EUROPEAN COMMISSION

Community Research

SEVENTH FRAMEWORK PROGRAMME

ICT Call 8

PHYLAWS

PHYsical LAyer Wireless Security

Advisory Board - Year 1 Meeting - Part E2

Telecom Paris Tech, room B603, 46 rue Barrault, 75013 Paris, 2 october 2013

Contacts : F. Delaveau : François.Delaveau@thalesgroup.com tel : 01 46 13 31 32 ; mob : 06 73 28 25 89

A. Sibille : alain.sibille@telecom-paristech.fr tel : 01 45 81 70 60

Task T3.1: Study and development and test of "propagation dependant" random generators (M1 – M27)

Task leader: ICL Task contributors: TPT, TCS

- **Objectives**
  - use the radio channel randomness between two legitimate users to generate secrecy
  - use this secrecy in secret key generation (or initial vectors)
- **Major issues**
  - size of the generated key
  - degree of secrecy
  - methods for secret key agreement
- **Key parameters and use cases**
  - frequency and band width
  - number of antennas at Bob-Alice-Eve
  - time variability
  - richness of the radio channel
  - spatial separation between Alice-Bob & Eve
- **Interactions with other tasks**
  - T4.1 New RATs based on SISO, MISO and MIMO technologies
  - T5.1 CIR measurement and modeling

Task T3.1: following…

- **Work plan**
  - develop a simulation tool to evaluate the secrecy capacity
    - based on a discrete multipath channel model
    - enabling SISO, MISO, MIMO schemes
    - allowing any antenna pattern characteristics
  - consider "realistic" site specific channel models (ray-tracing with digital maps)
  - investigate measured channels (also linked with WP5)

- **1st year's work**
  - assessment of the SoA
  - 1st version of a simulation tool, based on a circular disc model of scatterers
  - analysis of the relevance of the concept of secrecy capacity vs. the knowledge available to Eve

How to compute the mutual information?

If

- $h_a \sim CN(0, R_A)$
- $h_{a'} \sim CN(0, R_{A'})$
- $h_c \sim CN(0, R_C)$
- $h_b \sim CN(0, R_B)$

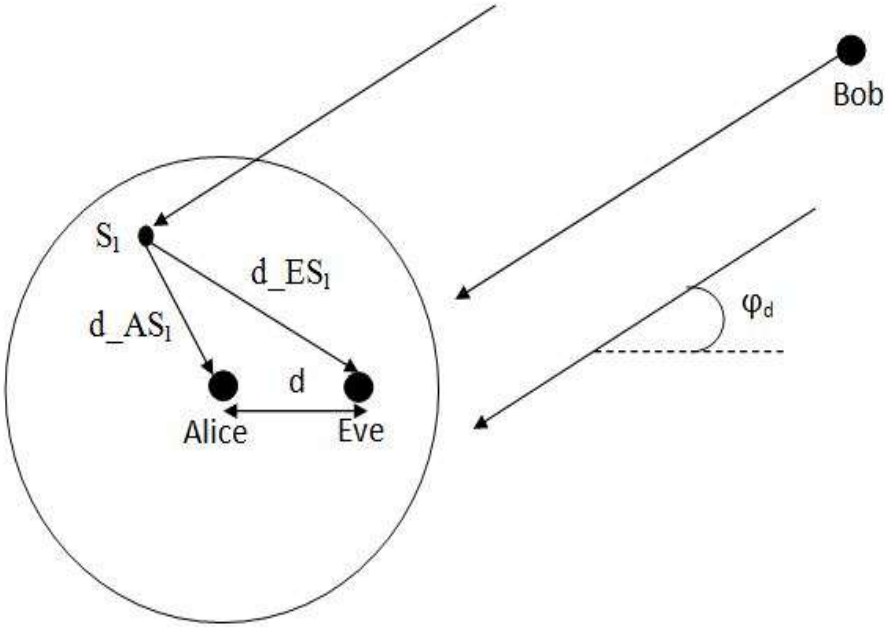
- $I_K = I(h_a, h_{a'}) = \log_2 \frac{|R_A||R_{A'}|}{|R_{AA'}|}$
- $I_{SK} = I(h_a, h_{a'}/h_c, h_b) = \log_2 \frac{|R_{ABC}||R_{A'BC}|}{|R_{BC}||R_{AA'BC}|}$
- $I_{VK} = I_K - I_{SK}$

Else

- *Complicated*

A geometry-based channel model where scatterers are uniformly distributed within a disc

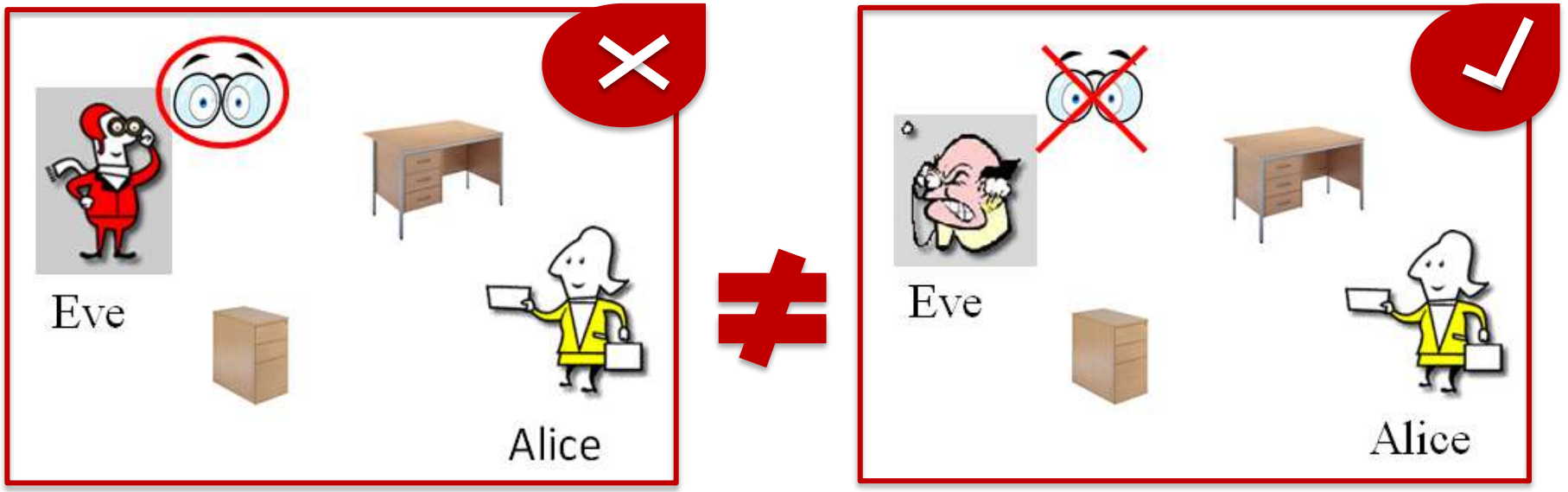
- Assumptions:
  - Directivity at Bob level
  - Omnidirectional antennas
  - Non LOS propagation
  - Omnidirectional scatterers



General considerations

- I_K, I_{SK} and $I_{VK} = I_K - I_{SK}$ are statistical quantities
  - The need to define the statistical set
- The channels statistics depending on the terminals knowledge about their environment
  - Knowledge → Scenario parameters
  - Lack of knowledge → Large statistical set
- The information owned by the triplet Alice-Bob-Eve determines the relevant statistical sets
  - The resulting randomness impacts the degree of secrecy

General considerations



Knowledge: large number of I_{VK}

Lack of knowledge: small number of I_{VK}

Scenarios

Scenario 1: Nearly perfect environment knowledge

- **Channel estimation based on:**
  - The knowledge of the departure angle
  - The knowledge of scatterers locations
- **A Gaussian behavior**
- **A non realistic scenario**

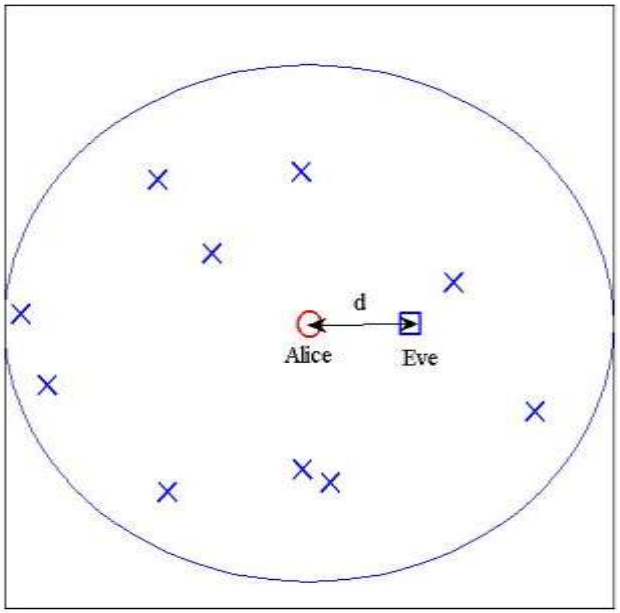
Scenario 2: No information

- **No information about the environment is available for Alice/Eve**
  - Statistically definition of all the parameters
- **Non Gaussian behavior**
- **A realistic scenario**

Scenarios

- Hypothesis: The mean of I_K computed in the scenario 1 corresponds to a single value computed in the realistic scenario 2

Parameter	Value
The frequency	2 GHz
The disc radius	100 λ
SNR	15 dB
Scatterers number	10

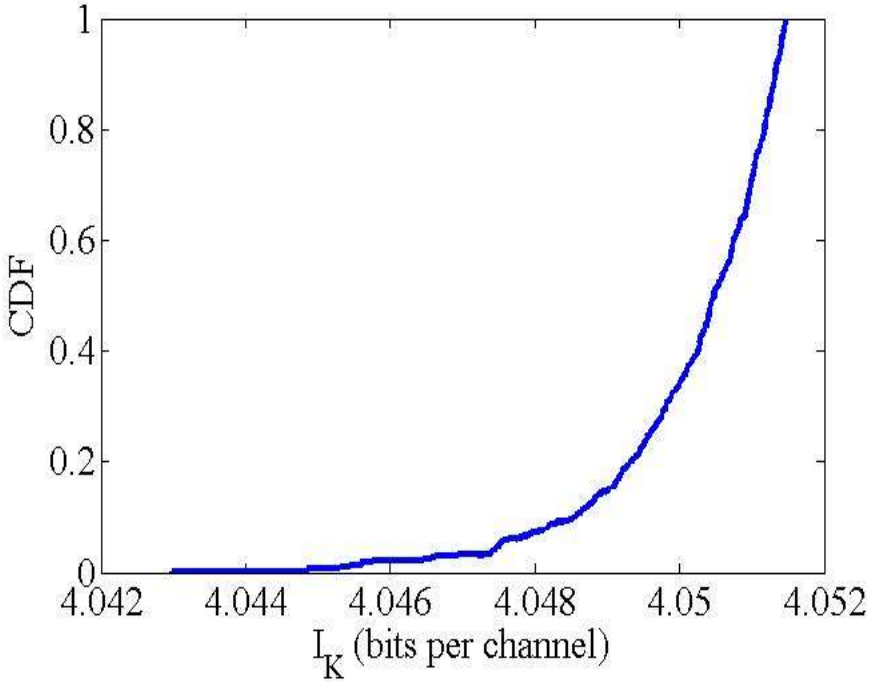


- $SNR = \frac{E\{\|h\|_F^2\}}{\sigma^2}$
  - $\|.\|_F$: The Frobenius norm
  - σ^2: The mean power of the noise

Scenarios

- Various environment → several values of I_K
- For SISO, I_K depends only on the SNR:

$$I_K = log_2(1 + \frac{SNR^2}{1 + 2\,SNR})$$



SNR	I_K (bits)
15 dB	4.05
20 dB	5.67
25 dB	7.31

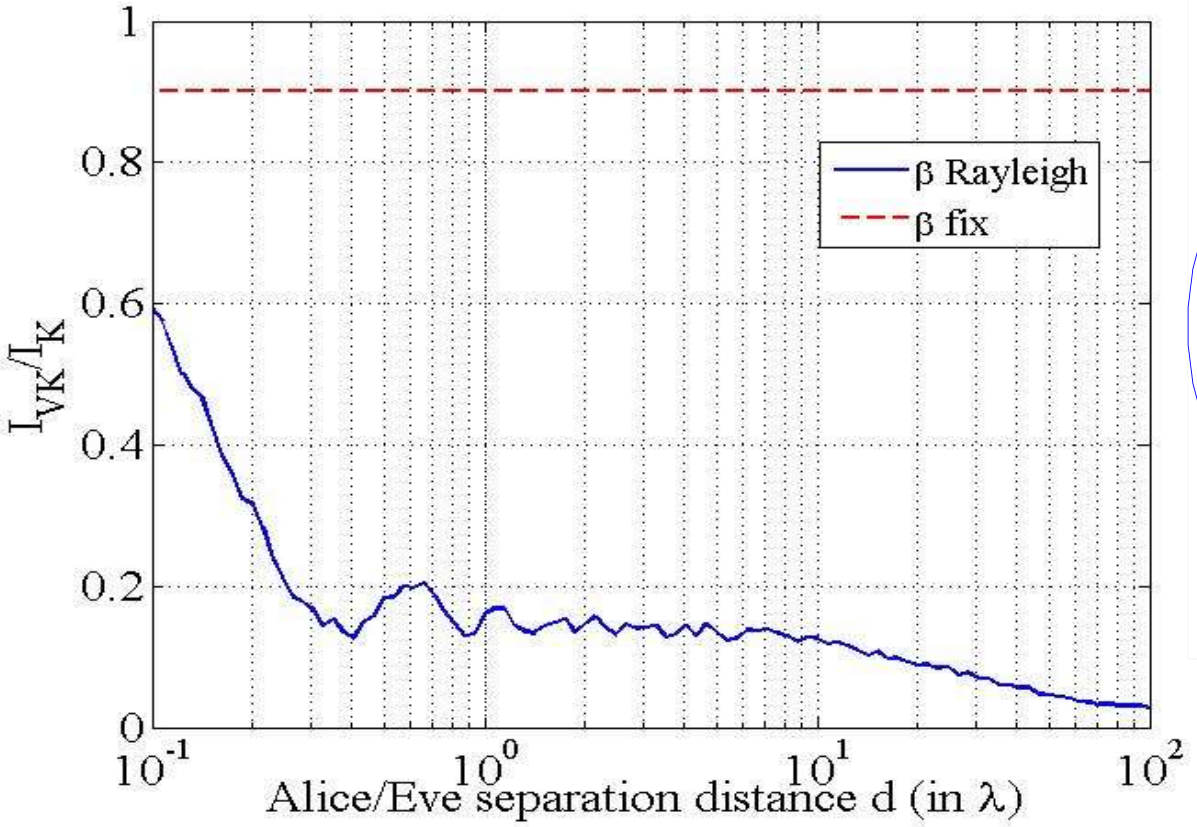
Security condition: randomness

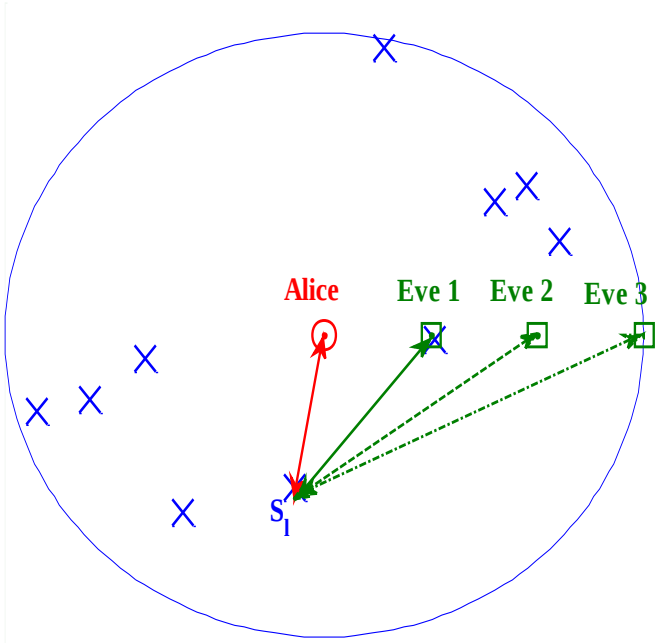
- Two cases for the complex amplitude β_l
  - Rayleigh fix: The same scattering coefficients for all scatterers
  - Rayleigh β: We assume that scattererd waves exhibit random Rayleigh fading towards Alice/Eve

PHYLAWS FP7 ICT call 8 - Id 317562

Security condition: randomness

- **β fix:** Almost all the bits are vulnerable
- **β Rayleigh:** More variability and more secrecy

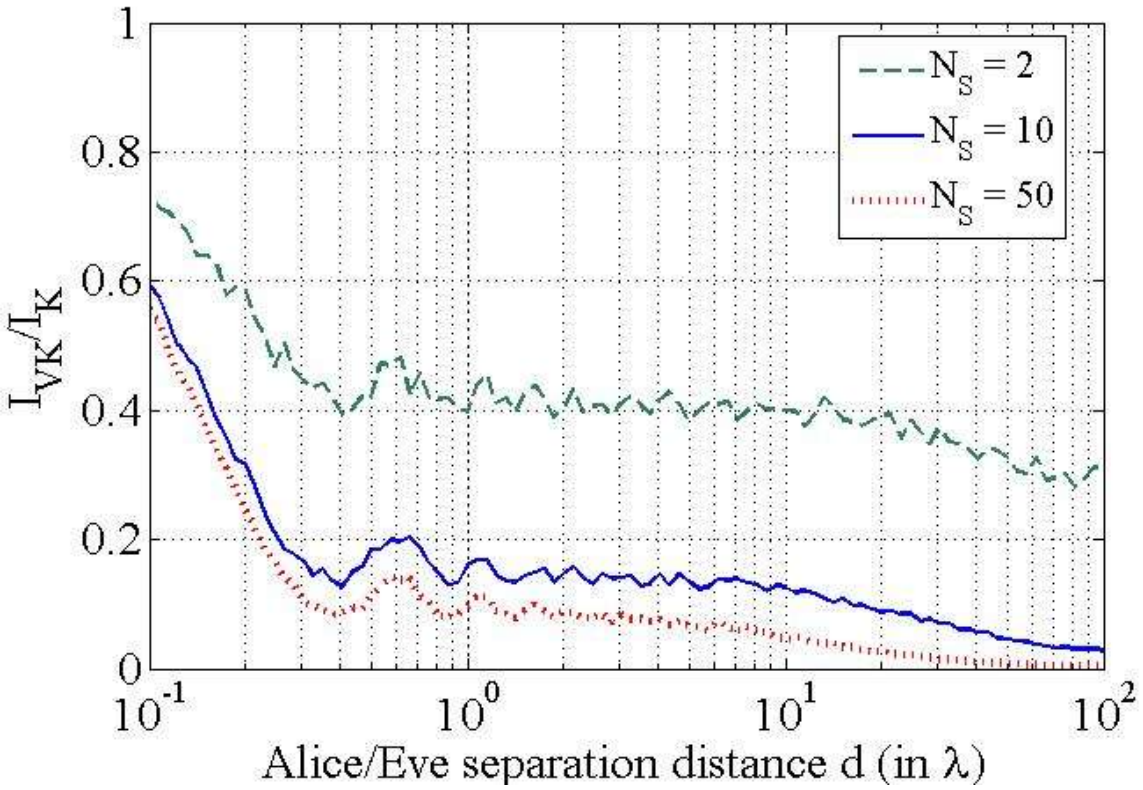




PHYLAWS FP7 ICT call 8 - Id 317562

Security condition: randomness

- More complexity for eavesdropping when the diversity increases with the number of scatterers



Interactive discussion of partners with Advisory Board members

See deliverable D.1.12
"Advisory Board Year 1 Meeting Report"