

**Soutenance de
l'Habilitation à Diriger les Recherches**

Codage dans les réseaux

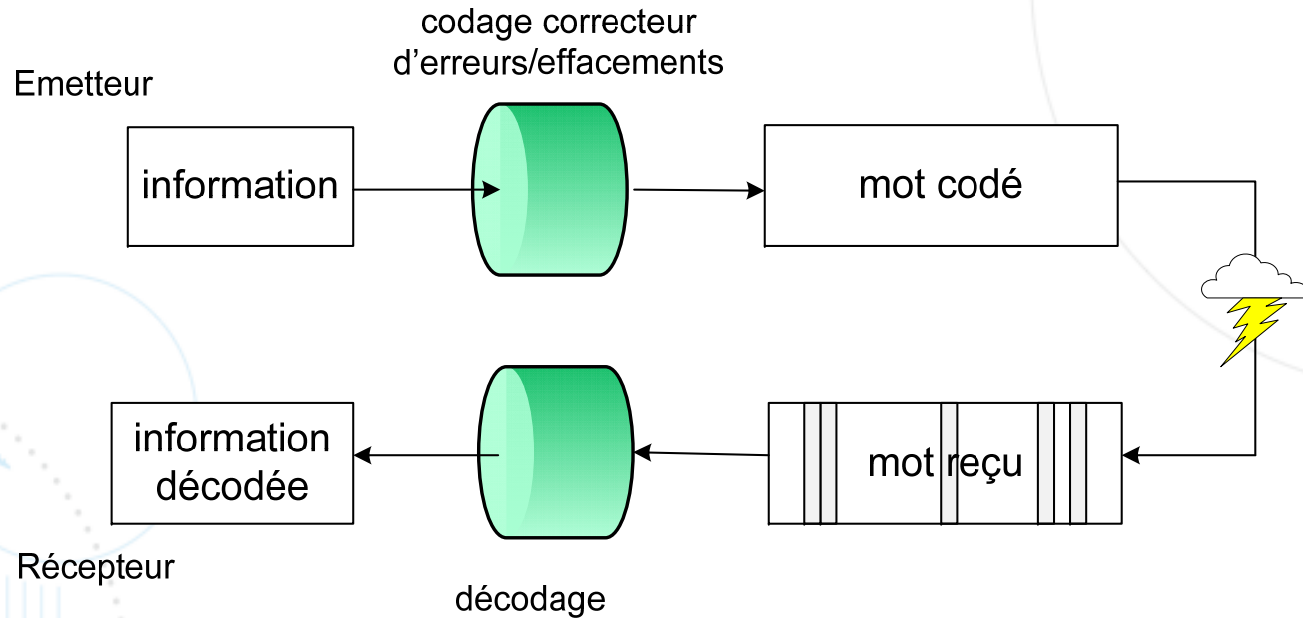
Jérôme Lacan

**Université de Toulouse
ISAE / TésA / LAAS-CNRS**

campus ENSICA, Toulouse, 5 décembre 2008

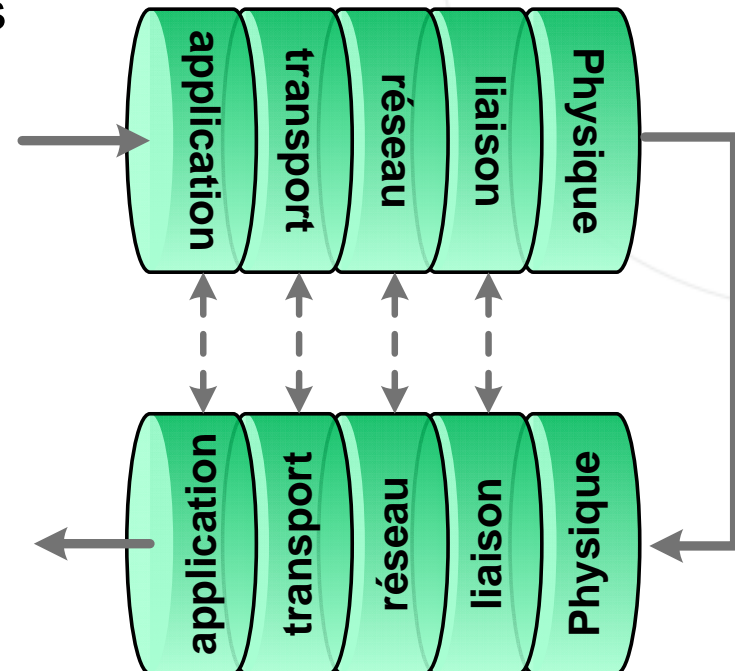
Introduction au codage correcteur d'erreurs dans les réseaux

- schéma classique de protection contre les erreurs/effacements :

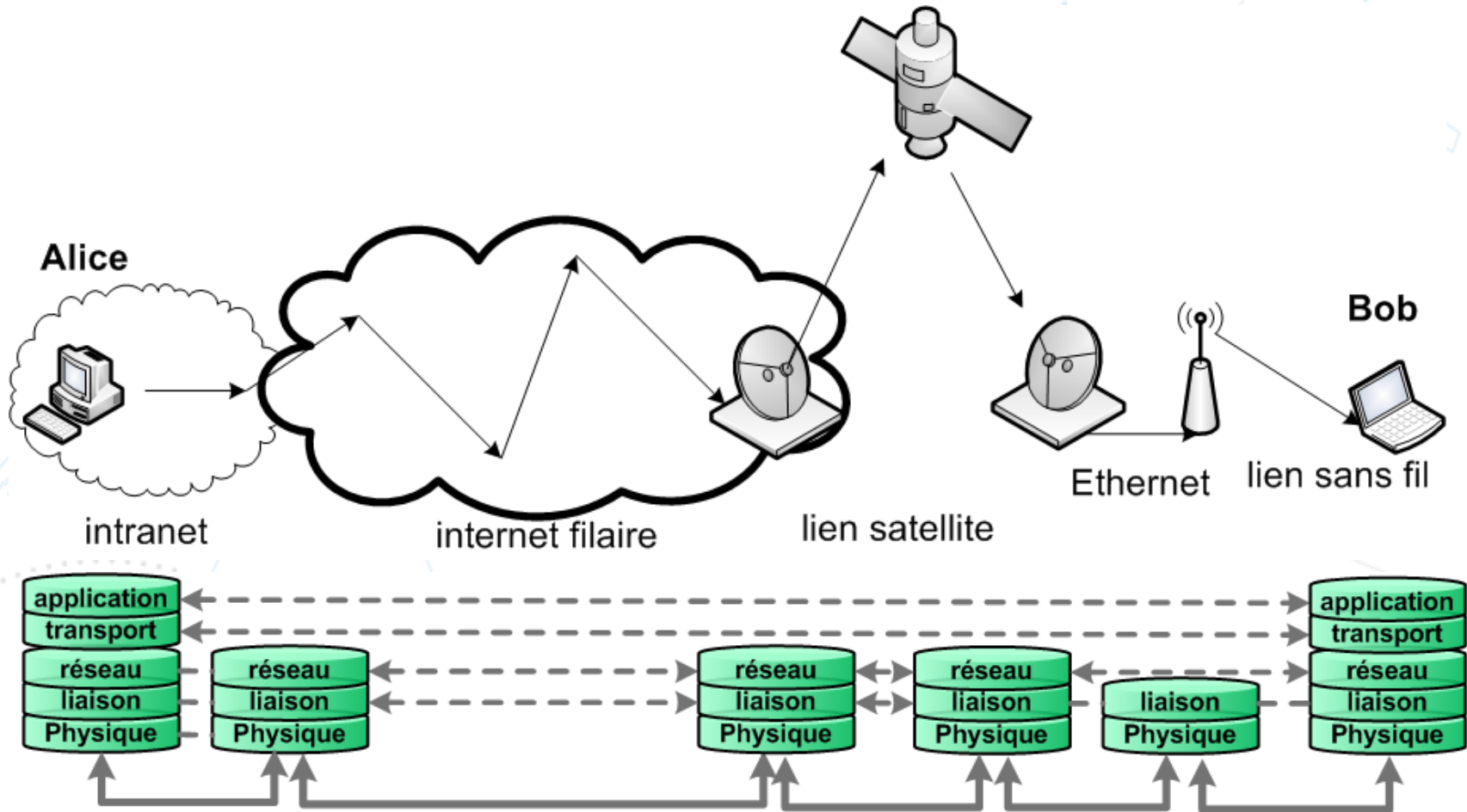


Introduction – en pratique

- En pratique, en plus de la fiabilité, un réseau de communication doit pouvoir :
 - identifier les différentes machines
 - trouver le chemin d'une machine à une autre
 - gérer le contrôle de flux et de congestion
 - assurer la sécurité des données



Introduction – encore plus pratique ...



Introduction –

gestion de la fiabilité par les différentes couches protocolaires

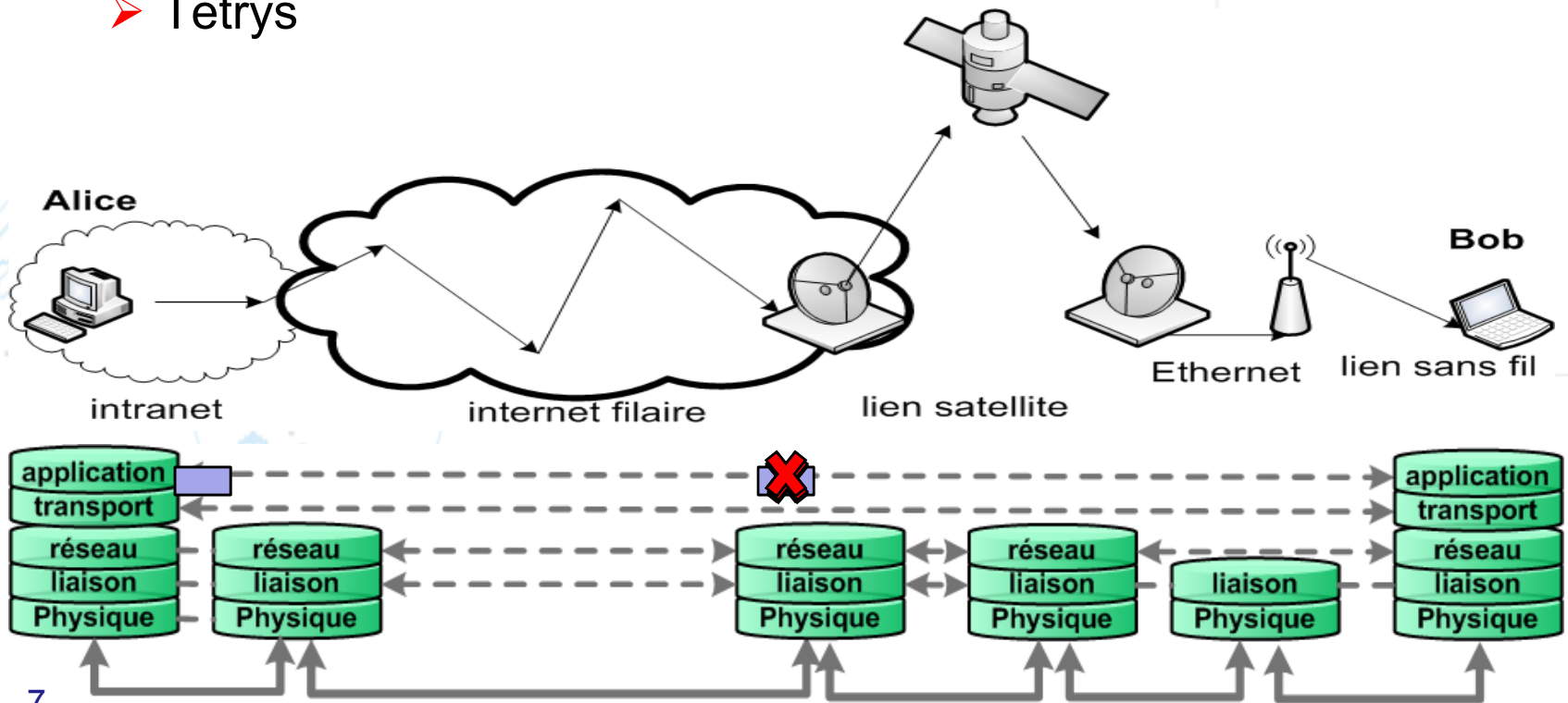
- Chaque couche protocolaire a des contraintes différentes. Par exemple,
 - la couche physique doit combattre les erreurs sur les bits ou sur les symboles transmis
 - la couche liaison doit détecter des unités de données erronées et les récupérer
 - la couche transport doit gérer des pertes de données liées aux congestions dans les routeurs
- 3 classes de mécanismes de fiabilité sont disponibles :
 - mécanismes réactifs : retransmissions (ARQ)
 - mécanismes proactifs : ajout de redondance à priori (code correcteur d'erreurs, code à effacement).
 - mécanismes hybrides : combinaisons de mécanismes réactifs et proactifs

Plan de la soutenance

- Contributions à la construction des codes à effacements
- Codage multi-couches
- Applications des codes correcteurs d'erreurs dans les réseaux
- Conclusion et perspectives

Contributions à la construction des codes à effacements

- Codes à effacements : génération d'unités de données redondantes pour combattre les pertes de données :
 - codage à protection inégale
 - Tetrys



Codes à effacements – codage à protection inégale

- Contexte :
 - les flux transmis par certaines applications peuvent contenir des données d'importance différentes
 - il peut donc être nécessaire de construire des mécanismes de protection inégale
 - Etat de l'art :
 - ✓ modulation hiérarchique
 - ✓ code correcteurs d'erreurs à protection inégale
 - ✓ une partie des travaux sur le codage conjoint source-canal
 - ✓ système de protection inégale des paquets de données (Priority Encoding Transmission –PET – M. Luby 1995)
 - ✓ ...

Codes à effacements – codage à protection inégale

- Contribution (2006 - avec A. Bouabdallah) : méthode de construction d'un code à effacement intégrant les dépendances entre les données : DA-UEP (Dependency-Aware Unequal Erasure Protection)
- Principe : modifier la matrice génératrice d'un code MDS en remplaçant certains coefficients par 0 de telle sorte à respecter la règle suivante :

Un symbole de redondance protégeant un symbole source s doit protéger tous les symboles source dont s dépend.

Pour la vidéo , ceci implique qu'un paquet redondant protégeant un paquet issu d'une image t doit

- protéger tous les paquets issus de cette image
- protéger toutes les images dont dépend l'image t

Codes à effacements – codage à protection inégale

- Exemple:

➤ Soit le GOP suivant :

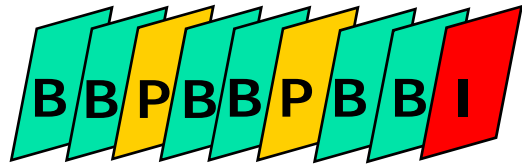
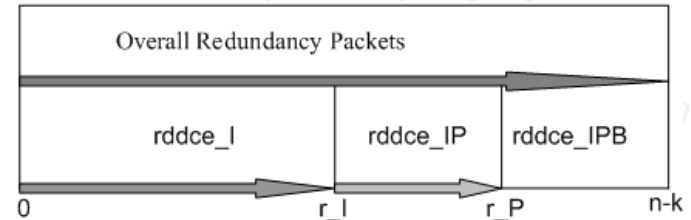


Image	I	P	B
Nb de paquets	5	2	1

$k = 15, n = 20, r_I = 2, r_P = 2$

➤ Méthode de décodage similaire aux codes MDS



$$G_{20,15} = \begin{pmatrix} \alpha_{1,5} & \dots & \dots & \dots & \alpha_{1,5} \\ \vdots & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & \vdots \\ \alpha_{5,1} & \dots & \dots & \dots & \alpha_{5,5} \\ 0 & 0 & 0 & 0 & \alpha_{6,5} \\ 0 & 0 & 0 & 0 & \alpha_{7,5} \\ 0 & 0 & \alpha_{8,3} & \alpha_{8,4} & \alpha_{8,5} \\ 0 & 0 & \alpha_{8,4} & \alpha_{9,4} & \alpha_{9,5} \\ 0 & 0 & 0 & 0 & \alpha_{10,5} \\ 0 & 0 & 0 & 0 & \alpha_{11,5} \\ 0 & 0 & 0 & \alpha_{12,4} & \alpha_{12,5} \\ 0 & 0 & 0 & \alpha_{12,5} & \alpha_{13,5} \\ 0 & 0 & 0 & 0 & \alpha_{14,5} \\ 0 & 0 & 0 & 0 & \alpha_{15,5} \end{pmatrix} \begin{matrix} \text{I} \\ \text{B} \\ \text{B} \\ \text{P} \\ \text{P} \\ \text{P} \\ \text{P} \\ \text{P} \\ \text{P} \end{matrix}$$

Codes à effacements – codage à protection inégale

- Exemple de résultats de simulation :

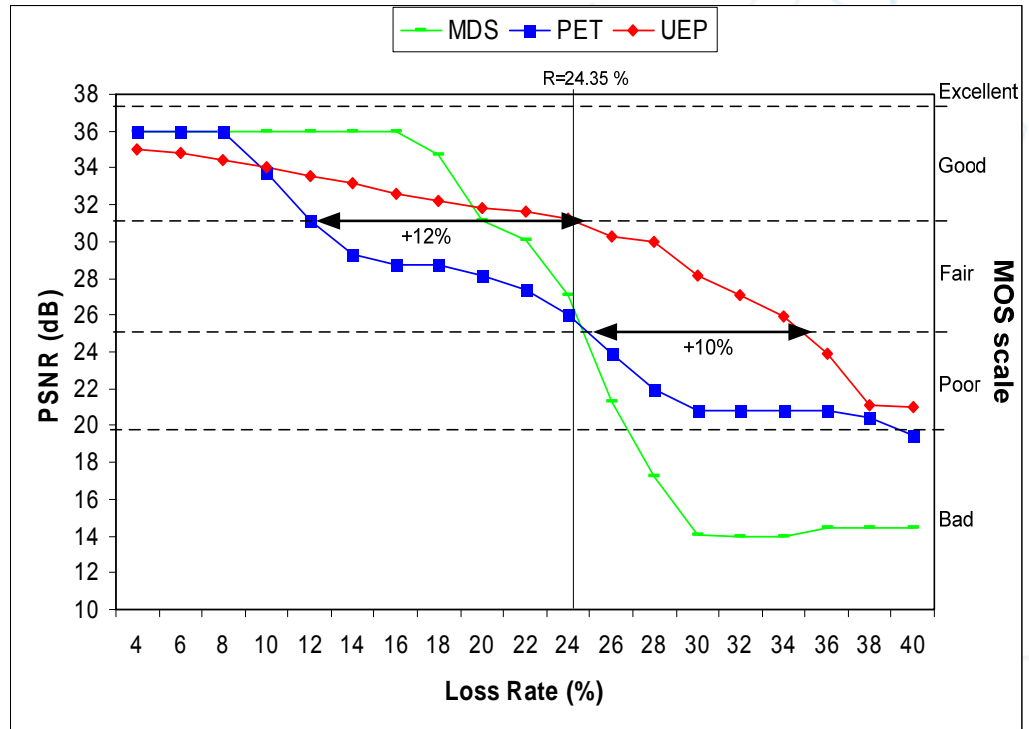
- DA-UEP

- $r_I = 40\%$
- $r_P = 60\%$

- PET

- I packets: 60%
- P packets: 75%
- B packets: 90%

- niveau de redondance moyen
 $r = 24,35\%$



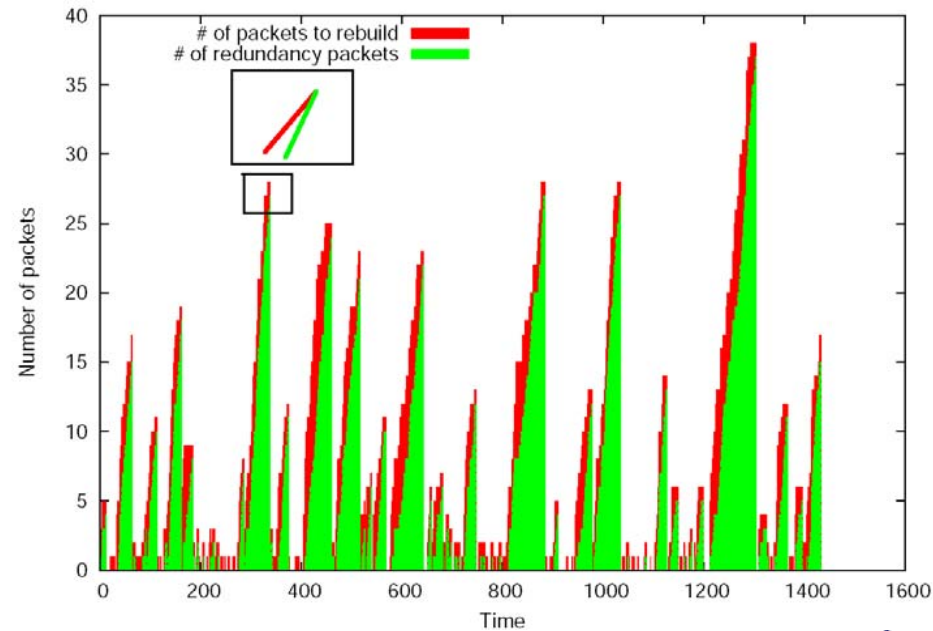
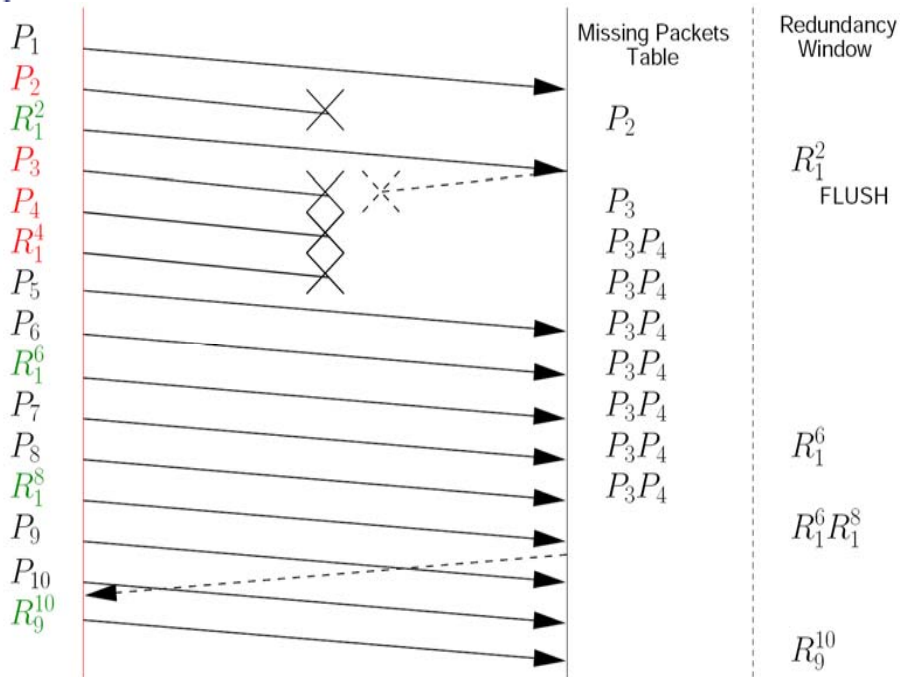
- Modélisation des performances réalisée en considérant ces codes comme des codes « emboîtés »

Codes à effacements – Tetrys

- Objectif : améliorer l'intégration des codes à effacement dans les protocoles de communication
- Contribution (2008 - avec E. Lochin) : suppression de la notion de code en bloc tout en assurant une fiabilité totale grâce aux acquittements.
- Gain en termes de délai de récupération des paquets, de temps de calcul et de niveau de fiabilité. De plus, le mécanisme est tolérant aux pertes des acquittements.
- Travaux relatifs :
 - hybride-ARQ, codes rateless (LT, Raptor, online), codes convolutifs sur la canal à effacement de paquets, ...
 - codage réseau avec acquittements et application à TCP

Codes à effacements – Tetrys

- Principe : les paquets de redondance sont générés en fonction des paquets source non encore acquittés
- Exemple:



Codes à effacements – Tetrys

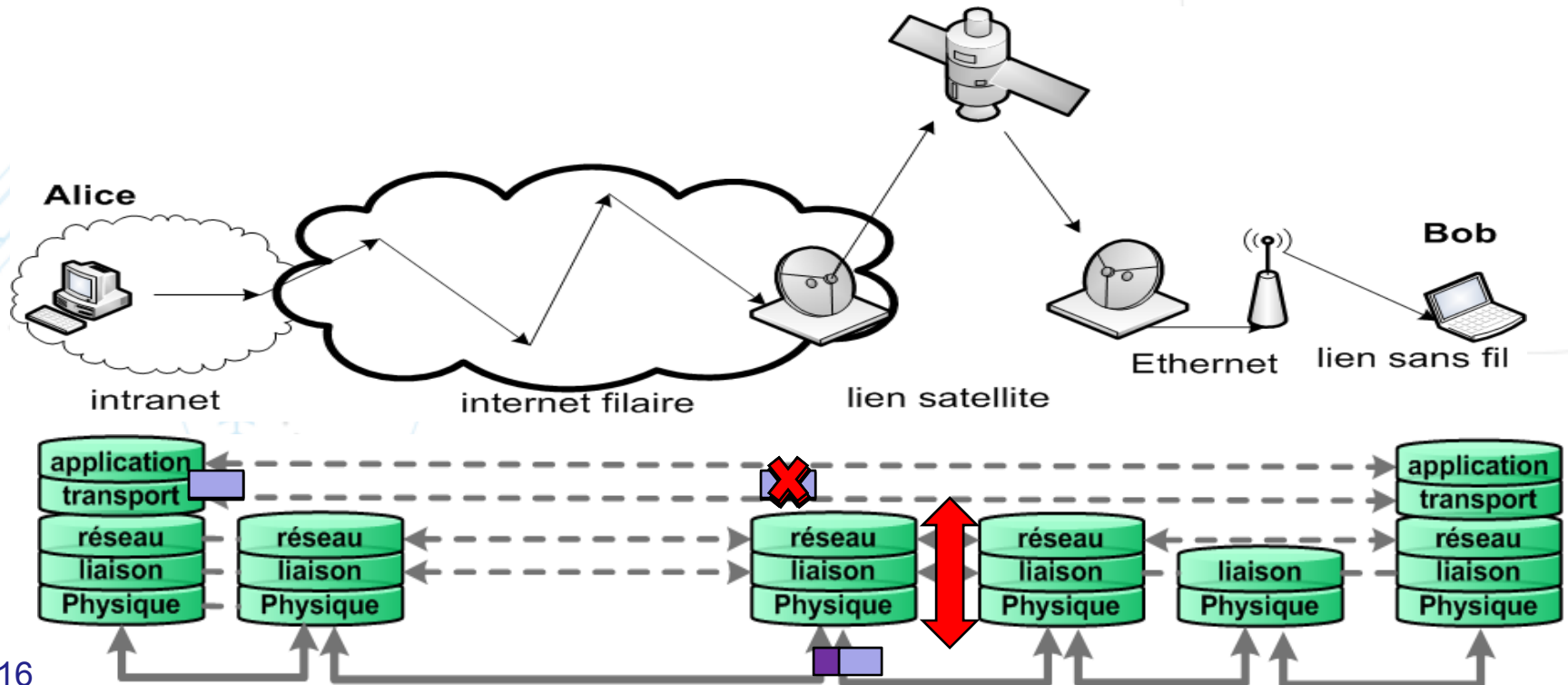
- Modélisation du comportement de Tetrys sur un canal avec des pertes indépendantes : problème de la marche aléatoire sur les entiers positifs
 - délai de récupération des paquets
 - taille des matrices à inverser
 - temps de récurrence
- Simulations du mécanisme :
 - influence de la différence entre le taux de redondance et le taux de perte sur le délai de récupération
 - influence de la taille du corps fini : GF(8) semble suffisant
 - influence des bursts de perte
- Validations théorique et pratique du concept

Codes à effacements – Conclusion et perspectives

- Travaux à court terme :
 - développement de Tetrys (par exemple, intégration de la protection inégale)
- Travaux à moyen terme :
 - adaptation des codes à effacements aux contraintes des applications et des protocoles

Codage multi-couches-

- Problématique : comment combiner des techniques de codage utilisées sur plusieurs couches ?
 - transmissions satellite-mobile : cas du DVB-SH
 - HERACLES

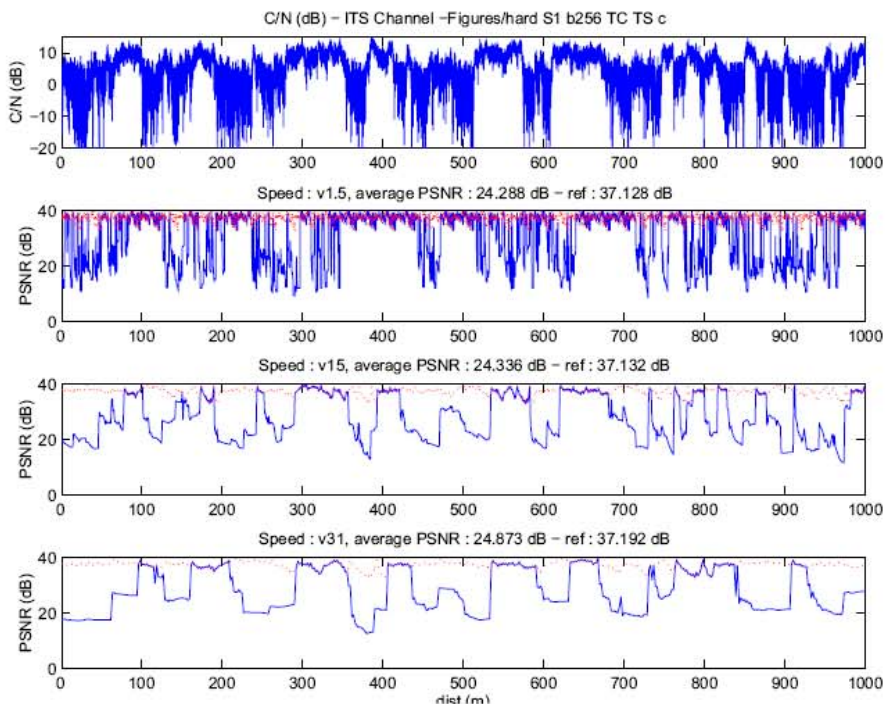


Codage multi-couches- transmissions satellite-mobiles

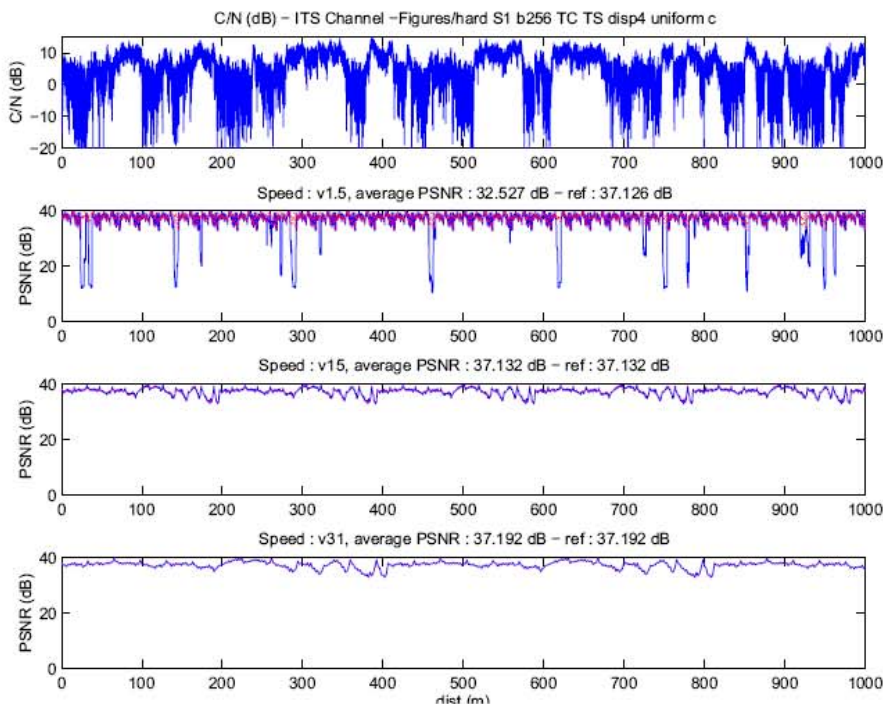
- Contexte : l'utilisation du codage sur les couches hautes pose naturellement la question de la cohabitation avec le codage de la couche physique
- Travaux précédents (2004 -avec F. Arnal, L. Dairaine et G.Maral) : étude de la possibilité de laisser remonter les erreurs bits vers un code à effacements vers les couches hautes
- Etudes CNES (2006-2007 - avec A. Bouabdallah, M.Kieffer, G. Sabeva, P. Duhamel, C. Bazile, G. Scot) : diffusion vidéo satellite vers des mobiles (S-DMB, DVB-SH)
 - transmission uni-directionnelle en bande S
 - canal extrêmement variable
 - codage correcteur envisagé sur les couches physique et liaison + codage vidéo
 - un récepteur mobile reçoit directement le flux satellite → possibilité d'utiliser de manière réaliste des mécanismes multi-couches

Codage multi-couches- transmissions satellite-mobile

- Le canal étant extrêmement variable, il est nécessaire que les unités de données codées soient envoyées dispersées dans l'espace :
 - dispersion naturelle due à la mobilité du récepteur
 - dispersion artificielle rajoutée par un entrelaceur temporel



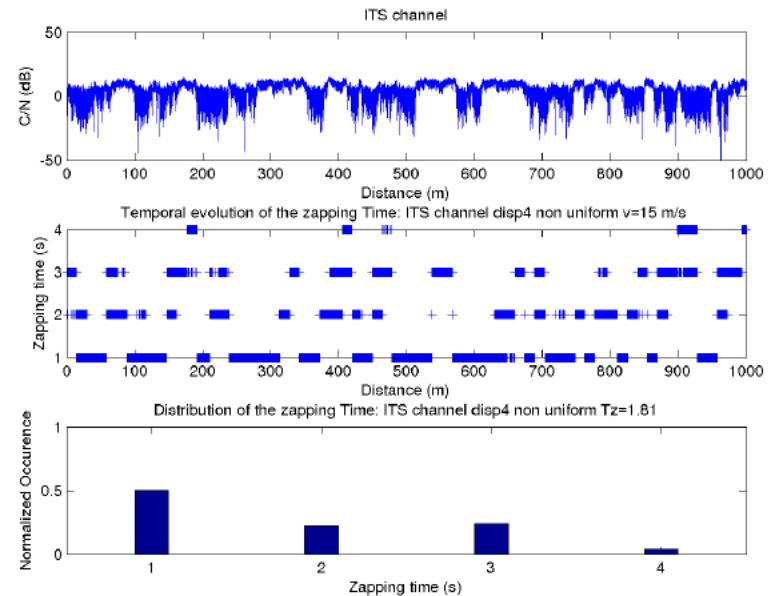
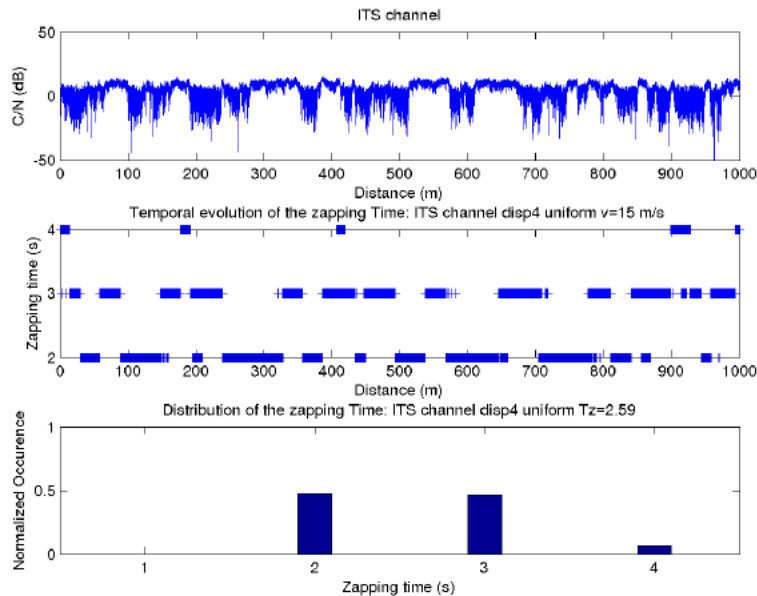
(a) variation du PSNR sans entrelaceur



(b) variation du PSNR avec un entrelaceur de 4 secondes

Codage multi-couches- transmissions satellite-mobile

- Influence de l'entrelaceur temporel sur le temps de zapping : possibilité d'utiliser un entrelaceur non uniforme



(a) Distribution du temps de zapping pour un entrelaceur uniforme de 4s (b) Distribution du temps de zapping pour un entrelaceur non uniforme de 4s

Codage multi-couches-transmissions satellite-mobile

- Distribution de la redondance sur les différentes couches :

➤ vidéo vs code à effacement

R	T_{block} (s)				Noise-free
	0	1	2	3	
250 kbps	24.5				36.8
200 kbps	24.6	26.2 RS(261, 157)	26.5 RS(521, 313)	27.5 RS(782, 469)	35.8
150 kbps	23.9	28.2 RS(196, 118)	30.1 RS(391, 235)	30.8 RS(586, 252)	34.4
100 kbps	23.1	28.4 RS(131, 79)	30.1 RS(261, 157)	30.1 RS(391, 233)	32.3

Tab. 4.1 – PSNR moyen (PLR) pour $v = 15$ m/s, pour différentes combinaisons de débit de la vidéo et pour plusieurs longueurs de $T_{\text{block}} = 0$.

➤ code à effacement vs code correcteur d'erreurs de la couche physique

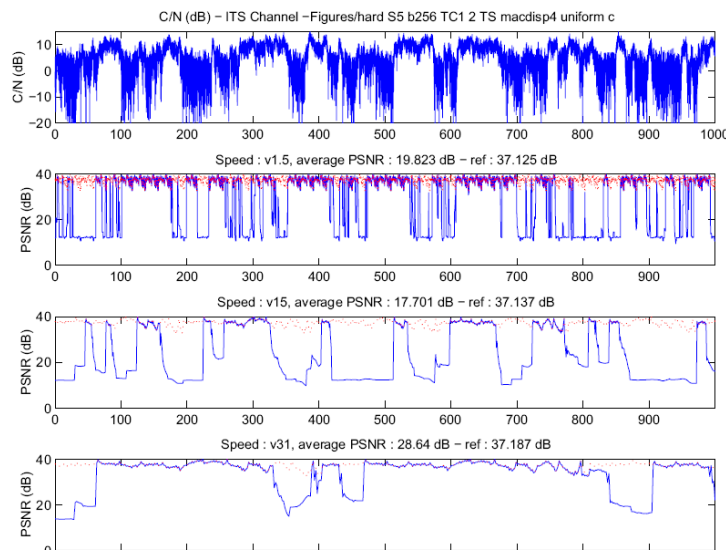


FIG. 4.6 – PSNR avec un Turbo code de taux de codage 1/2 sur la couche physique et un code à effacement de taux de codage 2/3 sur la couche liaison

Codage multi-couches- transmissions satellite-mobile

- plusieurs autres solutions de mécanismes de protection étudiées :
 - remontées des erreurs jusqu'au code à effacement (utilisé en mode « erreur ») et jusqu'à la couche application
 - code à effacement à protection inégale
 - dans le codage vidéo, augmentation de la proportion de données codées en intra
- Conclusion : excellent cas d'étude montrant toutes les solutions de protection contre les erreurs et l'intérêt de l'approche multi-couche

Codage multi-couches- HERACLES

- Observation : l'indépendance des couches protocolaires et le fait que chaque paquet doit être acheminé indépendamment entraînent que chaque paquet contient une quantité de redondance importante.
- Contribution (2005 – avec J. Cantillo, M. L. Boucheret, I Buret et F. Arnal) : utilisation de cette redondance pour la délimitation des paquets et pour la correction contre les erreurs de transmission :

HERACLES (Header-Redundancy-assisted Cross-Layer Error Suppression)

Ethernet IP TCP FTP_data

```
00 0d 60 cc 55 15 00 02 b3 ec 6c d4 08 00 45 00
00 30 00 00 40 00 2e 06 de 3d d4 1b 3f 03 cb b2
8f b9 00 15 05 3f ae 56 1c f2 95 7a 7f 79 70 12
16 d0 18 24 00 00 02 04 05 b4 01 01 04 02 00 00
```

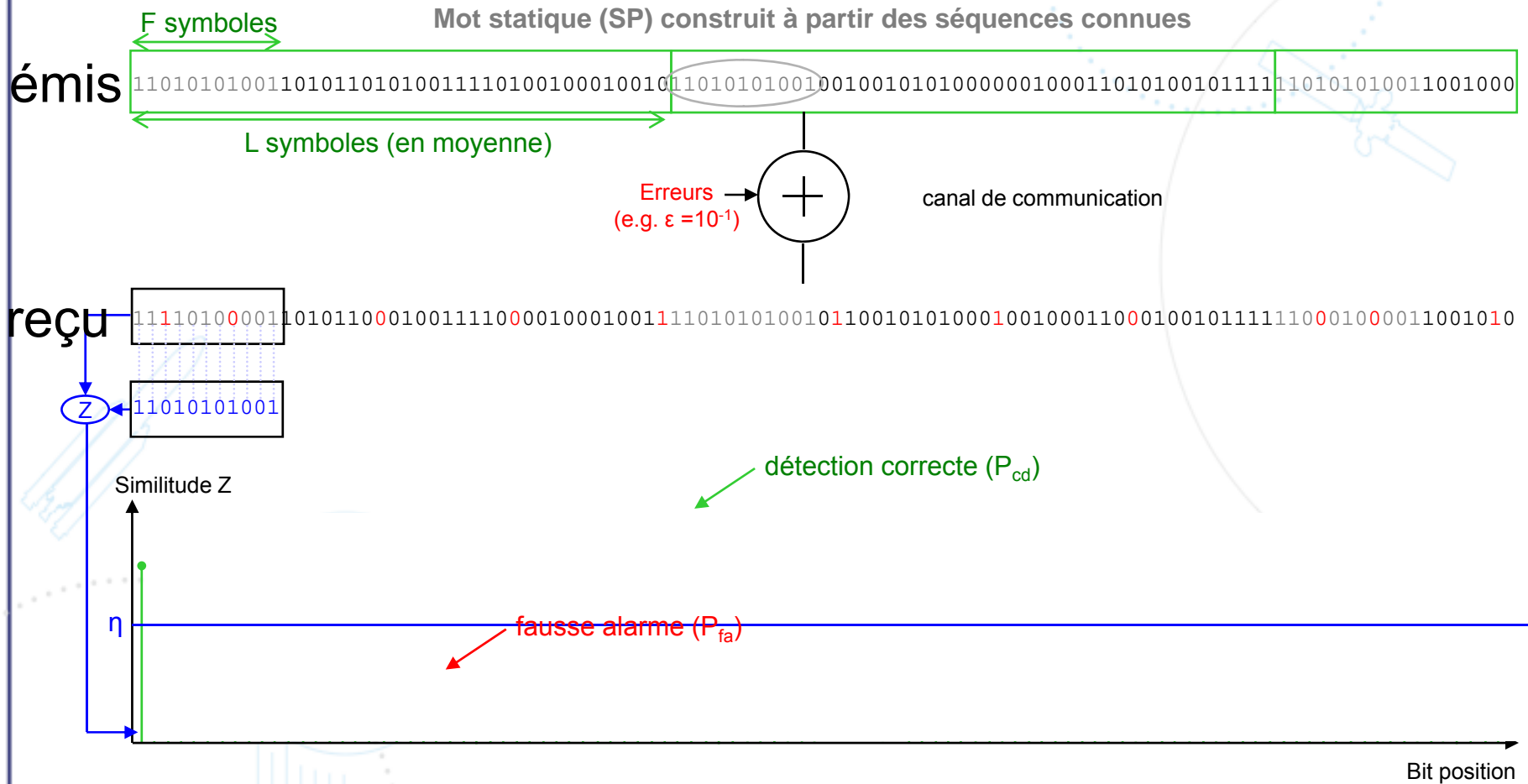
```
00 0d 60 cc 55 15 00 02 b3 ec 6c d4 08 00 45 00
00 7e 19 dc 40 00 2e 06 c4 13 d4 1b 3f 03 cb b2
8f b9 00 15 05 3f ae 56 1c f3 95 7a 7f 79 50 18
16 d0 45 05 00 00 32 32 30 20 53 65 72 76 65 75
72 20 64 65 20 6d 69 73 65 20 61 20 6a 6f 75 72
20 64 65 73 20 70 61 67 65 73 20 70 65 72 73 6f
20 64 65 20 46 72 65 65 2e 66 72 20 76 65 72 73
69 6f 6e 20 5b 46 65 62 20 31 31 20 32 30 30 37
20 32 30 3a 32 32 3a 31 34 5d 0d 0a
```

```
00 0d 60 cc 55 15 00 02 b3 ec 6c d4 08 00 45 00
00 4d 19 de 40 00 2e 06 c4 42 d4 1b 3f 03 cb b2
8f b9 00 15 05 3f ae 56 1d 49 95 7a 7f 88 50 18
16 d0 95 60 00 00 33 33 31 20 50 61 73 73 77 6f
72 64 20 72 65 71 75 69 72 65 64 20 66 6f 72 20
77 77 77 2e 6a 75 61 6e 2e 0d 0a
```

```
00 0d 60 cc 55 15 00 02 b3 ec 6c d4 08 00 45 00
00 5e 19 e7 40 00 2e 06 c4 28 d4 1b 3f 03 cb b2
8f b9 00 15 05 3f ae 56 1e 26 95 7a 7f bc 50 18
16 d0 53 1a 00 00 31 35 30 20 4f 70 65 6e 69 6e
67 20 41 53 43 49 49 20 6d 6f 64 65 20 64 61 74
61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f 72
20 66 69 6c 65 20 6c 69 73 74 0d 0a
```

Exemple d'une capture d'un flux FTP

Codage multi-couches-HERACLES

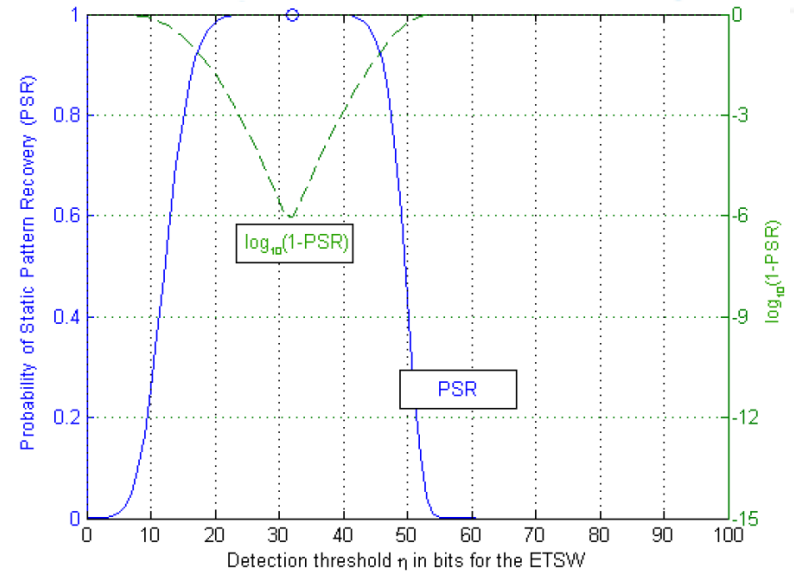


Codage multi-couches- HERACLES

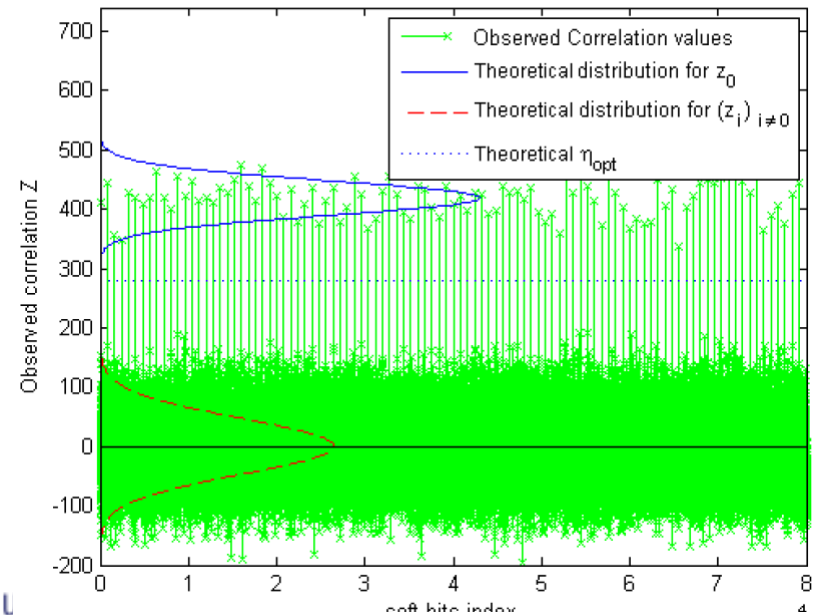
- Utilisation de HERACLES en mode « délinéation »

- détermination du seuil η_{opt} qui maximise $PSR = P_{cd} \times (1 - P_{fa})^{L-1}$

- fonctionne au niveau des bits ou des LLR reçus



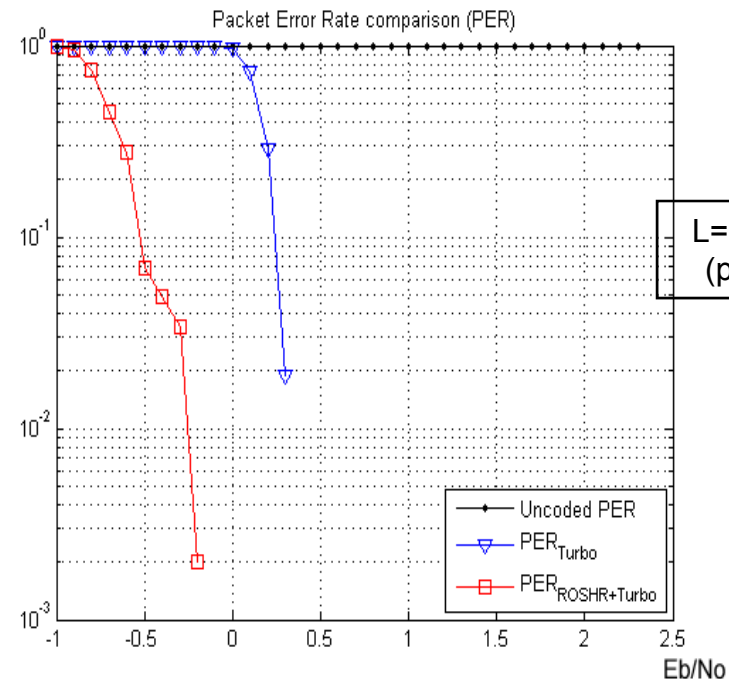
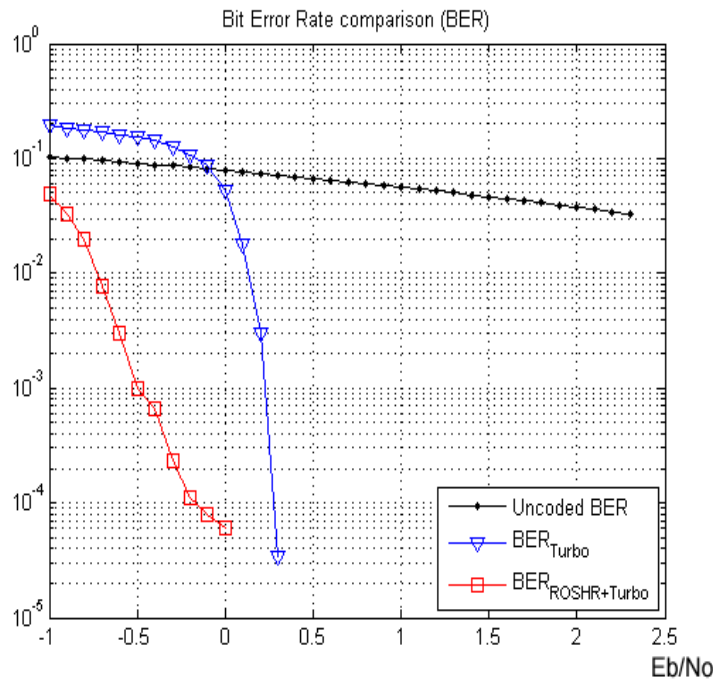
$F = 128$ bits (16 B) $\eta_{opt} = 280$ $PSR = 1 - 10^{-5.7} = 0.999998$



Observation des valeurs PSR sur un canal gaussien

Codage multi-couches- HERACLES

- Utilisation de HERACLES en mode « correction »
 - principe : chaque séquence détectée est « nettoyée » de ses erreurs
 - Lorsque ceci est fait par le récepteur avant le décodeur canal, amélioration du niveau de correction sur l'ensemble des bits
 - Exemple dans le cas du turbo code 3GPP2 - DVB-SH



L= 100 B, F= 40 B
(paquets VoIP_{v6})

Codage multi-couches – Conclusion et perspectives

- Travaux à court terme :
 - HERACLES :
 - ✓ utilisation d'autres types de redondance
 - ✓ analyse des performances en mode correction
 - transmissions satellite-mobile : modélisation et analyse de la couche physique DVB-SH, puis interactions avec les couches supérieures
- Travaux à moyen terme :
 - modélisation de la distribution de la redondance sur les couches.

Applications des codes correcteurs d'erreurs dans les réseaux

- Le codage peut aussi avoir des applications dans le domaine des réseaux hors du contexte spécifique « émetteur-récepteur »
- Parmi ces applications, le codage réseau (*network coding*) est la plus prometteuse.
- Les contributions suivantes peuvent être considérées comme appartenant à cette catégorie :
 - Réduction du nombre de retransmissions pour des liens unipoints utilisant un canal à diffusion
 - PeerFect
 - Réduction des bornes de délai de bout-en-bout avec le codage réseau

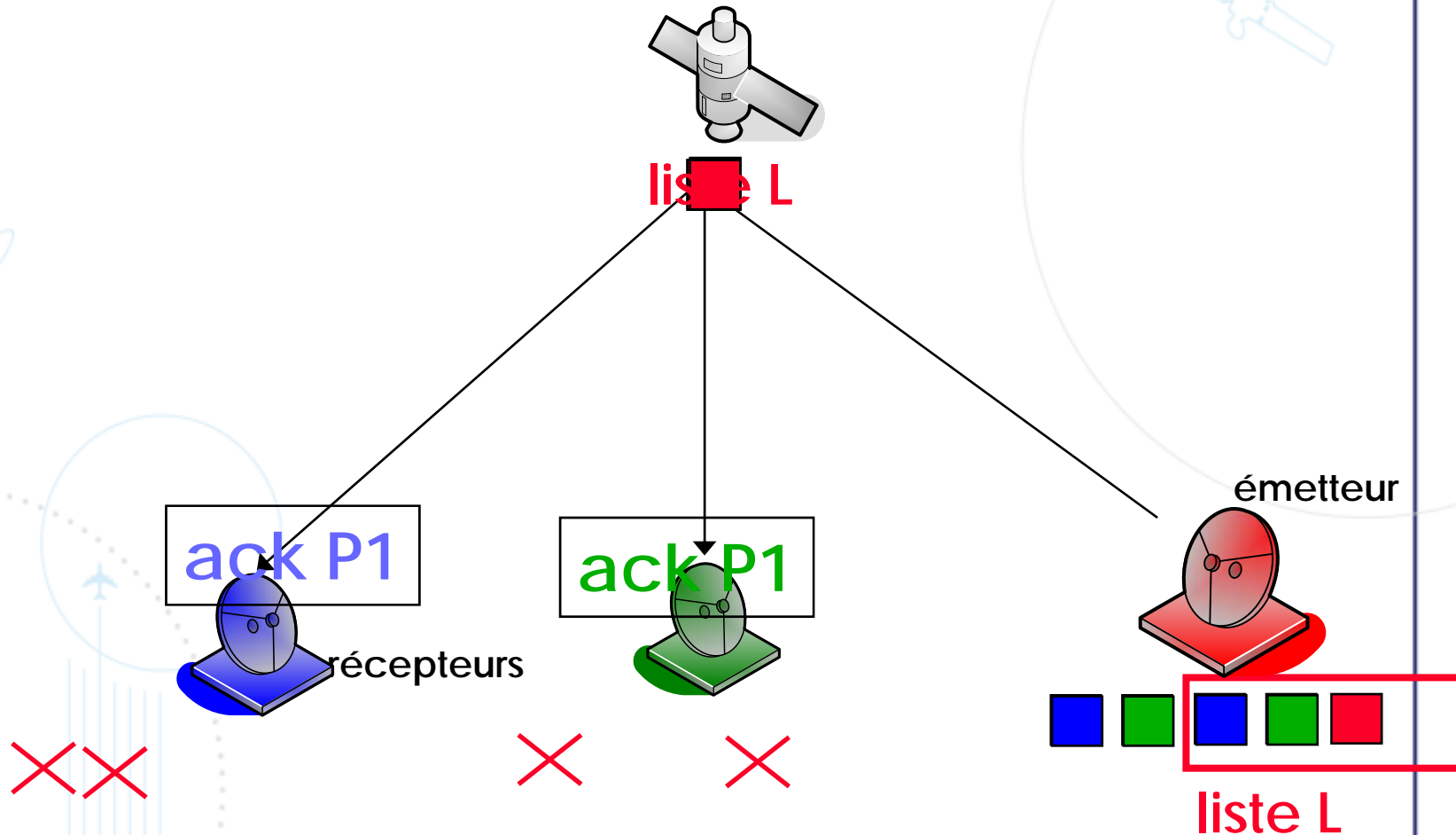
Applications -

Retransmissions sur un canal à diffusion

- Contexte : Une des situations où le codage est intéressant par rapport aux retransmissions est la transmission vers des groupes de récepteurs
- Les canaux sans fil sont des canaux à diffusion. Ceci implique que lorsque plusieurs utilisateurs partagent la même connection sans fil, ils peuvent « entendre » les paquets destinés au autres récepteurs.
- Dans ce contexte, au niveau liaison, la fiabilité est très souvent assurée par des retransmissions.
- Contribution (2004 – avec T. Perennou) : réduire le nombre de retransmissions en utilisant un système de codage basé sur le caractère « diffusion » du canal.

Applications - Retransmissions sur un canal à diffusion

- Principe : l'émetteur génère des paquets de redondance à partir des paquets perdus par **leur** récepteur



Applications -

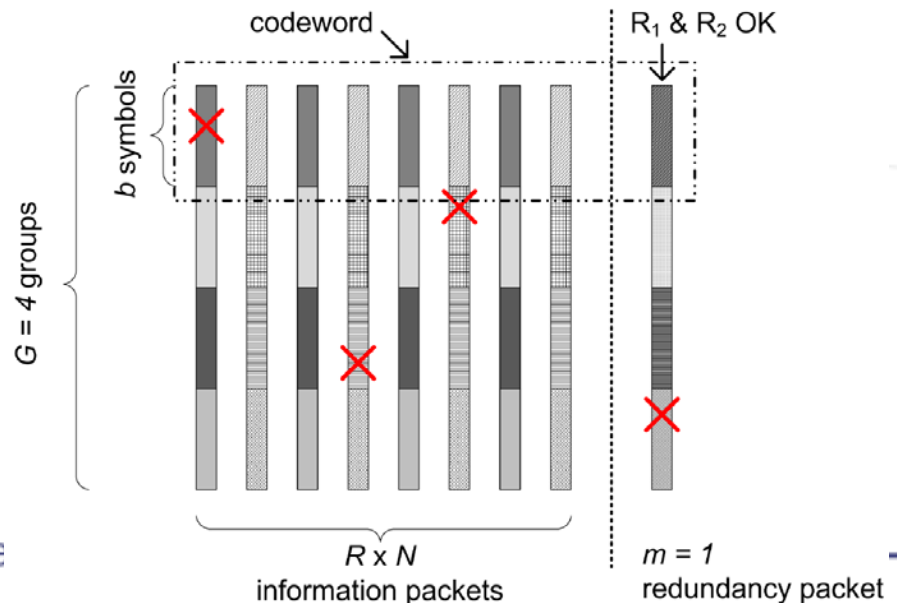
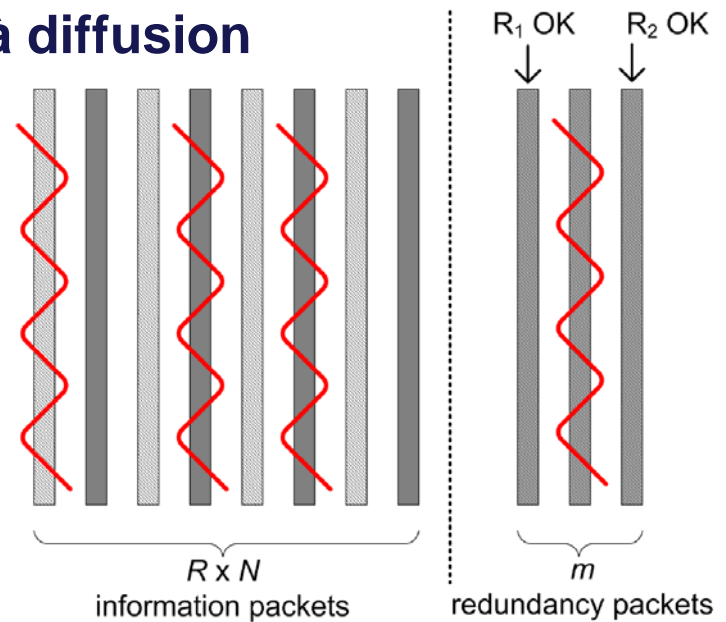
Retransmissions sur un canal à diffusion

- Définition du mécanisme pour le canal

➤ à effacements

➤ à erreurs

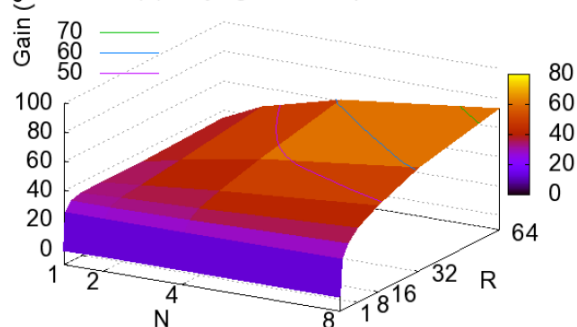
R : nombre de récepteurs
 N: nombre de paquets par récepteur



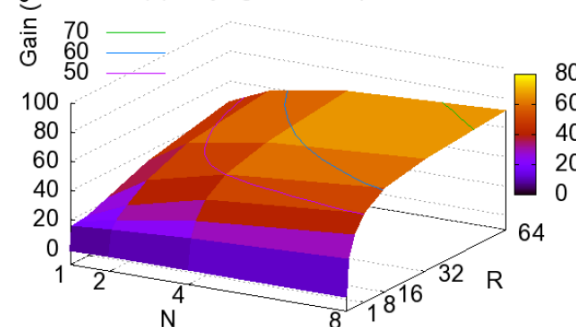
Applications - Retransmissions sur un canal à diffusion

- Modélisation sur le canal avec des pertes et des erreurs indépendantes

(b) Varying N and R, $p=0.01$

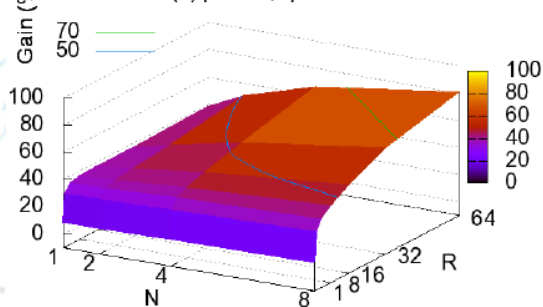


(c) Varying N and R, $p=0.15$

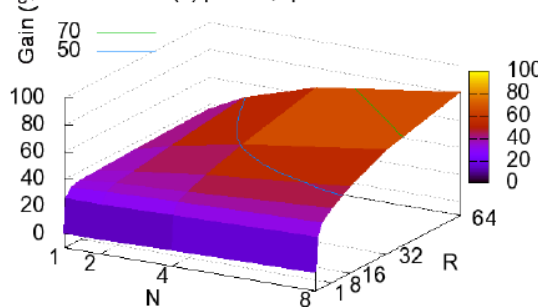


canal à effacement : Influence de N et R sur le gain

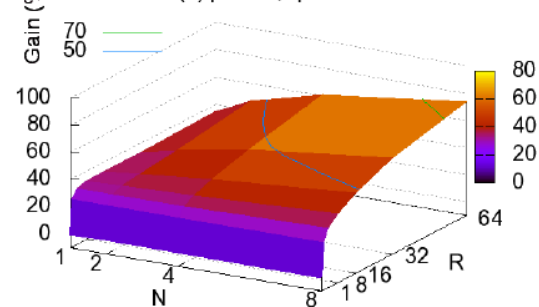
(a) $p=0.01, q=0.01$



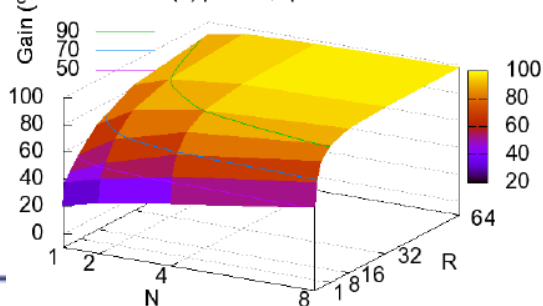
(b) $p=0.01, q=0.10$



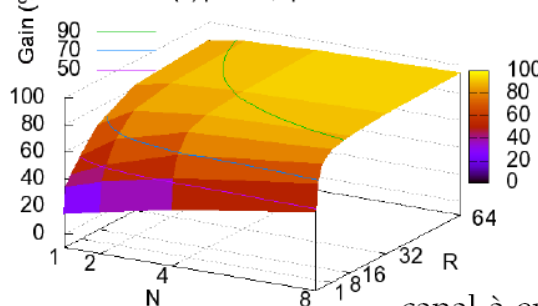
(b) $p=0.01, q=0.30$



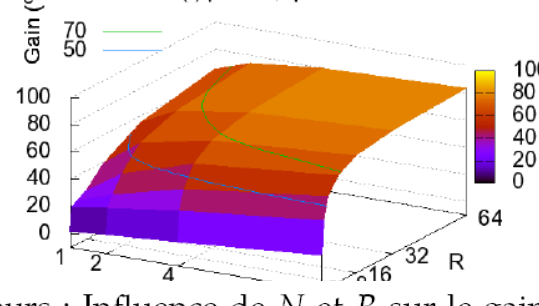
(d) $p=0.15, q=0.01$



(e) $p=0.15, q=0.10$



(f) $p=0.15, q=0.30$



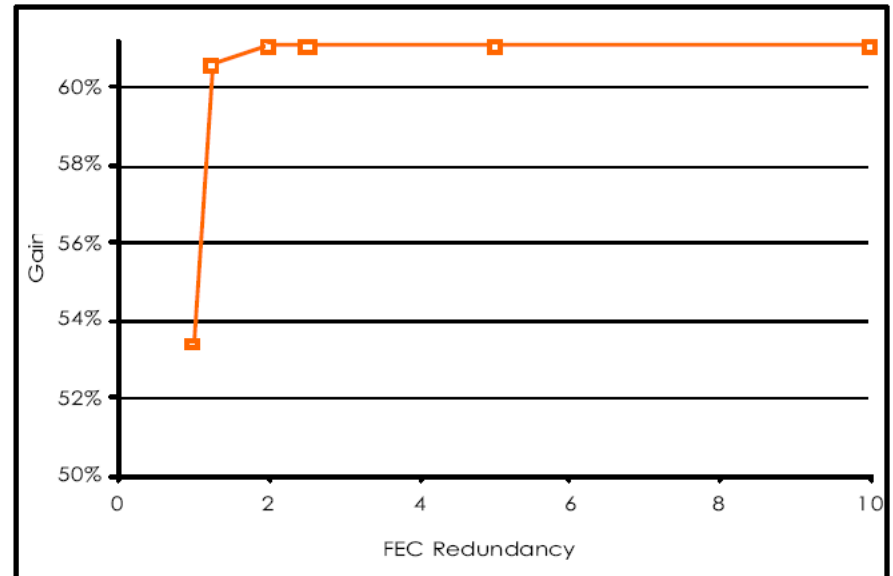
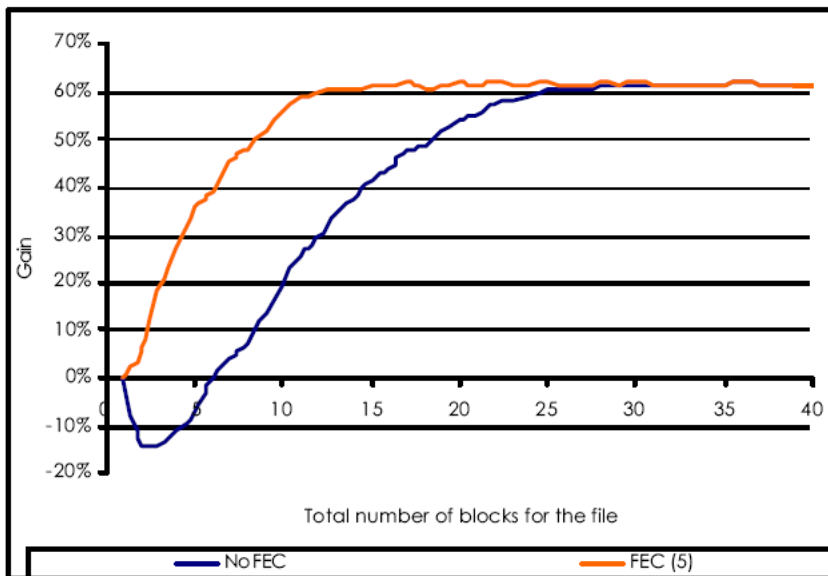
canal à erreurs : Influence de N et R sur le gain

Applications - PeerFect

- Les codes à effacements sont utilisés dans le cadre du stockage distribué (e. g. disques RAID) pour améliorer la fiabilité du stockage.
- Contribution (2002- avec L. Dairaine et L. Lancerica) : les codes permettent d'améliorer les temps de téléchargement dans des réseaux pair-à-pair
- Le principe consiste à :
 - découper les fichiers partagés en k blocs
 - générer des blocs de redondance avec un code MDS
 - disséminer les blocs codés dans le réseau
 - Un nœud qui veut récupérer le fichier choisit alors les k blocs les plus proches

Applications - PeerFect

- Pour réaliser une évaluation « réaliste », mesures sur le réseau Gnutella pour évaluer la distribution des bandes passantes
- Evaluation à partir des distributions trouvées pour des téléchargements séquentiels et parallèles (ci-dessous)



(a) Influence du nombre de blocs k par fichier. $n = 5.k$, $r = 10$ et $r' = 2$.

(b) Influence du facteur de redondance n/k . $k = 20$, $r = 10$ et $r' = r.k/n$

Applications –

Réduction des bornes de délai par paquet avec le codage réseau

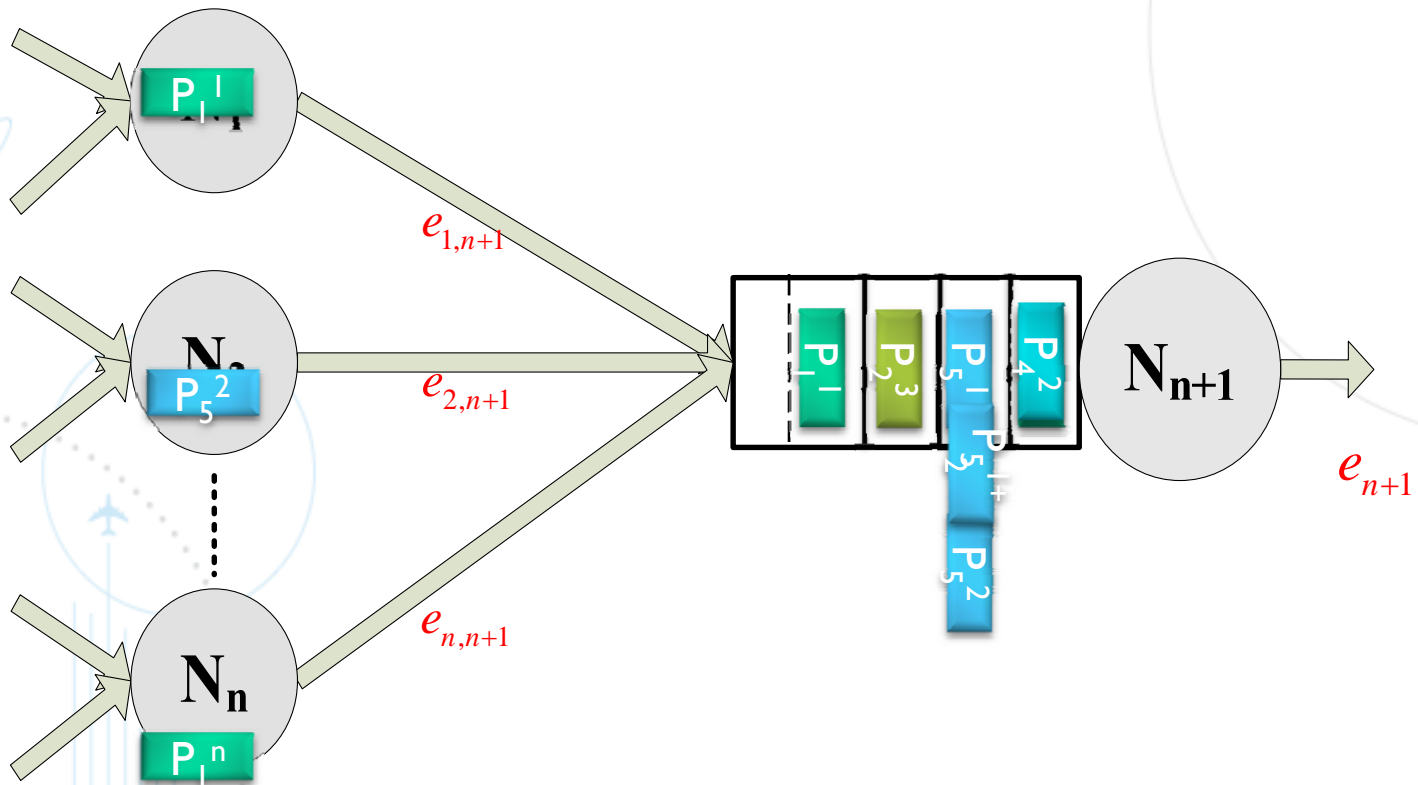
- Contexte : dans des réseaux fournissant de la qualité de service, les délais maximums de traversée du réseau par un paquet sont un des paramètres clé.
- Les délais de transmission sont générés par :
 - des délais de propagation,
 - les délais de service des composants du réseau
 - les délais dus aux congestions.
- Contribution (avec A. Mahmino et C. Fraboul) : réduire les délais de congestion grâce au *codage réseau*
 - proposition de stratégies pour le codage réseau dans ce contexte
 - analyse avec des outils de calcul réseau

Applications –

Réduction des bornes de délai par paquet avec le codage réseau

- Stratégie orientée réseau :
 - objectif : réduire au maximum le nombre de paquets dans les files d'attente
 - chaque T unités de temps, un paquet sort de chaque nœud. Il est la combinaison des paquets présent dans les files d'attente au moment du codage
 - stratégie de codage aléatoire
- Pour cette stratégie, expression du service offert par le réseau à chaque flux
 - basé sur une matrice de transfert du réseau dont les composants sont les courbes de service offert par les composant réseau (élément de calcul réseau)
 - matrice construite en faisant le parallèle avec la matrice de transfert du codage réseau proposée par [Koetter/Médard-2002]

- Stratégie de transmission rapide (Fast Forwarding Strategy)
 - assure une fiabilité totale
 - utilise le concept de générations de paquets



Applications –

Réduction des bornes de délai par paquet avec le codage réseau

- Stratégie de transmission rapide (Fast Forwarding Strategy)
 - nécessite une somme de contrôle (checksum) inséré par les sources sur chaque paquet
 - Au niveau du récepteur, le décodeur produit des paquets avec les paquets d'une génération reçus
 - Si les checksums sont corrects, les paquets source ont bien été récupérés. Sinon, il faut attendre la réception d'autres paquets de la même génération.
- Calcul des délais maximums en calculant le nombre maximum de générations présentes dans un nœud.

Applications – Conclusion et perspectives

- Travaux à court terme :
 - Réduction des bornes de délai avec le codage réseau :
 - ✓ application à des réseaux à qualité de service réels
 - ✓ analyse de la stratégie de transmission rapide dans un contexte « non qualité de service »
 - Réduction du nombre de retransmissions
 - ✓ extension de ces travaux dans le contexte du « codage opportuniste »
- Travaux à moyen terme :
 - autres applications du codage réseau

Conclusions

- Contributions diverses dans le domaine du codage dans les réseaux :
 - constructions de codes à effacements
 - codage multi-couches
 - applications des codes à effacements dans différents types de réseaux
- Publications :
 - 11 revues internationales
 - 30 conférences nationales et internationales
 - 13 drafts IETF
 - 2 brevets
 - gestion et/ou participation à 9 contrats et projets industriels

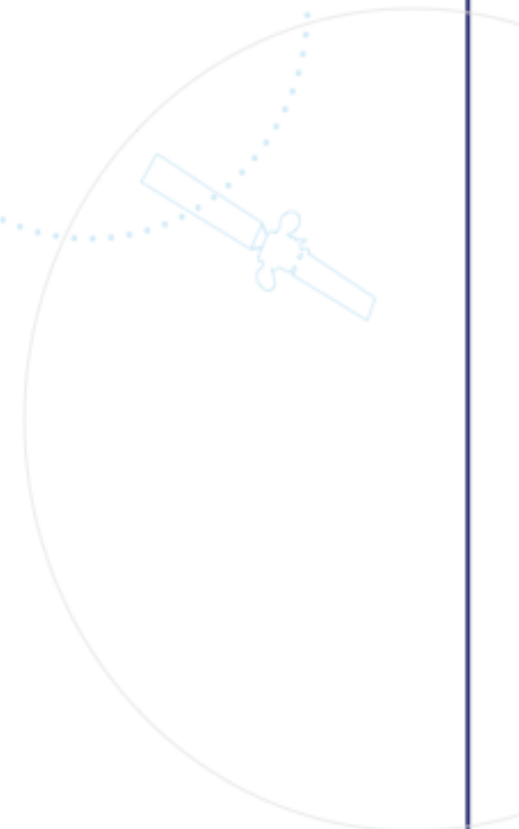
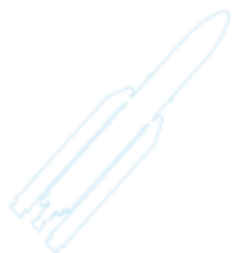
Perspectives

- Perspectives présentées dans chacun des domaines de contribution.
- Le domaine de la théorie de l'information/communications et celui des réseaux ont de plus en plus de sujets en commun.
- Ces deux domaines ont des intérêts à collaborer :
 - la recherche en réseau atteint un certain niveau de maturité : les futures avancées technologiques devront s'appuyer sur des bases théoriques solides
 - les chercheurs en théorie de l'information peuvent trouver des sujets de recherche « neufs » dans les réseaux
- Cette besoin de développement de compétences communes semble désormais intégré par tous les acteurs (académiques, industriels, groupes de standardisation, ...)

Merci de votre attention

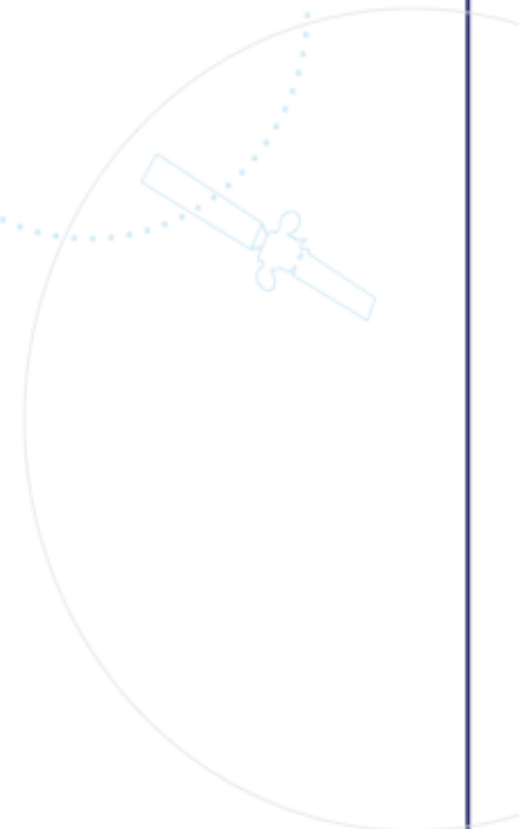
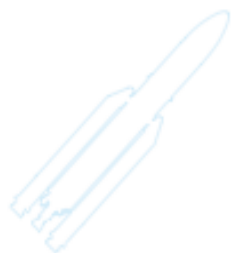


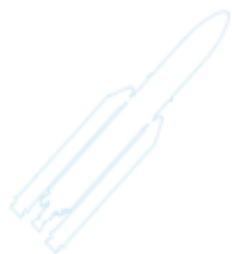
isae





isae





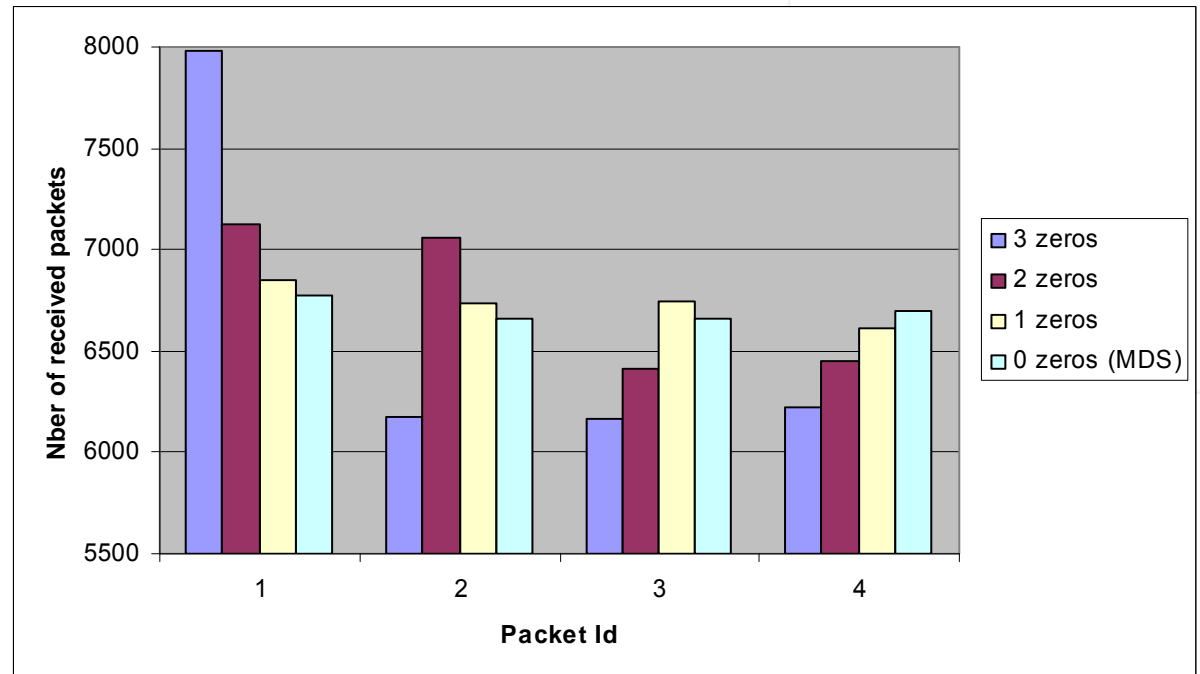
exemple du code DA-UEP

- Dans un code MDS (7, 4) nous avons fait varier le nombre d'éléments nuls dans la matrice génératrice
- Taux de redondance de $r \sim 43\%$, taux de perte $p = 50\%$, Nombre d'itération = 10000

$$G = \begin{bmatrix} Id_4 & \begin{matrix} \alpha_{1,1} & \cdot & \alpha_{1,3} \\ \cdot & \cdot & \cdot \\ \alpha_{3,1} & \cdot & \cdot \\ 0 & \alpha_{4,2} & \alpha_{4,3} \end{matrix} \end{bmatrix}$$

$$G = \begin{bmatrix} Id_4 & \begin{matrix} \alpha_{1,1} & \cdot & \alpha_{1,3} \\ \alpha_{2,1} & \cdot & \cdot \\ 0 & \cdot & \cdot \\ 0 & \alpha_{4,2} & \alpha_{4,3} \end{matrix} \end{bmatrix}$$

$$G = \begin{bmatrix} Id_4 & \begin{matrix} \alpha_{1,1} & \cdot & \alpha_{1,3} \\ 0 & \cdot & \cdot \\ 0 & \cdot & \cdot \\ 0 & \alpha_{4,2} & \alpha_{4,3} \end{matrix} \end{bmatrix}$$



Codes à effacements – amélioration des codes MDS

- Codes MDS – Maximum Distance Separable-
 - optimaux en termes de capacité de correction
 - relativement coûteux en terme de calcul à cause des opérations sur des corps finis non binaires et des opérations sur des matrices « pleines »
 - codes définis à partir de 2 types de matrices
 - ✓ matrices de Vandermonde : codes de Reed-Solomon
 - ✓ matrice de Cauchy

Codes à effacements – amélioration des codes MDS

- 1^{ère} contribution (avec J. Fimes 2003) : amélioration des vitesses de codage et de décodage en définissant ces codes sur le corps fini $GF(2^{16}+1)$.
- Les éléments de ce corps pouvant être vus comme des entiers codés sur 16 bits, les processeurs classiques les manipule plus facilement.

k	Codage (en Mb/s)			Décodage (en Mb/s)		
	code sur les entiers	Cauchy [61]	Vandermonde [57]	code sur les entiers	Cauchy [61]	Vandermonde [57]
16	305.18	99.83	91.55	457.76	299.48	249.69
32	166.46	54.45	55.49	332.92	87.65	85.83
64	107.71	26.62	25.97	209.26	67.81	46.36
128	55.07	13.54	11.48	115.34	33.82	21.39
256	28.28	6.75	4.94	71.81	19.95	11.80
512	13.93	3.41	1.93	37.56	10.27	5.02
1024	7.14	1.70	0.89	18.96	5.12	1.19
2048	3.45	0.82	0.43	9.09	2.40	0.17

Codes à effacements – amélioration des codes MDS

- 2^{ème} contribution (avec J. Fimes 2003) : construction de codes MDS systématiques basés sur des matrices de Vandermonde
- Principe : la matrice génératrice est le produit de l'inverse d'une matrice de Vandermonde et d'une matrice de Vandermonde.
- Intérêt : les opérations « produit matrice-vecteur » et « inversion de matrice » sont de faible complexité avec les matrices de Vandermonde.
- Résultat : Complexité du codage et du décodage $O(k \log k)$ ou $O(k \log^2 k)$ où k est le nombre de symboles source
- Application aux codes MDS de L. Rizzo → contribution à IETF

Codes à effacements – principe de base

- codage d'un code avec 4 symboles sources et 3 symboles de redondance. Les symboles appartiennent à un corps fini $GF(q)$.

$$\begin{bmatrix} i_1 & i_2 & i_3 & i_4 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 & \alpha_{1,5} & \alpha_{1,6} & \alpha_{1,7} \\ 0 & 0 & 0 & 0 & \alpha_{2,5} & \alpha_{2,6} & \alpha_{2,7} \\ 0 & 1 & 0 & 0 & \alpha_{3,5} & \alpha_{3,6} & \alpha_{3,7} \\ 0 & 0 & 0 & 1 & \alpha_{4,5} & \alpha_{4,6} & \alpha_{4,7} \end{bmatrix} = \begin{bmatrix} i_1 & \times & i_3 & \times & \times & r_2 & r_3 \end{bmatrix}$$

- décodage

$$\begin{bmatrix} i_1 & i_3 & r_2 & r_3 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & \alpha_{1,6} & \alpha_{1,7} \\ 0 & 0 & \alpha_{2,6} & \alpha_{2,7} \\ 0 & 1 & \alpha_{3,6} & \alpha_{3,7} \\ 0 & 0 & \alpha_{4,6} & \alpha_{4,7} \end{bmatrix}^{-1} = \begin{bmatrix} i_1 & i_2 & i_3 & i_4 \end{bmatrix}$$