SAPIENZA
UNIVERSITÀ DI ROMA

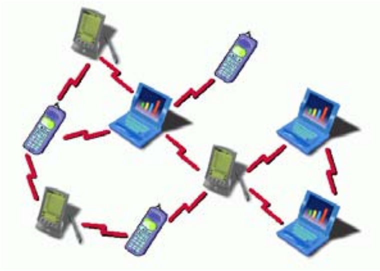
Challenges and limits for Secrecy in Wireless Networks: An information theoretic framework

Mauro Biagi

February 9, 2010

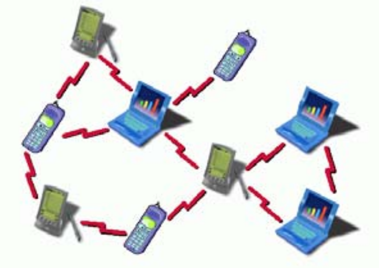
SAPIENZA
UNIVERSITÀ DI ROMA

Ad-hoc networking 1/2



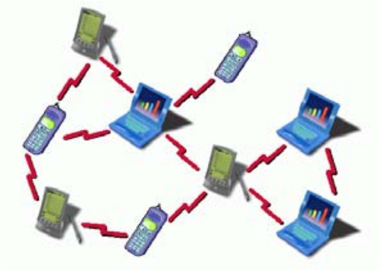
- Wireless multipath connected nodes;

Ad-hoc networking 1/2



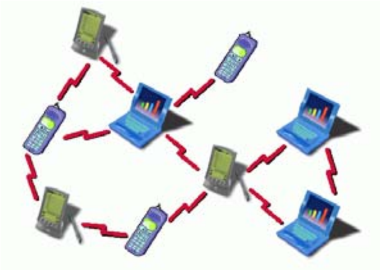
- Wireless multipath connected nodes;
- No network infrastructure;

Ad-hoc networking 1/2



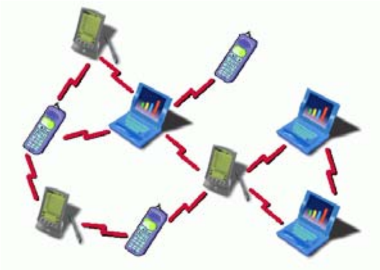
- Wireless multipath connected nodes;
- No network infrastructure;
- "self-creating", "self-organizing" and "self-administering";

Ad-hoc networking 1/2



- Wireless multipath connected nodes;
- No network infrastructure;
- "self-creating", "self-organizing" and "self-administering";
- "anytime, anywhere" ;

Ad-hoc networking 1/2



- Wireless multipath connected nodes;
- No network infrastructure;
- "self-creating", "self-organizing" and "self-administering";
- "anytime, anywhere" ;
- Dynamic topology (new nodes asking access, old nodes leaving network)

Ad-hoc networking 2/2

Problems:

- Access

Ad-hoc networking 2/2

Problems:

- Access
- Routing

Ad-hoc networking 2/2

Problems:

- Access
- Routing
- **Secrecy**

Secrecy in the Literature 1/2

- Shannon introduced “Secrecy” from an information theoretic point of view
- Wyner considered Wiretap channel (WTC) for wireline links
- Csizar and Korner extend the analisys to broadcast channels
- Hellman studied the Gaussian Wire-Tap Channel
- Parada and Blaut considered the Secrecy capacity in Gaussian SISO Wire-Tap Channels

Secrecy in the Literature 2/2

- Ulukus studied MISO WTC
- Negi and Goel tried to transmit in the null-space of the eavesdropper
- Poor introduced a Helper Interferer able to cooperate with reference transmitter

Work Goal 1/2

The main goal is to evaluate how much a communication can preserve confidentiality without cryptography, but only by resorting to waterfilling-like approaches, by paying attention to the information rate both for the main link (Alice-Bob) and the eavesdropping one (Alice-Eve).

Work Goal 2/2

The idea of using MIMO comes from the problem of assuring some secrecy.
With a single antenna system we can use time, frequency of code (CDMA) approaches, but the spatial dimension gives us an added value with respect to secrecy

Scalar model

The sequence at the j-th receive antenna is

$$y_j(n) = \sqrt{\frac{d^{-u}}{t}} \sum_{i=1}^{t} h_{ji} \phi_i(n) + v_j(n), \; 1 \le n \le T, \qquad (1)$$

where the sequences $v_j(n) \triangleq q_j(n) + w_j(n), \; 1 \le j \le r$, account for the overall disturbances (e.g., possible Multiple Access Interference (MAI) plus thermal noise) experienced by the receiver and d is the transmit-receive distance with u the path-loss exponent and T the packet length.

Vector model

The signal vector collected at the r receive antennas

$$\mathbf{y}(n) = \sqrt{\frac{d^{-u}}{t}}\mathbf{H}^T\phi(n) + \mathbf{v}(n), \quad 1 \leq n \leq T, \tag{2}$$

where $\{\mathbf{v}(n) \triangleq [v_1(n)...v_r(n)]^T, \ 1 \leq n \leq T\}$ is the temporally-white spatially-colored Gaussian sequence of disturbances with spatial covariance matrix given by $\mathbf{K}_v \triangleq \mathrm{E}\{\mathbf{v}(n)\mathbf{v}(n)^\dagger\}$ and $\mathbf{H}$ is the $(r \times t)$ matrix collecting the path gains in eq.(1).

Eavesdropper link

$$\mathbf{y}_e(n) = \sqrt{\frac{d_e^{-u}}{t}}\mathbf{H}_e^T\phi(n) + \mathbf{v}_e(n), \quad 1 \leq n \leq T, \qquad (3)$$

where d_e is the distance between Alice and Eve, $\mathbf{H}_e^T$ is the eavesdropping link channel and $\mathbf{v}_e(n)$ is the possible disturbance experienced by Eve (that is different from $\mathbf{v}(n)$) and it can be statistically described by $\mathbf{K}_{v_e} \triangleq \mathrm{E}\{\mathbf{v}_e(n)\mathbf{v}_e(n)^\dagger\}$.

Link quality metric 1/2

The channel capacity is the maximum of the information rate given by

$$I(X,Y) = H(X) - H(X/Y) \tag{4}$$

The information rate depends on the information sent on the channel and that lost in the channel. This suggests to 'operate' at transmit side.

Link quality metric 2/2

The link quality can be evaluated through

$$I(A,B) \cong \log\det\left(\mathbf{I}_r + \frac{d^{-u}}{t}\mathbf{K}_v^{-1/2}\hat{\mathbf{H}}^T\boldsymbol{\Psi}\hat{\mathbf{H}}^*\mathbf{K}_v^{-1/2} + d^{-u}\sigma_{\varepsilon m}^2 P\mathbf{K}_v^{-1}\right) = \sum_{i=1}^{\min(r,t)}\log\left(1+\frac{\psi_i\hat{\lambda}_i^2 + tP\xi_i\sigma_{\varepsilon m}^2}{t}\right) \quad (5)$$

where ξ_i in (5) is the i-th singular value of $d^{-u}\mathbf{K}_v^{-1}$, while $\hat{\lambda}_i^2$ is th i-th singular value accounting for $\mathbf{K}_v^{-1/2}\hat{\mathbf{H}}^T\boldsymbol{\Psi}\hat{\mathbf{H}}^*\mathbf{K}_v^{-1/2}d^{-u}$ and ψ_i is the power allotted on i-th channel mode.

Secrecy Metric

The "insecureness" can be measured by

$$I(A,E) \cong r \log \left(\frac{1 + d_e^{-u} P\sigma_\varepsilon^2 / (Tra(\mathbf{K}_{v_e}))}{(1 + d_e^{-u} P\sigma_\varepsilon^2 / (Tra(\mathbf{K}_{v_e})t))^t} \right)$$

$$+ \log\det \left(\mathbf{I}_r + \frac{d_e^{-u}/(Tra(\mathbf{K}_{v_e}))}{t(1 + d_e^{-u}/(Tra(\mathbf{K}_{v_e})))} \mathbf{K}_{v_e}^{-1/2} \hat{\mathbf{H}}_e^T \boldsymbol{\Psi} \hat{\mathbf{H}}_e^* \mathbf{K}_{v_e}^{-1/2} \right)$$

$$= r \log \left(\frac{1 + d_e^{-u} P\sigma_\varepsilon^2 / (Tra(\mathbf{K}_{v_e}))}{(1 + d_e^{-u} P\sigma_\varepsilon^2 / (Tra(\mathbf{K}_{v_e})t))^t} \right)$$

$$+ \sum_{i=1}^{\min(r,t)} \log \left(1 + \frac{\psi_i a_i}{t(1 + d_e^{-u} P\sigma_\varepsilon^2 / (Tra(\mathbf{K}_{v_e})))} \right) \quad (6)$$

where a_i is the i-th singular value of $d_e^{-u}/(Tra(\mathbf{K}_{v_e}))\mathbf{K}_{v_e}^{-1/2} \hat{\mathbf{H}}_e^T \hat{\mathbf{H}}_e^* \mathbf{K}_{v_e}^{-1/2}$ and σ_ε^2 is the estimation error variance for the A-E link.

Problem formulation 1/3

As previously detailed, we proceed to maximize the main link information rate by maximizing the quantity

$$\max_{\boldsymbol{\psi}} I(A, B). \qquad (7)$$

The maximization is performed subject to the following three constraints

$$\psi_i \geq 0,\ i = 1, ..., \min(r, t) \quad \sum_{i=1}^{\min(r,t)} \psi_i \leq P, \quad I(A, E) \leq \mathfrak{I}. \qquad (8)$$

The first constraint requires that all the power levels ψ_i have to be nonnegative, while the second is about the total power P available for the transmission (according to eq.(3)). Finally, the last constraint requires that the information rate of the eavesdropping link is limited up to the $\mathfrak{I}$ value.

Problem formulation 2/3

This constrained problem can be stated by resorting to methods based on Lagrangian function so as to express the objective function as

$$\Lambda(\boldsymbol{\psi},\alpha,\boldsymbol{\beta},\gamma)=\sum_{i=1}^{\min(r,t)}\log\left(1+\frac{\psi_i\hat{\lambda}_i^2+tP\xi_i\sigma_{\varepsilon m}^2}{t}\right)$$
$$-\alpha\left(\sum_{i=1}^{\min(r,t)}\psi_i-P\right)+\sum_{i=1}^{\min(r,t)}\beta_i\psi_i$$
$$-\gamma\left(r\log\left(\frac{1+d_e^{-u}P\sigma_\varepsilon^2/(Tra(\mathbf{K}_{v_e}))}{(1+d_e^{-u}P\sigma_\varepsilon^2/(Tra(\mathbf{K}_{v_e})t))^t}\right)\right.$$
$$\left.+\sum_{i=1}^{\min(r,t)}\log\left(1+\frac{\psi_i a_i}{t(1+d_e^{-u}P\sigma_\varepsilon^2/(Tra(\mathbf{K}_{v_e})))}\right)-\Im\right). \quad (9)$$

Problem formulation 3/3

The constraint equations related to parameters $\psi_i, \alpha, \beta_i, \gamma$ follow

$$\nabla_{\psi_i}\Lambda(\boldsymbol{\psi}, \alpha, \boldsymbol{\beta}, \gamma) = \frac{g_i}{(1 + Pt\xi_i\sigma^2_{\varepsilon m}) + g_i\psi_i} - \alpha + \beta_i - \gamma\frac{z_i}{1 + z_i\psi_i} = 0, \quad (10)$$

$$\alpha\left(\sum_{i=1}^{\min(r,t)} \psi_i - P\right) = 0, \quad (11)$$

$$\beta_i\psi_i = 0, \; i = 1, ..., \min(r, t) \quad (12)$$

$$\gamma\left(r\log\left(\frac{1 + d_e^{-u}P\sigma^2_\varepsilon/(Tra(\mathbf{K}_{v_e}))}{(1 + d_e^{-u}P\sigma^2_\varepsilon/(Tra(\mathbf{K}_{v_e})t))^t}\right) + \sum_{i=1}^{\min(r,t)} \log\left(1 + \frac{\psi_i a_i}{t(1 + d_e^{-u}P\sigma^2_\varepsilon/(Tra(\mathbf{K}_{v_e})))}\right) - \Im\right) = 0, \quad (13)$$

where we pose $g_i = \hat{\lambda}_i^2/t$ and $z_i = a_i/(t(1 + d_e^{-u}P\sigma^2_\varepsilon/(Tra(\mathbf{K}_{v_e}))))$.

Problem solution 1/4

In order to solve this system composed by non-linear equations, we can adopt the Newton method.
The system can be generally expressed as

$$\begin{cases} f_1(\psi_1, ..., \psi_c, \alpha, \beta_1, ..., \beta_c, \gamma) = 0 \\ f_2(\psi_1, ..., \psi_c, \alpha, \beta_1, ..., \beta_c, \gamma) = 0 \\ ... \\ f_{2c+2}(\psi_1, ..., \psi_t, \alpha, \beta_1, ..., \beta_c, \gamma) = 0 \end{cases} \tag{14}$$

where the functions are related to the above equations and $c = \min(r, t)$.

Problem solution 2/4

After gathering all the variables in the following vector shape

$$\mathbf{s} = [\psi_1, ..., \psi_c, \alpha, \beta_1, ..., \beta_c, \gamma] \quad (15)$$

we can restate the problem as

$$F(\mathbf{s}) = \mathbf{0} \quad (16)$$

where $\mathbf{0}$ is the $(2c+2) \times 1$ null vector and F is the function collecting the elements $f_1, ..., f_{2c+2}$.

Problem solution 3/4

The Newton method aims at solving non-linear equations by an iterative procedure in which the $(k+1)$-th step solution approximation is a function of the (previous) k-th step one

$$\mathbf{s}_{k+1} = \mathbf{\Phi}(\mathbf{s}_k). \tag{17}$$

In this way, from the theory of numerical methods, we can write the iteration relationship as

$$\mathbf{s}_{k+1} = \mathbf{s}_k - \rho_k \mathbf{J}^{-1}(\mathbf{s}_k) F(\mathbf{s}_k), \tag{18}$$

Problem solution 4/4

the parameter ρ_k is determined according to

$$\|F(\mathbf{s}_{k+1})\| = \|F(\mathbf{s}_k - \rho_k \mathbf{J}^{-1}(\mathbf{s}_k)F(\mathbf{s}_k))\|$$

$$= \min_{\rho>0} \|F(\mathbf{s}_k - \rho \mathbf{J}^{-1}(\mathbf{s}_k)F(\mathbf{s}_k))\|, \quad (19)$$

and matrix inversion $\mathbf{J}^{-1}(\mathbf{s}_k)$ is obtained by inverting the Jacobi's matrix

$$\mathbf{J}(\mathbf{s}) \triangleq \begin{bmatrix} f_{1,s_1}(\mathbf{s}) & f_{1,s_2}(\mathbf{s}) & \dots & f_{1,s_{2c+2}}(\mathbf{s}) \\ \dots & \dots & \dots & \dots \\ f_{2c+2,s_1}(\mathbf{s}) & f_{2t+2,s_2}(\mathbf{s}) & \dots & f_{2c+2,s_{2c+2}}(\mathbf{s}) \end{bmatrix}, \quad (20)$$

where the general term $f_{i,s_l}(\mathbf{s})$ is given by $\partial f_i(\mathbf{s})/\partial s_l$.

Problem formulation 1/3

This approach maximizes the secrecy level by minimizing the Alice-Eve link information rate

$$\min_{\boldsymbol{\psi}} I(A, E) \tag{21}$$

by considering as constraints

$$\psi_i \geq 0,\; i = 1, ..., \min(r, t), \quad \sum_{i=1}^{\min(r,t)} \psi_i \leq P, \quad I(A, B) \geq \mathfrak{C}. \tag{22}$$

Differently from the MR case, the last constraint requires for the Alice-Bob link information rate a minimum level of $\mathfrak{C}$.

Problem formulation 2/3

We proceed, also in this case, by considering the Lagrangian function that is represented by the following expression

$$\Upsilon(\boldsymbol{\psi},\theta,\boldsymbol{\kappa},\nu) = r\log\left(\frac{1+d_e^{-u}P\sigma_\varepsilon^2/(Tra(\mathbf{K}_{v_e}))}{(1+d_e^{-u}P\sigma_\varepsilon^2/(Tra(\mathbf{K}_{v_e})t))^t}\right)$$

$$+\sum_{i=1}^{\min(r,t)}\log\left(1+\frac{\psi_i a_i}{t(1+d_e^{-u}P\sigma_\varepsilon^2/(Tra(\mathbf{K}_{v_e})))}\right)$$

$$+\theta\left(\sum_{i=1}^{\min(r,t)}\psi_i - P\right)$$

$$-\sum_{i=1}^{\min(r,t)}\kappa_i\psi_i - \nu\left(\sum_{i=1}^{\min(r,t)}\log\left(1+\frac{\psi_i\hat{\lambda}_i^2+tP\xi_i\sigma_{\varepsilon m}^2}{t}\right)-\mathfrak{C}\right). \quad (23)$$

Problem formulation 3/3

By considering derivative and constraints (Lagrange multipliers) we arrive at the non-linear system-equations described by the following four relationships

$$\nabla_{\psi_i} \Upsilon(\boldsymbol{\psi}, \theta, \boldsymbol{\kappa}, \nu) = \frac{z_i}{1 + z_i \psi_i} - \theta - \kappa_i - \nu \frac{g_i}{(1 + Pt\xi_i \sigma_\varepsilon^2) + g_i \psi_i} = 0, \quad (24)$$

$$\theta \left(\sum_{i=1}^{\min(r,t)} \psi_i - P \right) = 0, \quad (25)$$

$$\kappa_i \psi_i = 0, \; i = 1, \ldots, \min(r,t), \quad (26)$$

$$\nu \left(\sum_{i=1}^{\min(r,t)} \log \left(1 + \frac{\psi_i \hat{\lambda}_i^2 + tP\xi_i \sigma_\varepsilon^2}{t} \right) - \mathfrak{C} \right) = 0. \quad (27)$$

Interference Mitigation

By considering Eve as a smart node, since it is reasonable that it is equipped with additional modules for acquiring information, we assume that it is capable to spatially process information. This capability directly leads to a eavesdropper's rate increment due to the potential implementation of an interference mitigator.

Interference Mitigation details 1/2

Hence, the information rate of $I(A, E)$ link is now given by

$$I(A,E) \cong r \log\left(\frac{1 + d_e^{-u} P\sigma_\varepsilon^2 / (Tra(\mathbf{K}_{v_\varepsilon}))}{(1 + d_e^{-u} P\sigma_\varepsilon^2 / (Tra(\mathbf{K}_{v_\varepsilon})t))^t}\right)$$

$$+ \log\det\left(\mathbf{I}_r + \frac{d_e^{-u}/(Tra(\mathbf{K}_{v_\varepsilon}))}{t(1 + d_e^{-u}/(Tra(\mathbf{K}_{v_\varepsilon})))}\mathbf{K}_{v_\varepsilon}^{-1/2}\hat{\mathbf{H}}_e^T \mathbf{\Psi} \hat{\mathbf{H}}_e^* \mathbf{K}_{v_\varepsilon}^{-1/2}\right) \quad (28)$$

interference mitigation details 2/2

where the matrix $\mathbf{K}_{v_\varepsilon}$ is given by

$$\mathbf{K}_{v_\varepsilon} = (\mathbf{I}_r - \mathbf{Q})\mathbf{K}_{v_e}, \tag{29}$$

being $\mathbf{Q}$

$$\mathbf{Q} = \left\{ \frac{d_e^{-u}}{t} \left[\hat{\mathbf{H}}_e^T \mathbf{\Psi} \hat{\mathbf{H}}_e^* + t\sigma_\varepsilon^2 \mathbf{I}_r \right] \mathbf{K}_{v_e}^{-1} + \mathbf{I}_r \right\}^{-1}. \tag{30}$$

Interference Mitigation comments

Enabling this Interference Mitigation (IM) opportunity for the eavesdropper, does not influence on the links between Carol and Dave or Alice and Bob, since it is performed only at Eve side. It is important to stress that, when considering the possible secrecy loss induced by an IM module, solutions like MR and MS acquire more importance, since they are conceived to increase confidentiality.

SAPIENZA
UNIVERSITÀ DI ROMA

WF-vs.-MR

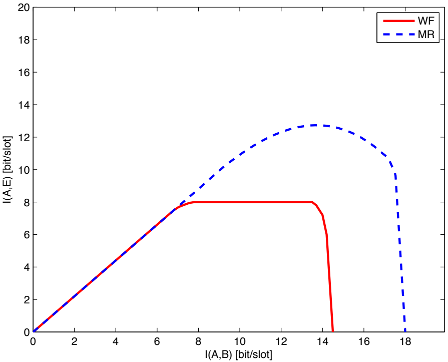


Figure: Information-secrecy region for standard Waterfilling approach and Maximum Rate Algorithm ($t = r = 4, \sigma^2_{\varepsilon m} = 0.1, \sigma^2_{\varepsilon} = 0.7$).

WF-vs.-MR (crypto regions)

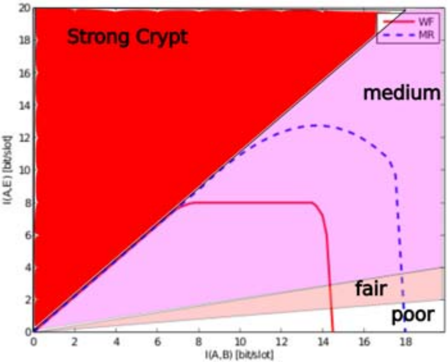


Figure: Information-secrecy region for standard Waterfilling approach and Maximum Rate Algorithm ($t = r = 4, \sigma^2_{\varepsilon m} = 0.1, \sigma^2_{\varepsilon} = 0.7$).

SAPIENZA UNIVERSITÀ DI ROMA

WF-vs.-MS

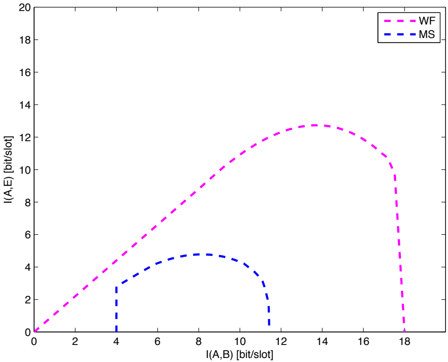


Figure: Information-secrecy region for standard Waterfilling approach and Maximum Secrecy Algorithm ($t = r = 4, \sigma^2_{\varepsilon m} = 0.1, \sigma^2_{\varepsilon} = 0.7$).

WF-vs.-MS with interference

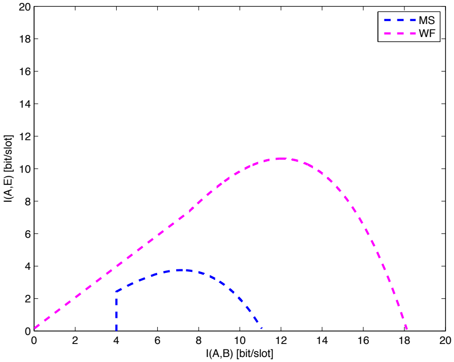


Figure: Information-secrecy region for standard Waterfilling approach and Maximum Secrecy Algorithm when Carol-Dave (interference) link is active ($t = r = 4, \sigma^2_{\varepsilon m} = 0.1, \sigma^2_{\varepsilon} = 0.7$).

MS with interference mitigator

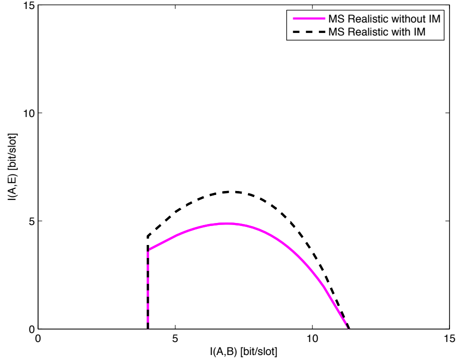


Figure: Information-secrecy region Maximum Secrecy Algorithm when Carol-Dave (interference) link is active and IM is performed by Eve ($t = r = 4, \sigma^2_{\varepsilon m} = 0.1, \sigma^2_{\varepsilon} = 0.7$).

Comparison

	WF_R	WF_S	MR_R	MR_S	MS_R	MS_S
t=r=2	8.8	6.15	8.2	3	5.9	1.5
t=r=4	18	12.5	14.3	8	11.4	5.1
t=r=6	24.13	19.6	19.7	8	18.3	6.3
t=r=8	33.7	28.5	27.8	8	26.2	7.9

Table: Maximum information and secrecy rates for different antenna configurations.

Multi-user case

N	Rate_{MR}	Sec_{MR}	Rate_{MS}	Sec_{MS}	Rate_{WF}	Sec_{WF}
1	14.3	8	11.4	4.53	18	14
2	12.2	8	10.9	3.89	17.2	12.5
3	11.7	8	9.87	3.52	16.38	11.88
4	10.96	7.12	9.16	3.21	14.95	11.02
5	9.78	6.19	8.75	2.96	14.03	10.86
6	9.11	5.43	8.31	2.61	13.21	10.42
7	8.76	4.62	7.9	2.22	11.16	9.87
8	8.13	4.02	7.56	1.97	9.93	9.23

Table: Average rate per transmit/receive pair and secrecy level

An examination of the Table shows that the WF, for increasing number of users, is the best approach from a rate point of view even if the gain with respect to the other methods tends to reduce when the number of transmit/receive pairs N increases and, more, it does not care of possible eavesdropping.

Conclusions

- The solutions we pursued in this work modify the WF performances and, moreover, requires different procedures in order to solve the problem.
- The numerical results show that by introducing the new constraints implies to lose in the main link (Alice-Bob) information rate, but, at the same time, allows a good level of secrecy.
- This is also true when the presence of interference is considered. In fact the presence of an UH is able to increase the secrecy level, both for the standard approaches and the presented ones.

SAPIENZA UNIVERSITÀ DI ROMA

Future Investigations

Possible future works on this topic will deal with

- integration between these results and cryptography
- integration with access
- integration with routing