2 takes the MAI into account. It is modelled as a zero-mean temporally white spatially colored Gaussian complex r -variant sequence, whose covariance matrix

$$K_v \triangleq E\left\{\underline{\dot{v}}(n)\left(\underline{\dot{v}}(n)\right)^{\dagger}\right\} \equiv \begin{bmatrix} c_{11} & \cdots & c_{1r} \\ \vdots & \ddots & \vdots \\ c_{r1} & \cdots & c_{rr} \end{bmatrix}, \quad (4.4)$$

is supposed to be constant over a packet transmission. Since its value may be different over temporally adjacent packets, we assume that both Tx and Rx nodes of Fig. 4.2 do not exactly know the overall disturbance covariance matrix

$$\mathbf{K}_d \triangleq \mathrm{E}\left\{\underline{\dot{d}}(n)\left(\underline{\dot{d}}(n)\right)^{\dagger}\right\} \equiv \mathbf{K}_v + \mathcal{N}_0\mathbf{I}_r, \qquad (4.5)$$

at the beginning of any new packet transmission period. In the following we illustrate a method to estimate the overall disturbance matrix.

4.2.2 Training Phase

Based on the MAI covariance matrix **K**d, the Tx node can now optimally shape the pilot streams $\{\tilde{x}_i(n)\mathbb{C}^1, T_L + 1 \le n \le T_L + T_{tr}\}, 1 \le i \le t$ which are used by Rx to estimate the MIMO forward channel path gains$\{h_{ij}, j = 1, \dots, r; i = 1, \dots, t\}$. Specifically, when the pilot streams are transmitted, the sampled signals $\{\tilde{y}_i(n)\mathbb{C}^1, T_L + 1 \le n \le T_L + T_{tr}\}, 1 \le j \le r$ that were received at the output of the jthreceive antennas are

$$\tilde{y}_j(n) = \frac{1}{\sqrt{t}}\sum_{i=1}^{t} h_{ji}\tilde{x}_i(n) + d_j\,(n) \quad (4.6)$$

$$T_L + 1 \le n \le T_L + T_{tr}; \quad 1 \le j \le r$$

where the overall disturbances

$$\tilde{d}_j(n) \triangleq \tilde{v}_j(n) + \tilde{w}_j(n) \qquad (4.7)$$

$$T_L + 1 \le n \le T_L + T_{tr}; \quad 1 \le j \le r$$

are independent from the path gains { hji } and still described by 4.4 and 4.5. Hence, by assuming the (usual) power constraint on the average transmitted power $\tilde{P}$,

$$\frac{1}{t}\sum_{i=1}^{t}\|\tilde{x}_i(n)\|^2 = \tilde{P}T_L + 1 \le n \le T_L + T_{tr} \qquad (4.8)$$

the resulting signal-to interference- plus-noise ratio (SINR) $\tilde{\gamma}_j$at the output of the jth receive antenna is equal to

$$\tilde{\gamma}_J = \tilde{P}/\left(\mathcal{N}_0 + c_{jj}\right), \quad 1 \le j \le r \quad (4.9)$$

where$\mathcal{N}_0 + c_{jj}$ is the jth diagonal entry of **K**d. All the (complex) samples in 4.6 may be collected into the $(T_{tr} \times r)$ matrix $\tilde{Y} \triangleq [\underline{\tilde{y}}_1, \dots, \underline{\tilde{y}}_r]$ which are given by

$$\tilde{\mathbf{Y}} \triangleq \frac{1}{\sqrt{t}}\tilde{\mathbf{X}}\mathbf{H} + \tilde{\mathbf{D}} \quad (4.10)$$

where$\tilde{X} \triangleq [\underline{\tilde{X}}_1, \dots, \underline{\tilde{X}}_t]$ is the pilot matrix, $H \triangleq [\underline{h}_1, \dots, \underline{h}_r]$ is the (t × r) channel matrix, and $\tilde{d} \triangleq [\underline{\tilde{d}}_1, \dots, \underline{\tilde{d}}_r]$ is the (Ttr× r) disturbance matrix. Since the pilot streams are power limited, the resulting power constraint on $\tilde{X}$becomes

$$\mathrm{Tra}\left[\tilde{\mathbf{X}}\tilde{\mathbf{X}}^{\dagger}\right] = tT_{tr}\tilde{P} (4.11)$$

The training observations $\tilde{\mathbf{Y}}$ in 4.10 are employed by Rx in Fig. 4.2 for computing the MMSE channel estimates matrix $\hat{H} \triangleq E\{H \setminus \tilde{Y}\}$. At the end of the training phase (e.g., at n = TL +Ttr), $\hat{H}$ is transmitted by Rx back to Tx through the (ideal) feedback link of Fig. 4.2

.

4.2.3 Payload Phase

Based on **K**dand $\hat{\mathbf{H}}$, the Tx node in Fig. 4.2 may properly shape the (random) signal information streams $\{\tilde{\phi}_i(n)\mathbb{C}^1, T_L + T_{tr} + 1 \le n \le T\}, 1 \le i \le t$ to be radiated. After their transmission, the resulting (sampled) signals $\{\tilde{y}_j(n)\mathbb{C}^1, T_L + T_{tr} + 1 \le n \le T\}, 1 \le j \le r$ that were received by Rx are

$$\tilde{y}_j(n) = \frac{1}{\sqrt{t}}\sum_{i=1}^{t} h_{ji}\Phi_i(n) + d_j(n) \quad (4.12)$$

$$T_L + T_{tr} + 1 \le n \le T; \quad 1 \le j \le r$$

where the disturbance sequences $d_j(n) \triangleq v_j(n) + w_j(n), \ 1 \le j \le r$ are mutually independent from the channel coefficients{ hji } and the radiated information streams { Φj}. As for the pilot streams, the signals{Φj(n)} that are radiated during the payload phase are also assumed to be power limited as in

$$\frac{1}{t}\sum_{i=1}^{t}\|\Phi_i(n)\|^2 = P \qquad T_L + T_{tr} + 1 \le n \le T \quad (4.13)$$

so that the SINR γ_j at the output of the jth receive antenna is equal to [see 4.5 and 4.12]

$$\tilde{\gamma}_J = P/(\mathcal{N}_0 + c_{JJ}), \quad 1 \le j \le r \quad (4.14)$$

Now, from 4.12, we may express the (r × 1) column vector $\underline{y}(n) \triangleq [y_1(n), \dots, y_r(n)]^T$ of the observations that were received during the nth slot as

$$\underline{\mathbf{y}}(n) = \frac{1}{\sqrt{t}}\mathbf{H}^T\underline{\phi}(n) + \underline{\mathbf{d}}(n), \qquad T_L + T_{tr} + 1 \le n \le T \quad (4.15)$$

where$\{\underline{\mathbf{d}}(n) \triangleq [d_1(n), \dots, d_r(n)]^T, \ T_L + T_{tr} + 1 \le n \le T\}$ is the temporally white Gaussian MAI vector with spatial covariance matrix still given by 4.5, **H** is the previously defined $(t \times r)$channel matrix, and$\underline{\boldsymbol{\phi}}(n) \triangleq [\phi_1(n), \dots, \phi_t(n)]^T$collects the symbols that are transmitted by the t transmit antennas.

Furthermore, after denoting the spatial covariance matrix of $\underline{\boldsymbol{\phi}}(n) \triangleq [\phi_1(n), \dots, \phi_t(n)]^T$as $\mathbf{R}_\phi \triangleq E\left\{\underline{\phi}(n)\underline{\phi}(n)^\dagger\right\}$,from 4.13, the latter must meet the following power constraint:

$$E\left\{\underline{\phi}(n)\underline{\phi}(n)^\dagger\right\} \equiv \mathrm{Tra}[\mathbf{R}_\phi] = tP, \qquad T_L + T_{tr} + 1 \le n \le T \quad (4.16)$$

Finally, by stacking the Tpayobserved vectors in 4.15 into the (Tpayr × 1) block vector $\vec{\underline{y}} \triangleq \left[\underline{y}^T(T_L + T_{tr} + 1), \dots, \underline{y}^T(T)\right]^T$, we arrive at the following final observation model:

$$\vec{\underline{\mathbf{y}}} \triangleq \frac{1}{\sqrt{t}}\left[\mathbf{I}_{T_{pay}} \otimes \mathbf{H}\right]^T \vec{\underline{\phi}} + \vec{\underline{\mathbf{d}}} \quad (4.17)$$

where the (Tpayr×1) (block) disturbance vector is $\vec{\underline{d}} \triangleq \left[\underline{d}^T(T_L + T_{tr} + 1), \dots, \underline{d}^T(T)\right]^T$ is Gaussian distributed, with the covariance matrix given by

$$E\{\underline{\vec{d}}\underline{\vec{d}}^{\dagger}\} = \mathbf{I}_{T_{pay}} \otimes \mathbf{K}_d \quad (4.18)$$

and the (block) signals vector $\underline{\vec{\phi}} \triangleq \left[\underline{\phi}^T(T_L + T_{tr} + 1), \ldots, \underline{\phi}^T(T)\right]^T$ is power limited as in

$$E\left\{\underline{\vec{\phi}}^{\dagger}\underline{\vec{\phi}}\right\} = T_{pay}tP. \quad (4.19)$$

4.3 Topology-Based MAI Model for Multiantenna "ad hoc" Networks

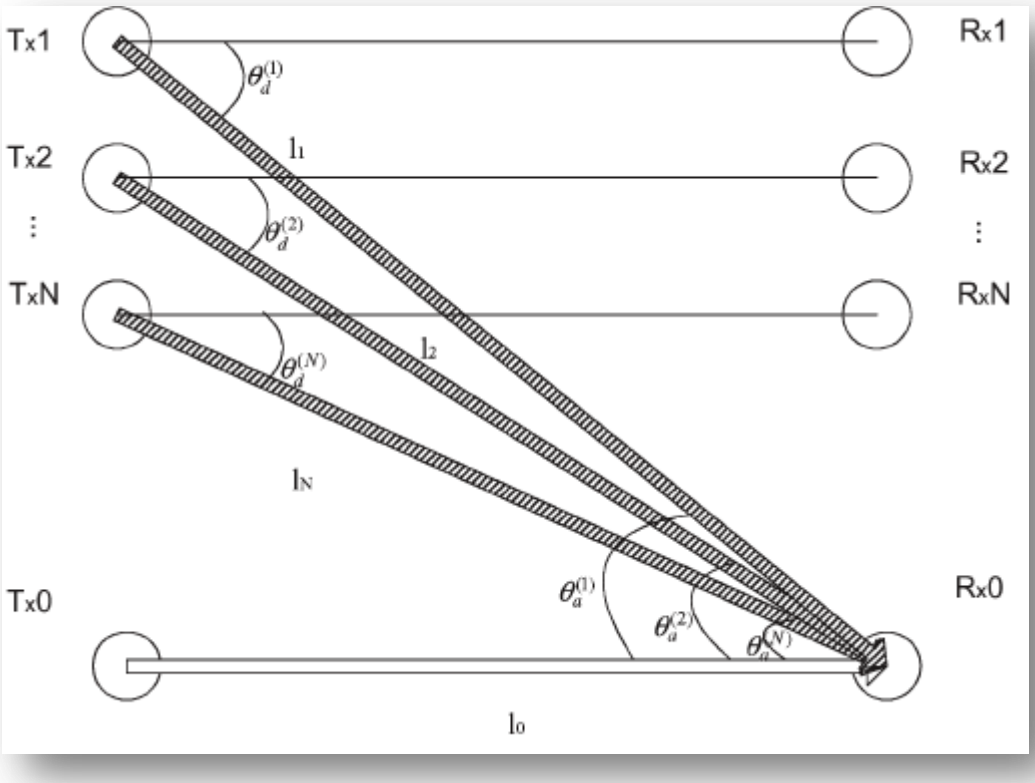

Fig 4.4: General scheme for an "ad hoc" network composed of (N + 1) point-to-point links active over the same hot-spot area.

We consider the application scenario of Fig. 4.4 that captures the key features ofmultiantenna "ad hoc" networks that are impaired by spatial MAI.

Shortly, we assume that the network of Fig. 4.4 is composed of (N + 1) nocooperative mutually interfering point-to-point links $Txf \rightarrow Rxf$, 0 ≤ f ≤ N. Thesignal received by the reference node Rx0 is the combined effect of that transmittedby Tx0 and those radiated by the other interfering transmitters (Txf, 1≤f≤N).The transmit node Txf and the receive node Rxf are equipped with t_f and $r_f$antennas, respectively.Thus, after denoting the Txf→ Rx0 distance as l_f, thenthe **d**(n) disturbance vector in Eq. 4.15 may be modeled as

$$\underline{d}(n) = \sum_{f=1}^{N} \sqrt{\left(\frac{l_0}{l_f}\right)^4} \frac{1}{\sqrt{t_f}} \chi_f H_f^T \underline{\phi}^{(f)}(n) + \underline{w}(n). \quad (4.20)$$

The vector **w**(n) in Eq.4.20 accounts for the thermal noise. The $\underline{\phi}^{(f)}(n)$ term representsthe t_f -dimensional (Gaussian) signal that was radiated by the Txf transmitter. χ_f accounts for the shadowing effects. The matrix $\mathbf{H}_f$ models theRicean-distributed fast fading affecting the interfering link $Txf \rightarrow Rx0$. Furthermore the channel matrix$\mathbf{H}_f$ in Eq. 4.20may be modelled as

$$\mathrm{H}_f \equiv \sqrt{\frac{k_f}{1+k_f}} H_f^{(sc)} + \sqrt{\frac{1}{1+k_f}} H_f^{(sp)} \qquad 1 \le f \le N \quad (4.21)$$

where $k_f \in [0, +\infty)$ is the fthRicean factor, and all the $(t_f \times r_0)$ terms of matrix $\boldsymbol{H}_f^{(sc)}$ are mutually independent zero-mean unit-variance Gaussian-distributed that account for the scattering phenomena impairing the fth interfering link $Txf \rightarrow$ Rx0. The$(t_f \times r_0)$ matrix $\boldsymbol{H}_f^{(sp)}$f in Eq. 4.21 contains the specular components of theinterfering signal and may be modelled as

$$\mathbf{H}_f^{(sp)} = (\underline{\mathrm{a}}(f)\underline{\mathrm{b}}(f))^{\mathrm{T}}, \qquad 1 \le f \le N \quad (4.22)$$

where$\underline{\mathbf{a}}$(f)and $\underline{\mathbf{b}}$(f) are (r_0× 1) and (t_f×1) column vectors, respectively. Theyare used to model the seculars array responses at receive node Rx0 and transmitnode Txf, respectively.When isotropic regularly spaced linear arrays areemployed at the Txf and Rx0 nodes, the preceding vectors may be evaluated as

$$\underline{\mathbf{a}}(f) = \left[1, \exp\left(j2\pi\vartheta \cos\left(\theta_A^{(f)}\right)\right), \ldots, \exp\left(j2\pi\vartheta(r_0 - 1)\cos\left(\theta_A^{(f)}\right)\right)\right]^T \quad (4.23)$$

$$\underline{\mathbf{b}}(f) = \left[1, \exp\left(j2\pi\vartheta \cos\left(\theta_d^{(f)}\right)\right), \ldots, \exp\left(j2\pi\vartheta(t_f - 1)\cos\left(\theta_d^{(f)}\right)\right)\right]^T \quad (4.24)$$

where $\theta_A^{(f)}$and$\theta_d^{(f)}$ are the arrival and departure angles of the radiated signals, respectively (see Fig. 4. 4), whileϑ is the antenna spacing in multiples of RF wavelengths.

4.3.1 Model for the MAI Covariance Matrix

Therefore, after assuming the spatial covariance matrix$\mathbf{R}_\phi^{(f)} \triangleq E\{\phi^{(f)}(n)\phi^{(f)}(n)^\dagger\}$, of signals that are radiated by the fth transmit node Txf power-limitedas

$$Tra\left[\boldsymbol{R}_\phi^{(f)}\right] = t_f P^{(f)} \quad (4.25)$$

then the covariance matrix $\mathbf{K}_d$ of the MAI vector in Eq. 4.20 is equal to

$$\boldsymbol{K}_d \triangleq E\{\underline{\boldsymbol{d}}(n)\underline{\boldsymbol{d}}(n)^\dagger\} =$$
$$= \left\{\mathcal{N}_0 + \sum_{f=1}^{N}\left(\frac{l_0}{l_f}\right)^4 \frac{E\{\chi_f^2\}}{1+k_f} P^{(f)}\right\}\mathbf{I}_{r0}$$
$$+ \left\{\sum_{f=1}^{N}\left(\frac{l_0}{l_f}\right)^4 \frac{k_f}{1+k_f}\frac{E\{\chi_f^2\}}{t_f}\underline{\boldsymbol{a}}(f)\underline{\boldsymbol{b}}(f)\boldsymbol{R}_\phi^{(f)}\underline{\boldsymbol{b}}^*(f)\underline{\boldsymbol{a}}^\dagger(f)\right\} \quad (4.26)$$

This relationship captures the MAI effects due to the topological and propagationfeatures of the considered multiantenna ad hoc network. Specifically, Eq. 4.26 pointsout that MAI interference may be considered spatially white when all the interferinglinks' Ricean factors may be neglected. Conversely, for high Ricean factors, the MAIspatial coloration is not negligible.

4.4 MAI Covariance Matrix Estimation

We want to consider the case when an eavesdropper is able toestimate the interference product by other transmitter and to cancel it from thereceived signal. In some sense this is a worst case of eavesdropping.

Eq. 4.5, here rewritten, expresses the overall disturbance covariance matrix

$$\mathbf{K}_{\mathrm{d}} = \mathbf{K}_{\mathrm{v}} + \mathcal{N}_0 \mathbf{I}_{\mathrm{r}}$$

Since $\mathbf{K}_{\mathrm{v}}$may change from a packet to another, it is reasonable to assume thatboth Tx and Rx are not aware of the covariance matrix of the overall disturbanceat the beginning of each transmitted packet. However, since during the learningphase the signal received at the Rx equates the MAI plus noise, thus the Rx mayexploit its cognitive capabilities to learn$\mathbf{K}_{\mathrm{v}}$. A very simple way to accomplish thistask is suggested by the Law of Large Numbers. By fact, this last guarantees thatan unbiased and consistent (e.g., asymptotically exact) estimate $\breve{\mathbf{K}}_{\mathrm{v}}$of $\mathbf{K}_{\mathrm{v}}$ can beobtained and we anticipate that the effects of (possible) mismatches between actual$\mathbf{K}_{\mathrm{v}}$and its estimate $\breve{\mathbf{K}}_{\mathrm{v}}$will be evaluated by resorting to the following expression

$$\breve{\mathbf{K}}_{\mathrm{v}} = \mathbf{K}_{\mathrm{v}} + \sqrt{\frac{\|\mathbf{K}_{\mathrm{v}}\|}{r^2}\sqrt{\delta N}} \quad (4.27)$$

where the parameter δ takes into account for the power level of interference acquisitionerror, while N is a $r \times r$ matrix collecting zero mean, unit-variance, Gaussiannoise samples.

The ability of the receiver to perform interference statistics acquisition suggests proceeding with interference estimation and mitigation via a simple subtraction. Theinterference mitigation (IM) is performed according to the Orthogonal ProjectionLemma; in fact we have (for each time-frequency-code slot)

$$\tilde{\mathbf{v}} = \mathbf{M}\mathbf{y} \quad (4.28)$$

where**y** is the $r \times 1$ vector of spatially received signals and after orthogonal projectionlemma application we have

$$\mathrm{E}\{(\tilde{\mathbf{v}} - \mathbf{v})\mathbf{y}^{\dagger}\} = 0 \quad (4.29)$$

and this leads to

$$\mathbf{M}\mathrm{E}\{\mathbf{y}\mathbf{y}^{\dagger}\} = \mathrm{E}\{\mathbf{v}\mathbf{y}^{\dagger}\} \quad (4.30)$$

that gives

$$\mathbf{M} = \breve{\mathbf{K}}_{\mathrm{v}}(\mathbf{K}_{\mathrm{y}})^{-1} = \mathbf{K}_{\mathrm{v}}\left(\mathbf{K}_{\mathrm{d}} + \widehat{\mathbf{H}}^{\mathbf{T}}\mathbf{R}_{\boldsymbol{\phi}}\breve{\mathbf{H}}^{*}\right)^{-1} \quad (4.31)$$

This estimation procedure, by providing interference subtraction capability to thereceiver, allows us to evaluate the residual interference as

$$\mathbf{K}_{\mathrm{de}} = \mathrm{E}\{(\mathbf{d}-\tilde{\mathbf{v}})(\mathbf{d}-\tilde{\mathbf{v}})^{\dagger}\} = \mathbf{K}_{\mathrm{d}} - 2\mathrm{E}\{\mathbf{d}\mathbf{y}^{\dagger}\}\mathbf{M}^{\dagger} + \boldsymbol{M}\mathbf{K}_{\mathrm{y}}\boldsymbol{M}^{\dagger}$$
$$= \mathbf{K}_{\mathrm{d}} - 2\mathbf{K}_{\mathrm{d}}\mathbf{K}_{\mathrm{y}}{}^{-\dagger}\breve{\mathbf{K}}_{\mathrm{v}}{}^{\dagger} + \breve{\mathbf{K}}_{\mathrm{v}}\mathbf{K}_{\mathrm{y}}{}^{-\dagger}\breve{\mathbf{K}}_{\mathrm{v}}{}^{\dagger} \quad (4.32)$$

4.5 Information Throughput Under Spatially Colored MAI

As seen in the previous chapter, a measure of how much information that can betransmitted and received with a negligible probability of error is called the channelcapacity. To determine this measure of channel potential, assume that a channelencoder receives a source symbol every T_s seconds. With an optimal source code,the average code length of all source symbols is equal to the entropy rate of the source.If *S* represents the set of all source symbols and the entropy rate of the source iswritten as H(*S*), the channel encoder will receive on average H(*S*)=T_s informationbits per second. Assume that a channel codeword leaves the channel encoder everyT_c seconds. In order to be able to transmit all the information from the source, theremust be

$$R = \frac{H(S)T_c}{T_s} \quad (4.33)$$

information bits per channel symbol. The number R is called the information rateof the channel encoder. The maximum information rate that can be used causingnegligible probability of errors at the output is called the capacity of the channel.By transmitting information with rate R, the channel is used every Tc seconds.The channel capacity is then measured in bits per channel use. Assuming that thechannel has bandwidth W, the input and output can be represented by samples takenT_s = 1/2W seconds apart. With a band-limited channel, the capacity is measured ininformation bits per second. It is common to represent the channel capacity within aunit bandwidth of the channel. The channel capacity is then measured in bits/s/Hz.

It is desirable to design transmission schemes that exploit the channel capacityas much as possible. Representing the input and output of a memoryless wireless channel with the random variables *X* and *Y* respectively, the channel capacity isdefined as

$$C = \max_{p(x)} I(X;Y) \quad (4.34)$$

where $I(X;Y)$ represents the mutual information between X and Y . Eq. 4.34 statesthat the mutual information is maximized with respect to all possible transmitterstatistical distributions p(x). Mutual information is a measure of the amount ofinformation that one random variable contains about another variable. The mutualinformation between *X* and *Y* can also be written as

$$I(X;Y) = H(Y) - H(Y\backslash X), \quad (4.35)$$

where H(*Y**X*) represents the conditional entropy between the random variables*X* and *Y* .

The entropy of a random variable can be described as a measure ofthe amount of information required on average to describe the random variable. Itcan also describe as a measure of the uncertainty of the random variable. Dueto 4.35, mutual information can be described as the reduction in the uncertaintyof one random variable due to the knowledge of the other. Note that the mutualinformation between *X* and *Y* depends on the properties of the channel (through achannel matrix H) and the properties of *X* (through the probability distribution of*X*). The previous description is valid in general, now we refer to the communicationsystem introduced in the previous section. As said before, $\underline{\vec{y}}$ represent the $(T_{pay}r \times 1)$ block vector collecting the observations that were received, $\underline{\vec{\phi}}$is the $(T_{pay}t \times 1)$

blockvector representing the signals radiated during the payload phase. Under the powerconstraint for the radiated signal expressed in the Eq.4.19, the capacity of the MIMOchannel can be written as

$$C(\mathbf{H}) \triangleq \underset{\underline{\vec{\emptyset}}:\, \boldsymbol{R}_{\emptyset} = E\left\{\underline{\vec{\emptyset}}^{\dagger}\underline{\vec{\emptyset}}\right\} \leq tT_{pay}P}{sup} \frac{1}{T_{pay}} I\left(\underline{\vec{y}};\underline{\vec{\emptyset}}\,|\mathbf{H}\right) \quad (4.36)$$

where

$$I\left(\underline{\vec{y}};\underline{\vec{\phi}}\middle|\mathbf{H}\right) = T_{pay}\log\det\left(\boldsymbol{I}_r + \frac{1}{t}\boldsymbol{K}_d^{-1/2}\boldsymbol{H}^T\boldsymbol{R}_{\phi}\boldsymbol{H}^*\boldsymbol{K}_d^{-1/2}\right) \qquad (4.37)$$

4.6 Optimized Power Allocation UnderColored MAI

To evaluate covariance matrix Rf achieving the sup in eq.4.36, let us begin with thesingular value decomposition (SVD) of covariance matrix K_d according to

$$\mathbf{K}_{\mathrm{d}} = \mathbf{U}_{\mathrm{d}}\Lambda_{\mathrm{d}}\mathbf{U}_{\mathrm{d}}^{\dagger} \quad (4.38)$$

where

$$\Lambda_{\mathrm{d}} \triangleq diag\{\mu_1, \dots, \mu_r\} \qquad (4.39)$$

represent the $(r \times r)$ diagonal matrix of magnitude-ordered singular values of$\mathbf{K}_{d.}$Furthermore, we define by

$$\mathbf{A} = \mathbf{H}^*\mathbf{K}_{\mathrm{d}}^{-1/2}\mathbf{U}_{\mathrm{d}} \qquad (4.40)$$

the $(t \times r)$ matrix that simultaneously accounts for the effects of the imperfect channelestimate $\widehat{\mathbf{H}}$and MAI spatial coloration. The corresponding SVD is

$$\mathbf{A} = \mathbf{U}_{\mathrm{A}}\mathbf{D}_{\mathrm{A}}\mathbf{V}_{\mathrm{A}}^{\dagger} \qquad (4.41)$$

where$\mathbf{U}_A$ and $\mathbf{V}_A$ are unitary matrices, and

$$\mathbf{D}_{\mathrm{A}} \triangleq \begin{bmatrix} diag\{k_1, .., k_s\} & 0_{s\times r-s} \\ 0_{t-s\times r} & 0_{t-s\times r-s} \end{bmatrix} \qquad (4.42)$$

is the $(t \times r)$ matrix having the s = min **{**r, t**}**magnitude-ordered singular valuesk$_1$≥ k$_2$≥…≥k$_s$≥0 of **A** along the main diagonal of the submatrix starting fromelements (1,1) to (s,s). Finally, the resulting optimized covariance matrix R_(opt)of the radiated signals is given by

$$\mathbf{R}_{\phi}(\mathrm{opt}) = \mathbf{U}_{\mathrm{A}}\mathrm{diag}\left\{\mathrm{P}^*(1), \dots, \mathrm{P}^*(\mathrm{s}), \underline{0}_{\mathrm{t-s}}\right\}\mathbf{U}_{\mathrm{A}}^{\dagger} \quad (4.43)$$

The value of $P^*(s)$ depends on the allocating power algorithm chose.

In the following we first consider the waterfilling power allocation algorithm andthen we introduce the novel algorithm for allocating the transmitted power.

4.7 WATERFILLING ALGORITHM FOR POWER ALLOCATION

The adaptation of the transmit signal to the channel condition can typically bring a large improvement to the transmission rate. Adaptation is possible when the channel state is available to the transmitter, usually by a channel-estimation scheme and a reliable feedback mechanism. If the channel can be partitioned into parallel independent subchannels, the optimal transmit power adaptation scheme is the well-known waterfilling procedure. In a waterfilling power spectrum, more power is allocated to better subchannels with higher signal-to-noise ratios (SNRs), so that the sum of data rates in all subchannels is maximized, where the data rate in each subchannel is related to the power allocation by Shannon's Gaussian capacity formula $\frac{1}{2}\log(1+SNR)$. This solution is totally opposed to a criterion of equality or fairness because it assigns more power to the best channel.

The optimal energy is found iteratively through the "waterfilling algorithm", as we described on chapter 2: MIMO Systems.

4.8 INTRODUCTION OF RANDOMNESS

Some cooperation of the transmitter and the receiver is needed to put an eavesdropper at a relative disadvantage. One of the most common forms of cooperation, as we say in the chapter 3, is the use of a cipher to encrypt each data stream transmitted which can only be deciphered at the clientreceiver using a private shared key.

When channel state information is available to the transmitter, one can design the spatio-temporal modulation/demodulation to exploit known propagation and interference characteristics of the channel available to the client but not to the eavesdropper. For the memoryless channels considered here, this corresponds to spatial (multichannel) encryption and information hiding where the shared channel information plays the role of a shared private key that can be used to decrypt the message. As a practical matter, this private key is distributed to the transmitter and client receiver in the form of a training sequence, unknown to the eavesdropper. The initial portion of each coherent fade interval is reserved for transmission of the training sequence to the client receiver which permits it to estimate the set of channel coefficients.

Here it's shown that secrecy can be achieved by adding an extra matrix (matrix Q) to the transmit information signal such that it does not degrade the intended receiver's channel.

The idea is to create a matrix that changes the appearance of the channel. That, cheats on the eavesdropper, who thinks the power is allocate following a water-filling solution. In this case the eavesdropper has a wrong idea of who are the "better" subchannels with the higher signal-to-noise ratio (SNR), while the receiver has the perfect knowledge of how is allocate the power. This helps to conceal the secret message that it is transmitting.

The optimal matrix should be one that invert the appearance of the channel like it's shown in fig 4.5. In this case for example, the eavesdropper doesn't aspect much information in channel 2, so he will focus his resources to decrypt information in channel 1.

In these simulations we use matrix entries that are modelled as complex zero-mean unit-variance random variables. The result obviously is not the same that using a matrix that inverts the channel, but as we see in the following the secrecy region will decrease.

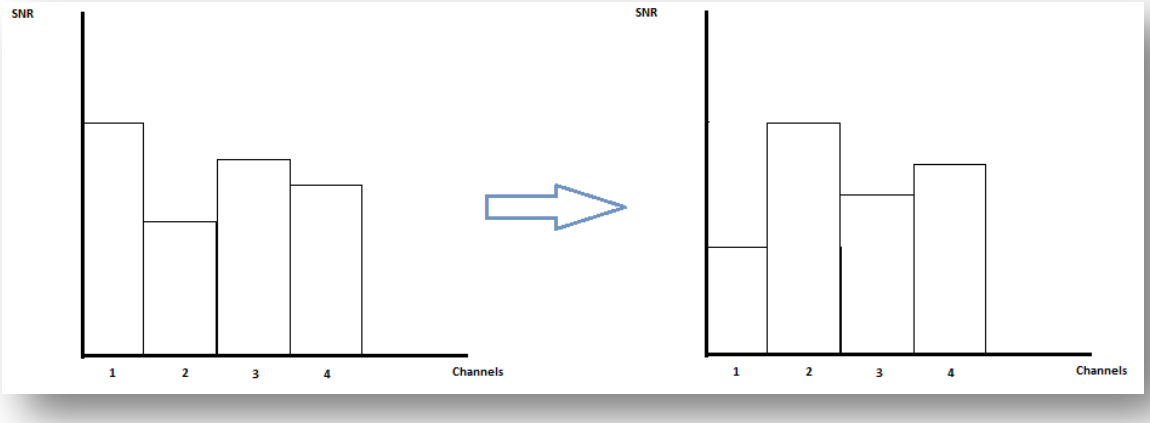

Fig 4.5: an ideal situation in which the addition of matrix Q cause a perfect inversion of the channel

4.9 SIMULATIONS

Our work proceeds as follows. It's important to note that we evaluated the confidentiality of a link by taking care of information rate of the possible eavesdropper one,so, low values of information rate for Alice-Eve link allow high level of confidentiality.

We first introduce the resulting of the simulationmakes with the use of the waterfilling power allocation algorithm in the presence ofan eavesdropper. Our simulation is done in a simple scenario without any MAIinterferer. Then we compare this one with the waterfilling power allocation algorithm by using the introduction of randomness.

Second, we propose an iterative algorithm for the optimized power allocation that minimizes the eavesdropper's information rate. All of these are done considering the case of Perfect Channel State Information at the transmitter side (Perfect CSI).

All the simulations are made doing a number of 100 iteration on the channelmatrix H and the matrix $\mathbf{Q}$. This is done because the channel matrix entries $\{\mathrm{hji}\}$ from the ith tothe jth receiver antenna are modelled as complex zero-mean unit-variance randomvariables and, if the antennas are properly spaced, they are mutually uncorrelated.

During the simulations we suppose a maximum transmitting power Pt = 10W and a noise power spectral density ratio $\mathrm{N}_0 = 10^{-3}$. We also suppose that Alice has four transmitting antennas and both Bob and Eve got the same number of receiving antennas.

4.9.1 WATERFILLING ALGORITHM WITH INTRODUCTION OF RANDOMNESS

In the simulating scenario we consider, there is one transmitter Tx1 (Alice), who wants to communicate with his respective receiver, Rx1 (Bob). There is also an unauthorized eavesdropper (Eve) at the same distance that the transmitter, that tries to intercept the communication between Tx1 and Rx1.

In this scenario the transmitter allocate the transmitting power by means of an iterative waterfilling algorithm. This means that Tx1allocates the power in a WF fashion considering the channel.

In the first simulation we compare the secrecy region attained by the waterfilling algorithm with and without using the random matrix Q in the same scenario. Notice that the information rate between Alice and Eve using the random matrix Q is decreased.

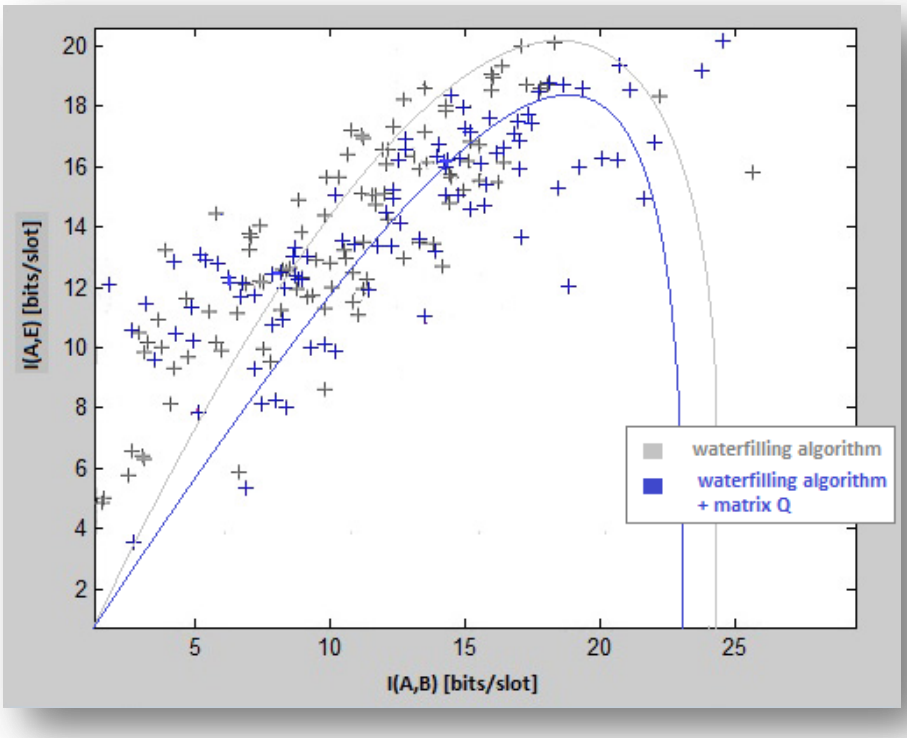

Figure 4.6: waterfilling algorithm with and without using matrix Q.

4.9.2 OPTIMIZED POWER ALLOCATION: The Maximum Rate Algorithm

With the goal to enhance the secrecy level of the communication between Alice and Bob we introduce a novel power allocation algorithm that allocates the transmitted power minimizing the rate Re, i.e. maximizing the information throughput between Alice and Bob constraining the information rate Alice-Eve at a fixed, and feasible value. In short, we want to find a power allocation algorithm that satisfies the converse problem:

$$\begin{cases} \max_{\psi_i} \sum_i \log(1 + g_i\psi_i) \\ s.t. \qquad \psi_i \geq 0 \\ \sum_i \psi_i \leq P_t \\ \sum_j \log(1 + z_j\psi_i) \end{cases} \tag{4.48}$$

with $g_i = \frac{\lambda^2{}_i}{tN_0}$ and $z_j = \frac{\eta^2{}_i}{tN_0}$ and we call this The Maximum Rate Problem. Following we rewrite the Maximum Rate Problem using the Lagrange multiplier.

$$\Lambda(\psi, \alpha, \beta, \gamma) = \sum_i \log(1 + g_i\psi_i) - \alpha\left(\sum_i \psi_i - P_t\right) + \sum_i \beta_i\psi_i - \\ -\gamma(\textstyle\sum_i \log(1 + z_i\psi_i) - \zeta) \tag{4.49}$$

and we get the following system of 2t+1 equations

$$\begin{cases} \Lambda_{\psi_i}(\psi,\alpha,\beta,\gamma) = \frac{g_i}{1+g_i\psi_i} + \alpha + \beta_i - \gamma\left(\frac{z_i}{1+z_i\psi_i}\right) = 0 \\ \Lambda_\alpha(\psi,\alpha,\beta,\gamma) = \alpha(\sum_i \psi_i - P_t) = 0 \\ \Lambda_\beta(\psi,\alpha,\beta,\gamma) = \beta_i\psi_i = 0 \\ \Lambda_\gamma(\psi,\alpha,\beta,\gamma) = \gamma(\sum_i \log(1+z_i\psi_i) - \zeta) = 0 \end{cases} \quad (4.50)$$

Now, we proceed with the Newton's method and calculate the k + 1th iteration by the following the equation:

$$X_{K+1} = X_K - J^{-1}(X_K)F(X_k) \quad (4.51)$$

where X_K is the kth iteration, $F(X_k)$ is the vector of the unknown quantities and $J^{-1}(X_K)$ is tha Jacobian matrix

$$J(X) = \begin{bmatrix} f_{1,x_1} & \cdots & f_{1,x_n} \\ \vdots & \ddots & \vdots \\ f_{n,x_1} & \cdots & f_{n,x_n} \end{bmatrix} (4.52)$$

where f_{n,x_n} is the nth derivative of the nth equation of the system. Applying the Newton's iterative method to our problem we obtain for the former vectors

$$X = [\psi_1 \cdots \psi_t \ \alpha \ \beta_1 \cdots \beta_t \ \gamma] (4.53)$$

$$F = [\frac{g_1}{1+g_1\psi_1} + \alpha + \beta_1 - \gamma\left(\frac{z_1}{1+z_1\psi_1}\right) \cdots \frac{g_t}{1+g_t\psi_t} + \alpha + \beta_t - \gamma\left(\frac{z_t}{1+z_t\psi_t}\right) \\ \alpha(\sum_i \psi_i - P_t)\beta_i\psi_i \cdots \beta_i\psi_i \ \gamma(\sum_i \log(1+z_i\psi_i) - \zeta)] \quad (4.54)$$

From the Newton's method we obtain a set of values, called S, of the unknown quantities that satisfy the problem in 4.48, from this set we bring the value of power toallocate to each antenna: 1, …, t.

One of the feature of the MR algorithm is that it can bring an information rate between Alice-Bob that is the same as the waterfilling but to do so we must properly choice the constraint to the Alice-Eve rate: to attain higher Alice-Bob rate the constraint on Alice-Eve can't be too stringent so it causes an higher Alice-Eve rate too. Conversely, forcing the constraint on the Alice-Eve rate we attain a higher secrecy but a lower information rate between Alice and Bob.

Now we proceed with the simulations applying the MR algorithm to the scenario where there isn't any interferer.

4.9.2.1 Maximum Rate Algorithm and matrix Q

We simulate the operating ability of the proposed allocation algorithm in ascenario where there aren't any interferer and where the network topology is the same as in Fig 4.5.

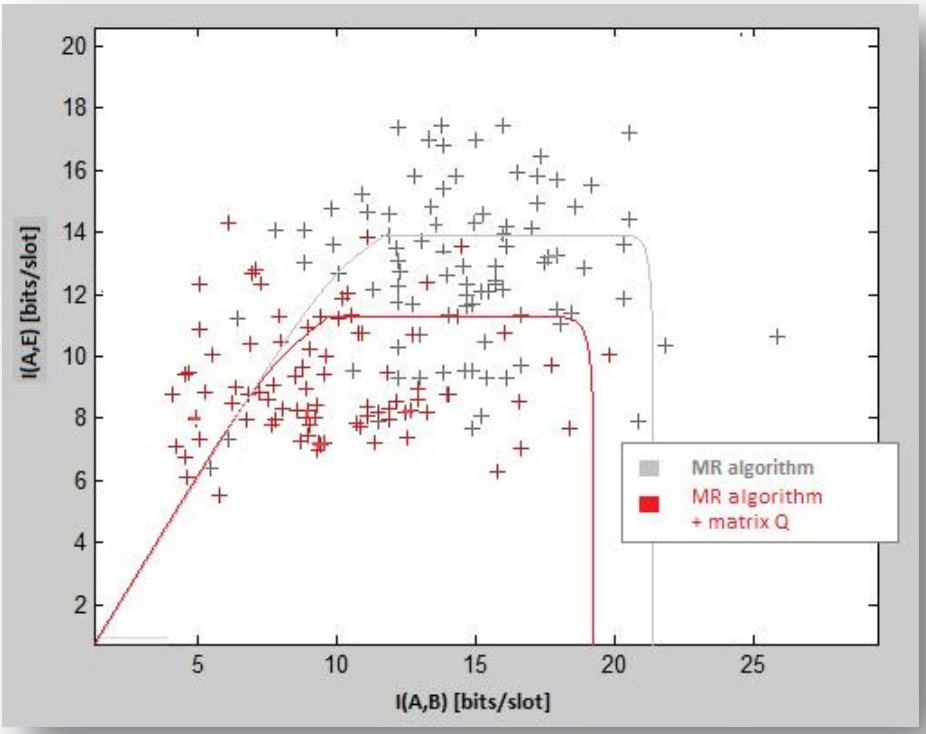

Fig 4.7 Information secrecy region for standard MR algorithm and the same algorithm plus addition of matrix Q

The picture compare the secrecy region attained by the MR algorithm with the obtained by adding that matrix Q in the same scenario. Notice that the information rate between Alice and Eve is decreased and a good level of information rate between Alice and Bob is attained as it happens with the waterfilling algorithm.

4.9.2.2 Maximum Rate Algorithm vs. waterfilling.

In the next scenario we compare the information-secrecy region attained by the MR algorithm with the one obtained by the waterfilling algorithm. The constraint on the rate Alice-Eve is set to14 bit/slot. The WF procedure allows achieving a maximum rate level (for (I(A,B)) that is higher than the achievable by MR algorithm. Specifically the Waterfilling approach achieves a maximum that is given by 25 bit/slot while the maximum rate of Alice-Eve link is limited to 22.5 bit/slot. Now, by paying attention to the secrecy level, we can note that the information rate of Alice-Eve link is higher in the waterfilling algorithm than in the MR, since in this case we have an additional constraint. While the maximum level of Waterfilling in Alice-Eve rate is 19 bit/slot, the approach with MR algorithm presents the maximum at 14 bit/slot. There is a trade-off between the secrecy rate I(A,E) and the conveyed information rate I(A,B). A lower constraint on I(A,E) will reduce the information rate I(A,B).

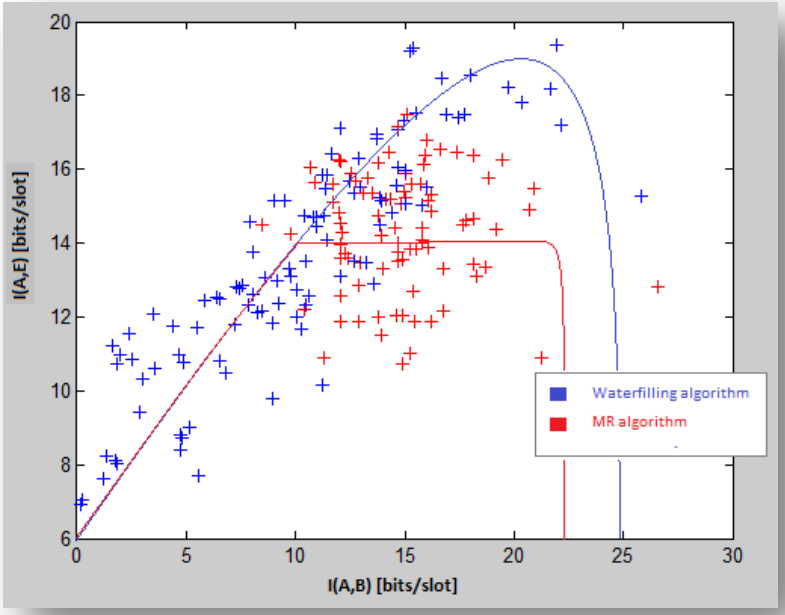

Fig 4.8: Information secrecy region for standard Waterfilling approach and Maximum Rate algorithm.

4.9.2.3 Maximum Rate Algorithm vs. waterfilling both with introduction of randomness

With respect to the previous simulation we impose the same constrains in the same scenario but in this case we expect that the introduction of the matrix Q when transmitting the message may reduce the secrecy region in both algorithms.

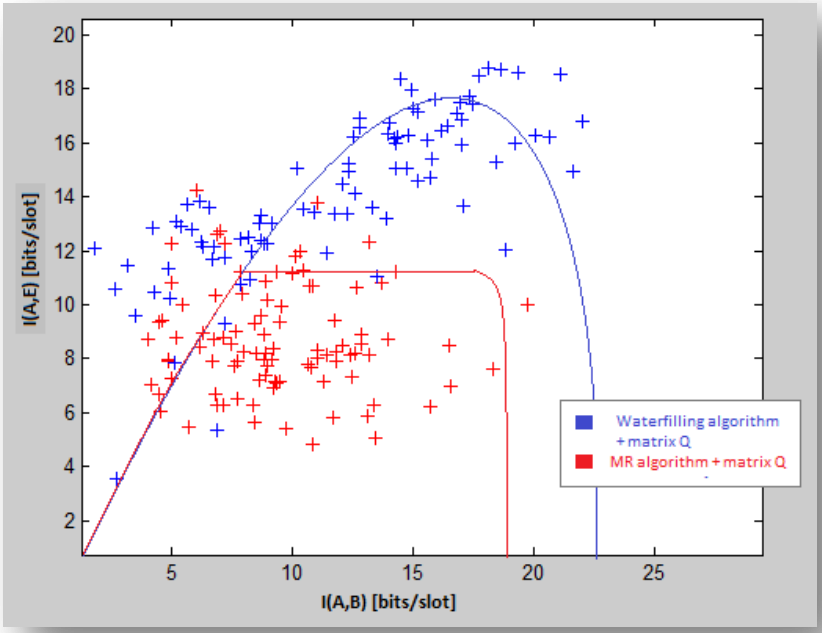

Fig 4.9:*Information secrecy region for Waterfilling approach and Maximum Rate algorithm both by addition of matrix Q*

When we decrease the maximum A-B link rate from 22.5 bit/slot to 18.5 bit/slot we decrease at the same time the maximum A-E link, which implies increasing the secrecy level, from 14 bit/slot to 11.5 bit/slot with the addition of the random matrix Q. This means also that we are gaining in secrecy respect to the standard Maximum Rate algorithm.

CHAPTER 5: CONCLUSIONS

In this thesis the issue of contention resolution in information-theoric-based security techniqueshas been discussed. We have studied waterfilling-like approach with additional constraint on the secrecy level. Twodifferentapproaches have been analyzed and simulated: the Maximum Rate Algorithm and the introduction of a random matrix. After analysing results obtained, the main contribution to the area of contention resolution are the following:

- The cooperation of the transmitter and the receiver is needed to put an eavesdropper at a relative disadvantage.
- When channel state information is available to the transmitter, one can design the spatio-temporal modulation/demodulation to exploit known propagation and interference characteristics of the channel available to the client but not to the eavesdropper.
- The solution found for the case of perfect knowledge of the channel transmitter is called water-filling.
- The introduction of the random matrix when transmitting the message implies to lose in the main link information rate but decreases the secrecy region.

Althoughintroducing the new constraints may suppose to lose in the main link (Alice-Bob) information rate, the numerical results show that, at the same time, it allows a good level of secrecy. Possible future works in this topic will deal with integration between these results and cryptography.

BIBLIOGRAPHY

[1] Jia Liu, Y. Thomas Hou, and Hanif D. Sherali. Optimal Power Allocation for Achieving PerfectSecrecy Capacity in MIMO Wire-Tap Channels. Virginia Polytechnic Institute and State University, Blacksburg, VA 24061

[2] S. K. Leung-Yan-Cheong and Martin E. Hellman. The Gaussian wire-tap Channel

[3] FréderiqueOggier and BabakHassibi. The Secrecy Capacity of 2x2 MIMO Wiretap Channel

[4] Tie Liu and ShlomoShamai (Shitz). A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel.

[5] ImreCsiszár and JánosKörner. Broadcast Channels with Confidential Messages.

[6] AshishKhisti and Gregory Wornell. On the Gaussian MIMO Wiretap Channel.

[7] Enzo Baccarelli, Mauro Biagi, Cristian Pelizzoni, Nicola Cordeschi. Optimized Power-Allocation for Multi-Antenna Systems impaired by Multiple Access Interference and Imperfect Channel Estimation.

[8] Xiaojun Tang, Ruoheng Liu, PredragSpasojevic and H. Vincent Poor. Interference-Assisted Secret Communication

[9] Mauro Biagi, Enzo Baccarelli, Nicola Cordeschi, Valentina Polli, Tatiana Patriarca. A Secrecy constrained power allocation for MIMO Wire-tap channels.

[10] Mauro Biagi, Enzo Baccarelli, Nicola Cordeschi, Valentina Polli, Tatiana Patriarca. SDMA with Secrecy Constraints.

[11] Ramy H. Gohary, Yao Huang, Zhi-QuanLuoand Jong-Shi Pang.A Generalized Iterative Water-filling Algorithmfor Distributed Power Control in the Presenceof a Jammer

[12] Wei Yu member IEEE, Wonjong Rhee, Stephen Boyd and John M. Cioffi.Iterative Water-filling for Gaussian Vector Multiple AccessChannels

[13] Wei Yu, Wonjong Rhee, Stephen Boyd, and John M. Cioffi. Iterative Water-filling for Gaussian Vector Multiple AccessChannels

[14] Wei Yu and John M. Cioffi.On Constant Power Water-filling

[15] Gerhard Münz, Stephan Pfletschinger, Joachim Speidel. An Efficient Waterfilling Algorithm for Multiple Access OFDM

[16] Pesamosca Giancarlo. Metodi dell'analisi numerica. Kappa, 1997

[17] A. Paulraj, R. Nabar and D. Gore. Introduction to Space-Time Wireless Communications, Cambridge Univ. Press, May 2003. Reprinted Chinese Ed. 2004, Reprinted Russian Ed. 2007