Réseaux locaux

Katia Jaffrès-Runser et Gentiane Jakllari

{kjr,jakllari}-at-n7.fr

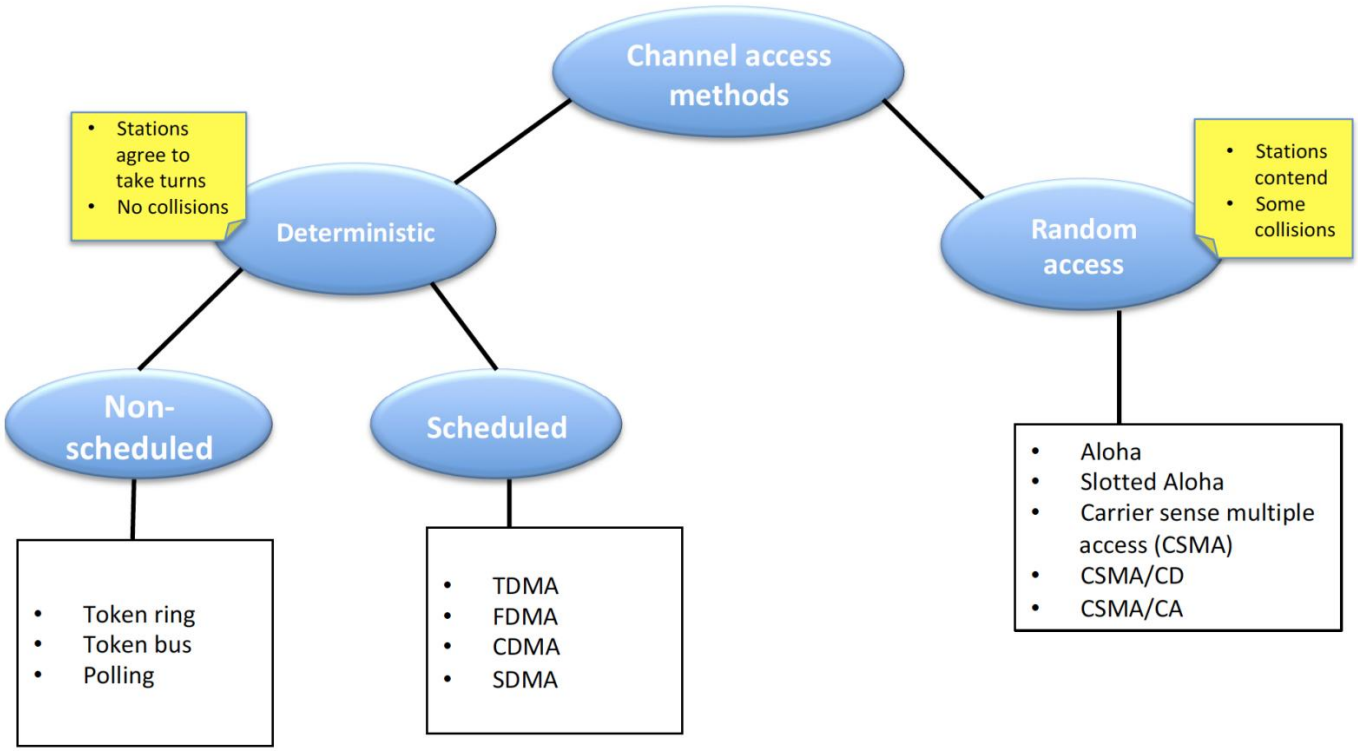
Toulouse INP - ENSEEIHT

Département Sciences du Numérique
1ère année

2017-2018

ALOHA

Accès multiple avec détection de porteuse



Réseaux ALOHA

ALOHA : l'origine de l'accès aléatoire1

Développé à la fin des années 60 par Norman Abramson et al pour permettre aux 7 campus de l'Univ. d'Hawai'i, situés sur 4 îles différentes, pour partager les ressources informatiques sur le campus principal

Les premiers terminaux utilisateurs sont entrés en service en juin 1971

Le protocole de communication a été mis en œuvre par un équipement à usage spécial - l'unité de contrôle du terminal (TCU)

Comparez-le à une carte wifi...

Un terminal utilisateur était rattaché à la TCU

1 N. Abramson, "The AlohaNet - surfing for wireless data [History of Communications]", dans IEEE Communications Magazine, vol. 47, non. 12, p. 21-25, décembre 2009.

Réseaux ALOHA

Décision clé : utiliser la forme directe de transmission des informations utilisateur dans une seule rafale de paquets à haut débit dans un canal sans fil partagé

Poussé par le besoin d'une conception simple; débit calculé plusieurs semaines après la décision

Le coût de la mémoire pour un tampon de paquets de 88 octets était

d'environ 300 $ Philosophie d'accès au canal : laisser les collisions se produire, détecter quand elles se produisent et réessayer.

N'importe quelle station peut envoyer des données

à tout moment Si, pendant la transmission, des données sont reçues simultanément, alors il y a une collision – vous devrez réessayer.

Réseaux ALOHA

Réseaux ALOHA

Décision clé : utiliser la forme directe de transmission des informations utilisateur dans une seule rafale de paquets à haut débit dans un canal sans fil partagé

Poussé par le besoin d'une conception simple; débit calculé plusieurs semaines après la décision

Le coût de la mémoire pour un tampon de paquets de 88 octets était

d'environ 300 $ Philosophie d'accès au canal : laisser les collisions se produire, détecter quand elles se produisent et réessayer.

N'importe quelle station peut envoyer des données

à tout moment Si, pendant la transmission, des données sont reçues simultanément, alors il y a une collision – vous devrez réessayer.

Comment réessayer ?

Renvoyer les données après une durée aléatoire appelée la période de Backoff

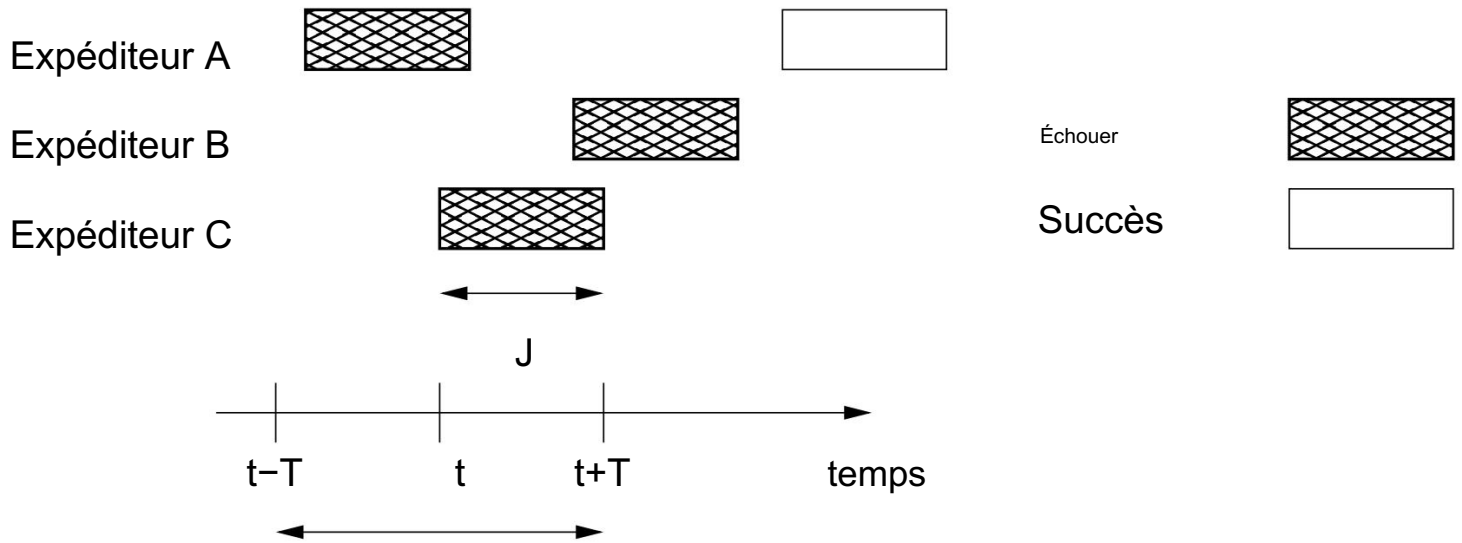
Évite les collisions répétées.

La façon dont ce choix aléatoire est fait influence la performance globale.

Réseaux ALOHA

Période de vulnérabilité

Le message transmis à l'instant t subit une collision si un autre message chevauche partiellement sa transmission.



Période de vulnérabilité 2T

Si tous les messages ont la même longueur T, alors la période de vulnérabilité est de taille 2T.

Débit atteint par ALOHA

Il peut être dérivé comme suit :

Supposons que le nombre de tentatives de transmission par durée de trame T suit une distribution de Poisson de moyenne G.

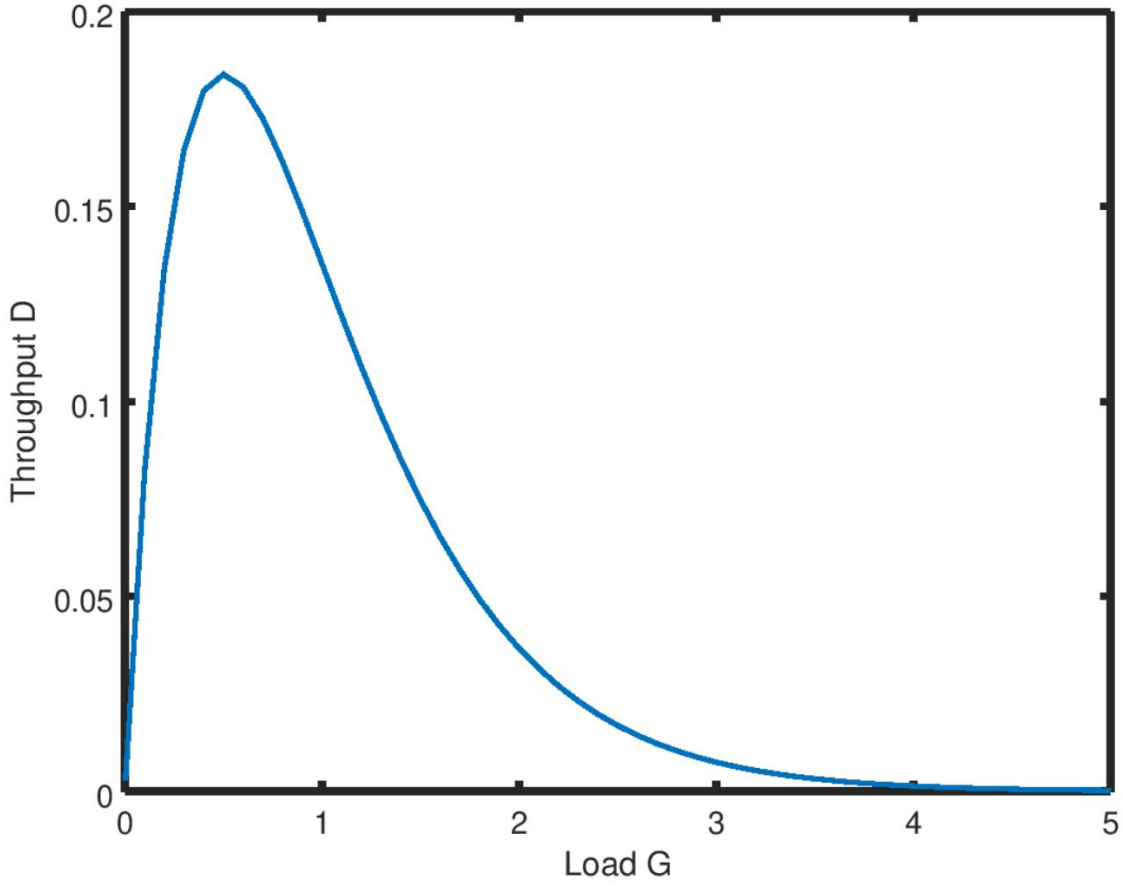
Ainsi la probabilité d'avoir k tentatives pendant T est : La probabilité $\frac{e^{k} \, G^{k}}{e \, k!}$

de n'avoir aucune collision pendant la période de vulnérabilité de 2T est donné par e^{-2G}

Ainsi, le débit est le nombre G de tentatives pendant T qui ne connaissent aucune collision :

$$D = G \cdot e^{-2G}$$

Débit pour ALOHA



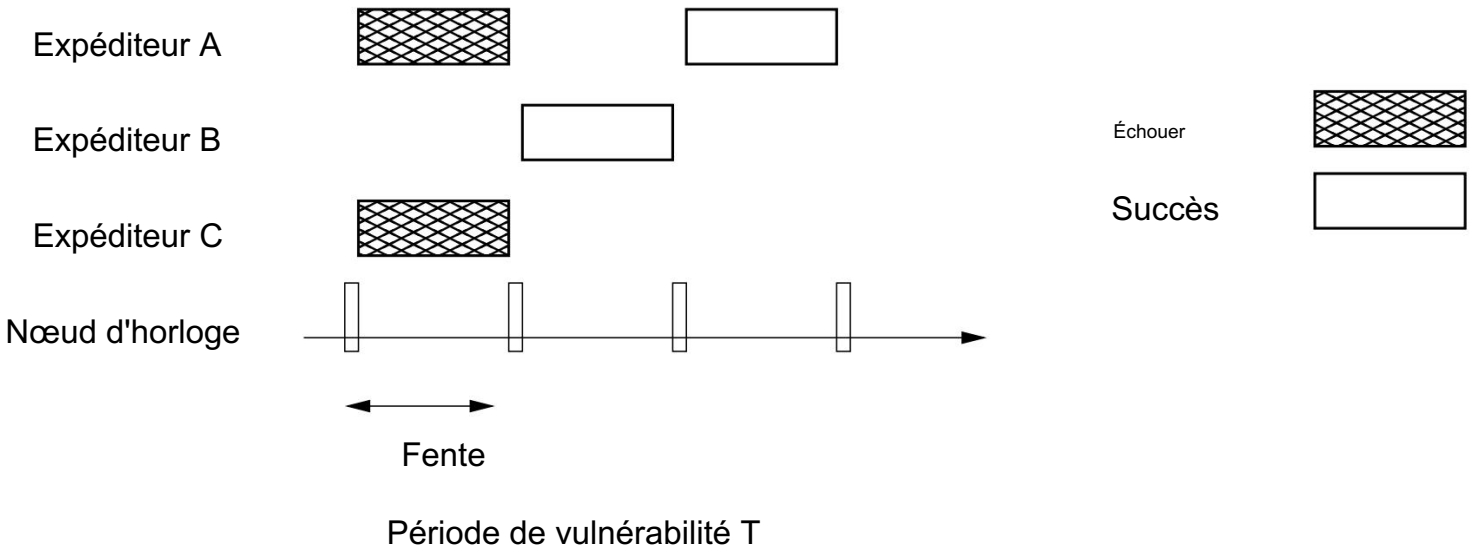
Le maximum d'un bout à l'autre est obtenu pour une charge G = 0,5, soit D = 0,5/e 0,184.

Très lent! Seuls 18 % des cadres ne se heurtent pas au mieux.

ALOHA fendu

Augmenter l'efficacité d'ALOHA

Idée : réduire la durée de la période de vulnérabilité en synchronisant les transmissions



Tous les nœuds sont synchronisés sur une tranche de durée donnée de taille TA. La transmission ne peut commencer qu'au début de la tranche. → la période de vulnérabilité est réduite à T.

ALOHA fendu

Efficacité de l'ALOHA à fentes

Lorsque la période de vulnérabilité est réduite à T, le débit augmente à :

$$D = G \cdot e^{-G}$$

avec e^{-G} les chances de subir 0 tentative pendant T pour la charge G.

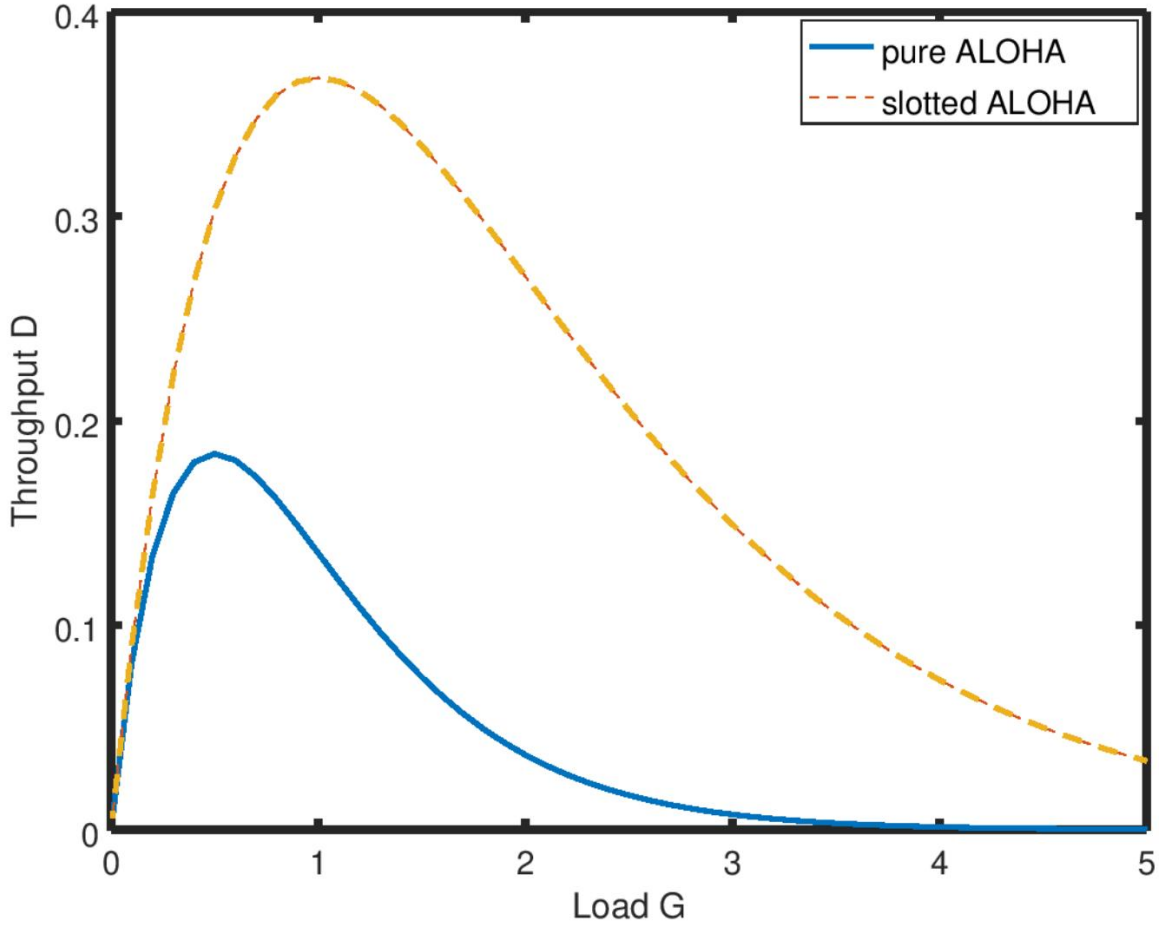
Le nombre de transmissions E pour

faire passer un message augmente de façon exponentielle avec G :

$$E = \sum_{k=1}^{k=\infty} kPk = e^{g}$$

avec Pk la probabilité de transmettre un message après k tentatives donnée par $Pk = e^{-G}(1 - e^{-G})^{k-1}$.

ALOHA à fente vs ALOHA pur



Ici, le pic d'utilisation est de 1/e, 36,8% si une tentative par slot est effectuée en moyenne.

Vers un meilleur accès aléatoire

Devenir un peu plus poli

Vers un meilleur accès aléatoire

Devenir un peu plus poli

Écouter avant de parler,

Si quelqu'un parle, reporter la transmission à une date ultérieure.

Vers un meilleur accès aléatoire

Devenir un peu plus poli

Écouter avant de parler, Si quelqu'un

parle, reporter la transmission à une date ultérieure.

Détection de

porteuse Le nœud doit détecter le canal pour détecter une transmission en cours.

Des collisions peuvent-elles encore se produire alors ?

Accès multiple avec détection de porteuse

CSMA

Aka Carrier Sense Multiple Access est une famille de protocoles où un nœud voulant transmettre un message :

Détecte le canal Si

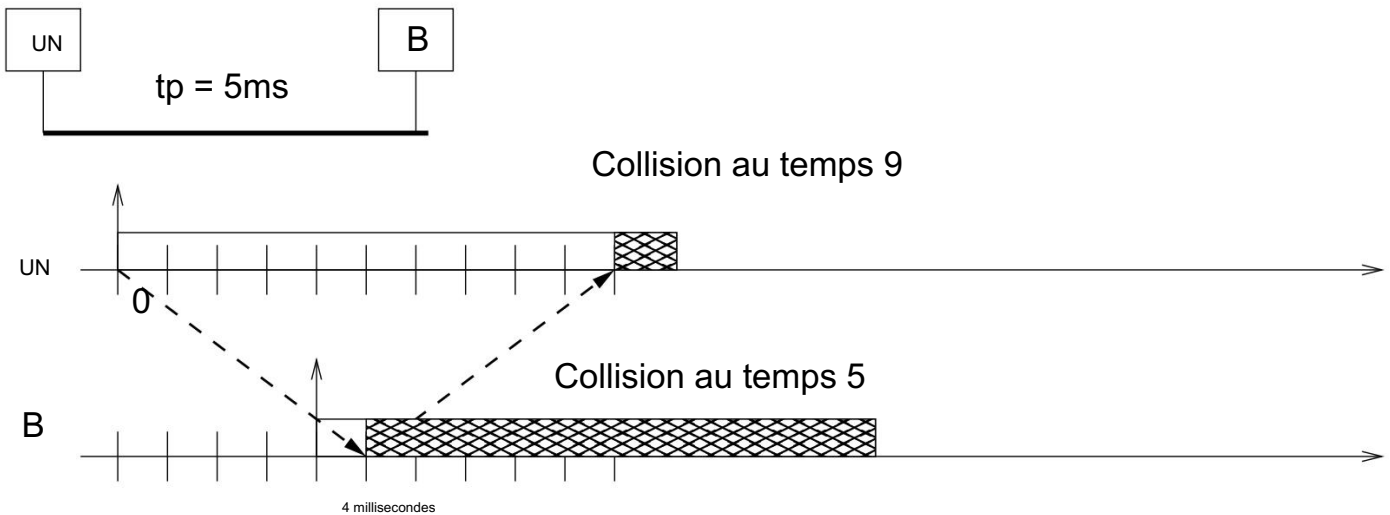
le canal est occupé, alors il diffère la transmission
Si le canal est inactif, alors il transmet

Chaque fois qu'un nœud commence à émettre, il envoie le message complet.

Accès multiple avec détection de porteuse

Des collisions peuvent-elles encore se produire ?

Le CSMA est très sensible au délai de propagation.



Pendant 5 ms, le canal est considéré comme libre pour les autres nœuds.

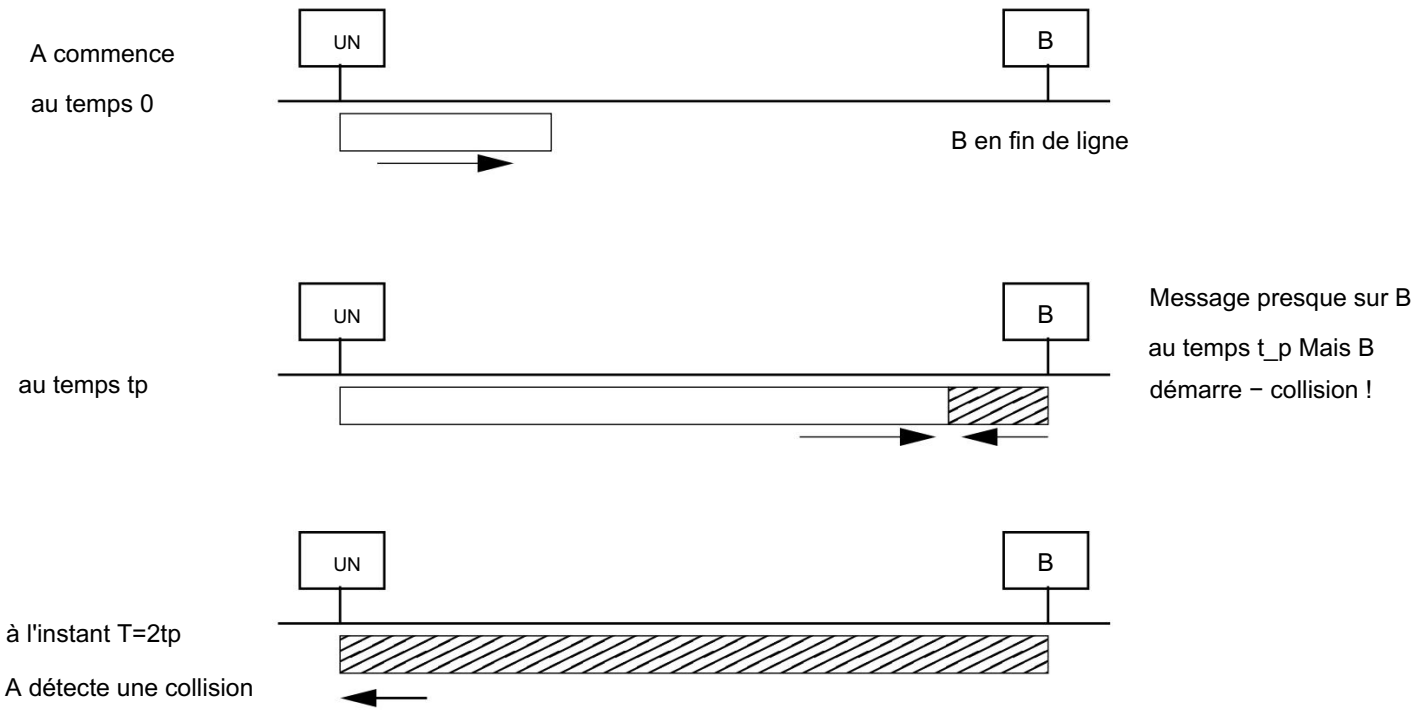
Le nœud A ne peut voir la collision qu'après 2.tp (durée de l'aller-retour).

Accès multiple avec détection de porteuse

Période de vulnérabilité

Dans CSMA, la période de vulnérabilité est la durée pendant laquelle le 1er bit voyage jusqu'à la fin de la ligne et revient, c'est-à-dire

$$T = 2tp$$



Accès multiple avec détection de porteuse

Plusieurs variantes de CSMA existent :

- CSMA 1-persistant
- CSMA non persistant
- CSMA p-persistant
- CSMA/CD (détection de collision)
- CSMA/CA (évitement des collisions)
- CSMA/CR (résolution des collisions)

1-CSMA persistant

Algorithme pour un nœud prêt à transmettre

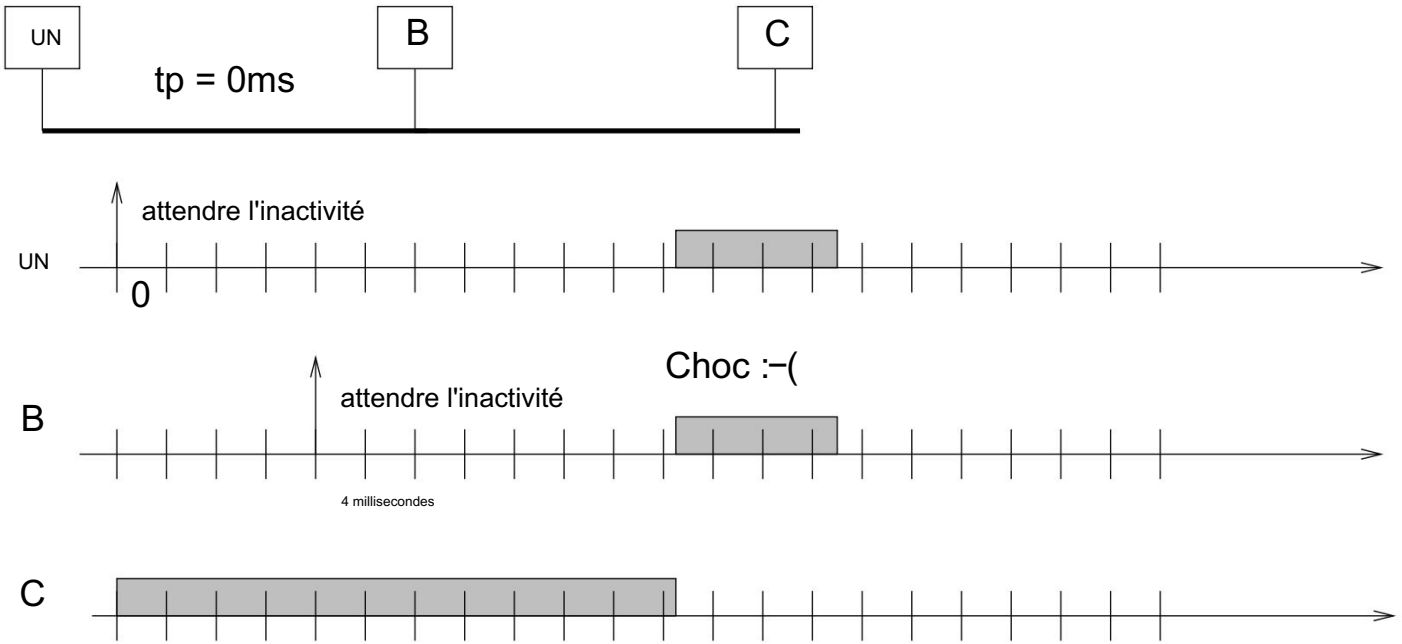
Sentez le canal

Si le canal est occupé, attendre la fin de la transmission en cours.
Si le canal est inactif, alors transmettre immédiatement (avec probabilité 1).

→ écoute constamment pendant la transmission
pour détecter l'état d'inactivité dès que possible.

1-CSMA persistant

Problème avec 1 CSMA persistant



Le débit de pointe est un peu meilleur que pour l'ALOHA à créneaux : 52,9 %

CSMA non persistant

Algorithme pour un nœud prêt à transmettre

Ici, l'émetteur n'écoute pas activement pour détecter la fin d'une transmission en cours.

Sentez le canal

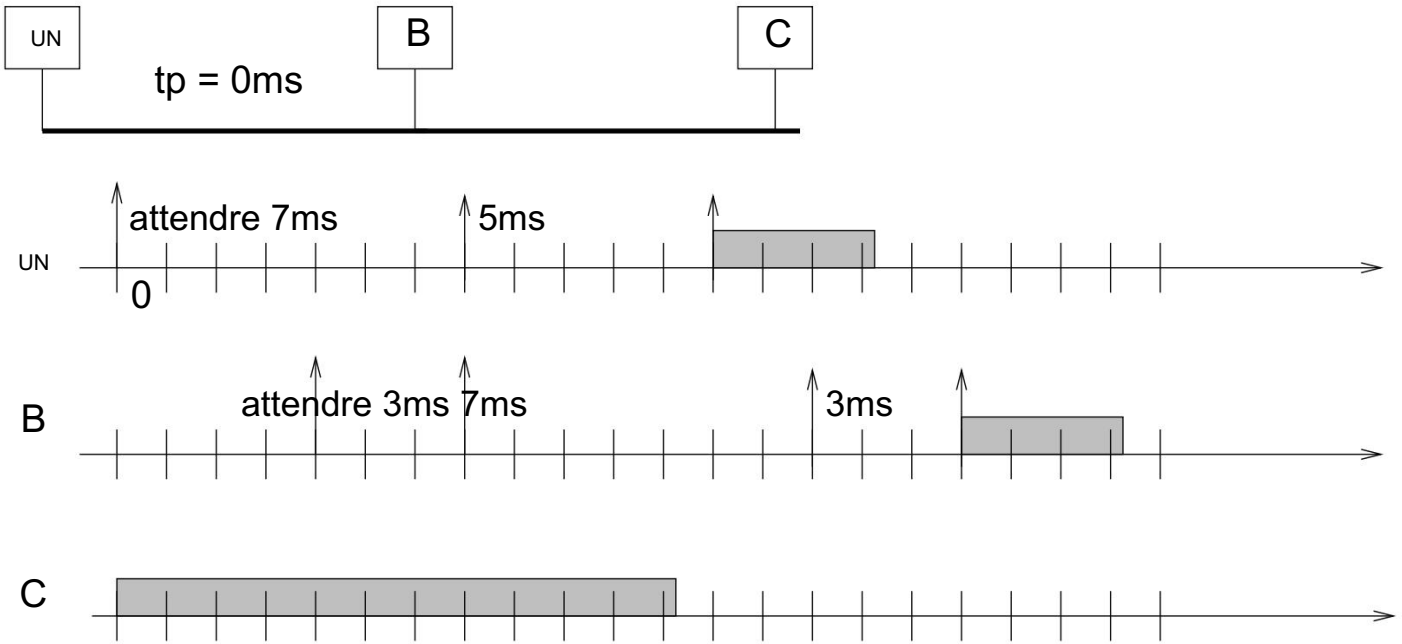
Si le canal est occupé, attendez un temps aléatoire et détectez à nouveau le canal

Si le canal est inactif, alors transmettez immédiatement

→ Pas d'écoute persistante pendant la transmission

CSMA non persistant

Exemple



Les collisions sont moins susceptibles de se produire ici, mais du temps peut être perdu après la fin de la transmission en cours.

Le débit de pointe est bien meilleur : 81,5 %.

CSMA p-persistant

Algorithme pour un nœud

prêt Un compromis entre CSMA 1-persistant et CSMA non persistant.

Supposons que les canaux sont répartis (mais pas globalement synchronisés).

Un slot est suffisamment long pour détecter à coup sûr une collision (c'est-à-dire de durée T = 2tp).

1. Détecter le canal Si le

   canal est inactif, alors transmettre avec probabilité p

   Si le message n'est pas transmis, attendez un créneau et passez à l'étape 1.

   Si le canal est occupé, attendez que le canal devienne inactif et passez à l'étape 1.

CSMA p-persistant

Performance

Les collisions sont réduites, le débit de pointe augmente :

Pour p = 0,1, S 79,1 % S

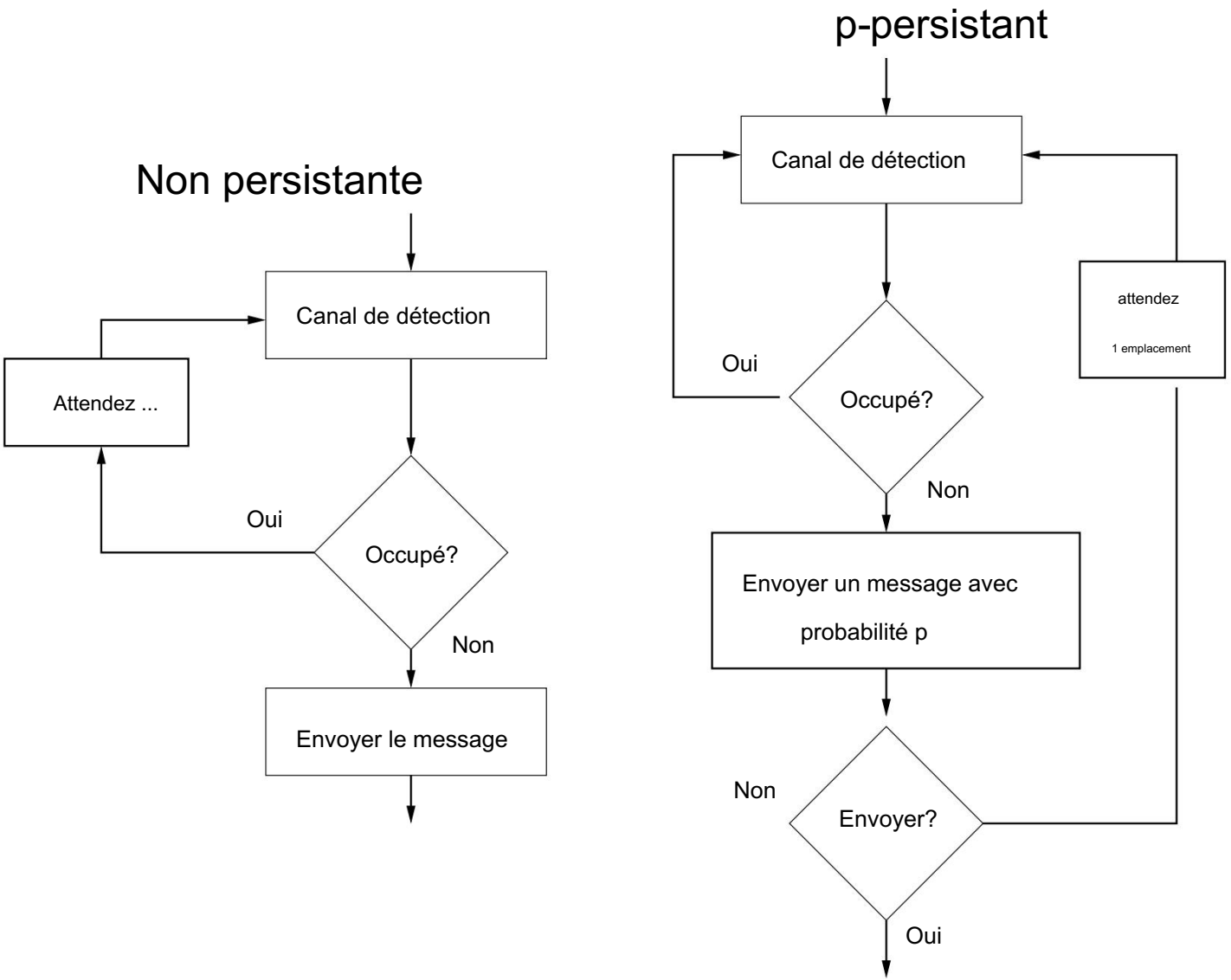
Pour p = 0,03, 82,7 %

Mais avec un p inférieur, plus il faut de temps pour envoyer un message.
Pour p donné, il faut

$$E[k] = \sum_{k=1}^{\infty} kp(1-p)^{k} = 1/p$$

slots pour envoyer un message si le canal est constamment inactif.

Non persistant vs persistant



Performances du CSMA

Supériorité de p-persistant/non persistant sur 1-persistant en termes de S.

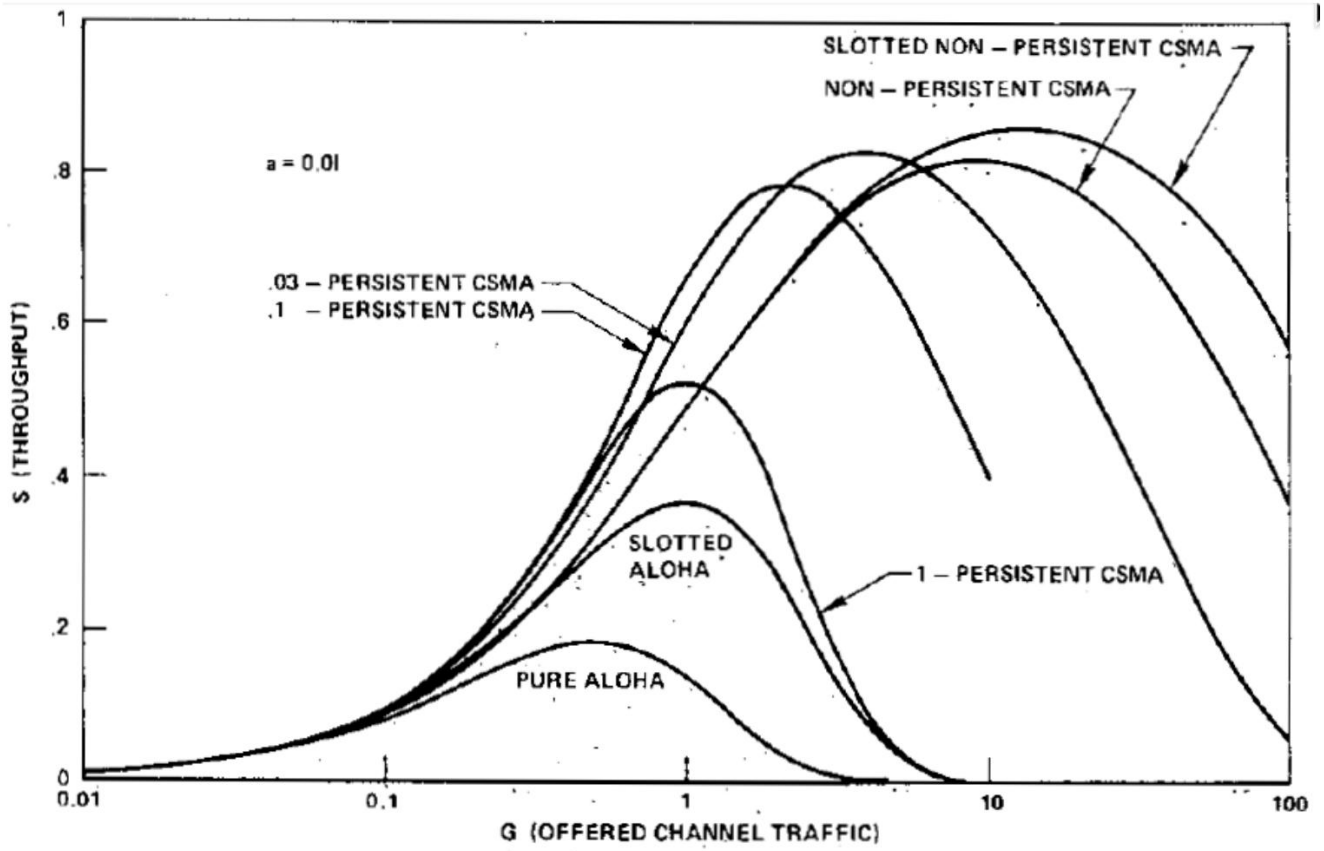


Fig. 9. Throughput for the various access modes ($a = 0.01$).

a = délai de propagation / délai de transmission.

Performances du CSMA2

Mais le délai pour transmettre un message avec succès augmente de façon exponentielle avec le débit S pour les schémas non persistants et p-persistants.

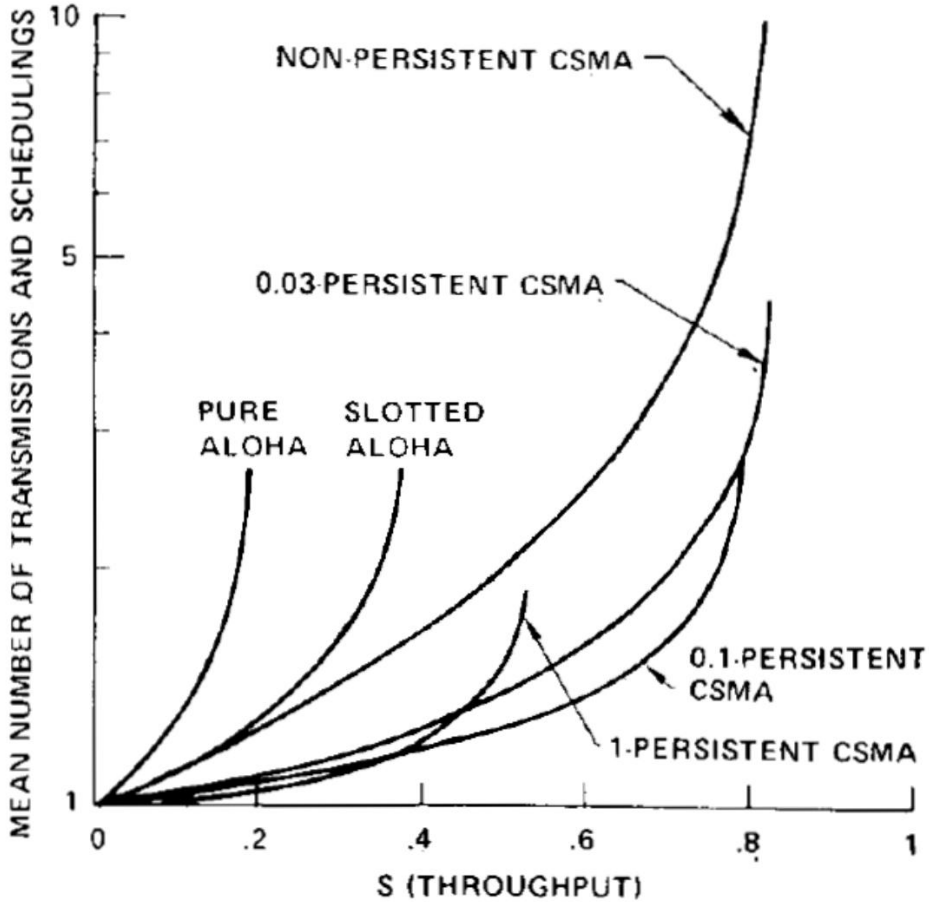


Fig. 11. G/S versus throughput ($a = 0.01$).

2 L. Kleinrock et F. Tobagi, « Commutation de paquets dans les canaux radio : Partie I - Modes d'accès multiples à détection de porteuse et leurs Caractéristiques de débit-retard », dans IEEE Transactions on Communications, vol. 23, non. 12, pages 1400-1416, décembre 1975.

Protocoles CSMA avancés

CSMA/CD

Un CSMA 1-persistant avec un mécanisme avancé de détection de collisions (CD).

1-CSMA persistant : débit de crête faible S mais accès au canal rapide en moyenne.

Améliorez le débit avec le CD grâce à

Détection de collision à l'expéditeur

Arrêter la transmission si une collision est détectée Durée d'attente aléatoire avant une nouvelle tentative de transmission.

Sera détaillé dans la conférence Ethernet.

Protocoles CSMA avancés

CSMA/CA Un

CSMA p-persistant avec un mécanisme avancé d'évitement des collisions (CA) conçu pour les systèmes sans fil.

CSMA p-persistant : débit de crête plus important S mais temps d'accès au canal plus lent en moyenne.

Réduisez le temps d'accès au canal avec les opérations CA :

Détection de collision au niveau du

récepteur Message d'accusé de réception pour avertir

l'expéditeur Durée de back-off aléatoire avant une nouvelle tentative de transmission, avec gel du back-off.

Sera détaillé dans la conférence WiFi.

Protocoles CSMA avancés

CSMA/CR pour l'accès au canal basé sur la priorité Un CSMA où la procédure de résolution de conflit élit le message ayant la priorité la plus élevée.

Chaque message reçoit un identifiant unique (ID) représentatif de sa priorité.
Plus l'ID est faible, plus la priorité est élevée.

Si deux messages d'ID différents sont envoyés simultanément, celui avec l'ID le plus bas remporte l'accès au canal.

L'expéditeur du message de priorité inférieure diffère la transmission jusqu'à ce que le canal redevienne inactif.

Fonctionne sur n'importe quelle voiture que vous conduisez...

Protocoles CSMA avancés

CSMA/CR pour l'accès au canal basé sur la priorité

Comment ça marche ?

Tous les expéditeurs sont synchronisés au niveau du bit.

Un mors peut être récessif ou dominant.

Le mors dominant l'emporte sur le mors récessif.

Valeurs logiques

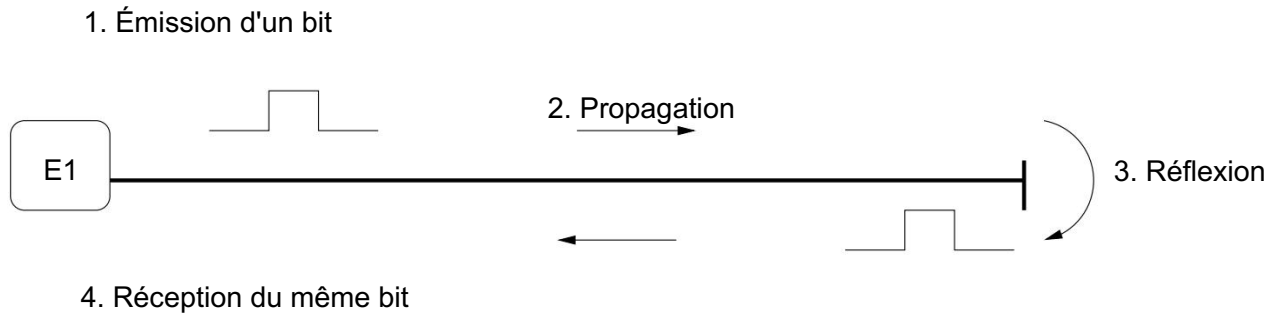
Récessif → valeur de bit 1

Dominante → valeur de bit 0

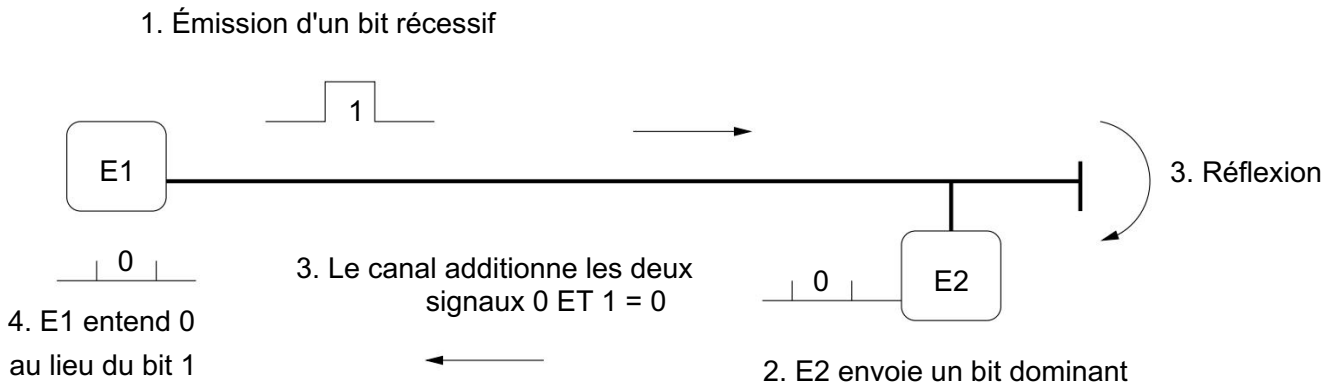
CSMA/CR

Résolution des conflits au niveau des bits

Pour chaque bit transmis, l'expéditeur vérifie s'il est resté inchangé.



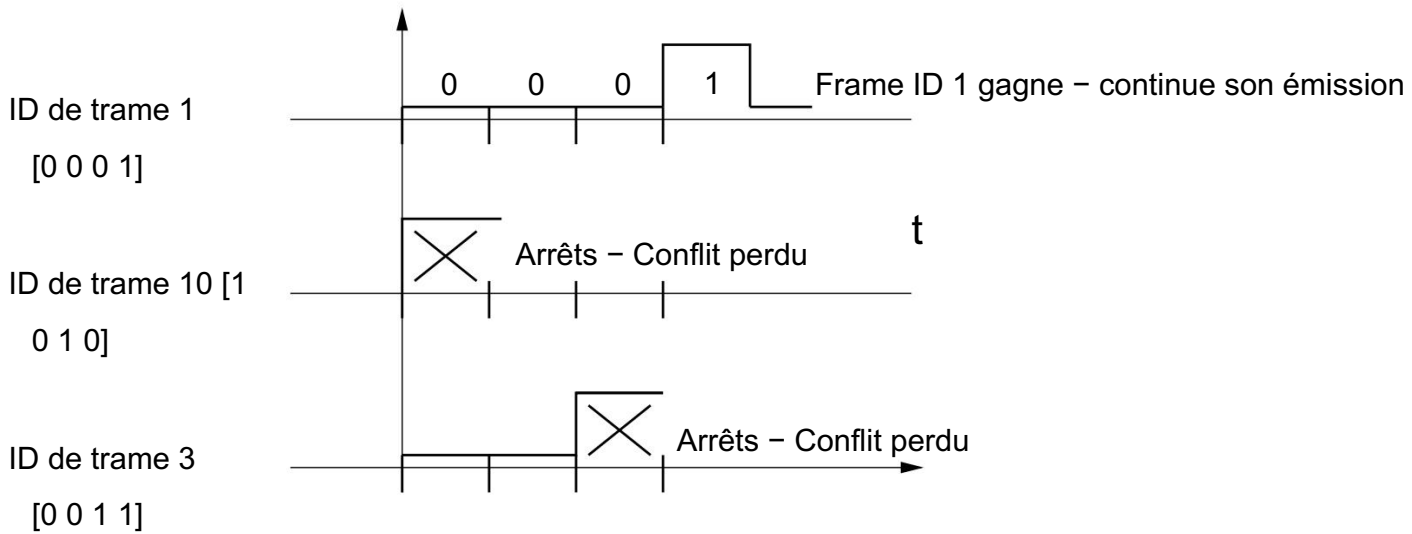
Si le bit reste inchangé, l'expéditeur continue d'envoyer, sinon il s'arrête.



E2 continue d'envoyer et E1 s'arrête.

CSMA/CR

Priorité avec résolution de conflit Chaque nœud envoie son ID (c'est-à-dire sa priorité) dans l'en-tête du message, avec un codage big-endian (le bit le plus significatif en premier).



Le message le plus prioritaire n'attend jamais. D'autres attendent que les messages de priorité supérieure soient transmis en premier.

Le débit est limité par la longueur maximale du fil.