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

(Thi Huyen Trang Nguyen et ***Jean-Pierre Barbot***)$\in$ SATIE
(Romain Soulat et Laurent Fribourg)$\in$ LSV

IFR Farman

1$^{\text{er}}$ décembre 2014

Overview

Le fonctionnement des systèmes MIMO sans fil (wireless) repose sur l'hypothèse$\rightleftharpoons$ les sous canaux radio sont **DECORR**élés

- Est-ce vrai ?
- Pourrions nous utiliser cette propriété pour sécuriser la transmission "wireless" de données sensibles ?
- Est-il possible d'atteindre le secret parfait ou la sécurité inconditionnelle définis dans les travaux de C. Shannon ?

Théorie de Shannon (résultats fondamentaux de la "Théorie de l'Information)

- Capacité limitée de transmission sans erreur
  - transmission de données numérique fiable et efficace,
  - mise en œuvre de code correcteur d'erreur.
- Transmission parfaitement secrète Perfect secrecy of transmission [1]
  - protection des données de potentielles écoutes ☹
  - plusieurs approches traditionnelles en cryptographie,
  - principalement basées sur la génération de clef de cryptage (clefs statiques)

Encryptage dynamique basé sur l'observation du canal de propagation électromagnétique

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

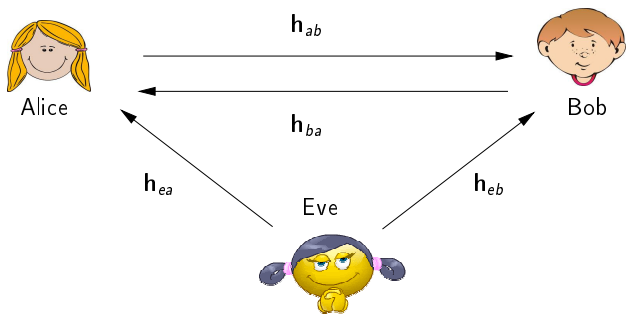
Théorie de Shannon (résultats fondamentaux de la "Théorie de l'Information)

pour un canal Gaussien

$$C = B.\log_2\left(1+\frac{S}{N}\right) \ [\text{bits/s}]$$

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

Modèle de canal



- Alice et Bob (nœuds légitimes) estiment respectivement les sous-canaux $\hat{\mathbf{h}}_{ab}$ et $\hat{\mathbf{h}}_{ba}$

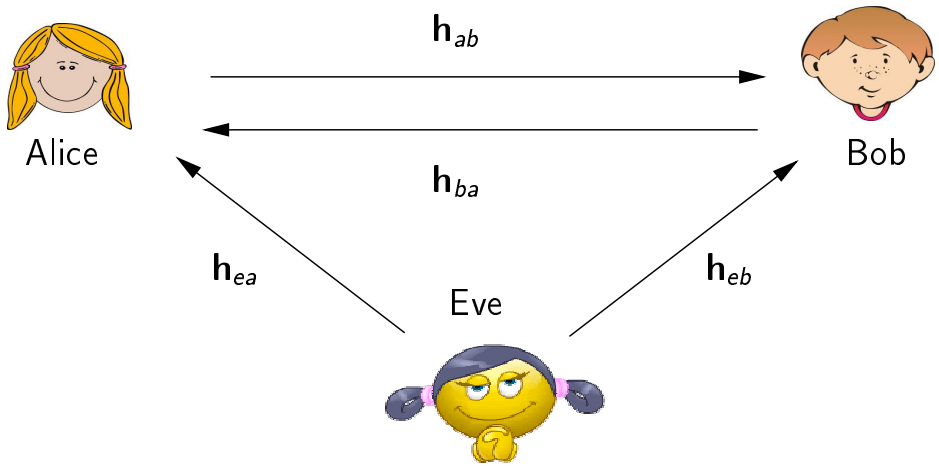
$$\begin{cases} \hat{\mathbf{h}}_{ab} &= \mathbf{h}_{ab} + \mathbf{n}_{ab} \\ \hat{\mathbf{h}}_{ba} &= \mathbf{h}_{ba} + \mathbf{n}_{ba}. \end{cases} \tag{1}$$

- Eve écoute Alice et Bob à travers les sous-canaux $\hat{\mathbf{h}}_{ea}$ et $\hat{\mathbf{h}}_{eb}$

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

- Alice et Bob générent leur clef d'encryptage à partir des paramètres $\rightsquigarrow$ "session key"
- Eve experieces independent characteristics of channel between Alice and Bob $\rightsquigarrow$ impossible to get the key

Modèle de canal



Hypothèse

Les sous-canaux entre nœuds légitimes : sont réciproques

c.à.d. $\mathbf{h}_{ab} = \mathbf{h}_{ba}$

Le canal de propagation UHF est :

- un système linéaire,
- supposé être invariant temporellement (au moins le temps de sa mesure),

$\Rightarrow$ complétement caractérisé par sa Réponse Impulsionnelle Complexe (RIC)

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

où
- y_{out}, x_{in} : respectivement l'entrée et la sortie,
- $\otimes$: le produit de convolution,
- $h(t)$: la réponse imulsionnelle complexe.

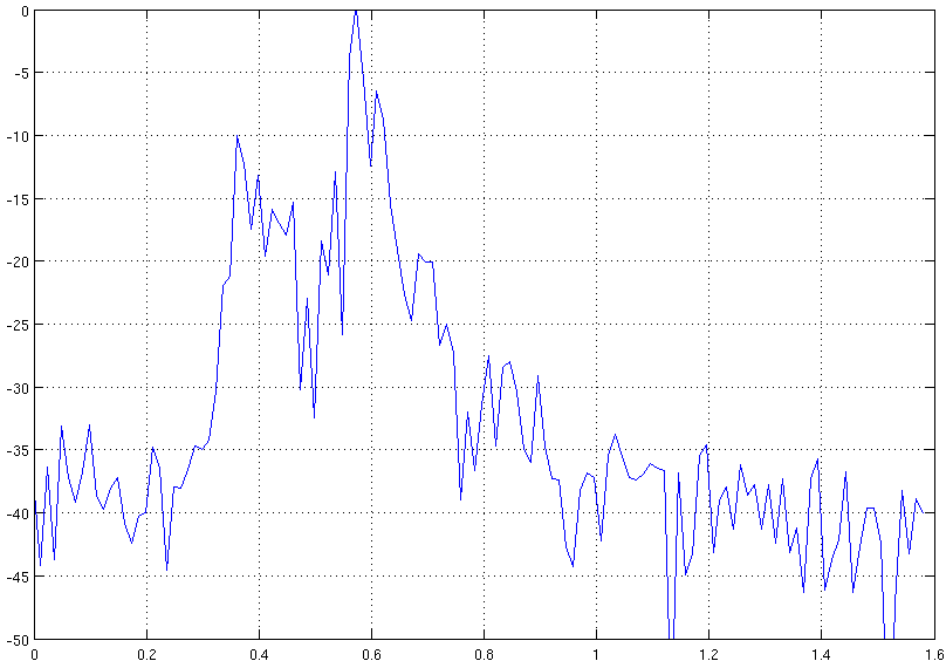
Dans notre problème, nous devons mesurer :

- $h_{ab} = h_{ba}$ la RIC liant Alice et Bob,
- h_{ea} la RIC utilisée par Eve pour écouter Alice,
- h_{eb} la RIC utilisée par Eve pour écouter Bob.

Ces RICs peuvent être mesurées à l'aide :

- d'un **sondeur de canal** (*c.à.d.* mesures des RICs dans le "domaine temporel"),
- un analyseur de réseau vectoriel (*c.à.d.* mesures de la fonction de transfert dans le domaine fréquentiel)
  ☹ durée de la mesure trop longue

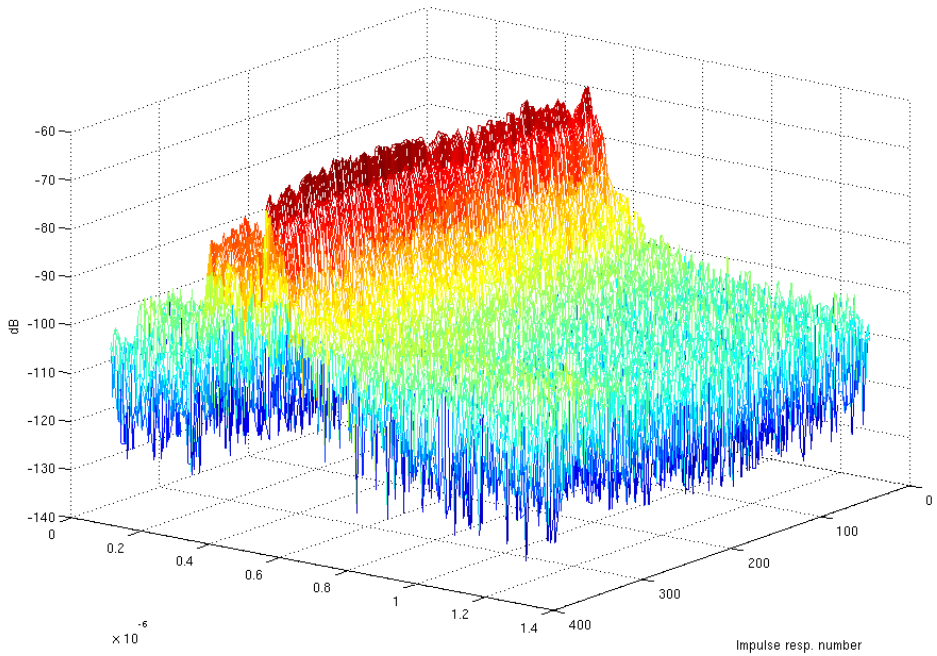
Exemple 1 : RIC mesurée (RIC individuelle)



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)

- utilisation d'une base de données de mesures enregistrées (RICs),
- évaluation de la DECORRelation : "coeff. de corrélation", "information mutuelle" (information theory),
- generation de clef "session key" $\mathbf{K} = \mathbf{K}_a = \mathbf{K}_b$ à partir de $\hat{\mathbf{h}}_{\mathbf{ab}}$ (1 pic et/ou 2 pics),
- utilisation de $\mathbf{K}$ dans un schéma de codage "turbo-code" [2].

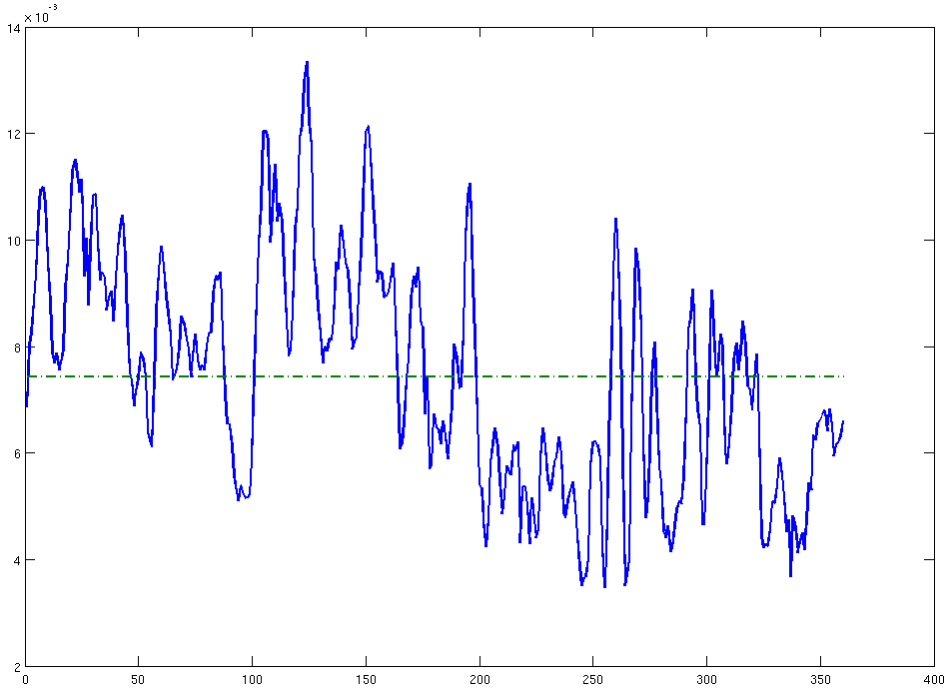
[2] T. H. T. Nguyen and J.-P. Barbot, "Joint error control and dynamic security coding," in the International IEEE Conference ATC'13, Ho Chi Minh City, Vietnam, Oct. 2013, pp. 285–290.

Key generator algorithm

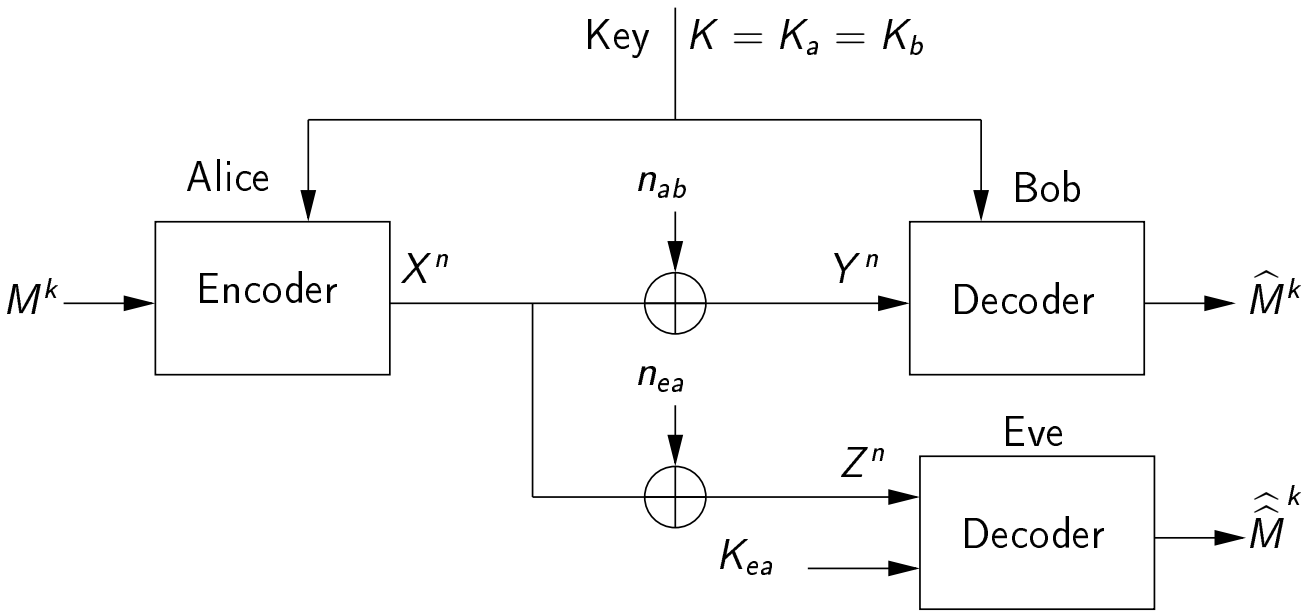
(i) determine $\mathrm{Max}(i)$, the maximum peaks of the i^{th} CIR,

(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

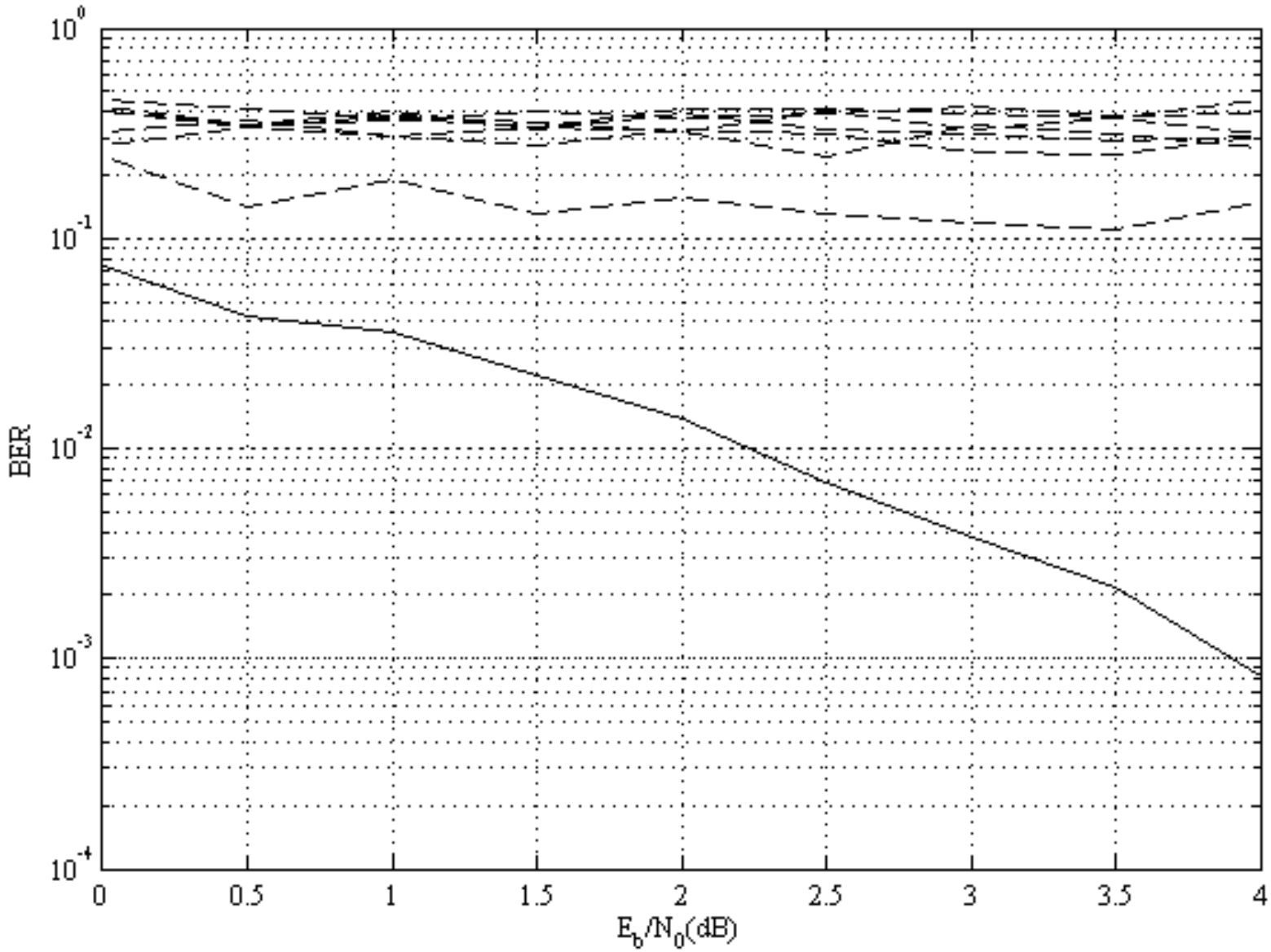


Evaluation de la DECORRelation : "Info mutuelle entre clefs" et coeff. de corrélation

Alice	Bob	Eve	Info. mut.	Corr-coeff.
Tx	pos60	pos30	0.1256	-0.4111
Tx	pos60	pos61	0.1634	0.4667
Tx	pos22	pos23	0.0108	-0.1222
Tx	pos22	pos24	0.0003	0.0222
Tx	pos22	pos18	0.0072	0.1000

Evaluation de la DECORRelation(après encryptage-desencryptage "turbo-code")

			Mut. info. punct.	
Alice	Bob ($\widehat{M}$)	Eve ($\widehat{\widehat{M}}$)	Pic princ.	2 pics
Tx	pos22	pos23	4.3e-03	5.8e-04
Tx	pos22	pos24	1.7e-03	5.6e-03
Tx	pos22	pos18	5.7e-03	1.8e-04


BER
10^{0}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
0
0.5
1
1.5
2
2.5
3
3.5
4
E_b/N_0(dB)

- 2 publications de conférence en 2014,
- Un jeu de mesure de RICs est utilisable :
  - évaluation de la DECORRelation,
  - l'amélioration de la DECORRelation due au schéma de codage a été testée,

Toutefois

- l'effort pour mieux comprendre la relation entre les "coefficients de corrélation" évalués et "l'information mutuelle" estimée,
- doit être pris en compte prudemment dans le schéma d'encryptage ⚠
- utilisation de "compressive sensing".