

Manipulation de backoff dans CSMA/CA

LSV, CNRS UMR 8643, ENS Cachan

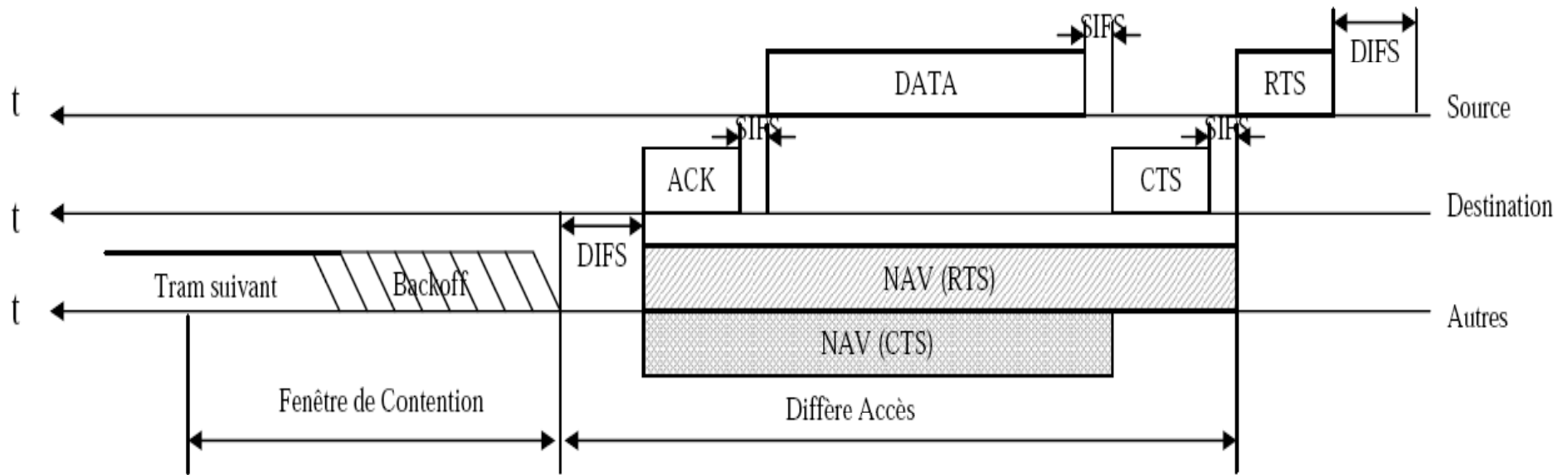
Plan

- Présentation de CSMA/CA.
- Triche dans CSMA/CA.
- DOMINO (système de détection de triche).
- Anciens résultats avec PRISM.
- Résultats avec APMC.
- Conclusion.

CSMA/CA

- La technologie sans fil permet à plusieurs utilisateurs d'accéder à une borne fournissant un service.
- Des utilisateurs peuvent tenter d'accéder à la borne en même temps → collision.
- Un protocole tente de minimiser le temps perdu par ces collisions tout en prenant en compte les spécificités des réseaux sans fil :
 - CSMA/CA
(Carrier Sense Multiple Access / Collision Avoidance)
 - Aussi appelé IEEE 802.11 ou WIFI

Description de CSMA/CA



Problème

- CSMA/CA contraint les utilisateurs pour rendre l'accès au médium équitable.

Problème

- CSMA/CA contraint les utilisateurs pour rendre l'accès au médium équitable.
- Les cartes réseaux sont devenues suffisamment modifiables pour qu'un utilisateur puisse modifier le protocole CSMA/CA.

Problème

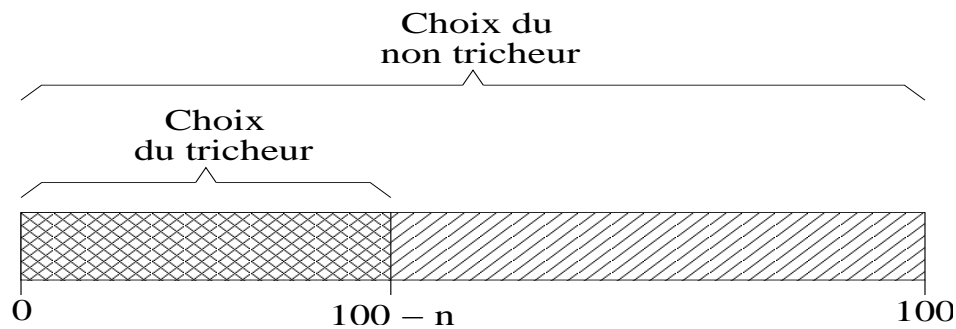
- CSMA/CA contraint les utilisateurs pour rendre l'accès au médium équitable.
- Les cartes réseaux sont devenues suffisamment modifiables pour qu'un utilisateur puisse modifier le protocole CSMA/CA.
- Possibilité de "tricher" en passant outre les contraintes.

Problème

- CSMA/CA contraint les utilisateurs pour rendre l'accès au médium équitable.
- Les cartes réseaux sont devenues suffisamment modifiables pour qu'un utilisateur puisse modifier le protocole CSMA/CA.
- Possibilité de "tricher" en passant outre les contraintes.
- Objectif :
 - Détecter les tricheurs.
 - Ne pas détecter des non tricheurs comme des tricheurs.
 - Pénaliser les tricheurs en proportion.

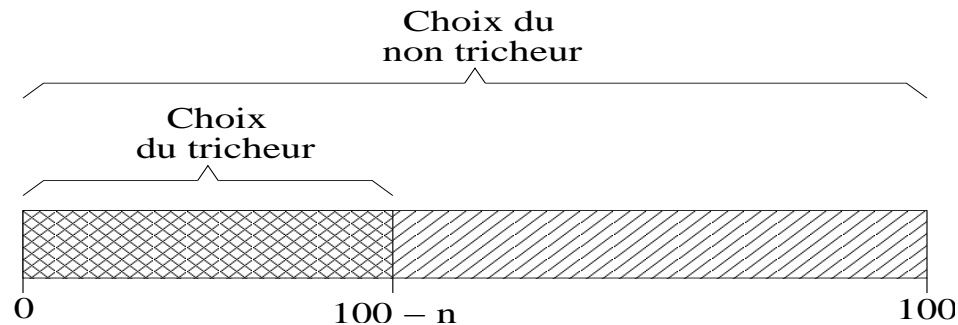
Triche

- Ces "tricheurs" respectent le protocole car sinon ils seraient facilement détectés.
- La triche à $n\%$ consiste à diminuer l'intervalle dans lequel on choisit le backoff.



Triche

- Ces "tricheurs" respectent le protocole car sinon ils seraient facilement détectés.
- La triche à $n\%$ consiste à diminuer l'intervalle dans lequel on choisit le backoff.



- Problème : on ne peut trouver un test qui détecte à coup sûr uniquement les tricheurs car un innocent a une probabilité non nulle pour choisir exactement les même backoff qu'un tricheur.

DOMINO

- DOMINO utilise plusieurs tests pour détecter des tricheurs dans CSMA/CA :
 - Des tests sur le respect du protocole.
 - Deux tests sur le respect du backoff :
 - **Maximal Backoff** : vérifie que sur une grande période, le backoff peut s'approcher du backoff maximal.
 - **Actual Backoff** : vérifie que la moyenne du backoff est proche de celle attendue.

DOMINO

- Pour tous les tests, il existe un compteur de triche.

```
if test=true then
  triche=triche+1
  if triche>K then
    tricheur détecté
    pénalisation
else if triche>0 then
  triche=triche-1
```

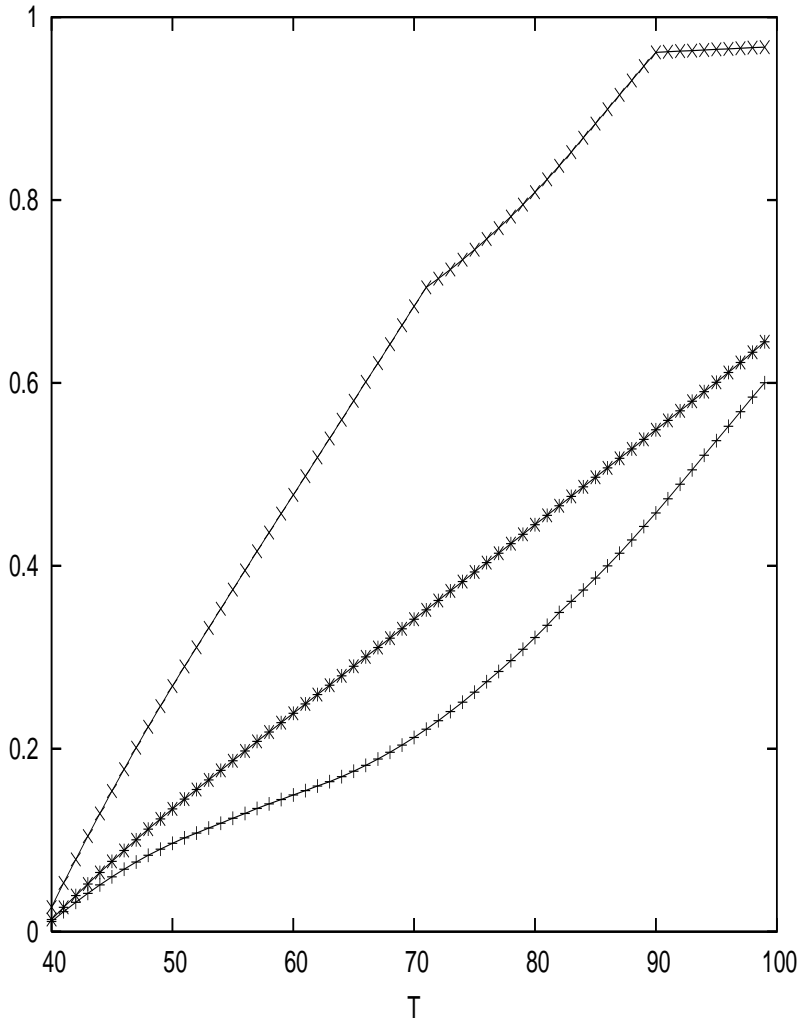
PRISM

- PRISM est un model checker probabiliste permettant d'introduire du non déterminisme.
 - Dans CSMA/CA, la taille des envois est non déterministe.
- Utilisation du modèle de CSMA/CA des auteurs de PRISM :
 - 2 utilisateurs.
 - 1 envoi par utilisateur.
 - 1 compteur de temps.

Favorisation du tricheur

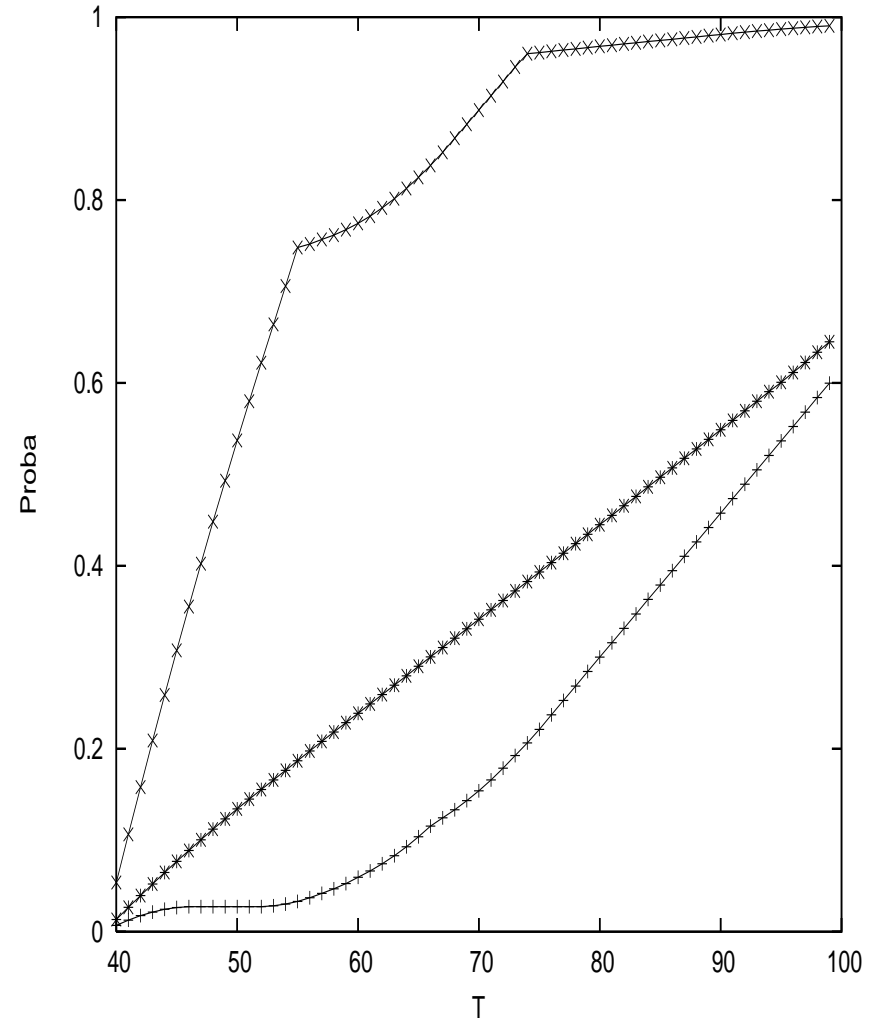
50%

Pmin=? [true U (s{1,2}=12 & t<=T)]



75%

Pmin=? [true U (s{1,2}=12 & t<=T)]



Détection par DOMINO

- Introduction de DOMINO par un compteur de triche au moment du choix du backoff.
- Le compteur est limité à 2.
- Calcul de la probabilité maximale pour que le tricheur ou le non tricheur ait son compteur de triche égal à 1 ou 2.

$$P_{max} =? [\text{true } U (\text{triche}\{1, 2\} = k)]$$

- Cas de la triche à 25% et 50% et pour 2 et 3 collisions initiales.

Détection par DOMINO

25% de triche

		triche=1	triche=2	taille du modèle
2 collisions	tricheur	0.032	5.1E-4	9 043 363
	non tricheur	0.024	3.8E-4	8 475 880
3 collisions	tricheur	0.670	0.011	9 025 166
	non tricheur	0.505	0.008	8 457 683

Limitation de l'approche

- Pour mieux représenter le problème :
 - Plus d'un utilisateur en face du tricheur.
 - Des envois multiples.
- Limitations :
 - Temps de calcul déjà long.
 - Tailles des modèles rapidement trop importantes.

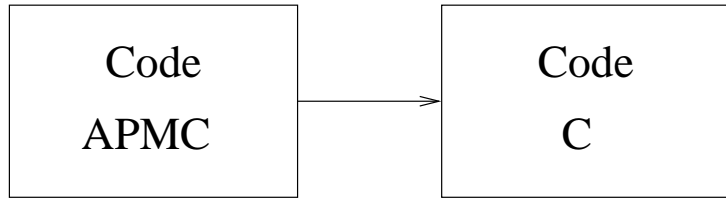
APMC

- APMC = Approximate Probabilistic Model Checking.
- Même syntaxe que PRISM.
- Calculs uniquement probabilistes.

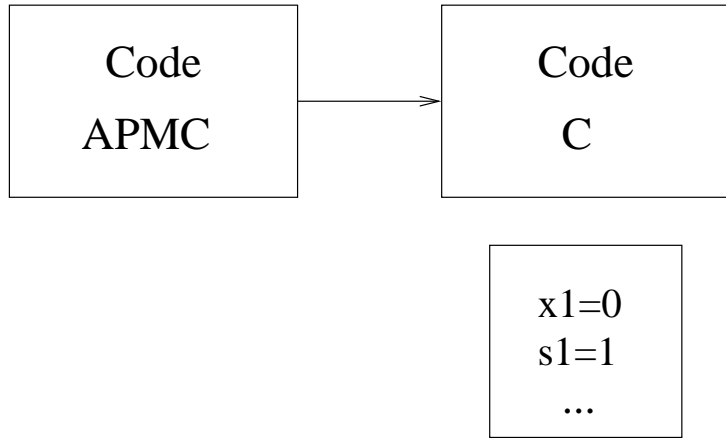
APMC demo

Code
APMC

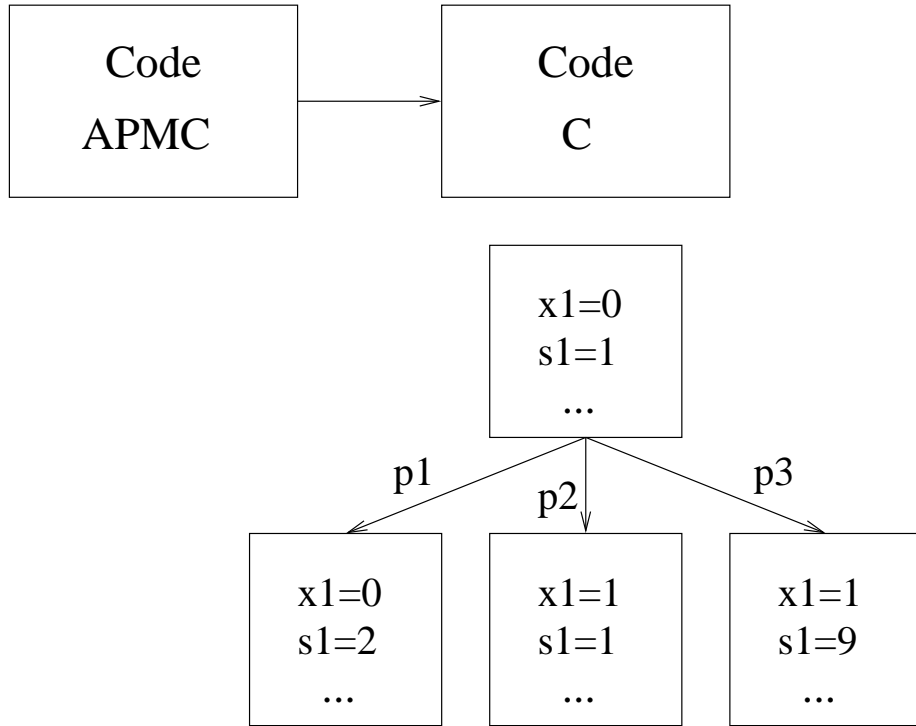
APMC demo



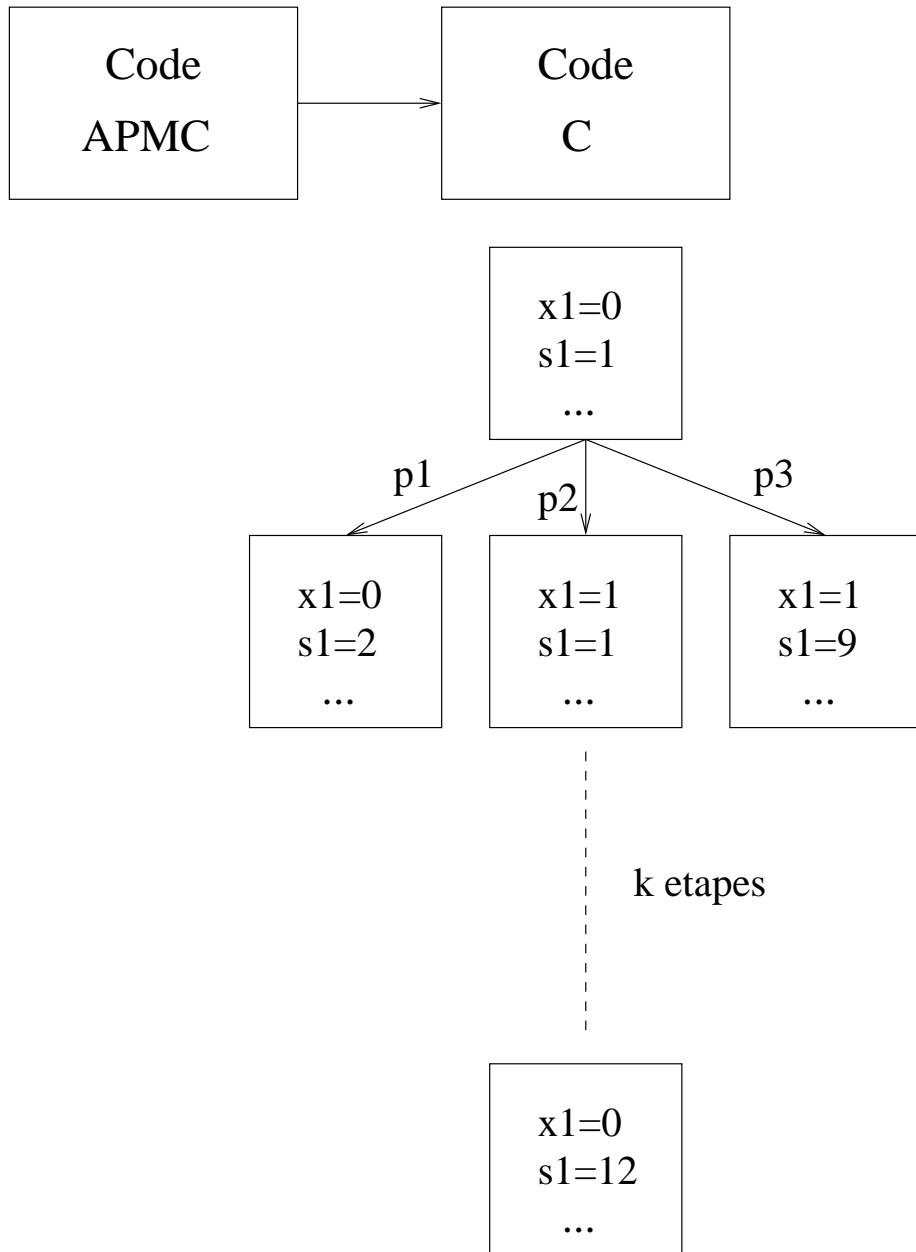
APMC demo



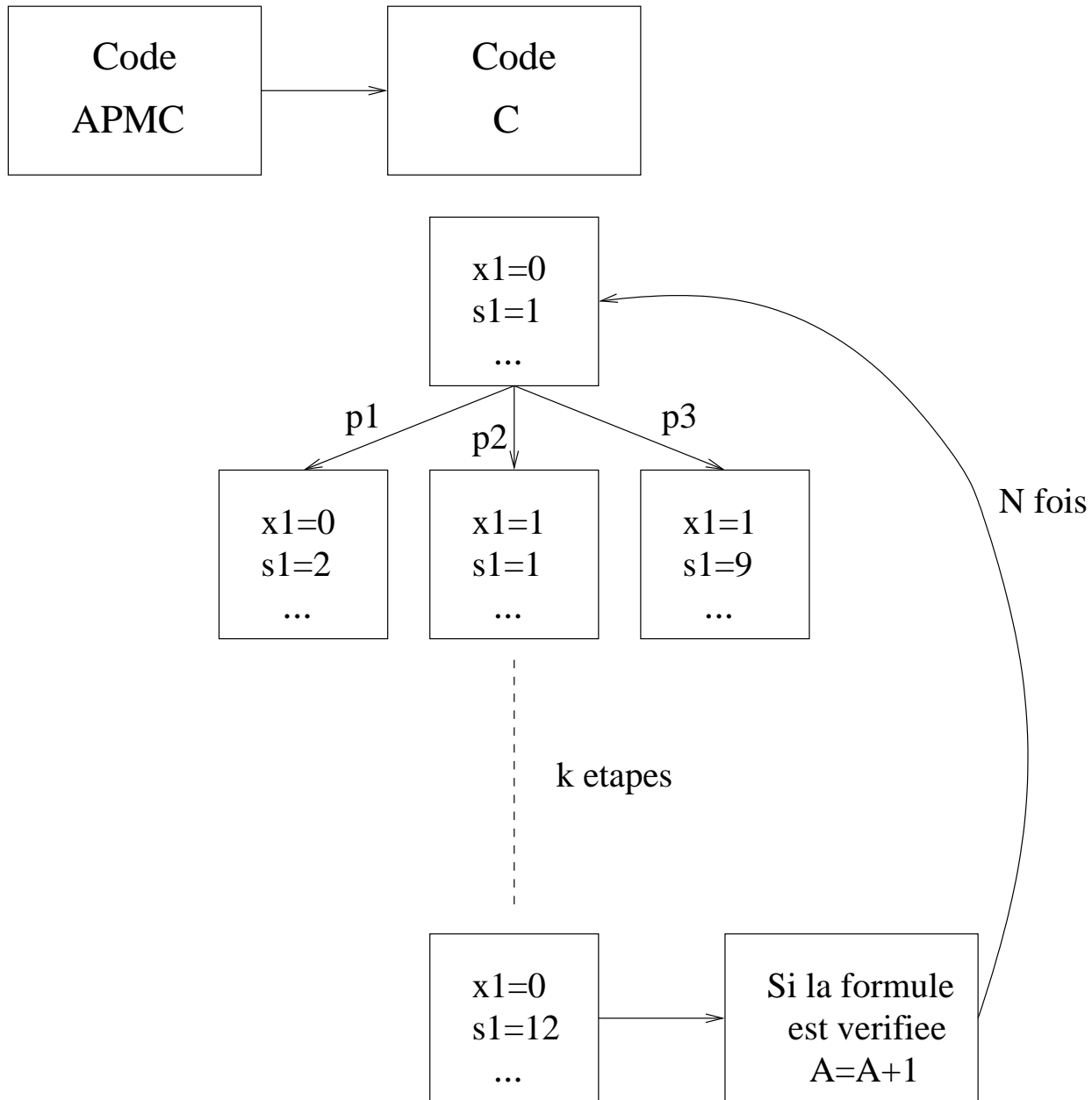
APMC demo



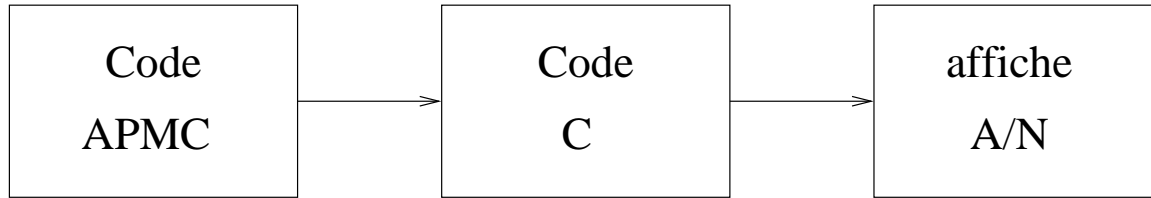
APMC demo



APMC demo



APMC demo



Avantages d'APMC

- Pas de construction de modèle :
 - Gain de temps.
 - Permet de vérifier des modèles dont la construction est trop longue ou volumineuse.

Avantages d'APMC

- Pas de construction de modèle :
 - Gain de temps.
 - Permet de vérifier des modèles dont la construction est trop longue ou volumineuse.
- Assurance d'obtenir un résultat à un moment.

Avantages d'APMC

- Pas de construction de modèle :
 - Gain de temps.
 - Permet de vérifier des modèles dont la construction est trop longue ou volumineuse.
- Assurance d'obtenir un résultat à un moment.
- Conception prévue pour déployer APMC sur un réseau.

Résultat théorique pour APMC

- On veut connaître $P^k(\psi)$ la probabilité pour que ψ soit vérifiée sur les chemins de longueur k .

Résultat théorique pour APMC

- On veut connaître $P^k(\psi)$ la probabilité pour que ψ soit vérifiée sur les chemins de longueur k .
- APMC calcule $P_{APMC}^k(\psi)$ une valeur approché de $P^k(\psi)$.

$$P[|P_{APMC}^k(\psi) - P^k(\psi)| \leq \epsilon] \geq 1 - \delta$$

Avec ϵ et δ calculés avec N .

- Pour nos expériences $\epsilon = 10^{-2}$ et $\delta = 10^{-10}$.

Utilisation d'APMC

- Résultats avec PRISM confirmés avec APMC.

Utilisation d'APMC

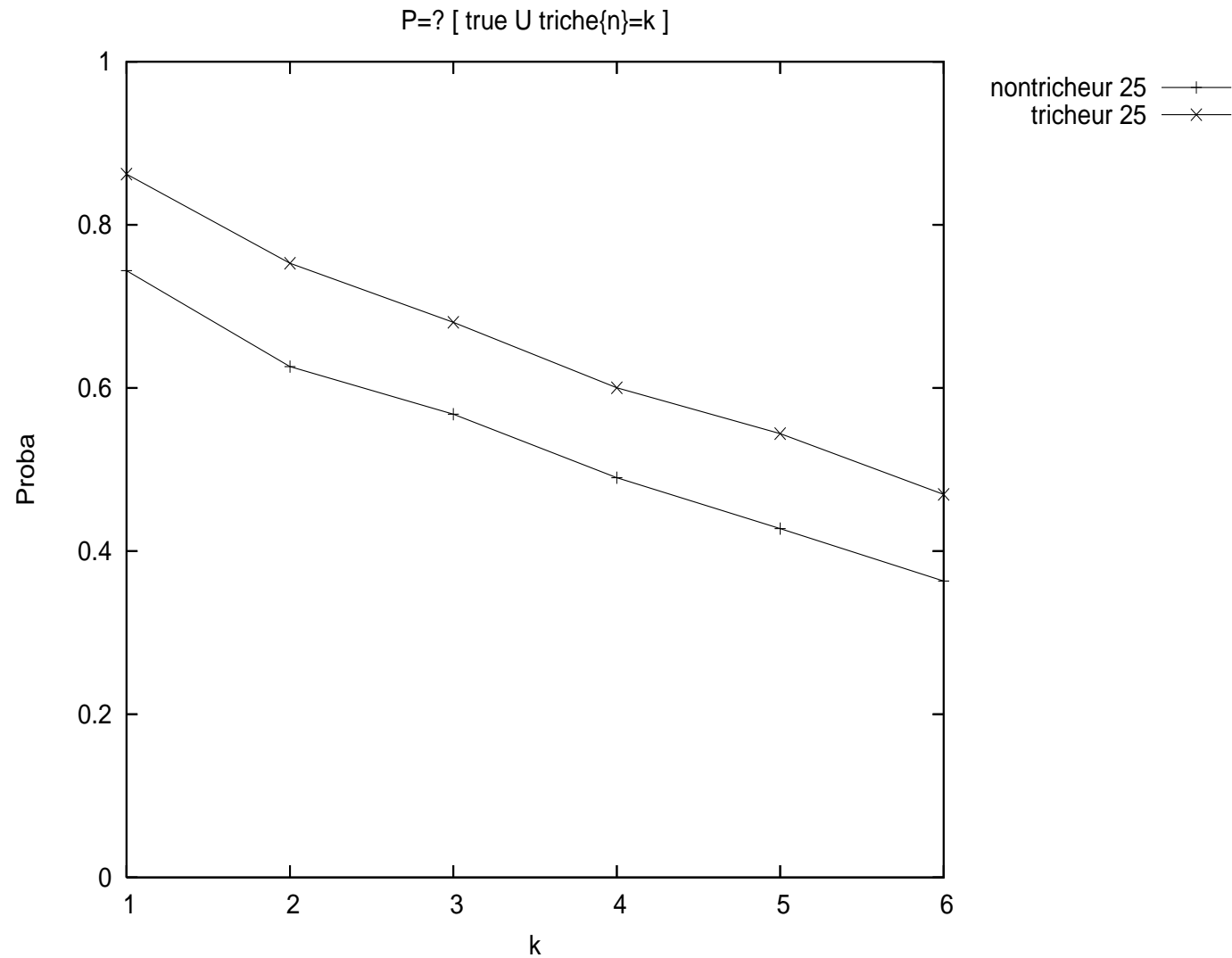
- Résultats avec PRISM confirmés avec APMC.
- Modification du modèle :
 - Pas de limite pour le nombre de messages envoyés.
 - Rajout d'utilisateurs : de 2 à 5 utilisateurs.

Utilisation d'APMC

- Résultats avec PRISM confirmés avec APMC.
- Modification du modèle :
 - Pas de limite pour le nombre de messages envoyés.
 - Rajout d'utilisateurs : de 2 à 5 utilisateurs.
- Nouveaux résultats sur DOMINO.

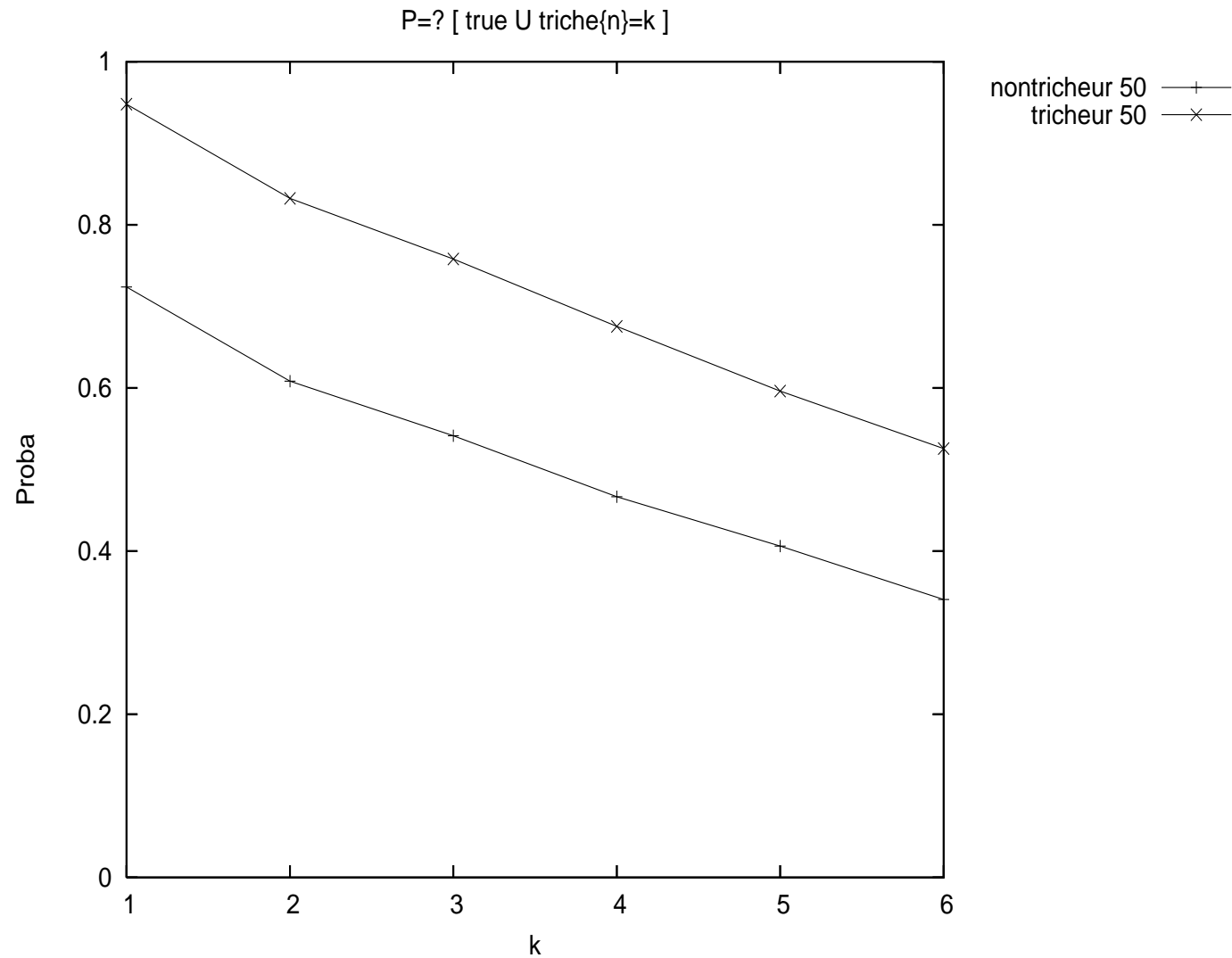
DOMINO avec APMC

2 utilisateurs 25%



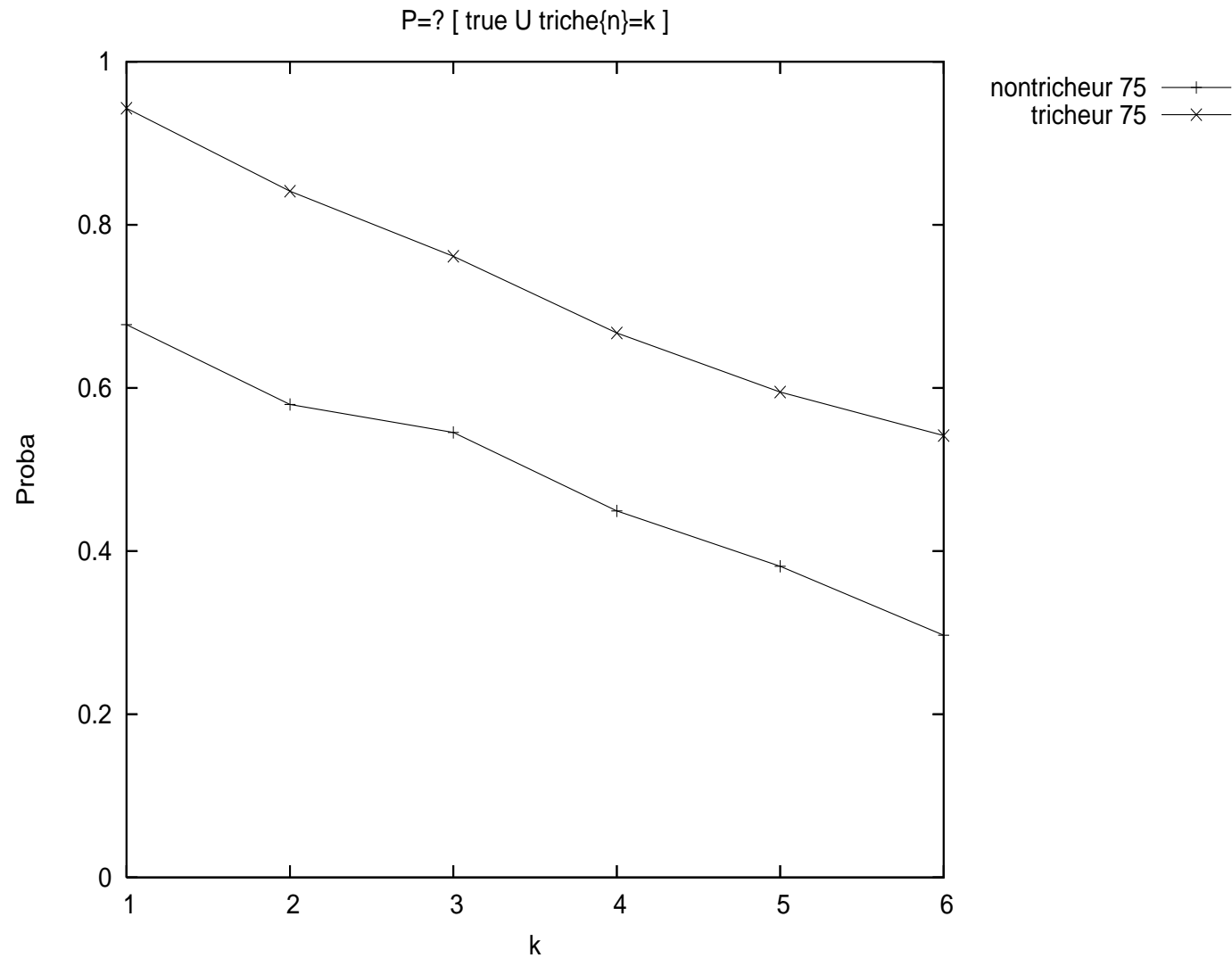
DOMINO avec APMC

2 utilisateurs 50%



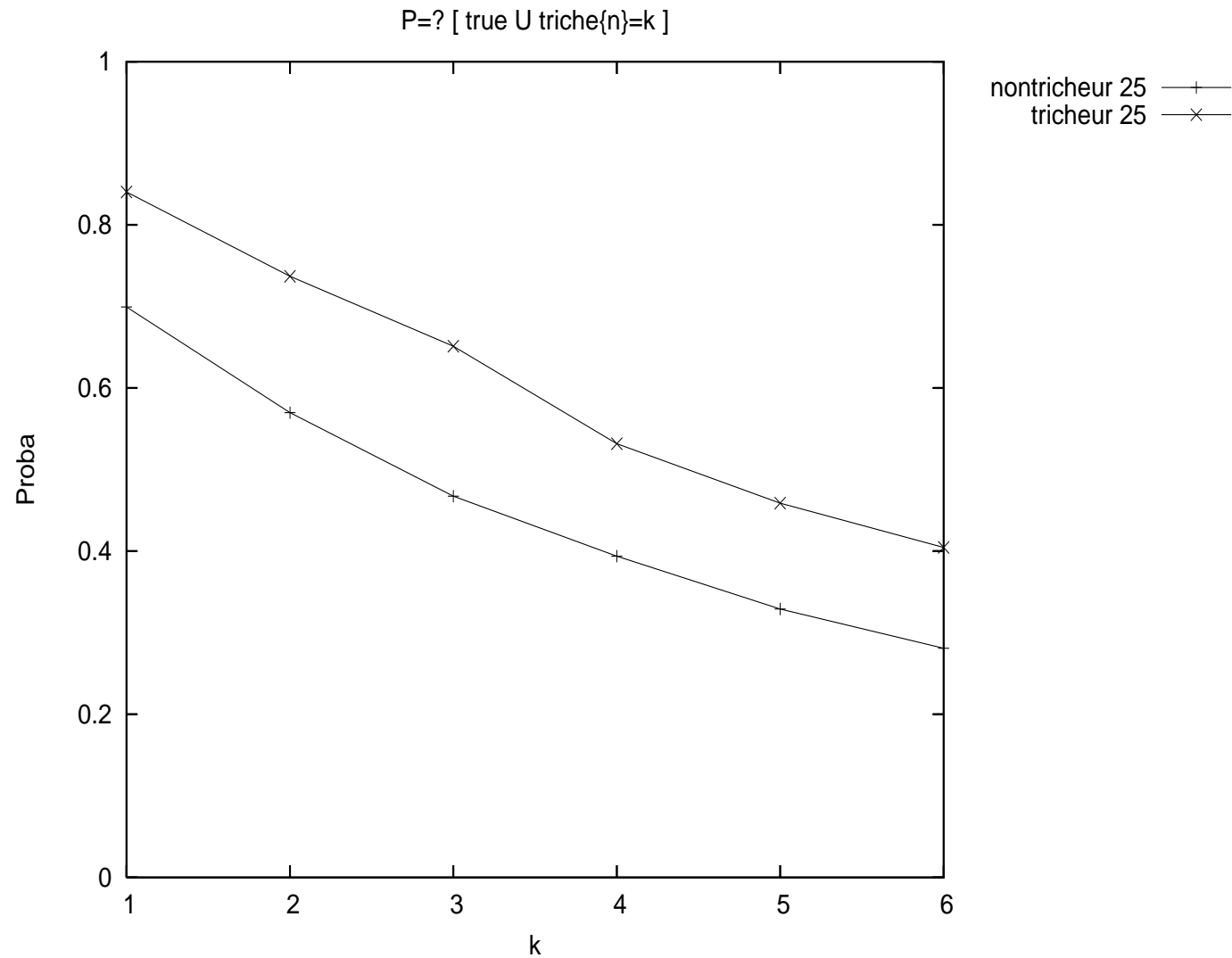
DOMINO avec APMC

2 utilisateurs 75%



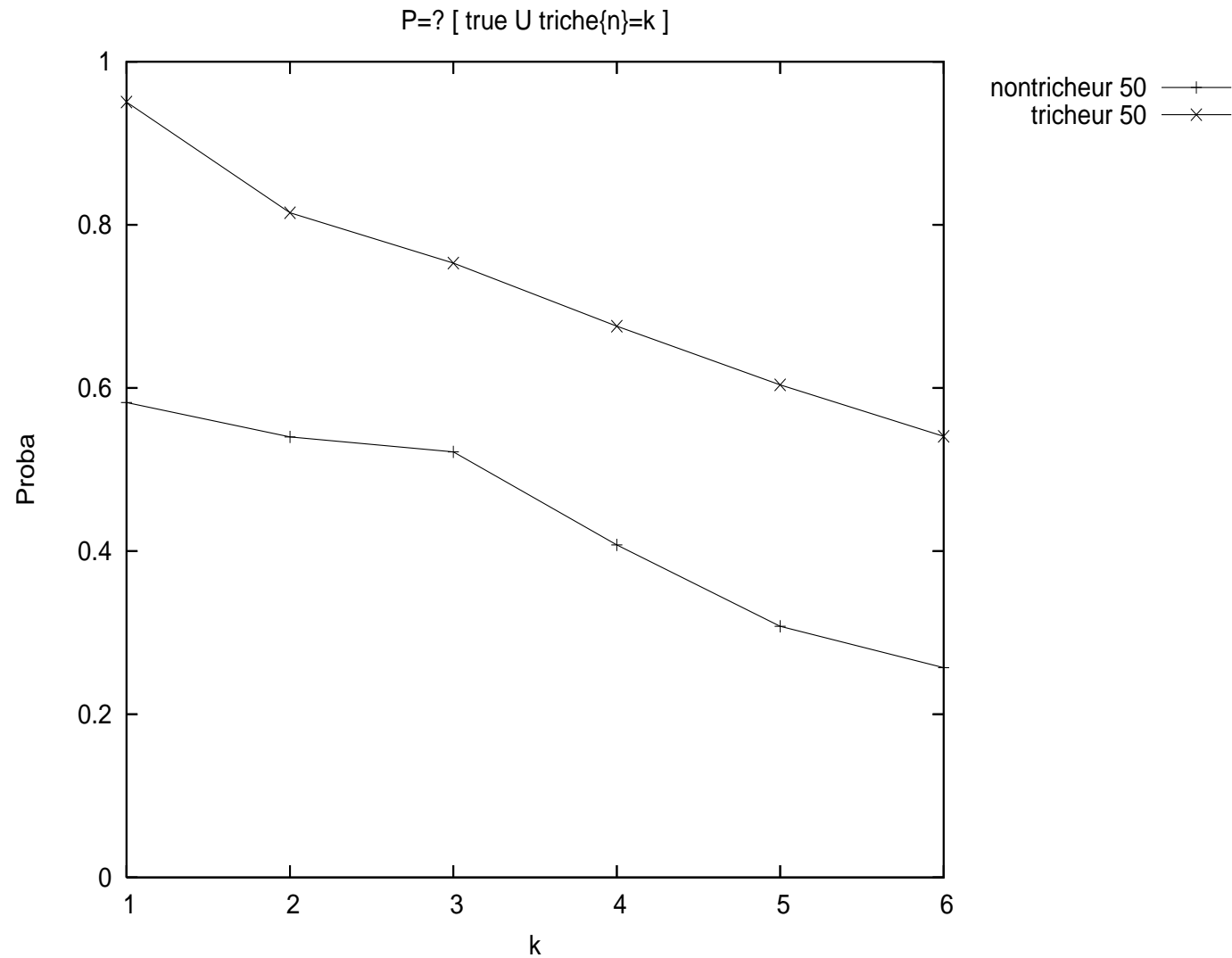
DOMINO avec APMC

3 utilisateurs 25%



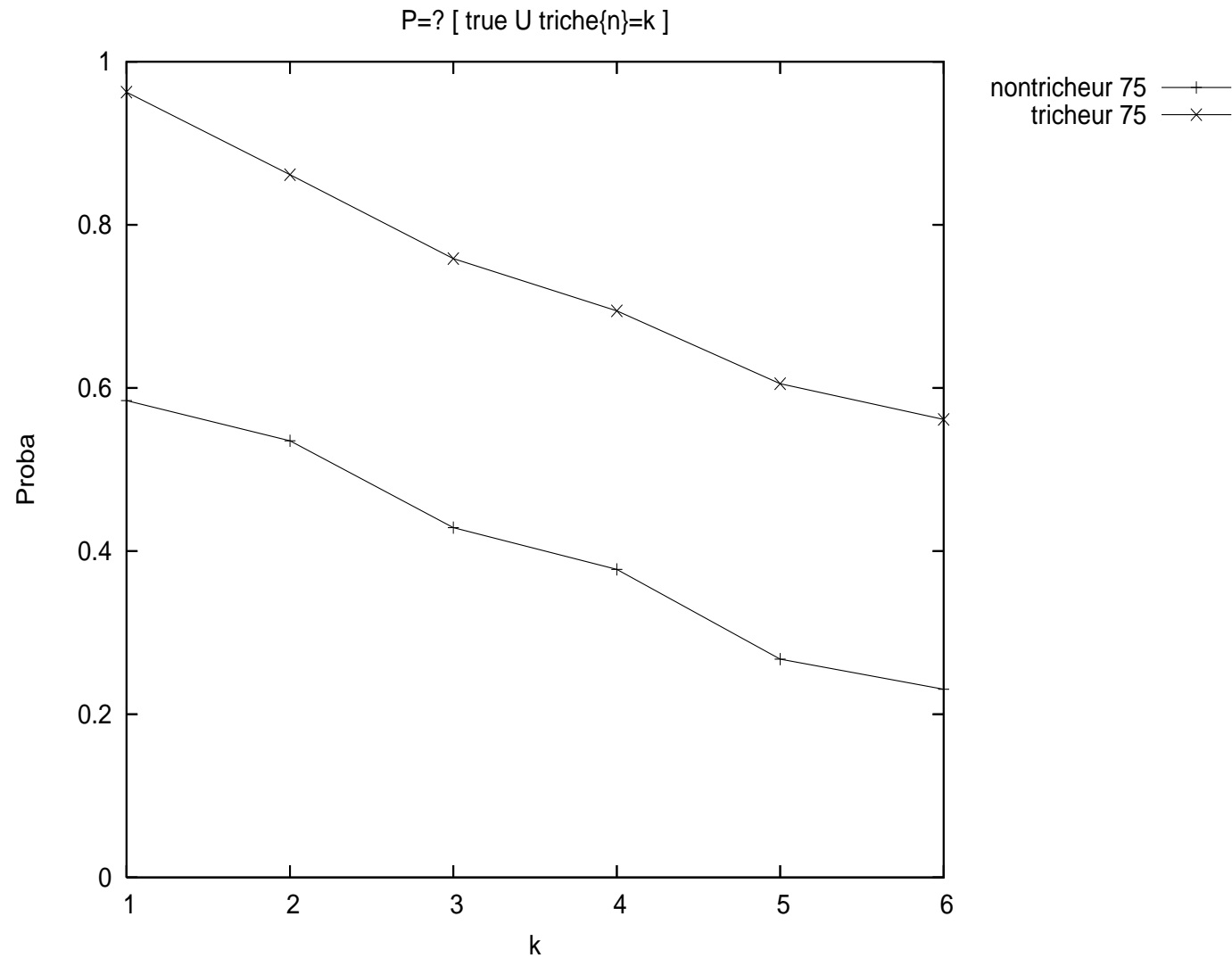
DOMINO avec APMC

3 utilisateurs 50%



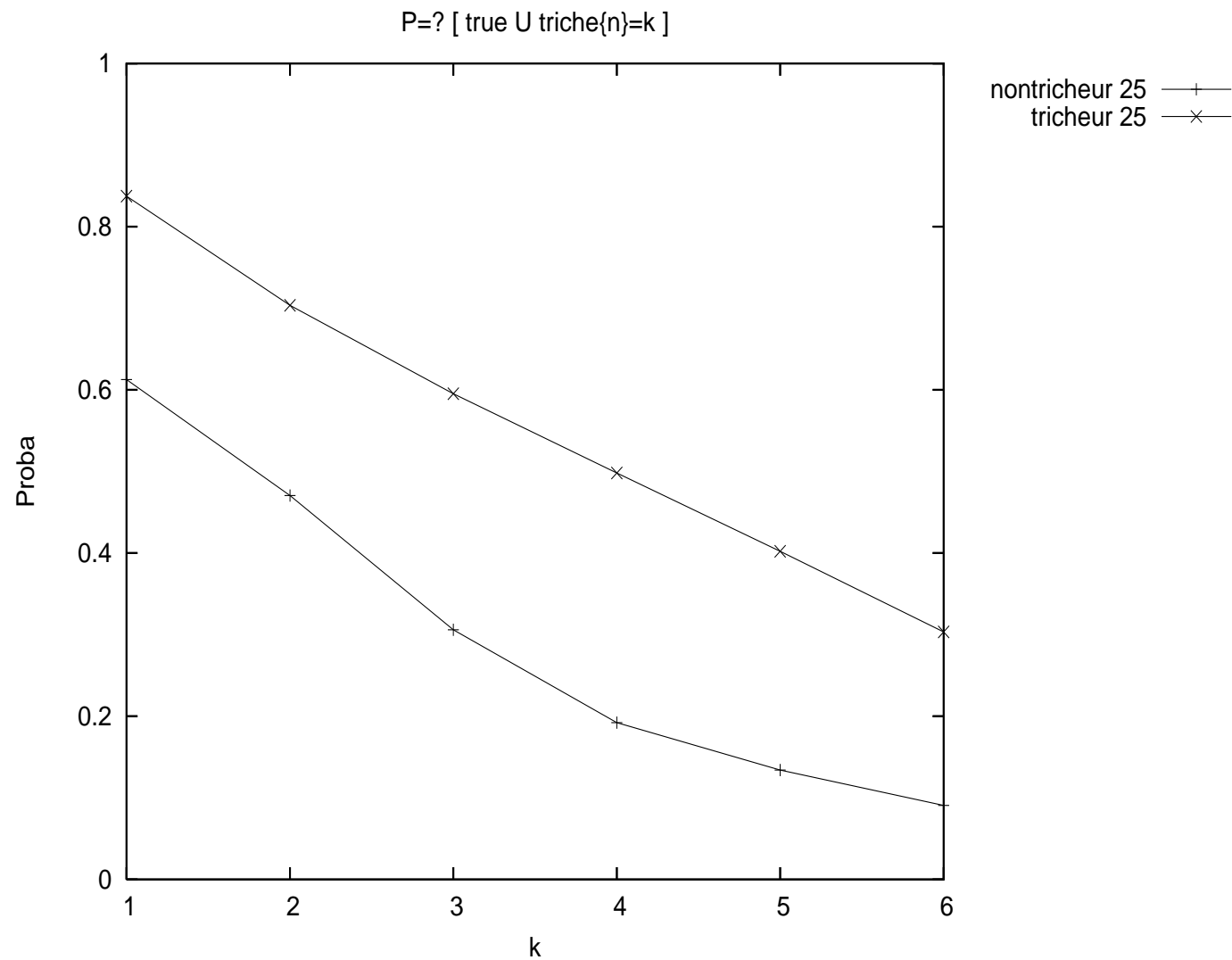
DOMINO avec APMC

3 utilisateurs 75%



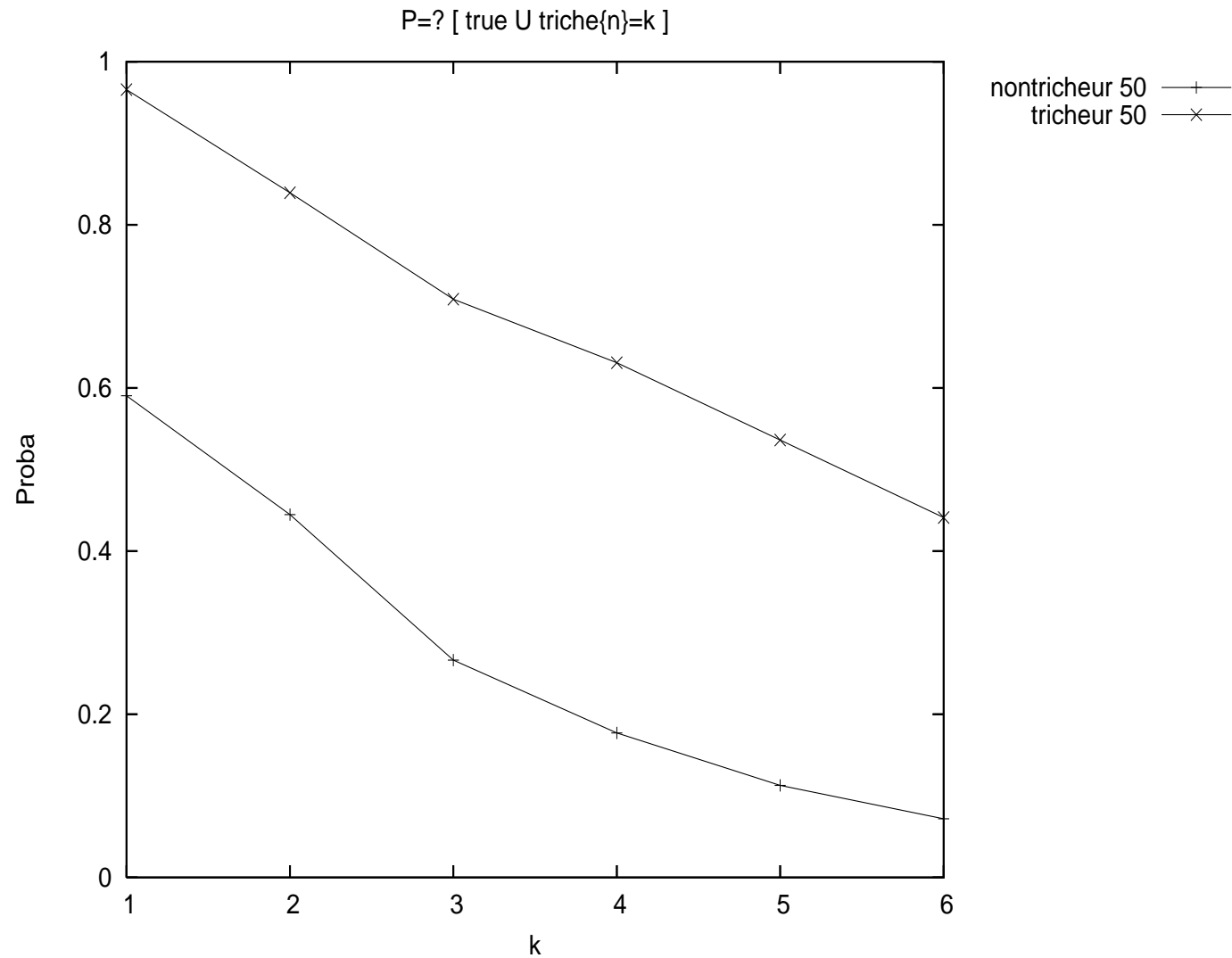
DOMINO avec APMC

4 utilisateurs 25%



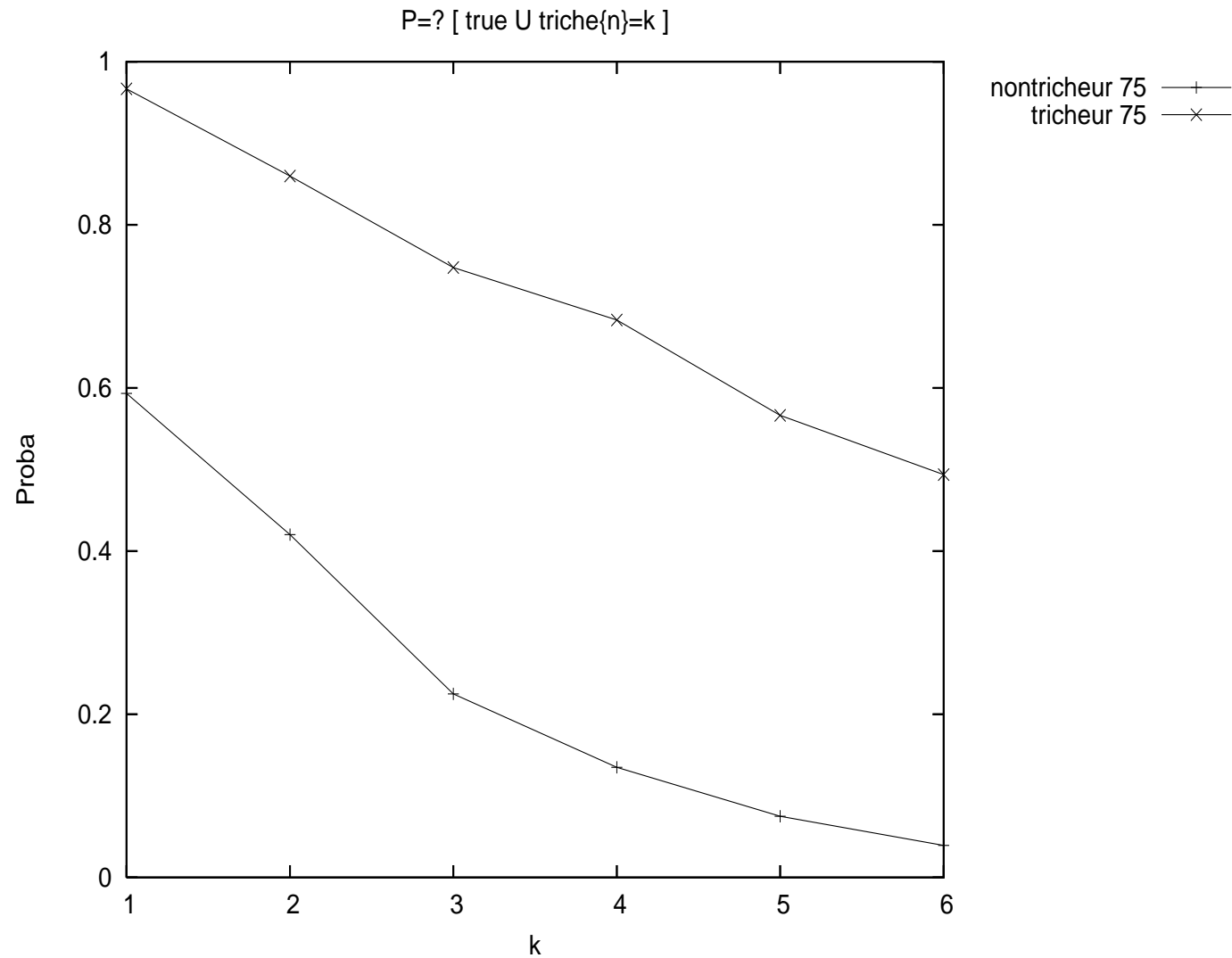
DOMINO avec APMC

4 utilisateurs 50%



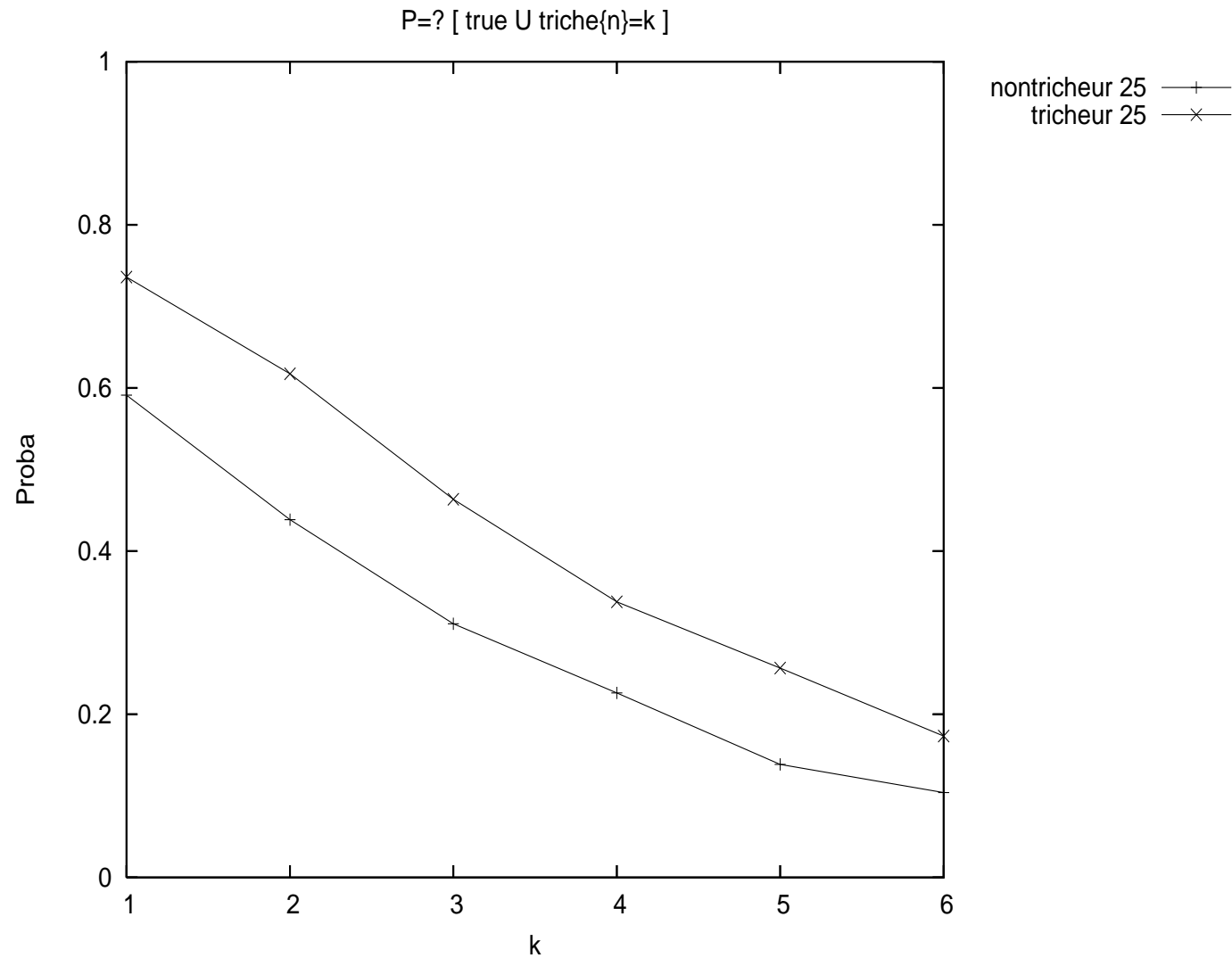
DOMINO avec APMC

4 utilisateurs 75%



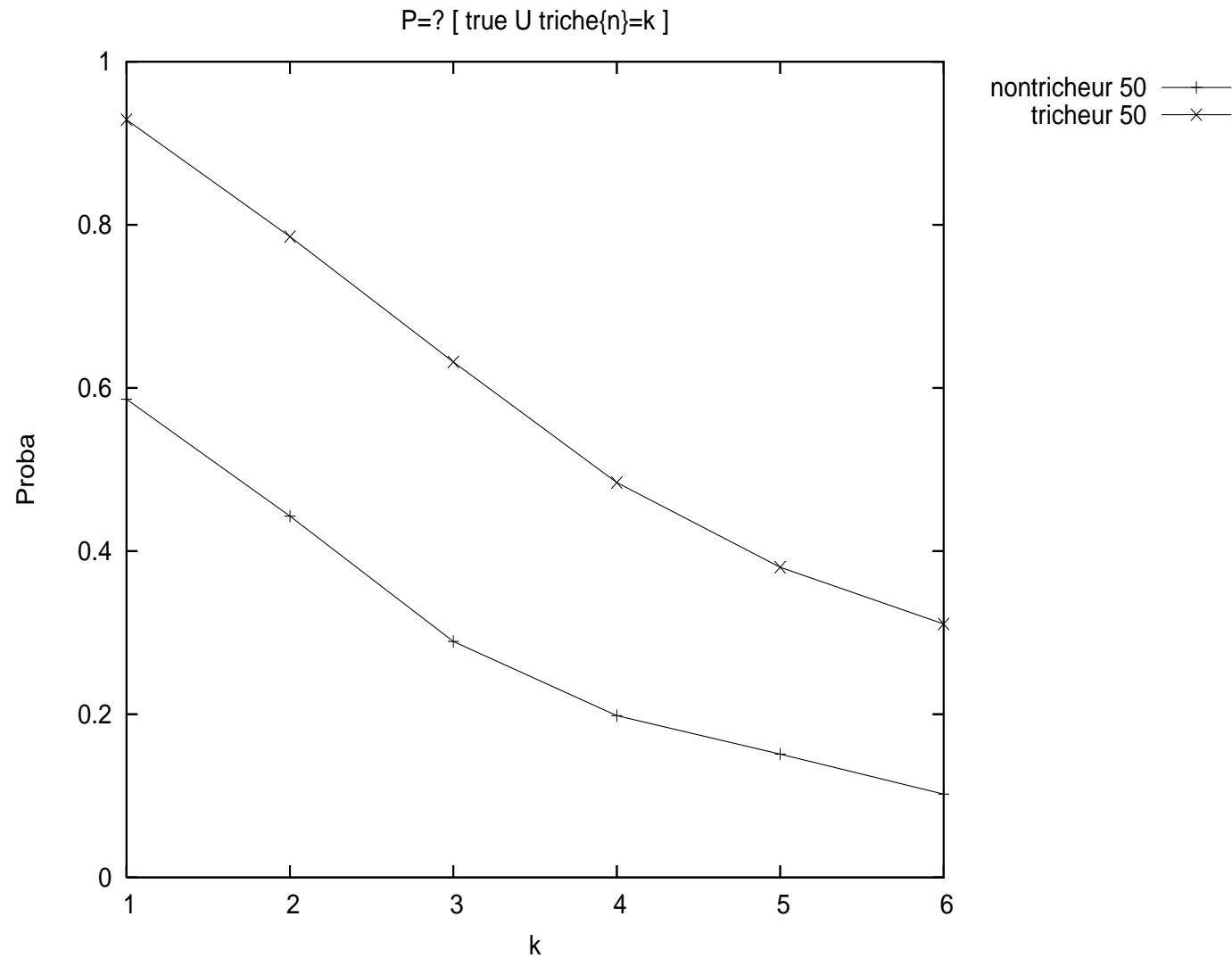
DOMINO avec APMC

5 utilisateurs 25%



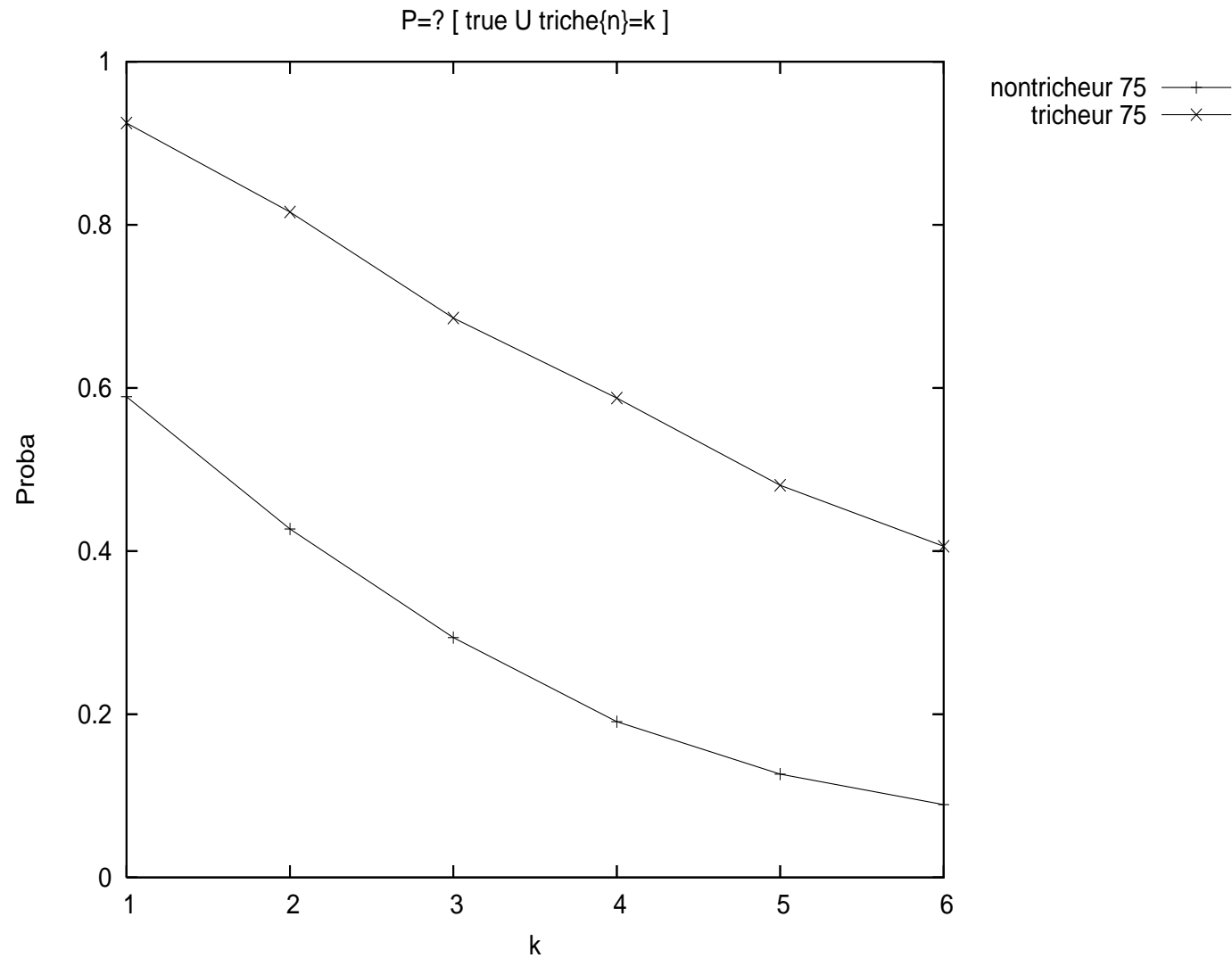
DOMINO avec APMC

5 utilisateurs 50%



DOMINO avec APMC

5 utilisateurs 75%



Conclusion

- PRISM permet de regarder les aspects non déterministes d'un système.
- APMC est plus adapté pour regarder les aspects probabilistes d'un système.
- DOMINO permet de détecter un tricheur dans les cas étudiés.
- Possibilité de cerner les valeurs acceptables de K .

Travaux futurs

- Entrer le nombre d'utilisateurs comme paramètre.
- Étudier la pénalisation.
- Étudier de nouvelles triches.
- Utiliser le déploiement d'APMC sur un réseau :
 - Résultats plus précis.
 - Modèles plus complexes.