A Disc of Scatterers based Channel Model for Secure Key Generation

Taghrid MAZLOUM, Francesco MANI, Alain SIBILLE
Telecom ParisTech/LTCI
Communication and Electronic Department

Outline

- Introduction
- Objectives
- Description of the channel model
- Available key bits performance
- Security evaluation
- Conclusion

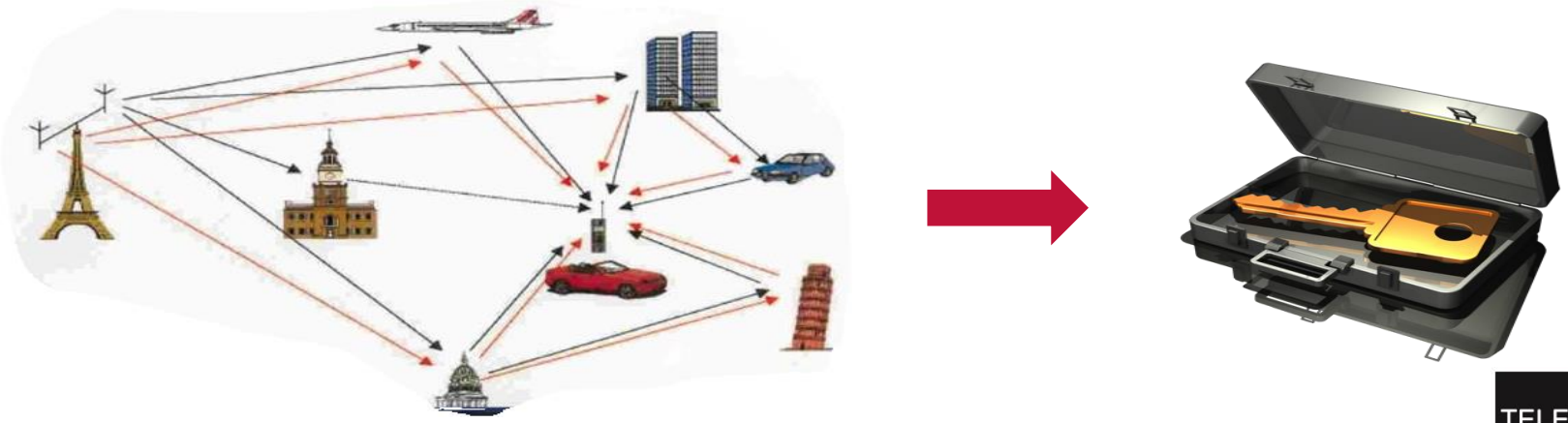
Introduction

- **Security as a challenge**
- **Ciphering messages using secret keys (SK)**
- **Issues of conventional cryptographic techniques**

Physical Layer Security (PhySec)

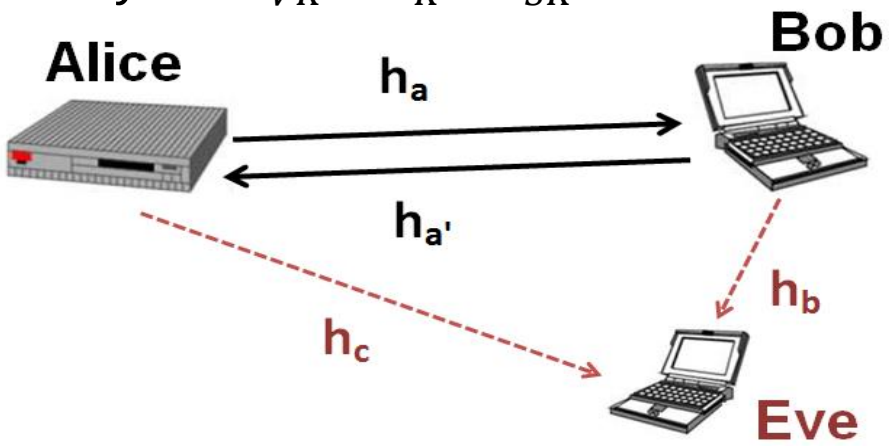
Introduction

- **Physical layer security (PhySec):**
  - The inherent properties of the **propagation channel**
  - Secret Key generation (SKG) from reciprocal fading channels
  - Confidentiality through spatial channel decorrelation



Introduction

- **Information-theoretic upper bounds**
  - Available key bits $I_K = I(h_a\,; h_{a'})$
  - SK bits $I_{SK} = I(h_a\,; h_{a'}|h_b, h_c)$
  - Vulnerable key bits $I_{VK} = I_K - I_{SK}$

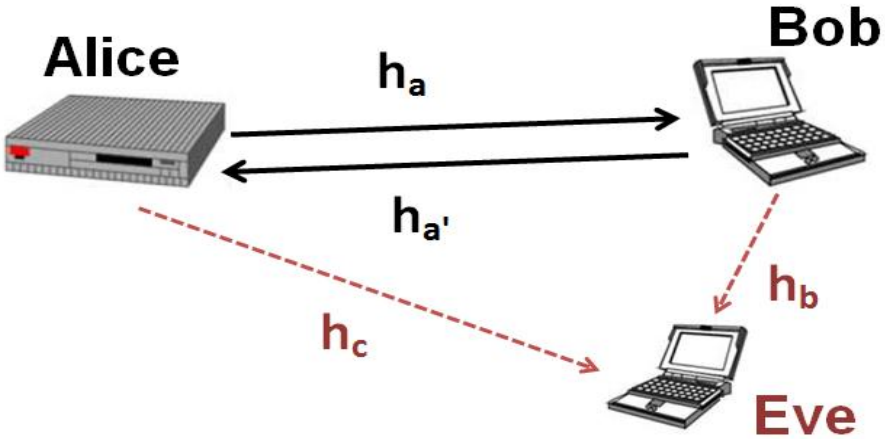


Introduction

- **Information-theoretic upper bounds**
  - For zero-mean complex Gaussian random channels

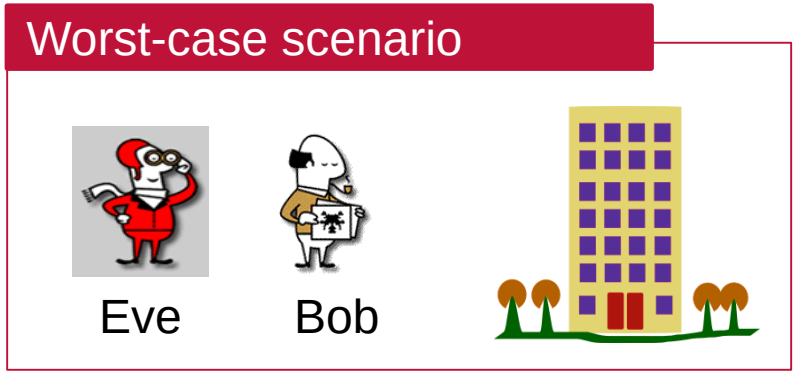
$$I_K = \log_2 \frac{\left|\hat{R}_{aa}\right|\left|\hat{R}_{a'a'}\right|}{\left|\hat{R}_{AA'}\right|}$$

$$I_{SK} = \log_2 \frac{\left|\hat{R}_{ABC}\right|\left|\hat{R}_{A'BC}\right|}{\left|\hat{R}_{BC}\right|\left|\hat{R}_{AA'BC}\right|}$$



Objectives

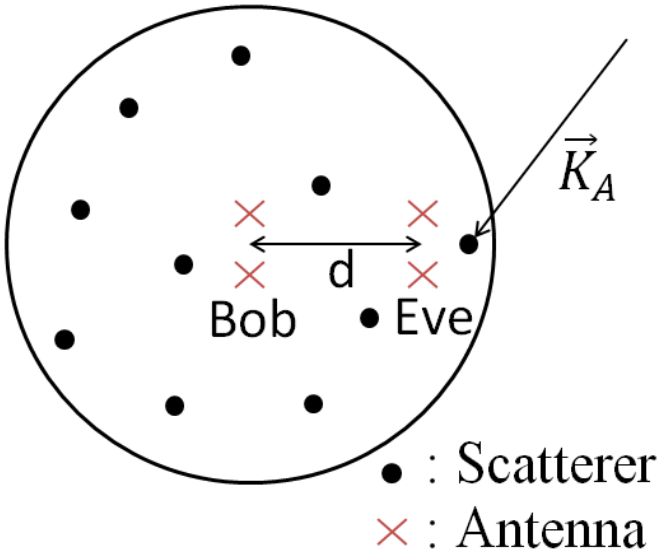
- **A worst-case scenario investigated in literature** [1]
- **Lack of spatial stationarity between Bob and Eve**
- **Impact of multiple antennas on the security**



[1] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis," *IEEE Trans. Inf. Forensics and Security*, vol. 5, no. 3, pp. 381-392, Sep. 2010.

Description of the channel model

- **A 2-D geometry-based stochastic channel model**
  - Macroscopic environment scenario
  - Uniform distribution of omnidirectional scatterers
  - NLOS from Alice to Bob/Eve

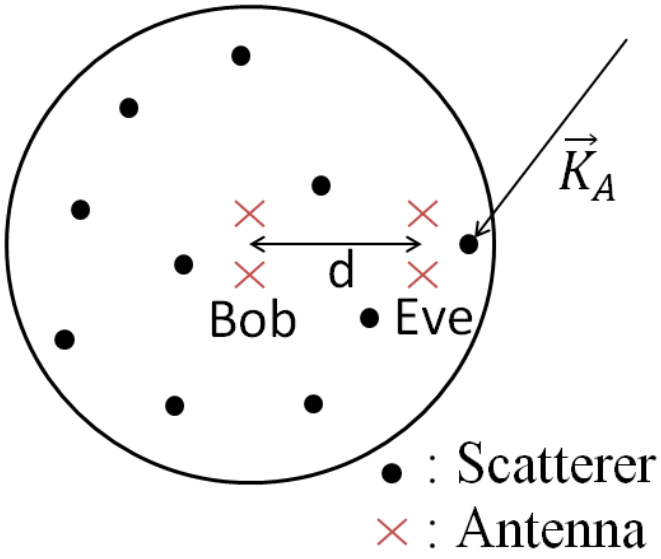


Description of the channel model

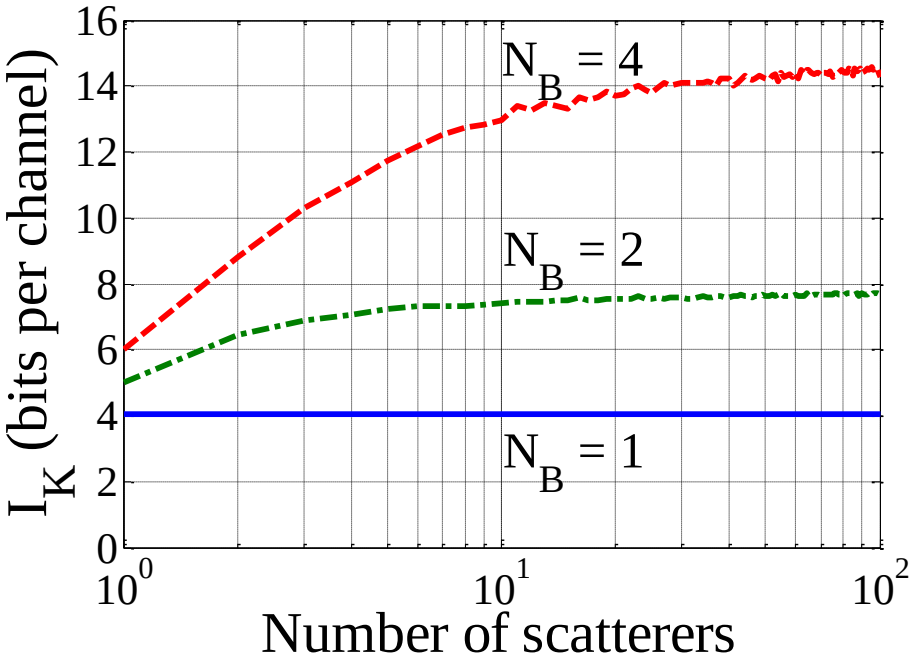
- **The narrowband complex channel gain**

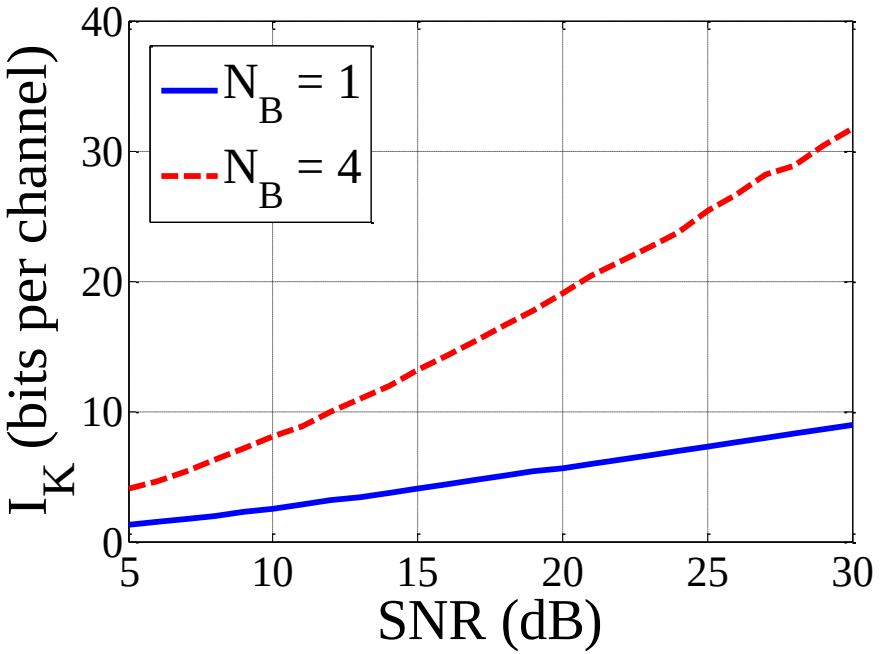
$$h_m = \sum_{l=1}^{N_S} \frac{\beta_l}{d_l} \exp\left\{j\left(K.d_{ml} + \overrightarrow{K_A}.\overrightarrow{r_l}\right)\right\}$$

  - LOS from scatterers to Bob/Eve
  - Rayleigh distribution for β_l
  - $SNR = \frac{E\{||H||_F^2\}}{N*\sigma^2}$



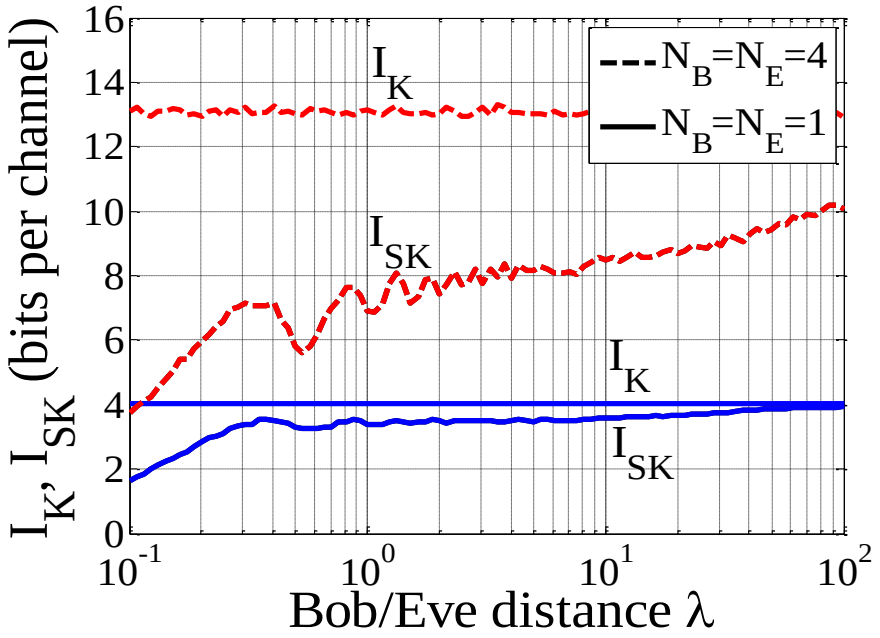
Available key bits performance





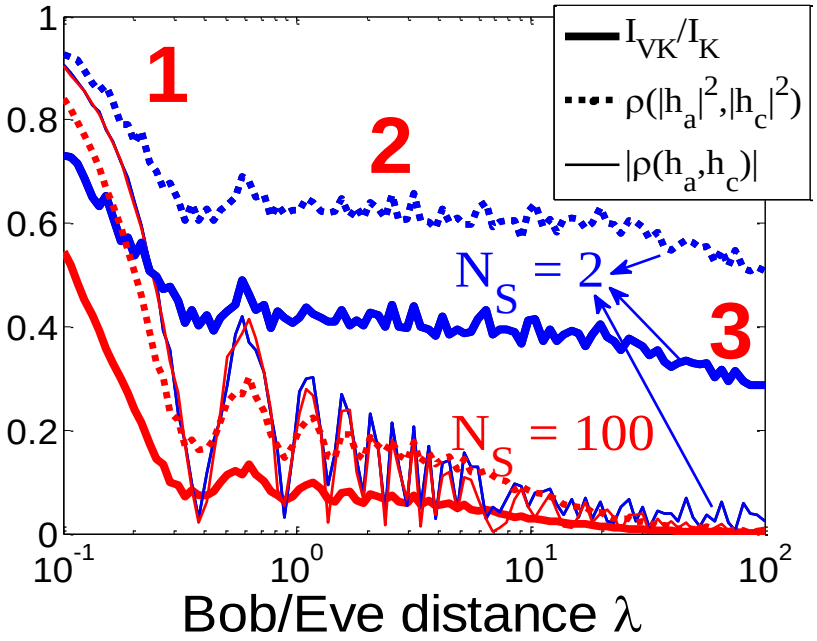
- Improvement of I_K with:
  - Multiple antennas
  - Rich multipath channels
  - High SNR

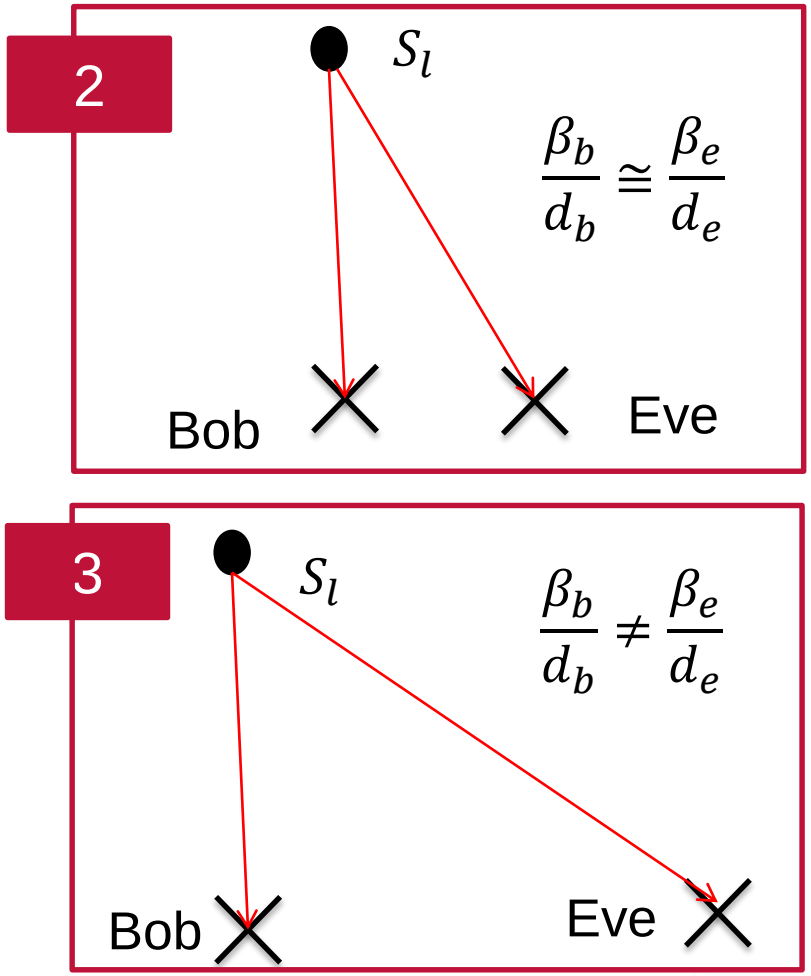
Security evaluation



- Security improvement for larger separation distances
- Both security and vulnerability improvement for larger arrays

Security evaluation



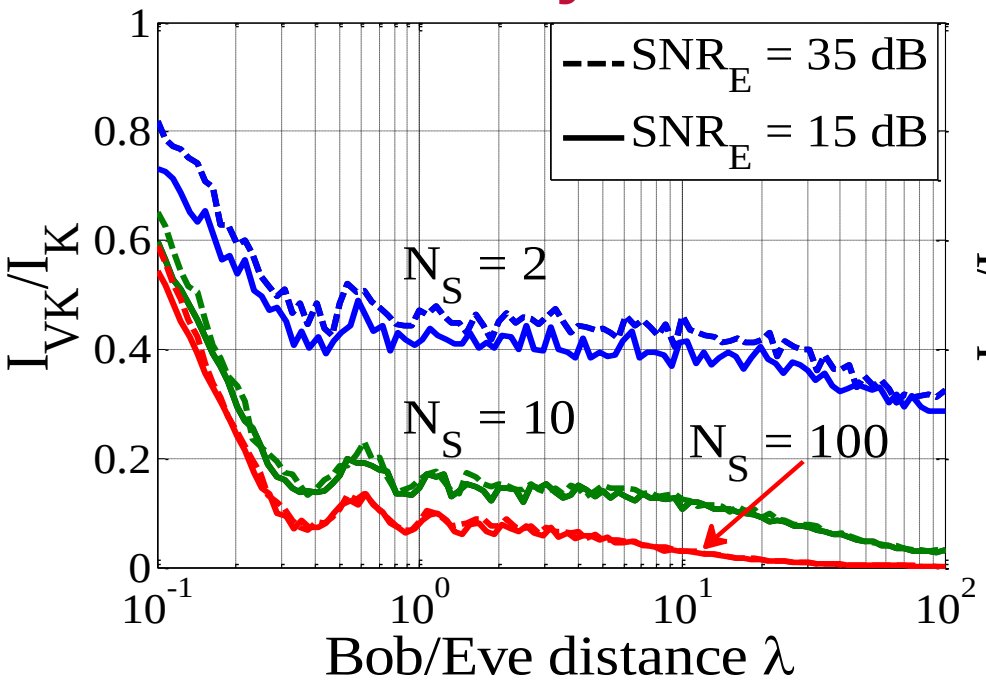


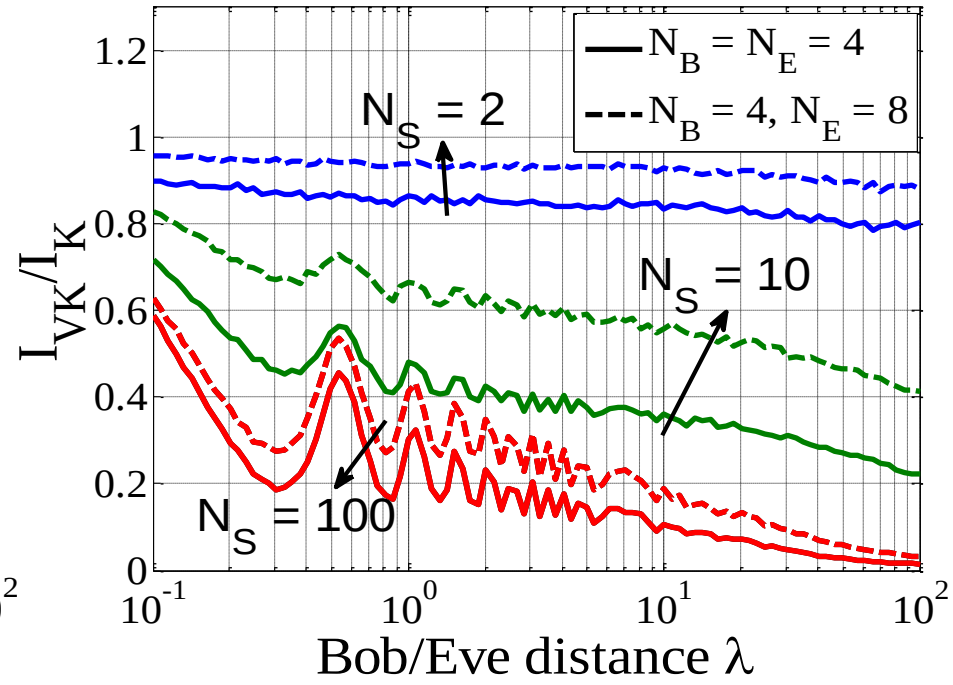
1. Phase decoherence

2. Channel memory effect

3. Power decorrelation

Security evaluation





- Security in rich multipath channels
- Security degradation for knowledgeable Eve, by either increasing her SNR or employing more antennas

Conclusion

- **Improvement of I_K by employing more antennas especially in rich scattered channels**
- **Confidentiality achievement owing to the spatial channel decorrelation**
- **Security degradation by employing more antennas by Eve**

Thank you for your attention

The work has been funded the European Commission through the FP7 project PHYLAWS (grant agreement n° 317562).