

# Traitement du Signal pour la Radio Cognitive

Philippe Ciblat

Université Paris-Saclay & Télécom ParisTech

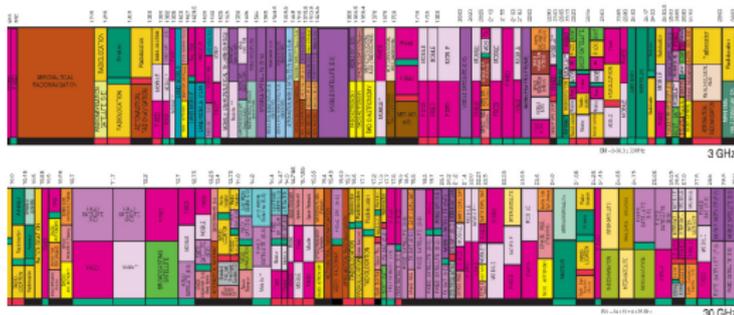
# Plan

- Le traitement du signal dépend du type de radio cognitive souhaitée
- Section 1 : Radio cognitive *interweave*
  - Sondage de canal (coopératif, distribué)
  - Classification de systèmes
- Section 2 : Radio cognitive *underlay*
  - Approche statique : bande ultra-large
  - Approche dynamique
- Section 3 : Un problème de sécurité

## Section 1 : Radio cognitive *interweave*

# Principe *interweave*

- En première approximation, le spectre semble plein



- Mais, à un instant donné, une sous-bande allouée peut être vide  
 ⇒ **trou spectral** (*white space*)
- Deux types d'utilisateurs
  - **Primaires** : ont payé pour utiliser des sous-bandes pré-allouées
  - **Secondaires** : sont autorisés à utiliser un trou spectral

Comment détecter les trous spectraux ?

# Sondage de canal (*spectrum sensing*)

## Différents types de détecteurs

- Energie
- Recherche de certaines propriétés sur le signal (*pattern/feature*)
  - cyclostationnarité,
  - matrice de covariance (en environnement multi-antennes),
  - corrélation interne au signal (préfixe cyclique en OFDM),
  - etc.

## Problématique du test d'hypothèse

### Deux hypothèses :

- $\mathcal{H}_0$  (**absence du primaire**)
- $\mathcal{H}_1$  (**présence du primaire**)

Probabilité de détection :  $P_D = \Pr(\mathcal{H}_1 | \mathcal{H}_1)$

Probabilité de fausse alarme :  $P_{FA} = \Pr(\mathcal{H}_1 | \mathcal{H}_0)$

Objectif : minimiser  $P_{FA}$  tel que  $P_D \geq P_D^{\text{target}}$

# Test de Neyman-Pearson

## Résultat

$$\Lambda(\mathbf{y}) = \log \left( \frac{p(\mathbf{y}|\mathcal{H}_1)}{p(\mathbf{y}|\mathcal{H}_0)} \right) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \mu,$$

avec

- $\Lambda$  le *Log Likelihood Ratio* (LLR)
- $\mathbf{y}$  le vecteur des observations
- $\mu$  le seuil/*threshold* permettant de satisfaire  $P_D^{\text{target}}$

## Application :

$$\begin{cases} \mathcal{H}_0 & : y(n) = w(n) \\ \mathcal{H}_1 & : y(n) = x(n) + w(n) \end{cases}, n = 1, \dots, N_s$$

avec

- $w(n)$  gaussien blanc de variance connue  $\sigma_w^2$ ,
- $x(n)$  signal de l'utilisateur primaire inconnu donc gaussien blanc de variance connue  $\sigma_x^2$ .

# Test d'énergie

## Test d'énergie

$$t(\mathbf{y}) = \frac{1}{\sqrt{\sigma_x^2 + \sigma_w^2}} \sum_{n=1}^{N_s} |y(n)|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\geq}} \eta$$

avec  $\mathbf{y} = [y(1), \dots, y(N_s)]^T$  et  $(.)^T =$  la transposition.

## Calcul du seuil

$t(\mathbf{y})$  suit une loi du  $\chi_2$  à  $2N_s$  degrés de liberté, d'où,

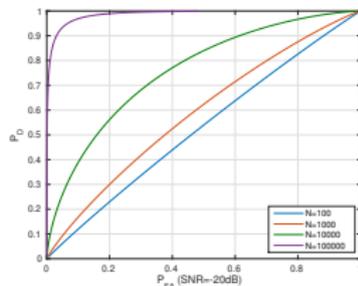
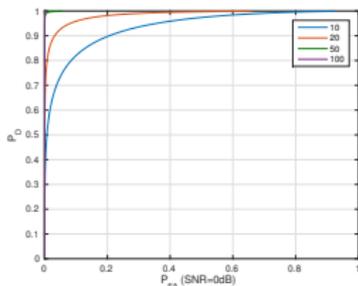
$$\Pr(t(\mathbf{y}) > \eta | \mathcal{H}_1) = P_D^{\text{target}} \Leftrightarrow 1 - \Gamma_{\text{inc}}(\eta, N_s) = \Gamma_c(N_s) P_D^{\text{target}}$$

avec des fonctions Gamma complète et incomplète.

# Performances

$$\begin{aligned}
 P_{FA} &= \frac{1 - \Gamma_{\text{inc}}\left(\eta \frac{\sigma_x^2 + \sigma_w^2}{\sigma_w^2}, N_s\right)}{\Gamma_c(N_s)} \\
 &= \frac{1 - \Gamma_{\text{inc}}\left(\Gamma_{\text{inc}}^{(-1)}(1 - \Gamma_c(N_s)P_D^{\text{target}}, N_s) \frac{\sigma_x^2 + \sigma_w^2}{\sigma_w^2}, N_s\right)}{\Gamma_c(N_s)}
 \end{aligned}$$

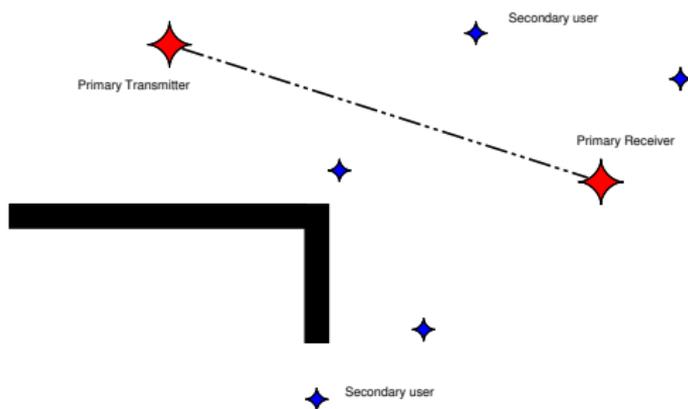
avec  $\Gamma_{\text{inc}}^{(-1)}$  la fonction réciproque de  $\Gamma_{\text{inc}}$



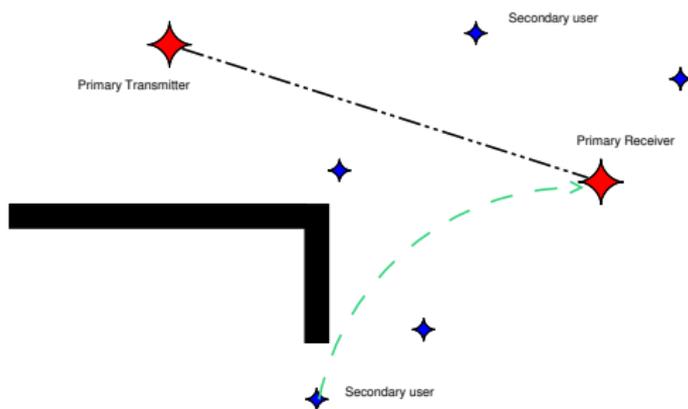
*Courbe "Receiver Operating Characteristic" (ROC)*

**N.B.** : il existe de nombreuses variantes dont la séquentielle

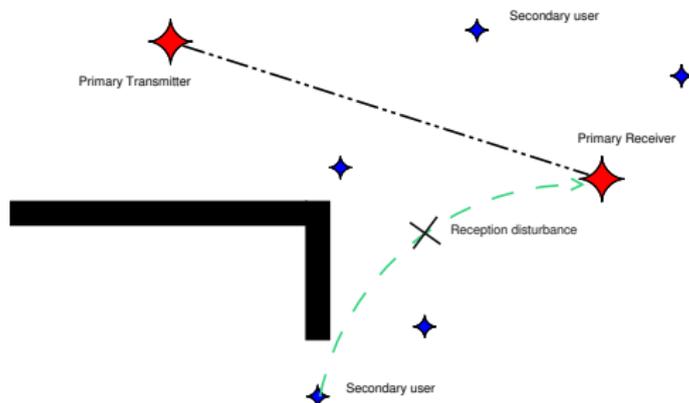
# Problème du terminal caché



# Problème du terminal caché



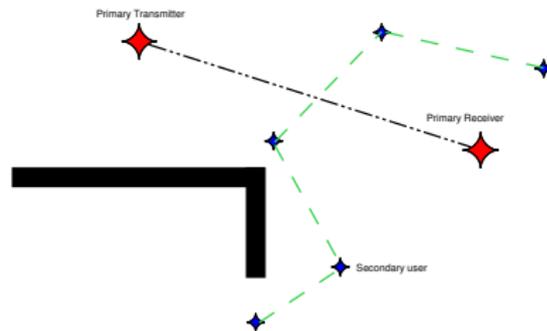
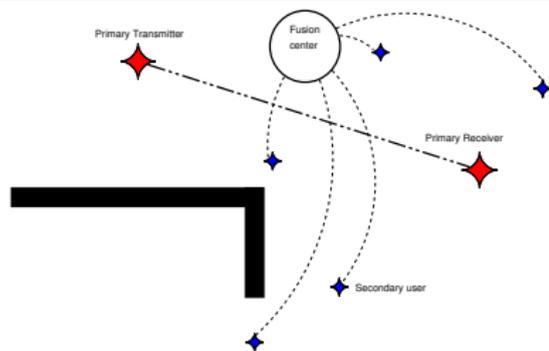
# Problème du terminal caché



**Problème** : un utilisateur secondaire perturbe un utilisateur primaire

**Solution** : les utilisateurs secondaires doivent coopérer pour détecter l'utilisateur primaire

# Sondage de canal coopératif



## Détection avec plus d'un capteur

- Si centre de fusion, détection coopérative ou distribuée
  - approche par décision dure (*hard*) : vote (AND, OR, majorité)
  - approche par décision souple (*soft*) : barycentre
- Si pas de centre de fusion, détection décentralisée ou **complètement**-distribuée
  - robuste à des attaques de nœuds
  - gestion simple du réseau
  - mais plus lent

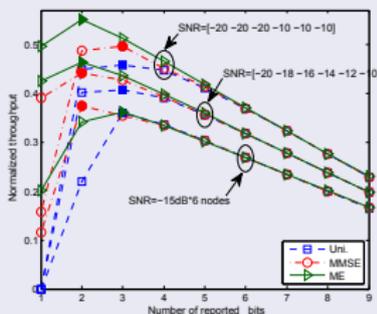
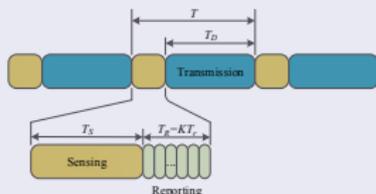
# Approche coopérative (souple) centralisée

$$T(\mathbf{y}) = \sum_{k=1}^K t_k(\mathbf{y}_k) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\geq}} \eta$$

## Problème

Remonter de l'information "continue" entre les capteurs et le centre de fusion

$$\text{Throughput} = \frac{T - T_{\text{sensing}} - T_{\text{reporting}}}{T} \pi_0 \text{Capacité} (1 - P_{FA})$$



# Approche décentralisée (1)

Sensing step of duration  $N_s$

$$t_k \propto \sum_{n=1}^{N_s} |x_k(n)|^2$$

Gossiping step of duration  $N_g$

$$T_\ell \approx \text{average}_k(t_k)$$

**Question** : Comment calculer la moyenne de  $t_k$  de manière distribuée

⇒ Algorithmes de consensus ou bavardage/*gossiping*

Un exemple d'algorithme (par paire)

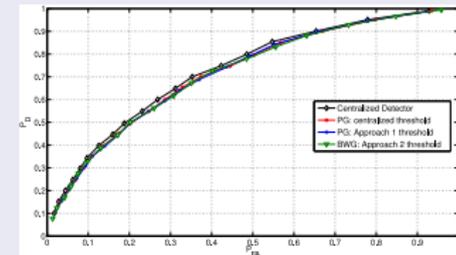
$\mathbf{t}(0) = [t_1, \dots, t_K]^T$  : valeurs initiales

A l'instant  $m$ , un nœud  $k$  se réveille et appelle un de ses voisins  $k'$ . Alors

$$t_k(m+1) = (t_k(m) + t_{k'}(m))/2$$

$$t_{k'}(m+1) = (t_k(m) + t_{k'}(m))/2$$

⇒  $\mathbf{t}(m+1) = \mathbf{W}(m)\mathbf{t}(m) \xrightarrow{m \rightarrow \infty} X_{\text{average}} \mathbf{1}$



$(N_s = N_g = 64, K = 10)$

# Approche décentralisée (2)

**sans coopération**

**avec coopération**

- Problème du terminal caché résolu

# Problèmes non traités

- Formation de coalition d'utilisateurs secondaires
- Optimisation de l'énergie dans les échanges de données
- Envoi régulier ou non d'information (*sensor approach*)
- Direction de Transmission (DoT) de l'utilisateur primaire
- Exploration multi-bandes
- etc

# Problèmes non traités

- Formation de coalition d'utilisateurs secondaires
- Optimisation de l'énergie dans les échanges de données
- Envoi régulier ou non d'information (*sensor approach*)
- Direction de Transmission (DoT) de l'utilisateur primaire
- **Exploration multi-bandes**
- etc

# Exploration multi-bandes

- Un utilisateur peut communiquer sur  $N_c$  canaux non-contigus (typiquement 4G avec l'agrégation de fréquence)
- Ne peut explorer simultanément que  $N_e$  canaux

**Problème : lesquels choisir à l'instant  $n$  ?**

## Processus de Markov décisionnel (MDP)

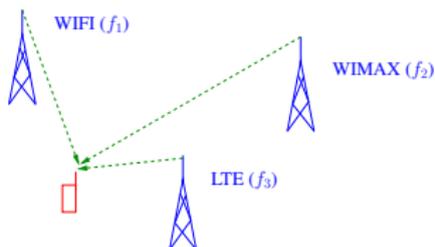
- Un décideur ..... l'utilisateur secondaire
- Des états (de l'instant  $n - 1$ ) ..... canaux vides/occupés
- Une action ..... choisir  $N_e$  canaux à explorer
- Noyau de transition  $\Pr(s_n | s_{n-1}, a_{n-1})$  ..... caractère markovien
- Un gain/*reward* :  $r(s_{n-1}, a_{n-1}, s_n)$  ..... 1 (si canal vide)
- Une politique/*policy*  $a_n = \pi(s_n)$  ..... (déterministe/aléatoire)

$$\text{Politique existe maximisant } \mathbb{E} \left[ \sum_n \gamma^n r(s_{n-1}, a_{n-1}, s_n) \right]$$

**Extension** : compétition entre utilisateurs  $\Rightarrow$  jeux stochastiques

# Classification des systèmes

Une fois les bandes libres détectées, **système** secondaire dessus



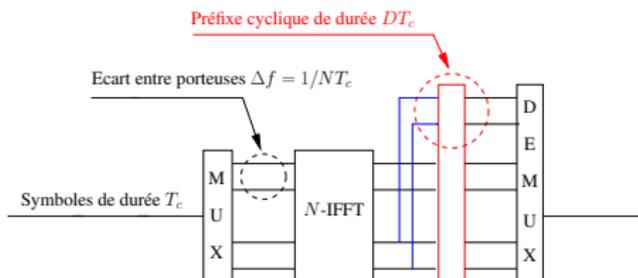
Par conséquent, un terminal cognitif doit pouvoir discriminer **rapidement** ces systèmes (standard) non nécessairement caractérisés par leur localisation spectrale.

- ▷ Structures intrinsèques à chaque système pour les différencier
- ▷ Systèmes actuels et futurs emploient l'OFDM (3GGP/LTE, WIFI, WIMAX, TNT, etc)

## Objectif

Discrimination de systèmes OFDM

# Discrimination de systèmes OFDM



- Préfixe cyclique : **NON**
- Nombre de sous-porteuses : **NON**
- Modulations linéaires affectées aux porteuses : **NON**
- Ecart entre porteuses ( $\Delta f = 1/NT_c$ ) : **OUI**

Système	LTE	Wifi	F-Wimax	M-Wimax	TNT
$\Delta f$ (kHz)	15	312.5	15.6	10.9	1.1

## Objectif

Discrimination de systèmes OFDM par estimation de  $\Delta f$

# Algorithmes possibles (1)

- Soit  $R(m, n) = \mathbb{E}[\overline{y(m+n)}y(m)]$  l'autocorrélation du signal OFDM reçu
- L'autocorrélation est non nulle pour  $R(m, 0)$  et  $R(m, \pm N)$  pour certains  $m$

Estimateur basé sur la corrélation (induite par le préfixe)

$$\hat{N} \propto \arg \max_{n \neq 0} \sum_{m=0}^M \overline{y(m+n)}y(m)$$

**Problème** : peu robuste au canal et à un court préfixe cyclique

# Algorithmes possibles (2)

La fonction  $m \mapsto R(m, \pm N)$  est périodique de période  $N + D$

- La fonction  $m \mapsto R(m, \pm N)$  se décompose en séries de Fourier

$$R(m, \pm N) = \sum_p R^{(p/(N+D))}(\pm N) e^{2i\pi \frac{mp}{(N+D)}}$$

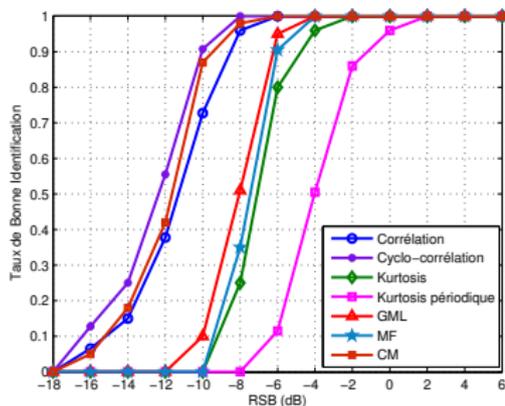
## Estimateur par cyclocorrélation

$$[\hat{N}, \hat{D}] = \arg \max_{n,d} \sum_{p=-N_b}^{N_b} \left| \hat{R}^{(p/(n+d))}(n) \right|^2$$

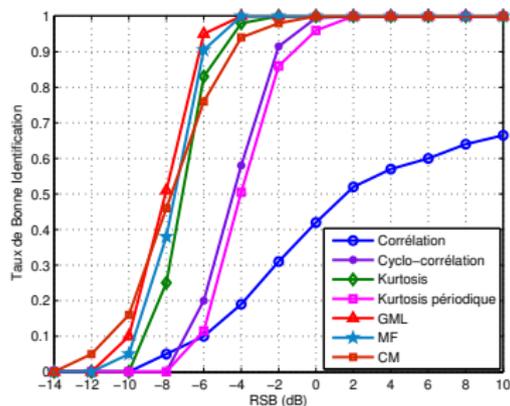
avec

$$\hat{R}^{(p/(n+d))}(n) = \sum_{m=0}^{M-1} \overline{y(m+n)} y(m) e^{-2i\pi \frac{mp}{(n+d)}}$$

# Simulations (1)

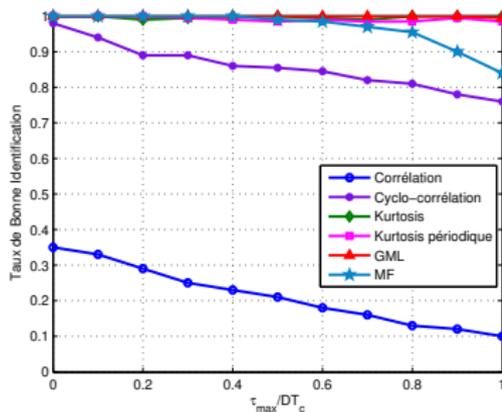


$D/N = 1/4$

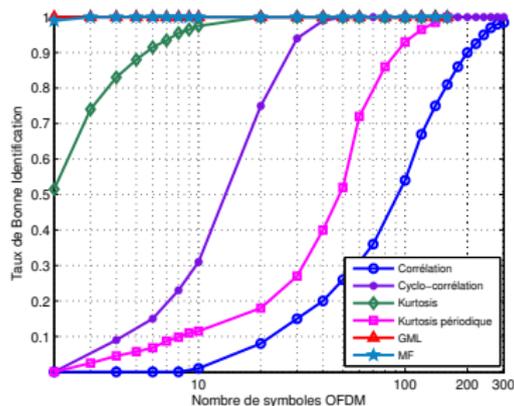


$D/N = 1/32$

# Simulations (2)



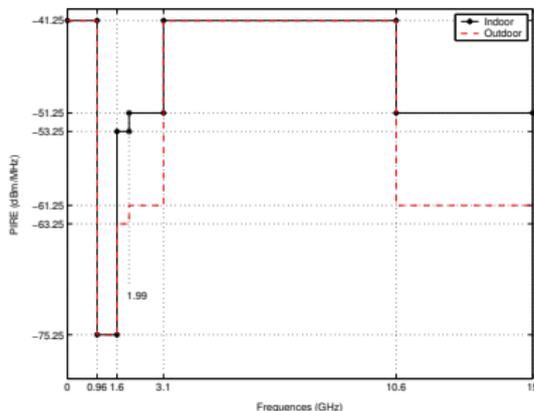
Canal de propagation



Durée d'observation

## Section 2 : Radio cognitive *underlay*

# Approche statique



## On “passe” sous les autres signaux primaires (*underlay*)

- Bande [3, 1 – 10, 6] GHz sans licence
- Contraintes sur les puissances d’émission
- Largeur de bande supérieure à 500 MHz
- Ultra-large bande/*ultra wide band* (UWB) autorisée par la FCC

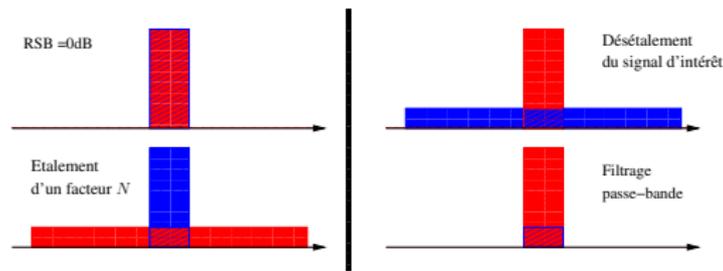
# Étalement de spectre

Moyen de transmission pour lequel les données occupent une bande largement supérieure à la bande minimale requise

- ▷ Lutte contre les brouilleurs
- ▷ Camouflage de l'information

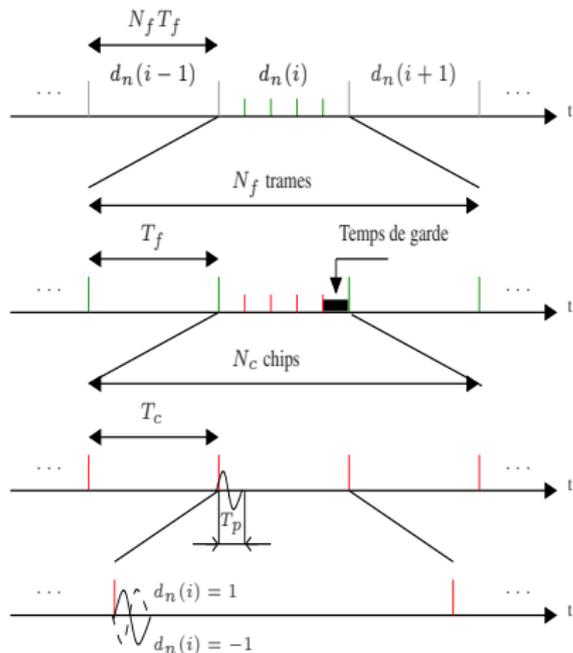
- $s(t)$  signal de données de bande  $1/T_s$
- $w(t)$  bruit à bande étroite de bande  $1/T_s$
- $e(t)$  fonction d'étalement de bande  $1/T_e \gg 1/T_s$  ( $|e(t)|^2 = 1$ )

Récepteur : Multiplier par  $\overline{e(t)}$



Gain d'étalement (en Rapport Signal-à-Bruit) :  $N = T_s/T_e$

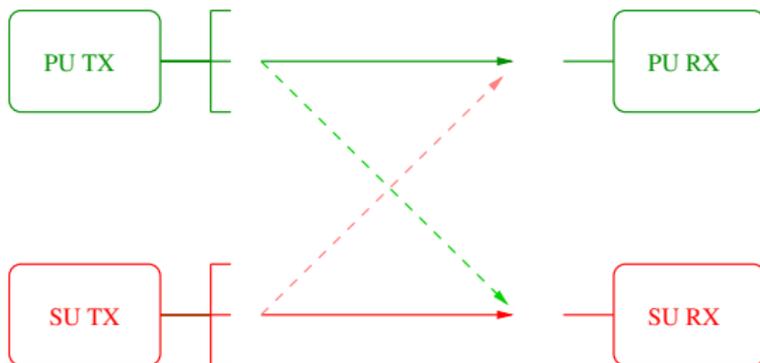
## IEEE 802.15.4a (bas débit et longue portée)



- $d_n(i)$  symboles émis
- $N_f$  nb de trames de durée  $T_f = N_c T_c$
- $N_c$  nb de chips de durée  $T_c$
- $p(t)$  impulsion de durée  $T_p \ll T_c$
- $\{c_n(j)\}_j \in \{0, N_c - 1\}$  code de saut temporel de l'utilisateur  $n$
- $\theta_n$  asynchronisme uniforme sur  $[0, N_f T_f[$

$$s_n(t) = \sum_{i=-\infty}^{+\infty} d_n(i) \sum_{j=0}^{N_f-1} p(t - iN_f T_f - jT_f - c_n(j)T_c - \theta_n)$$

# Approche dynamique



- Système MISO
- Canal  $\mathbf{h}_{p,p}$  (resp.  $\mathbf{h}_{s,s}$ ) connu par TX PU (resp. TX SU)
- Corrélation  $\mathbf{R}_{p,s} = \mathbb{E}[\mathbf{h}_{p,s}\mathbf{h}_{p,s}^H]$  connu
- Optimisation des *beamformers*  $\mathbf{w}_p$  et  $\mathbf{w}_s$

# Problème d'optimisation

$$\{\mathbf{w}_p, \mathbf{w}_s\} = \arg \max \mathbb{E} \left[ \log_2 \left( 1 + \frac{|\mathbf{h}_{s,s}^H \mathbf{w}_s|^2}{\sigma^2 + |\mathbf{h}_{p,s}^H \mathbf{w}_p|^2} \right) \right]$$

s.t.

$$\mathbb{E} \left[ \log_2 \left( 1 + \frac{|\mathbf{h}_{p,p}^H \mathbf{w}_p|^2}{\sigma^2 + |\mathbf{h}_{p,s}^H \mathbf{w}_s|^2} \right) \right] \geq \tau, \quad \|\mathbf{w}_p\|^2 \leq P_p^{\max}, \quad \|\mathbf{w}_s\|^2 \leq P_s^{\max}$$

## Problème très difficile à résoudre

Une solution sous-optimale (*primary-oriented*)

- $\mathbf{w}_p^* = \sqrt{P_p^{\max}} \mathbf{h}_p / \|\mathbf{h}_p\|$
- Utiliser convexité de  $x \mapsto \log_2(1 + 1/x)$  et inégalité de Jensen
- D'où

$$\mathbf{w}_s^* \propto \arg \min_{\mathbf{w}} \mathbf{w}^H \mathbf{R}_{p,s} \mathbf{w}$$

## Section 3 : Un problème de sécurité

# Attaque par émulation d'utilisateur primaire (PUE)

## Attaquant :

- Emule un utilisateur primaire durant l'étape de "sensing"
- Utilise le spectre ainsi bloqué dans l'étape "data"

## Défenseur :

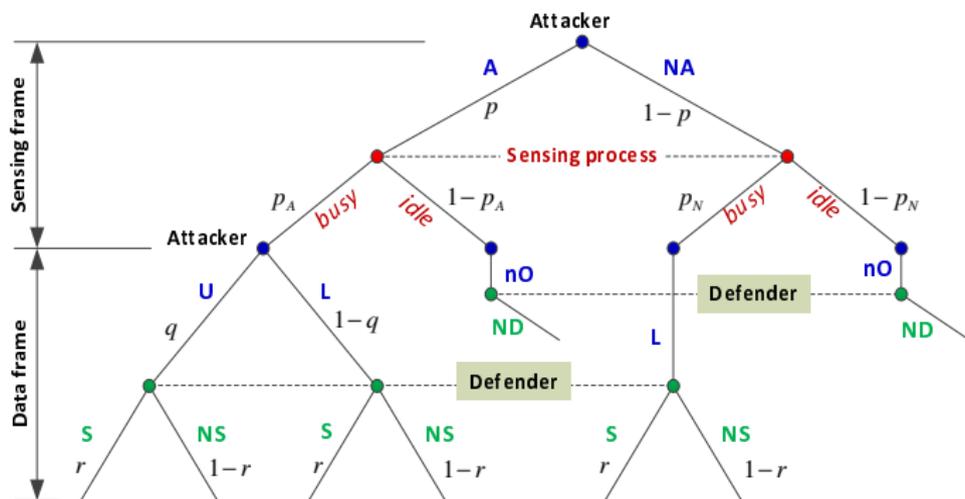
- Détermine l'identification de l'utilisateur durant l'étape "data"

## Problème de surveillance du canal

- Défenseur ne peut surveiller tout le temps car c'est cher
- Attaquant ne peut attaquer tout le temps de peur de se faire prendre

## Théorie de jeux

## Description du jeu



Déterminer les valeurs de  $p$ ,  $q$  et  $r$  de l'équilibre de Nash

$$U_n(x_n^{NE}, x_{-n}^{NE}) > U_n(x_n, x_{-n}^{NE}), \forall n$$

Autrement dit, aucun joueur n'a intérêt à dévier unilatéralement de sa stratégie  $x_n^{NE}$

# Equilibre de Nash

- $C_A$  : coût d'implémenter une attaque PUE
  - $C_U$  : coût de transmettre les données durant l'étape "data"
  - $G_U$  : gain d'utiliser le canal durant l'étape "data"
  - $\phi_C$  : pénalité de se faire prendre
- 
- $C_S$  : coût d'implémenter la surveillance
  - $G_S$  : gain de prendre un attaquant

$$\text{Si } C_A \geq C_A^{(0)} \quad p = 0, q = 0, r = 0$$

$$\text{Si } C_A < C_A^{(0)},$$

$$G_S \leq G_S^{(0)} \Rightarrow p = 1, q = 1, r = 0$$

$$G_S > G_S^{(0)} \Rightarrow p \neq \{0, 1\}, q = 1, r \neq \{0, 1\} (\text{si } C_A > C_A^{(1)})$$

$$p = 1, q = 1, r = 1 (\text{si } C_A \leq C_A^{(1)})$$

# Conclusion

- Grande variété de problème
- Grande variété d'outils
- Encore de nombreux problèmes ouverts

# Bibliographie

- E. Axell, E. Larsson, V. Poor, "Spectrum sensing for cognitive radio", IEEE Signal Processing Magazine, Mai 2012.
- L. Lunden, V. Koivunen, V. Poor, "Spectrum exploration and exploitation for cognitive radio", IEEE Signal Processing Magazine, Mai 2015.
- F. Iutzeler, P. Ciblat, "Fully distributed signal detection : application to cognitive radio", Conf. Eusipco, Septembre 2013.
- P. de Kerret, M. Filippou, D. Gesbert, "Statistically coordinated precoding for the MISO cognitive radio channel", Conf. Asilomar, Novembre 2014.
- N. Nguyen-Thanh, P. Ciblat, A.T. Pham, V.-T. Nguyen, "Surveillance strategies against primary user emulation attack in cognitive radio networks", IEEE Transactions on Wireless Communications, Septembre 2015.