Projet Farman DECORR
Evaluation de la DECORRélation entre canaux : application à la sécurisation des réseaux sans fil

(***Thi Huyen Trang Nguyen*** and Jean-Pierre Barbot)∈ SATIE
(Romain Soulat and Laurent Fribourg)∈ LSV

IFR Farman

Overview

1. Introduction
2. Model
3. Propagation channel measurements
4. Present results
5. Conclusion and futur works

1 Introduction

2 Model

3 Propagation channel measurements

4 Present results

5 Conclusion and futur works

Conventionnal wisdom in wireless MIMO systems $\rightleftharpoons$ the radio subchannels are **DECORR**elated

- Is it true ?
- Can we use this feature to securise wireless transmission of sensible data ?
- Is it a possible way to access to the perfect secrecy and the unconditional security defined in Shannon's work ?

Shannon theory (Information theory fondamental results)

- Limited capacity of transmission without error
  - Reliable and efficient digital data transmission
  - The use of coding for error control
- Perfect secrecy of transmission [1]
  - Protection the data against eveasdroppers becomes crucial ☹
  - Various traditional approaches of cryptography,
  - Focusing mainly on key generation (static keys)

Dynamic encryption based on the wireless propagation observation

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell Systems Technical Journal, vol. 28, pp. 656–715, 1949.

1 Introduction

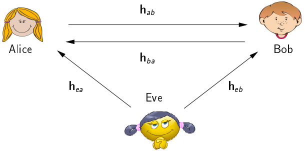
2 Model

3 Propagation channel measurements

4 Present results

5 Conclusion and futur works

Channel model



- Alice and Bob (legitimate nodes) estimate their sub-channel $\hat{\mathbf{h}}_{ab}$ and $\hat{\mathbf{h}}_{ba}$ correspondingly

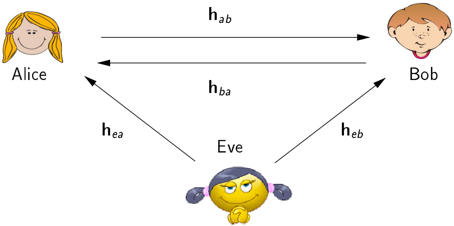
$$\begin{cases} \hat{\mathbf{h}}_{ab} & = & \mathbf{h}_{ab} + \mathbf{n}_{ab} \\ \hat{\mathbf{h}}_{ba} & = & \mathbf{h}_{ba} + \mathbf{n}_{ba}. \end{cases} \tag{1}$$

- Eve eavesdrops Alice and Bob by the mean of the sub-channels $\hat{\mathbf{h}}_{ea}$ and $\hat{\mathbf{h}}_{eb}$

$$\begin{cases} \hat{\mathbf{h}}_{ea} & = & \mathbf{h}_{ea} + \mathbf{n}_{ea} \\ \hat{\mathbf{h}}_{eb} & = & \mathbf{h}_{eb} + \mathbf{n}_{eb}. \end{cases} \tag{2}$$

- Alice and Bob extract their channel parameters to get the secret key ☞session key
- Eve experieces independent characteristics of channel between Alice and Bob ☞impossible to get the key

Channel model



Hypothesis

The sub-channels between legitimate nodes: Alice and Bob, are reciprocals *i.e.* $\mathbf{h}_{ab} = \mathbf{h}_{ba}$

1 Introduction

2 Model

3 Propagation channel measurements

4 Present results

5 Conclusion and futur works

UHF wireless propagation channel is:

- a linear system,
- assumed to be time invariant (invariant at least during its measurement),

⇒ then completely characterized by its Complex Impulse Response (CIR)

$$y_{\mathrm{out}}(t) = h(t) \otimes x_{\mathrm{in}}(t) = \int_{-\infty}^{+\infty} h(\tau)\, x(t-\tau)\, d\tau$$

where

$y_{\mathrm{out}},\ x_{\mathrm{in}}$	respectively the input and the output
$\otimes$	the convolution product
$h(t)$	the complex impulse response

In our problem, we have to measure:

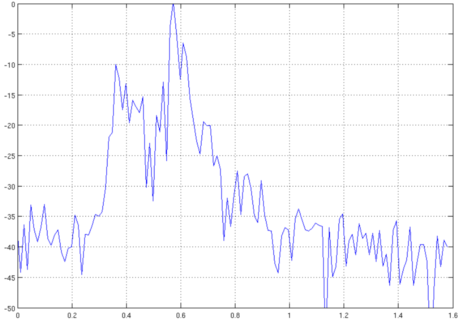
- $h_{ab} = h_{ba}$ the CIR linking Alice and Bob,
- h_{ea} the CIR used by Eve to eavesdrop Alice,
- h_{eb} the CIR used by Eve to eavesdrop Bob.

These CIRs may be measured with:

- a **channel sounder** (i.e. measurement of the CIRs in the "time domain"),
- a network analyzer (i.e. measurement of the transfert function in the frequency domain)

  ☹ too long measurement duration

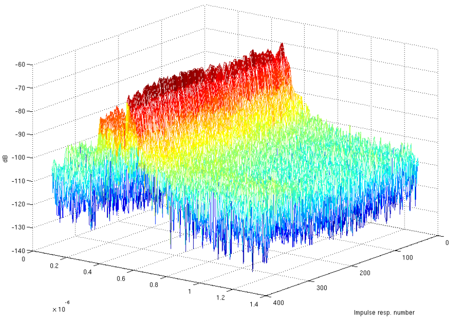
CIR measurement example 1 (an individual CIR)



Measurement parameters:

- carrier frequency $f_c = 2.2$ GHz,
- bandwidth around f_c, $B = 100$ MHz
- indoor context (Vélizy 2) 1st Impul. response. of a set of 360 CIRs

CIR measurement example 2 (here a set of 360 CIRs)



Measurement parameters:

- carrier frequency $f_c = 2.2$ GHz,
- bandwidth around f_c, $B = 100$ MHz
- indoor context (Vélizy 2) set of 360 CIRs (collect. with a rotating arm on a circle $R = 0.5$ m)

1 Introduction

2 Model

3 Propagation channel measurements

4 Present results

5 Conclusion and futur works

$\approx$ 6 first months

- make accessible the CIRs data base,
- first trial to evaluate the DECORRelation: "correlation coeff.", "mutual information" (information theory),
- generate the "session key" $\mathbf{K} = \mathbf{K}_a = \mathbf{K}_b$ from $\hat{\mathbf{h}}_{\mathbf{ab}}$ or/and $\hat{\mathbf{h}}_{\mathbf{ba}}$,
- use $\mathbf{K}$ in a turbo-code scheme [2].

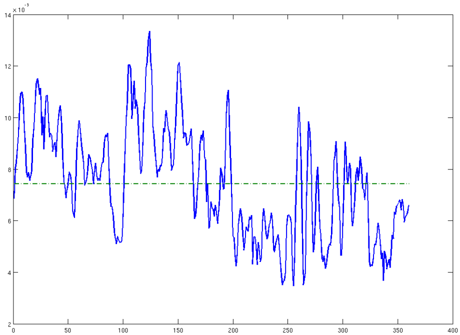
[2] T. H. T. Nguyen and J.-P. Barbot, "Joint error control and dynamic security coding," in the International IEEE Conference ATC'13, Ho Chi Minh City, Vietnam, Oct. 2013, pp. 285–290.

Key generator algorithm

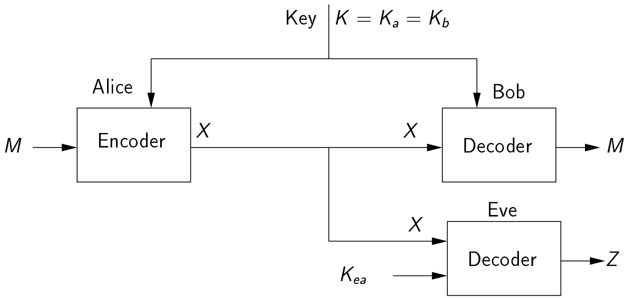
(i) determine $\mathrm{Max}\,(i)$, the maximum peaks of the i^{th} CIR,

(ii) estimate m, the median of the vector $\mathbf{Max}$,

(iii) if $\mathrm{Max}\,(i) \geq m$ then $K\,(i) = 1$, otherwise $K\,(i) = 0$.



Key vector **K** used in an error control scheme



First trial of DECORRelation evaluation: Mutual info. between the keys

Alice	Bob	Eve	Mutual Info.
Tx	CECO60	CECO30	0.1256
Tx	CECO60	CECO61	0.1634
Tx	CECO22	CECO23	0.0108
Tx	CECO22	CECO24	0.0003
Tx	CECO22	CECO18	0.0072

First trial of DECORRelation evaluation: Mutual info. between after Turbo_Coding

		Mutual information	
Bob (M)	Eve (Z)	Puncturing	Interleaver
CECO60	CECO30	1.0053e-04	0.0018
CECO60	CECO61	0.0018	8.5823e-04
CECO22	CECO23	0.0031	5.9574e-04
CECO22	CECO24	0.0190	0.0016
CECO22	CECO18	0.0012	0.0010

1. Introduction
2. Model
3. Propagation channel measurements
4. Present results
5. Conclusion and futur works

- A set a measured CIRs is now available:
  - DECORRelation evaluation tests are now possible (and have started),
  - the improvement of the DECORRelation due to coding scheme can be tested (and have to),

However

- an effort have to be done to understand the relationship between the evaluated “correlation coefficients” and the estimated “mutual information”,
- need to be carefully considered in security scheme ⚠