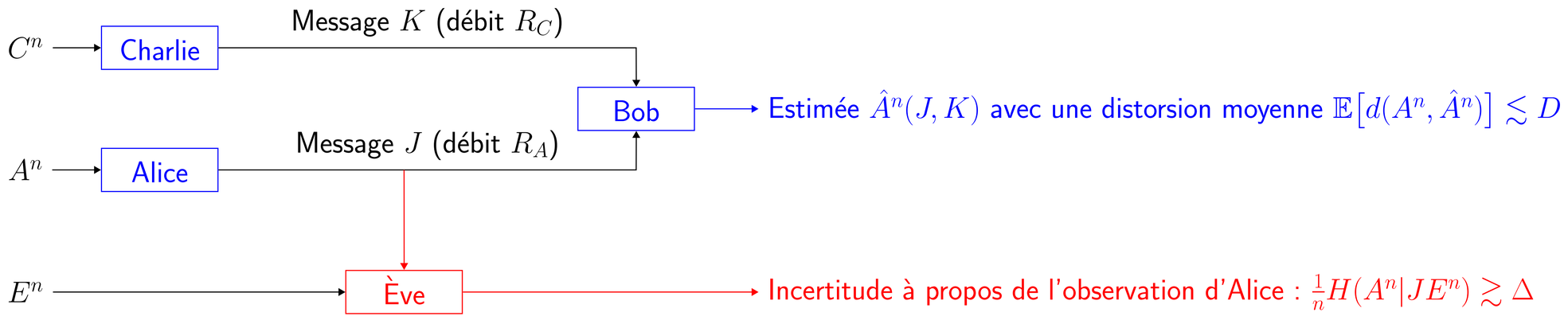
Codage de source avec contraintes de sécurité

Joffrey Villard

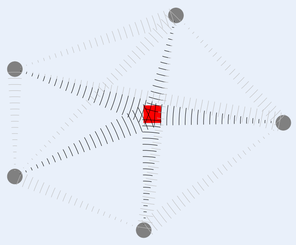
SUPÉLEC, Dpt. Télécommunications, Gif-sur-Yvette, France

Encadrants de thèse : Pascal Bianchi (Télécom ParisTech/CNRS-LTCI) et Pablo Piantanida (Supélec)

Correspondant DGA : Albin Dunand (DGA IP/TSI/TTS)



Contexte : les réseaux de capteurs sans fil



- un phénomène physique
- des capteurs
- un centre de fusion
- des canaux sans fil

- Phénomènes complexes
  - ▷ corrélation spatiale et temporelle
- Canaux de communication sans fil
  - ▷ observations dégradées (bruitées ou quantifiées) au centre de fusion
  - ▷ communications publiques

Champs d'application

- Défense : localisation/classification de cible, reconnaissance de terrain, monitoring d'équipement...
- Industrie : contrôles en cours de production, détection d'incidents...
- Veille environnementale et sanitaire : pollutions, incendies, séismes...

Théorie de l'information et sécurité

- Cryptographie "classique"
  - ▷ sécurité basée sur la complexité de certains problèmes, supposés insolubles (en temps raisonnable) par l'adversaire
  - ▷ algorithmes lourds (dans la couche applicative)
- Motivations
  - ▷ besoin d'une sécurité inconditionnelle (p. ex. pour des données très sensibles)
  - ▷ niveau de sécurité supplémentaire (dans la couche physique)
  - ▷ capteurs faible coût, aux capacités limitées
- L'entropie $H(\cdot)$, définie par Shannon,
  - ▷ mesure l'incertitude à propos d'une variable aléatoire
  - ▷ permet une nouvelle définition (quantitative) de la sécurité
- Idée : utiliser les propriétés statistiques du système pour maximiser l'incertitude "résiduelle" de l'adversaire
- Limitation : nécessite une certaine connaissance de la situation de l'adversaire

Objectifs généraux

- Calculer des bornes théoriques sur les performances du système
- En déduire des principes pour la réalisation de solutions optimales
- Proposer des protocoles (sous-)optimaux (traitement de signal, communications)

Le cas de 4 utilisateurs : Alice, Bob et Charlie vs. Ève

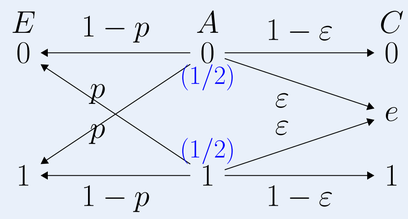
- Canaux de communication sans erreur et à débit limité
- Objectifs du système (a priori contraires) :
  - ▷ minimiser les débits R_A et R_C
  - ▷ minimiser la distorsion de Bob D
  - ▷ maximiser l'incertitude de Ève Δ
- But : Trouver tous les (R_A, R_C, D, Δ) atteignables

Résultats

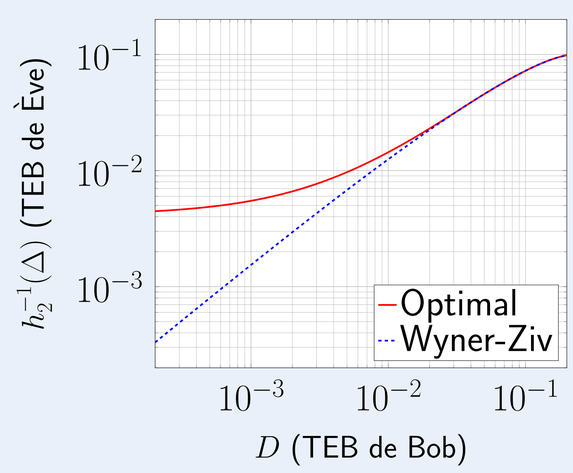
- Schéma atteignable :
  - ▷ Charlie transmet 1 message qui décrit sa source C^n
  - ▷ Alice transmet une description de A^n en 2 parties (commune et privée) judicieusement choisies
- Bornes générales sur les performances
- Optimalité dans certains cas, dont
  - ▷ compression distribuée : Bob souhaite retrouver parfaitement A et C
  - ▷ information adjacente non codée à Bob : Bob et Charlie sont confondus

Applications numériques

- Source binaire uniforme avec informations adjacentes CBE/CBS



- Avec $p = 0.1$, $\varepsilon = h_2(p) \approx 0.469$, et un débit R_A non limité :



- Le taux d'erreur binaire de Bob peut tendre vers zéro alors que celui de Ève reste supérieur à $4 \cdot 10^{-3}$
- Si la distorsion demandée D est peu contraignante, le codage classique (Wyner-Ziv) est suffisant

Perspectives

- Étudier le problème général du codage sécurisé source/canal :
  - ▷ prendre en compte la nature aléatoire des canaux de transmission
  - ▷ utiliser leurs propriétés statistiques pour accroître la sécurité
- Considérer plusieurs adversaires (fictifs) pour traiter le cas où on ne connaît pas (bien) la situation de l'adversaire réel
- Proposer des méthodes pratiques pour approcher les bornes théoriques

Publications récentes

- Villard, J. & Piantanida, P., "Secure Lossy Source Coding with Coded/Uncoded Side Information at the Receivers," soumis à *IEEE Transactions on Information Theory*
- Villard, J. & Bianchi, P., "High-Rate Vector Quantization for the Neyman-Pearson Detection of Correlated Processes," accepté pour publication dans *IEEE Transactions on Information Theory*.
- Villard, J., Piantanida, P. & Shamai, S., "Secure Lossy Source-Channel Wiretapping with Side Information at the Receiving Terminals," ISIT 2011, Saint-Pétersbourg, Russie.
- Villard, J. & Piantanida, P., "Codage de source sous contrainte de sécurité avec information adjacente aux récepteurs," soumis au GRETSI 2011, Bordeaux, France.

http://perso.telecom-paristech.fr/~villard/ Email : joffrey.villard@supelec.fr