# Physical layer secrecy in wireless systems with multiple antennas

Vinay Prabhu
Miguel.R.D.Rodrigues
Instituto de Telecomunicacoes
Dept. of Computer Science, University of Porto, Portugal

# Organisation of the talk

- **Scenario Description :**

*What is Physical layer Security all about?*

- **System model:**

*The Rayleigh fading SISOME/SIMOSE models*

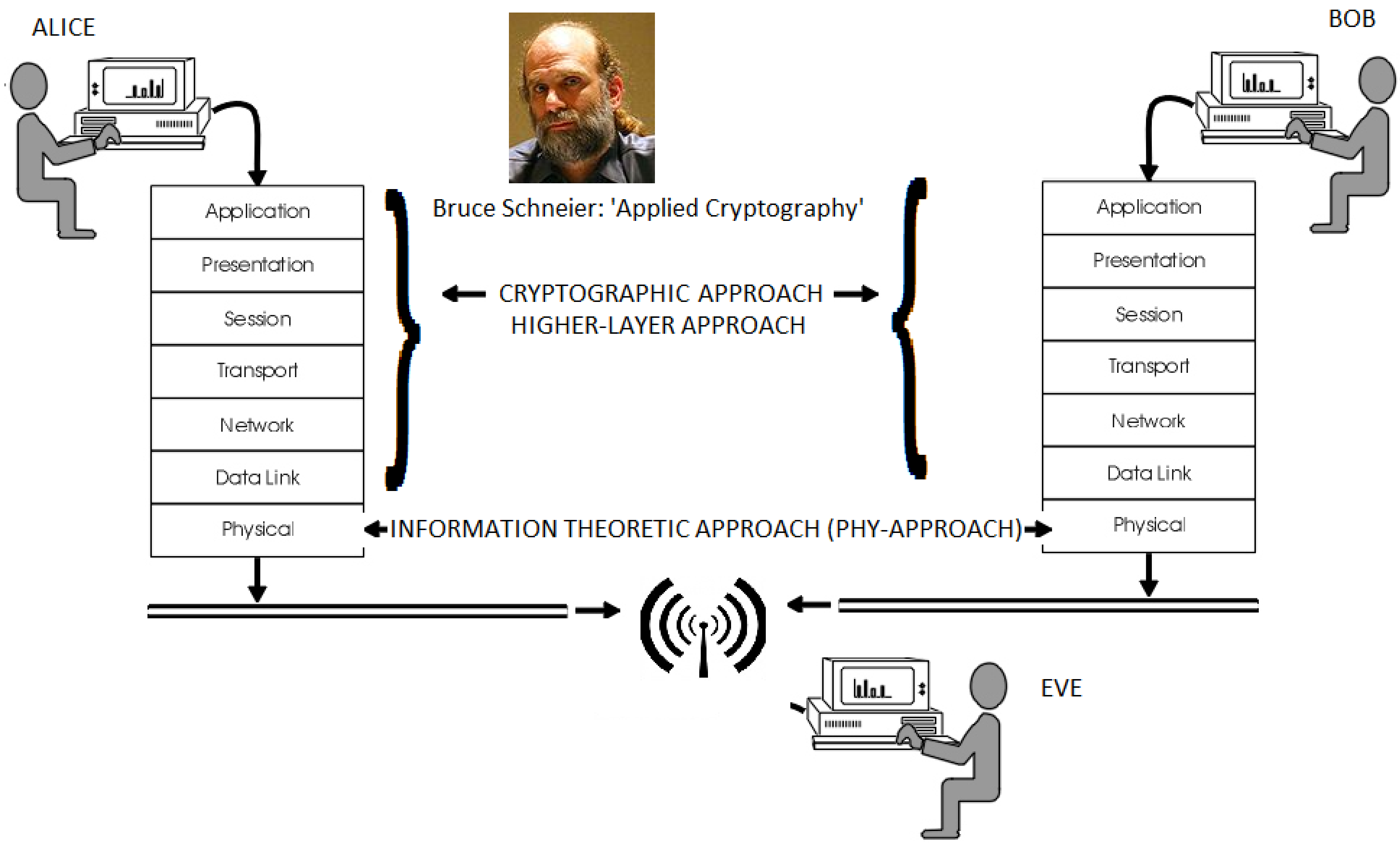
- **Definition of parameters of interest:**

*Probability of existence and Outage; Outage Secrecy capacity*

- **Main results**
- **Conclusions**

# Scenario Description and Problem Formulation:

*The jargon of Alice, Bob and the evil Eve ...*



# Scenario Description and Problem Formulation:

*The two approaches ...*

ACHIEVING SECURITY

CRYPTOGRAPHIC APPROACH
HIGHER-LAYER APPROACH
COMPUTATIONAL SECRECY

Use of block ciphers

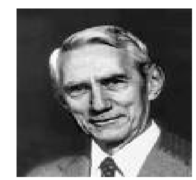
Advanced Encryption Standard (AES) (Rijndael block cipher)
Vincent Rijmen, Joan Daemen

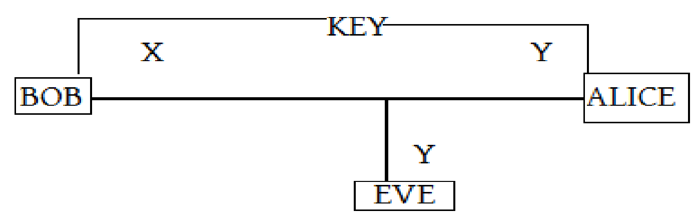
Cryptographic protocols: Transport Layer Security (TLS) and Secure Sockets Layer (SSL)

IPsec and Network Layer Security Protocol (NLSP) at the Internet Layer

INFORMATION THEORETIC APPROACH
(PHY-APPROACH)
PERFECT SECRECY

C. E. Shannon, *Communication theory of secrecy systems*, Bell System Technical Journal, vol. 28, pp. 656–715, Oct. 1949.



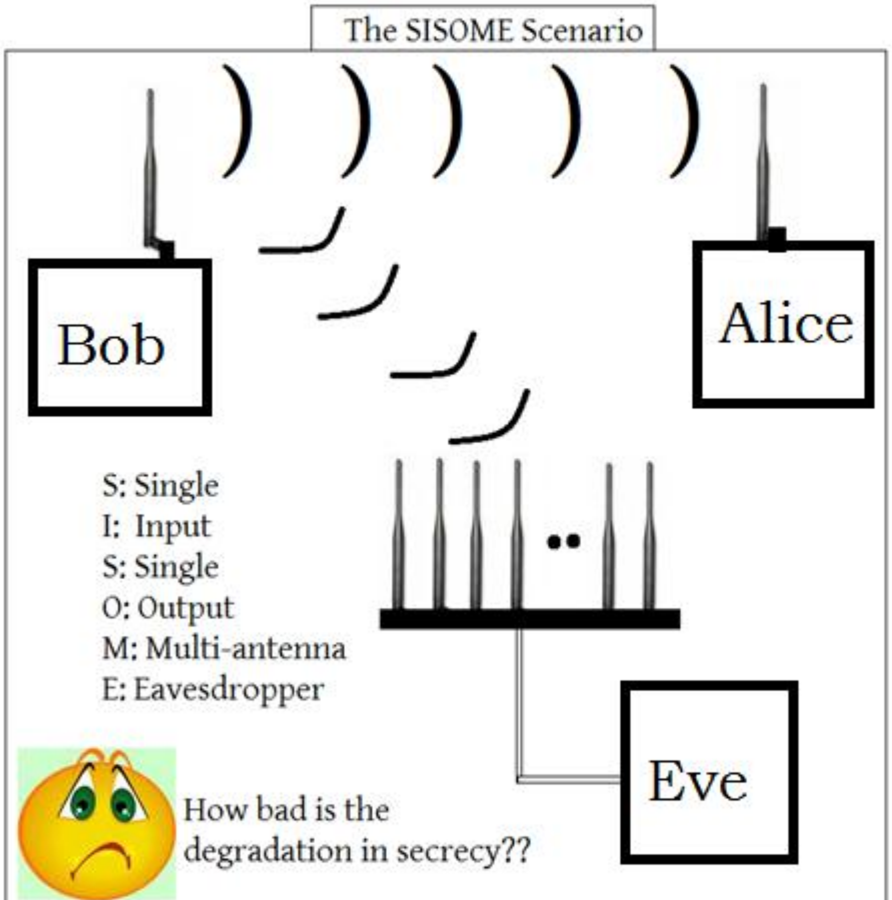


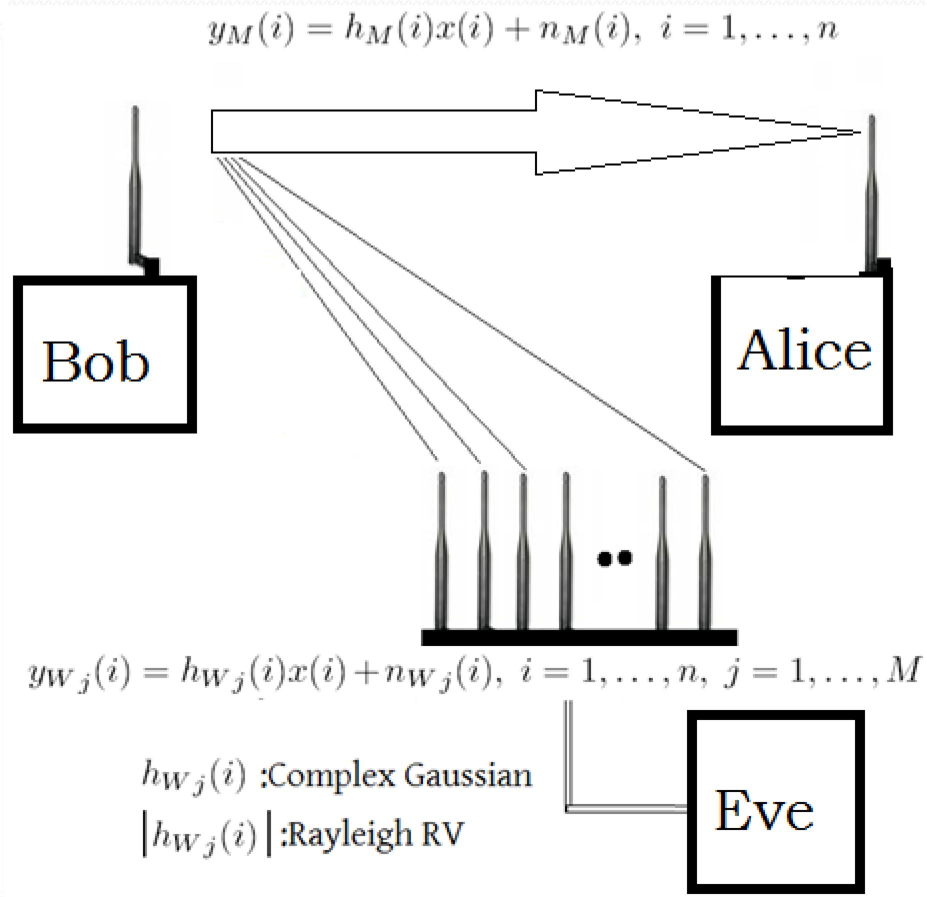

$$H(X|Y)=H(X)$$

- A related-key attack can break 256-bit AES with a complexity of $2^{119}$
- 192-bit AES can also be defeated in a similar manner, but at a complexity of $2^{176}$

# System model:

## *The Rayleigh fading SISOME/SIMOSE models*

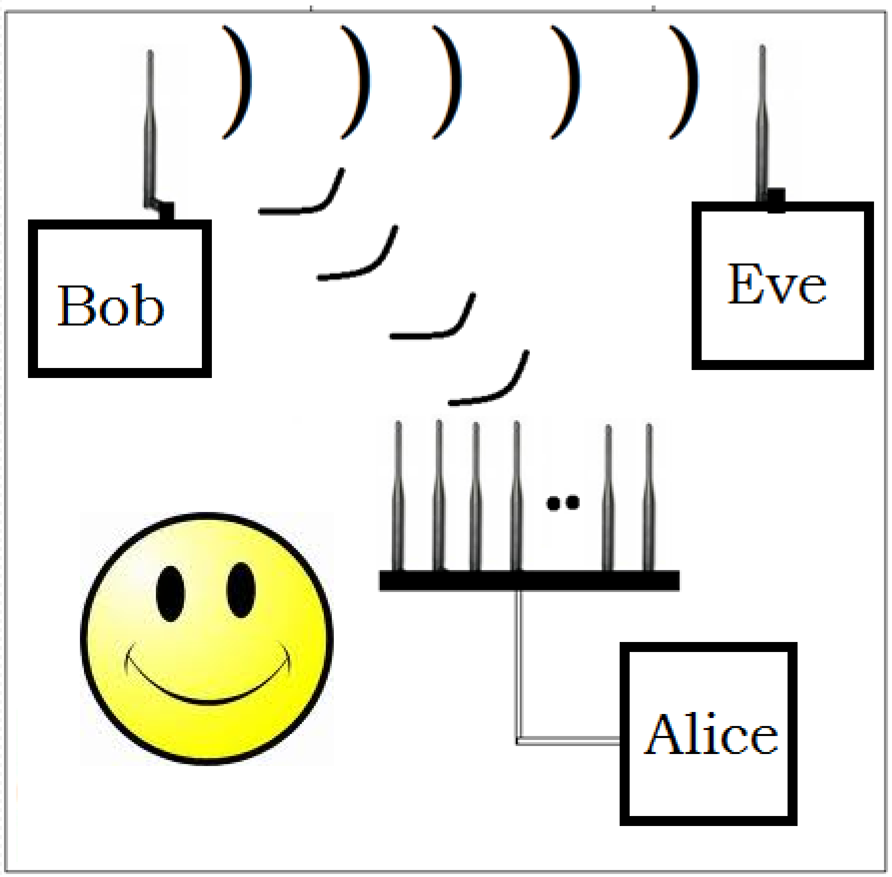


# System model:

## *The Rayleigh fading SISOME/SIMOSE models*

SIMOSE SCENARIO




By what degree did the secrecy 'improve'?

$$i = 1, \dots, n,$$

$$y_W(i) = h_W(i)x(i) + n_W(i),$$

$$y_{M\,j}(i) = h_{W\,j}(i)x(i) + n_{M\,j}(i),$$

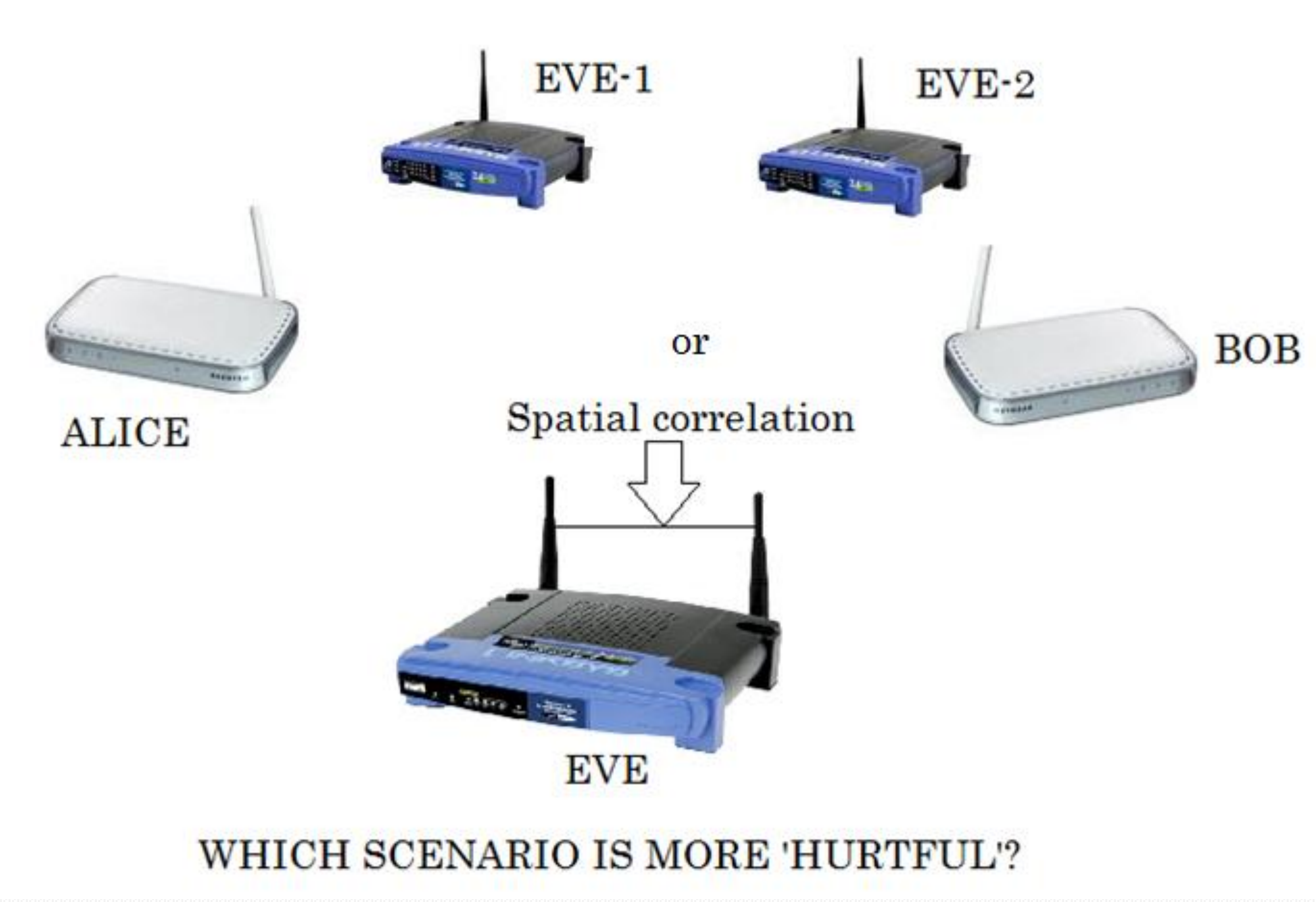
$$j = 1, \dots, M$$

# .... Other comparison scenarios...

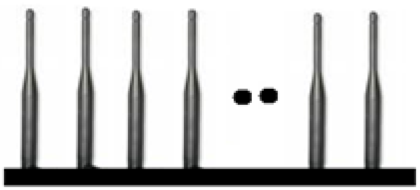
Outdoor-seated main Rx: Purely Rayleigh

Indoor-seated Eavesdropper: Rician with strong LOS

# ....OTHER COMPARISON SCENARIOS ...



# SDC AND MRC reception at the eavesdropper



$h_{W_j}(i)$ :Complex Gaussian

$|h_{W_j}(i)|$ :Rayleigh RV

$$y_{W_j}(i) = h_{W_j}(i)x(i) + n_{W_j}(i),\ i = 1, \ldots, n,\ j = 1, \ldots, M$$

**Selection Diversity Combining**

$$p = \arg\max \{\gamma_{W_j}(i)\}_{j=1}^{M}$$

$$\hat{x}_{SDC}(i) = \mathbf{e}_p(i)\mathbf{y}_W(i)$$

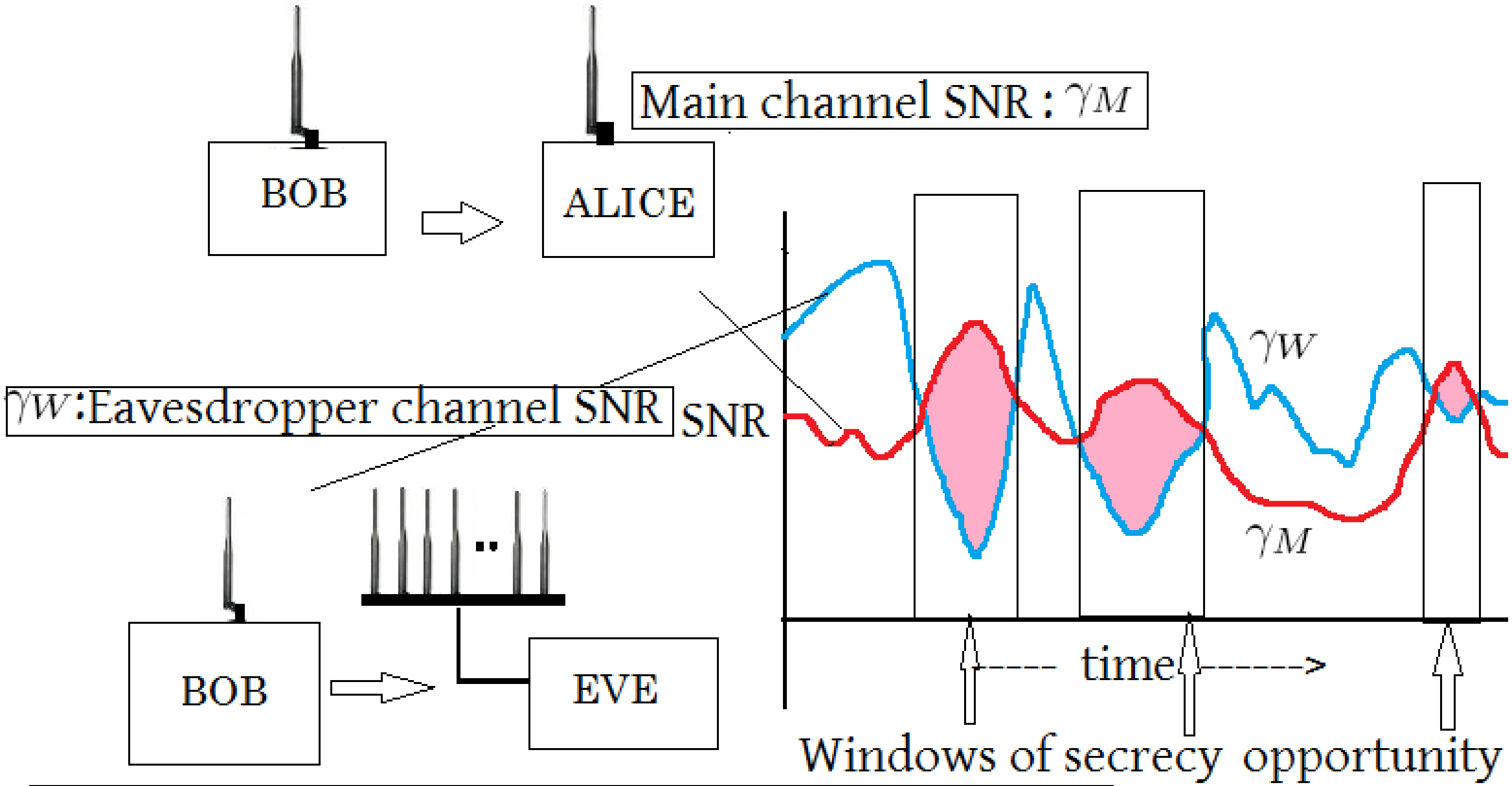
* Very practical
* Requires no channel knowledge

**Maximum Ratio Combining**

$$\hat{x}_{MRC}(i) = \frac{\mathbf{h}_W^H(i)\mathbf{y}_W(i)}{\|\mathbf{h}_W\|}$$

* Requires perfect channel knowledge
* Hard to implement
* Provides worst-case scenario

# An opportunistic secrecy achieving scheme



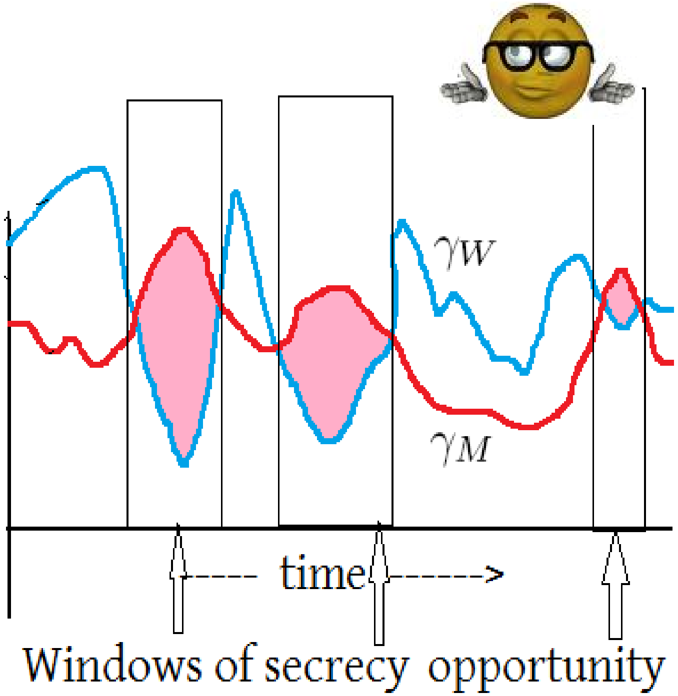

$$
\begin{aligned}
C_s &= \log(1+\gamma_M) - \log(1+\gamma_W), & \gamma_M \geq \gamma_W \\
C_s &= 0, & \gamma_M < \gamma_W
\end{aligned}
$$

## Secrecy Capacity of Wireless Channels


João Barros
Department of Computer Science & LIACC/UP
Universidade do Porto, Portugal
http://www.dcc.fc.up.pt/~barros

Miguel R. D. Rodrigues
Computer Laboratory
University of Cambridge, United Kingdom
http://www.cl.cam.ac.uk/Research/DTG/~mrdr3/

# Secrecy parameters of interest




How often? Whats its worth ?? How about outage???

1: Probability of existence of a non-zero secrecy capacity:

$$P_{ex} = P(C_s > 0) = P(\gamma_M > \gamma_W)$$

2: Probability of outage of the secrecy capacity for a target secrecy rate

$$P_{out}(R_s) = P(C_s < R_s)$$

3: $\varepsilon$-outage secrecy capacity, which is the largest secrecy rate such that the Probability of outage is less than or equal to $\varepsilon$.

$$P_{out}(C_{out}(\varepsilon)) = \varepsilon$$

# Secrecy parameters of interest

$$P_{ex} = \int_{\gamma_M=0}^{\infty} \int_{\gamma_W=0}^{\gamma_M} p(\gamma_M, \gamma_W) d\gamma_W d\gamma_M$$

$$P_{out}(R_s) = 1 - \int_{\gamma_W=0}^{\infty} \int_{\gamma_M=\ 2^{R_s}\cdot(\gamma_M+1)-1}^{\infty} p(\gamma_M) \cdot p(\gamma_W) d\gamma_M d\gamma_W$$

$$P_{ex} = 1 - P_{out}(0)$$

$$P_{out}(C_{out}(\varepsilon)) = \varepsilon$$

# The PDFs …

| |
|---|
| $p(\gamma_M) = \frac{1}{\bar{\gamma}_M} \cdot e^{\frac{-\gamma_M}{\bar{\gamma}_M}}$ |
| $p_{MRC}(\gamma_W) = \frac{\gamma_W^{M-1}}{(M-1)!\bar{\gamma}_W^M} \cdot e^{\frac{-\gamma_W}{\bar{\gamma}_W}}$ |
| $p_{SDC}(\gamma_W) = \frac{1}{\bar{\gamma}_W} \cdot M \cdot (1 - e^{\frac{-\gamma_W}{\bar{\gamma}_W}})^{M-1} \cdot e^{\frac{-\gamma_W}{\bar{\gamma}_W}}$ |

# Effect of introduction of the eavesdropper

$$P_{ex} = \frac{\bar{\gamma}_M}{0 + \bar{\gamma}_M} = 1$$

$$P_{out}(R_s) = 1 - e^{\frac{-(2^{R_s}-1)}{\bar{\gamma}_M}}$$

$$P_{ex} = \frac{\bar{\gamma}_M}{\boxed{\bar{\gamma}_W} + \bar{\gamma}_M}$$

$$P_{out} = 1 - e^{\frac{-(2^{R_s}-1)}{\bar{\gamma}_M}} \boxed{\left(\frac{\bar{\gamma}_M}{2^{R_s}\bar{\gamma}_W + \bar{\gamma}_M}\right)}$$

# ....with M-antenna eavesdroppers..

$$P_{ex} = \frac{\bar{\gamma}_M}{\boxed{\bar{\gamma}_W} + \bar{\gamma}_M} = \frac{1}{(1+r)}$$

$$P_{out}(R_s) = 1 - e^{\frac{-\left(2^{R_s}-1\right)}{\bar{\gamma}_M}} \boxed{\frac{1}{(1+r')}}$$

$$r = \bar{\gamma}_W / \bar{\gamma}_M \qquad r' = \frac{2^{R_s}\bar{\gamma}_W}{\bar{\gamma}_M}$$

$$P_{ex,MRC} = \frac{\bar{\gamma}_M}{\boxed{\bar{\gamma}_W} + \bar{\gamma}_M} = \frac{1}{(1+r)}^{\boxed{M}}$$

$$P_{out,MRC}(R_s) = 1 - e^{\frac{-\left(2^{R_s}-1\right)}{\bar{\gamma}_M}} \boxed{\frac{1}{(1+r')}}^{\boxed{M}}$$

$$P_{ex,SDC} = r.B(M+1,r) = \prod_{k=1}^{M} \frac{k}{(k+r)}$$

$$P_{out,SDC}(R_s) = 1 - e^{\frac{-\left(2^{R_s}-1\right)}{\bar{\gamma}_M}} \boxed{\prod_{k=1}^{M} \frac{k}{(k+r')}}$$

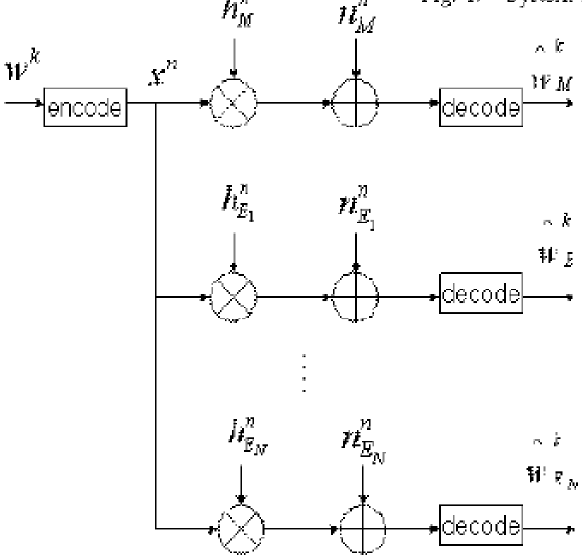
# M-antenna SDC = M independent eavesdroppers

ISIT2007, Nice, France, June 24 – June 29, 2007

## On the Secrecy Capacity of Fading Wireless Channel with Multiple Eavesdroppers

Peiya Wang, Guanding Yu, and Zhaoyang Zhang

Fig. 1. System Model




$$\theta = \bar{\gamma}_E/\bar{\gamma}_M.$$

$$\Pr(C_s > 0) = \prod_{i=1}^{N} \frac{1}{\bar{\gamma}_E} \frac{i}{\frac{i}{\bar{\gamma}_E} + \frac{1}{\bar{\gamma}_M}} = \prod_{i=1}^{N} \frac{i}{\theta + i}.$$

$$P_{out}(R_s) = 1 - \exp\left(-\frac{2^{R_s} - 1}{\bar{\gamma}_M P}\right) \prod_{i=1}^{N} \frac{i}{2^{R_s}\theta + i}.$$

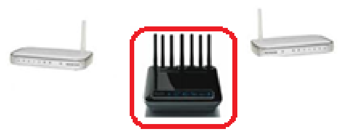
$$P_{ex,SDC} = r.B(M+1, r) = \prod_{k=1}^{M} \frac{k}{(k+r)}$$

$$P_{out,SDC}(R_s) = 1 - e^{\frac{-(2^{R_s}-1)}{\bar{\gamma}_M}} \boxed{\prod_{k=1}^{M} \frac{k}{(k+r')}}$$

M independent single antenna eavesdroppers

M-antenna SDC eavesdropper

# Single M-antenna eavesdropper is potentially more effective than M- single antenna eavesdroppers



M-antenna MRC eavesdropper

$$d_{ex} = \frac{P_{ex,SDC}}{P_{ex,MRC}} \geqslant 1$$

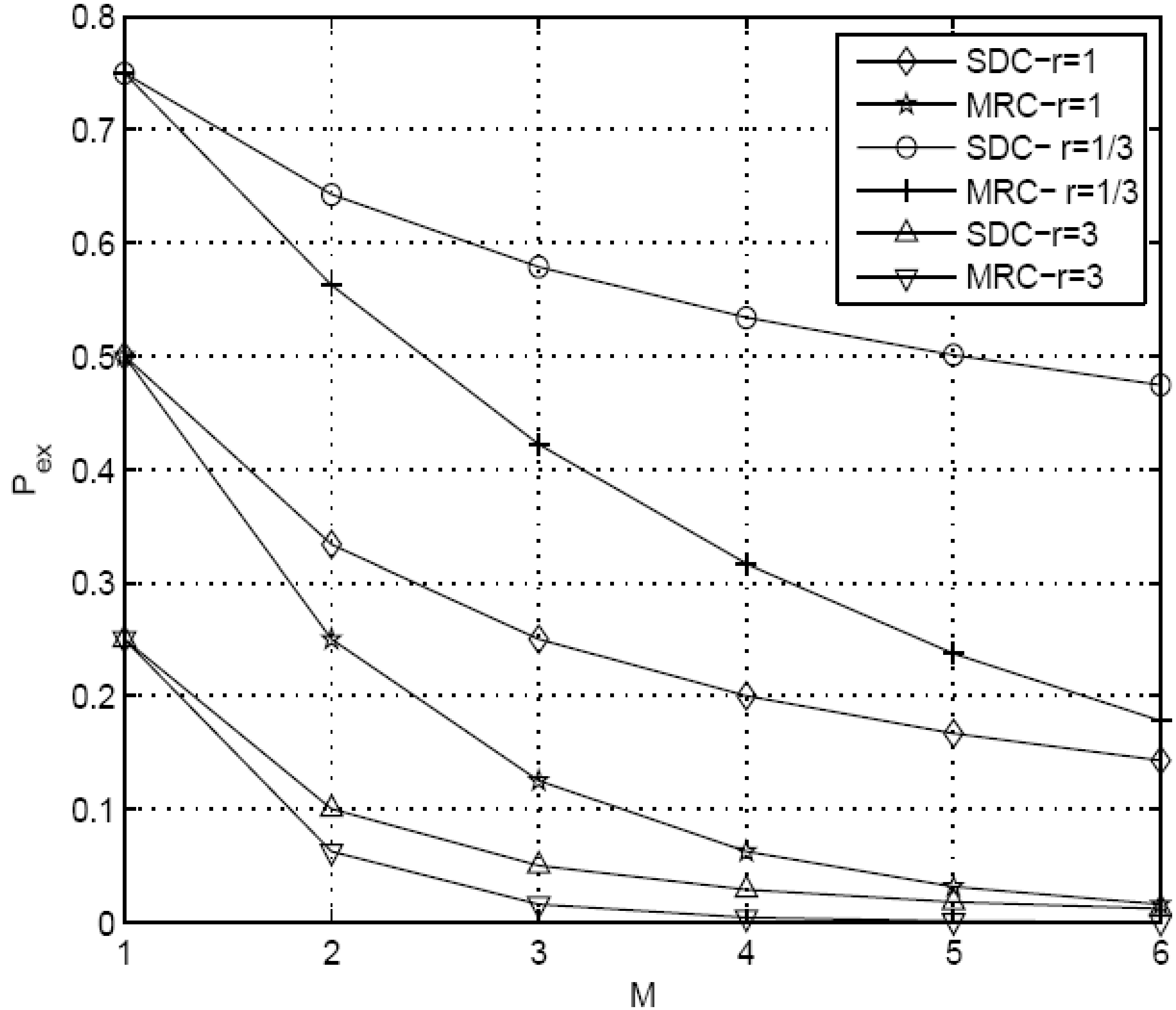
$$P_{ex,SDC} \geqslant P_{ex,MRC}$$

$$P_{out,MRC} \geqslant P_{out,SDC}$$

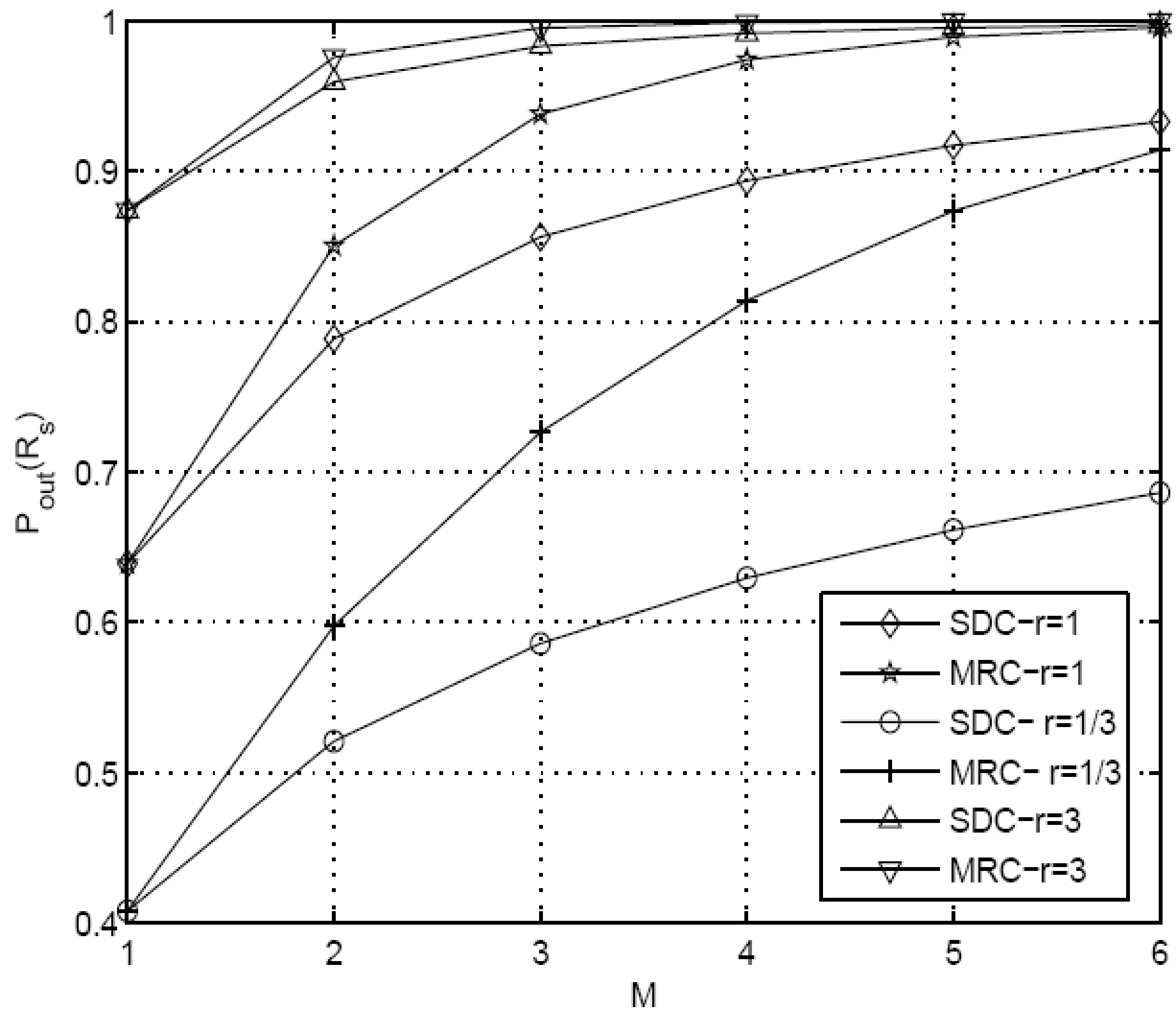
M independent single antenna eavesdroppers

$\equiv$

M-antenna SDC eavesdropper



Variation of probability of existence of secrecy capacity with respect to number of eavesdropper antennas ($\bar{\gamma_M} \in \{1, 1/3\}$ and $\bar{\gamma_W} \in \{1, 1/3\}$)



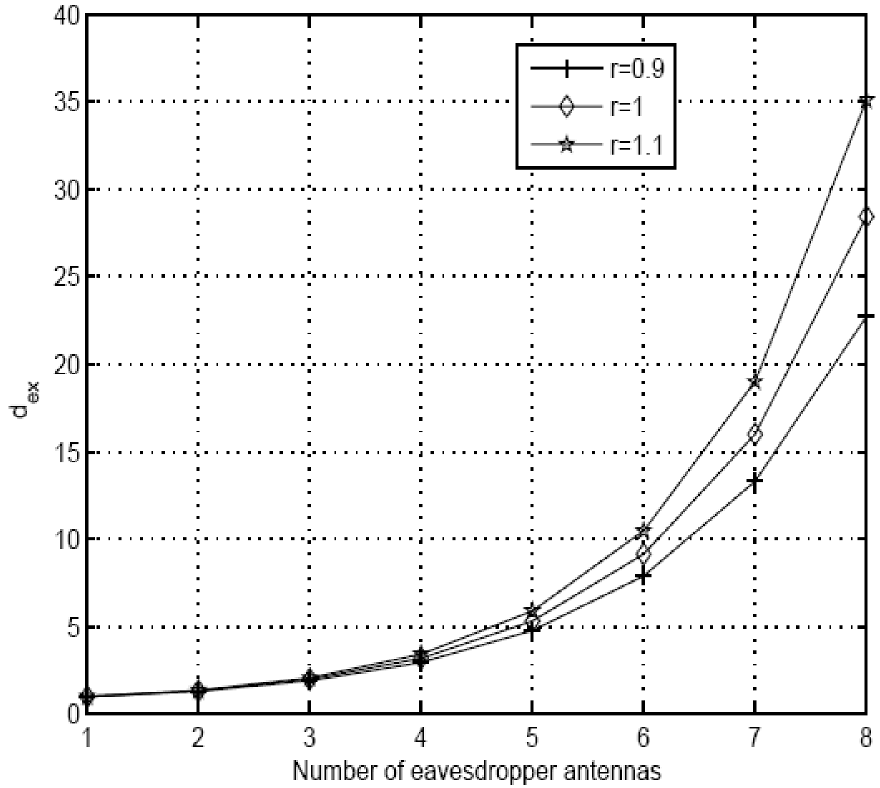

Variation of outage probability with respect to number of eavesdropper antennas $(\gamma_{\bar{M}} \in \{1, 3\}$ , $\gamma_{\bar{W}} \in \{1, 3\})$ and $\dot{R} = 0.5$

# Asymptotic analysis ...

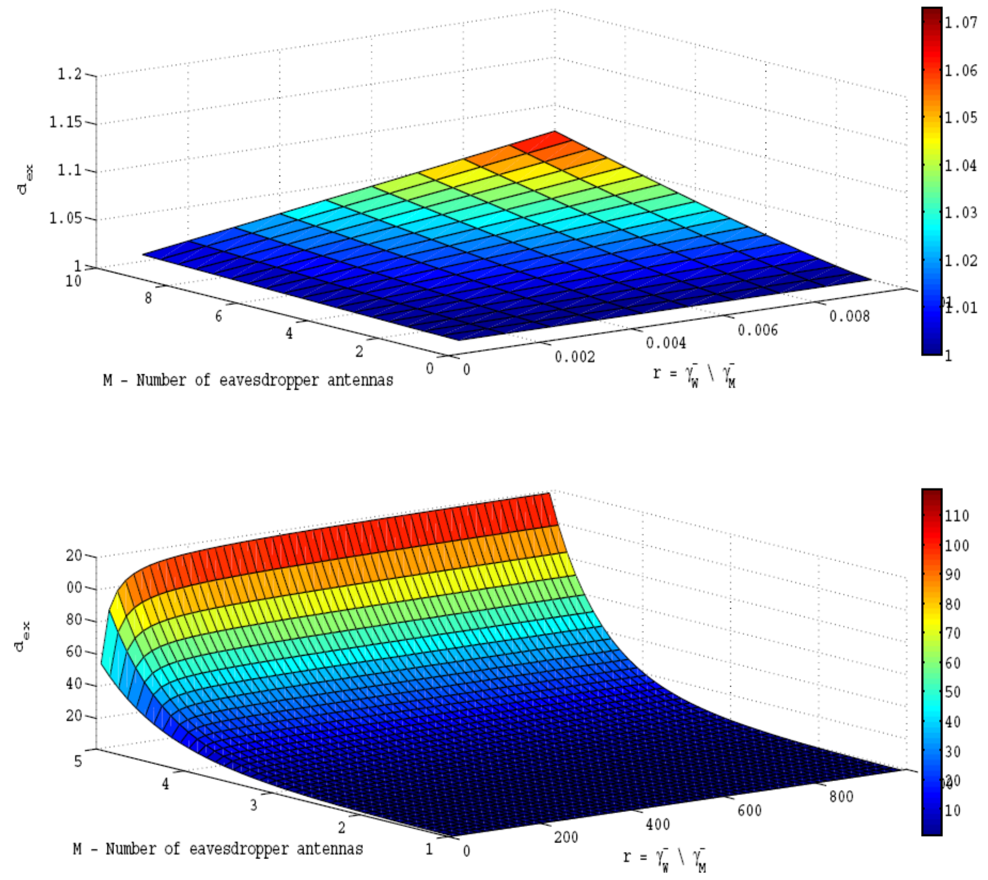
$$\lim_{r\to 1}\{d_{ex}\} = \frac{2^M}{(M+1)}$$

$$\lim_{r\to\infty}\{d_{ex}\} = M! \quad \bar{\gamma}_W >> \bar{\gamma}_M$$

$$\lim_{r\to 0}\{d_{ex}\} = (1+\frac{M}{r}) \quad \bar{\gamma}_W << \bar{\gamma}_M$$



# ...Transition from linear dominance to factorial dominance...



# Outage secrecy capacities ....

$$SISOSE:$$

$$C_{out}(\varepsilon) = \log_2(1+\varepsilon\overline{\gamma}_M) - \log_2(1+(1-\varepsilon)\overline{\gamma}_W)$$

$$SISOME-MRC:$$

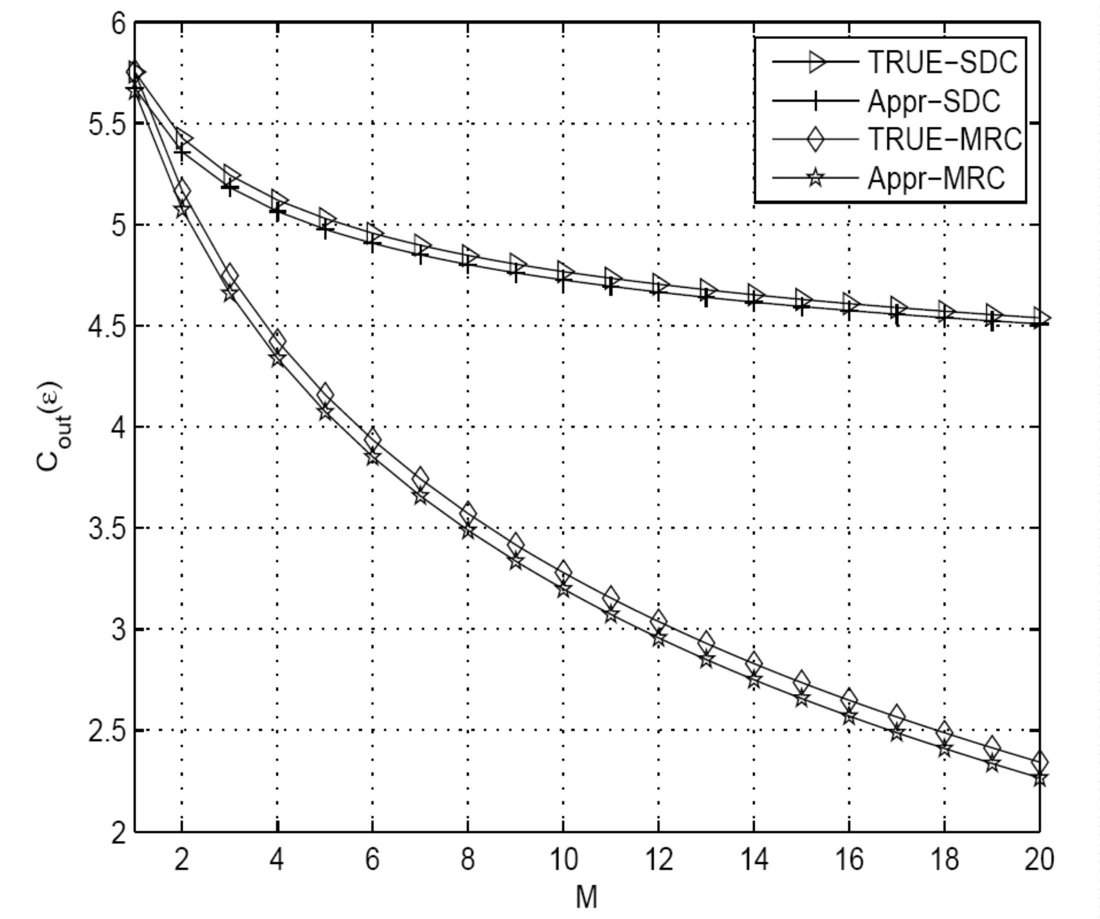
$$C_{out}(\varepsilon) = \log_2(1+\varepsilon\overline{\gamma}_M) - \log_2(1+(1-\varepsilon)\boxed{M}\,\overline{\gamma}_W)$$

$$SISOME-SDC/M\ eavesdroppers:$$

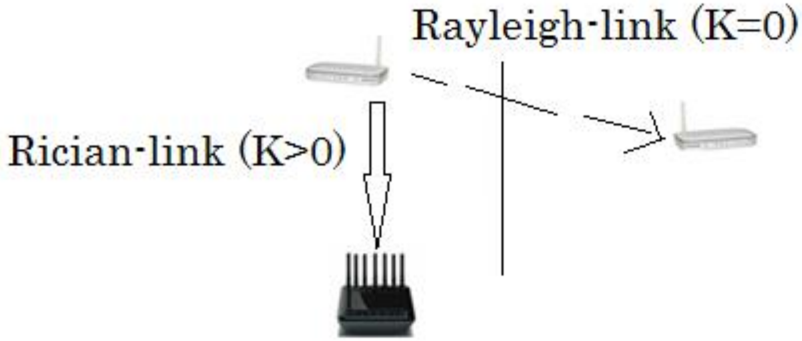
$$C_{out}(\varepsilon) = \log_2(1+\varepsilon\overline{\gamma}_M) - \log_2(1+(1-\varepsilon)\boxed{K}\,\overline{\gamma}_W)$$

$$K = \sum_{n=1}^{M}\left(\frac{1}{n}\right), K \approx \ln(M)$$

# Secrecy capacity comparisons..



# Most hostile scenario …




M-antenna MRC eavesdropper

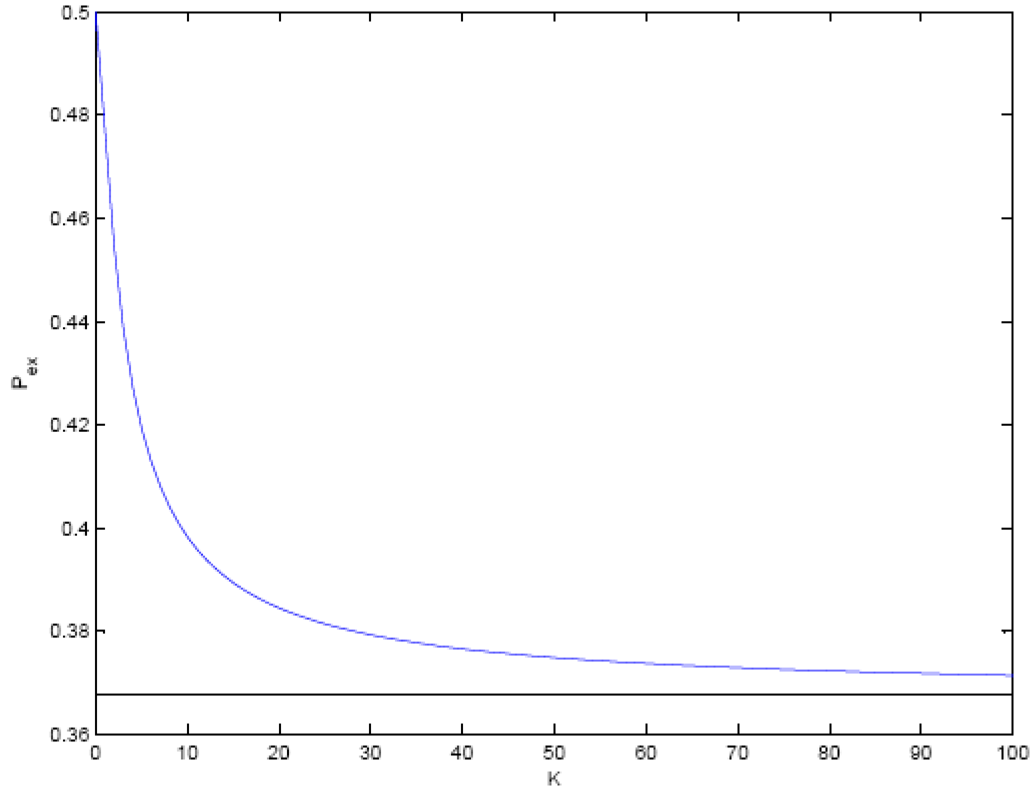
Outdoor-seated main Rx: Purely Rayleigh
Indoor-seated Eavesdropper: Rician with strong LOS

$$P_{ex,MRC,Rice} = \left\{ \left( \frac{K+1}{K+1+r} \right) e^{-\left(\frac{Kr}{K+1+r}\right)} \right\}^{M}$$

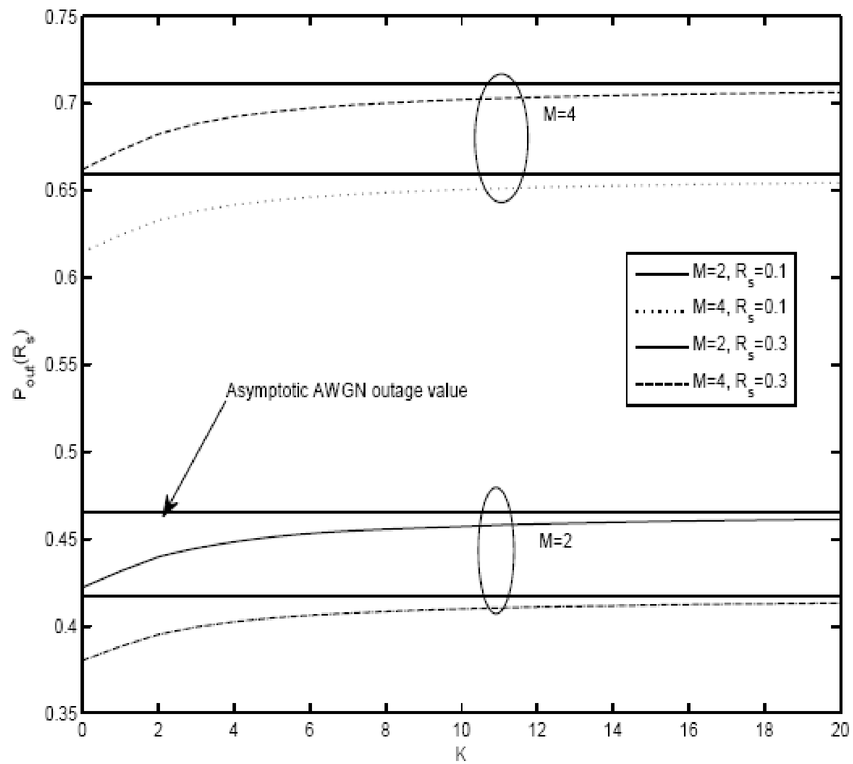
$$P_{out,MRC,Rice}(R_s) = 1 - e^{-\left(\frac{2^{R_s}-1}{\bar{\gamma}_M}\right)} \Phi_{MRC}(K, r', M)$$

$$\Phi_{MRC}(K, r', M) = \left\{ \left( \frac{K+1}{K+1+r'} \right) e^{-\left(\frac{Kr'}{K+1+r'}\right)} \right\}^{M}$$

# Effect of the Rician factor …

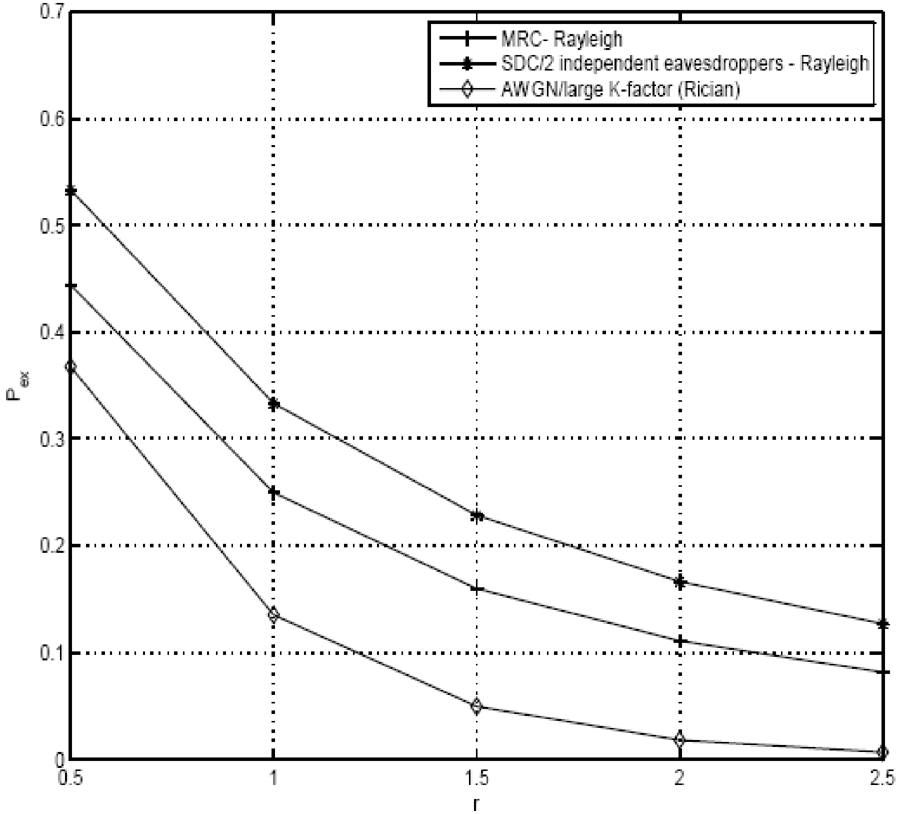


# Almost as if the eavesdropper had an AWGN link with the transmitter...




Comparison of outage probability versus the Rician factor $K$ for varying number of eavesdropper antennas

# Overall comparison …




Comparison of probability of existence versus the average SNR ratio $r$ for the Ricean and Rayleigh fading scenarios

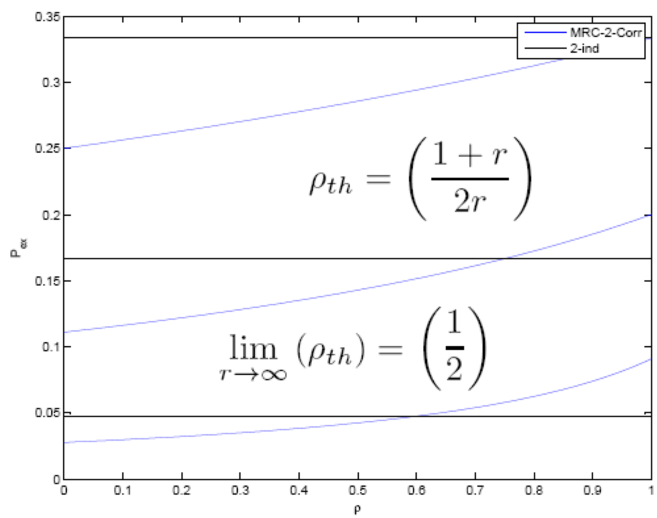
# Effect of spatial correlation between the eavesdropper antennas – The SISO2E system


$$P_{ex,MRC,2-corr} = \frac{1}{1 + r^2(1-\rho) + 2r}$$

$$P_{ex,SDC,2-corr} = \frac{2}{(1+r)(2+r(1-\rho))}$$

# 2 independent eavesdroppers VS one 2-antenna eavesdropper (with antenna correlation)

| | |
|---|---|
|  |  |
| $P_{ex,MRC,2-corr} = \frac{1}{1 + r^2(1-\rho) + 2r}$ | $P_{ex,2-ind} = \frac{2}{(1+r)(2+r)}$ |



# The revelations …

- One M-antenna eavesdropper performing SDC reception is equivalent to M single antenna independent eavesdroppers
- One M-antenna eavesdropper performing MRC/EGC reception is superior to M single antenna independent eavesdroppers
- The dominance of the M-antenna eavesdropper performing MRC reception over M single antenna independent eavesdroppers is ***LINEAR*** under high main channel SNR conditions and ***FACTORIAL*** under low main channel SNR conditions (with respect to the increase in the number of antennas.)

# The revelations …

One 2-antenna eavesdropper performing MRC reception is always superior to 2 single antenna independent eavesdroppers provided,

- The main channel average SNR is greater than the eavesdropper channel average SNR.

When main channel average SNR is lesser than the eavesdropper channel average SNR,

- The MRC eavesdropper enjoys superiority provided the spatial correlation coefficient ($\rho$)is less than 0.5
- If the eavesdropper has a strong LOS path with the transmitter, the fall in probability of existence is exponential.

*THANK YOU !!*

*QUESTIONS ??*