Examen du cours Mobilité
M2 Pro, Université Paris Diderot

Michel Habib

March 6, 2016

1 Questions de cours

1. Expliquer à quoi peut servir d'ajouter de l'aléatoire dans un algorithme (i.e., le déroulement de l'algorithme va dépendre du tirage d'une variable aléatoire) dans une application distribuée ou parallèle.
2. Détailler 4 exemples d'application différents.
3. Qu'est-ce un réseau d'overlay ?

2 Algorithmes parallèles sur Machines PRAM

Pour chacune des questions suivantes, on donnera une version séquentielle de l'algorithme et l'on précisera pour l'algorithme parallèle, le nombre de processeurs utilisés ainsi que la complexité en temps de votre algorithme et le travail. On précisera aussi le modèle de machine PRAM qui permet de faire tourner votre algorithme.

1. Ecrire un algorithme qui calcule le minimum et maximum d'un tableau d'entiers.
2. Ecrire un algorithme qui détermine les occurrences multiples dans un tableau d'entiers.
3. Ecrie un algorithme qui calcule l'élément médian d'un tableau d'entiers.

3 Spécification d'un système pair-à-pair de gestion de clés

Il s'agit de construire un système de cryptographie à clé public et privée. Pour coder un message à une personne A, on va chercher dans un table plublic le code de A qui permet de crypter le message et de l'envoyer à A.

Quand A reçoit le message il dispose d'une clé privée qui lui permet de décoder de décoder le message.

A Dans ce système pair-à-pair il faut donc assurer deux fonctionnalités distinctes : permettre à tout le monde de retrouver la clé publique d'un membre du réseau.

B Assurer la répartition sûre des clés privées à l'entrée d'un nouvel élément du réseau.

1. Quel est l'intérêt d'une architecture pair-à-pair pour un tel système ?
2. Préciser les spécifications de votre système pair-à-pair.
3. Comment résister aux attaques ?