Contrôle d'accès distribué à un réseau Pair-à-Pair

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong

Supélec, équipe SSIR (EA 4039)

15 juin 2007

Fil directeur du travail

Objectif

Assurer confidentialité, intégrité, disponibilité en Pair-à-Pair

Contraintes spécifiques des réseaux Pair-à-Pair

Réseaux *dynamiques* et *collaboratifs* sans autorité ponctuelle

Approche

1. Contrôle d'accès au réseau pour limiter le nombre d'attaquants
2. Protocoles de sécurité résistant à un nombre limité d'attaquants

Présentation des réseaux Pair-à-Pair

Spécificités des réseaux Pair-à-Pair

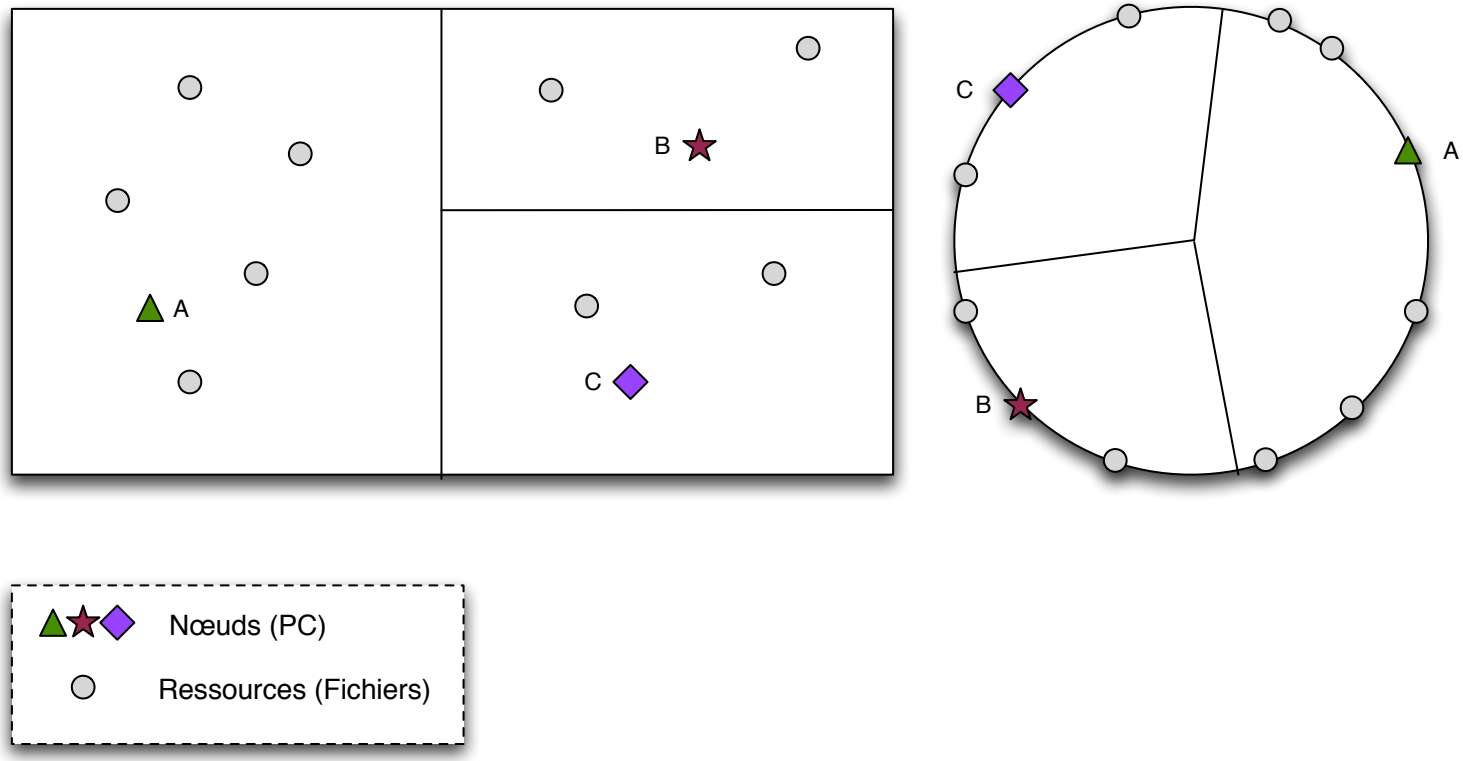
- Forte disponibilité
- Déploiement économique
- Passage à l'échelle
- Équité des pairs
- Absence d'autorité centrale

Applications

- Partage de fichiers
- Multidiffusion
- Sauvegarde ?

Réseaux P2P structurés

Implémentent une *Distributed Hash Table* (DHT) dans un *overlay*.



DHT : $key \mapsto value$

Plan

Fontionnement général

1. Un nouveau membre accède automatiquement au réseau (*Certification*)
2. Chaque membre est surveillé par les autres (*IDS*)
3. Un membre ne se conformant pas au protocole est exclu (*Exclusion*)

Le contrôle d'accès est *réactif* et non proactif.

Remarque

Le système présenté ne protège pas de la Sybil Attack

Contrôle d'accès par un ratio fixe des membres

Certification

Autorisation d'accès matérialisé par un *certificat* :

- Contenant la clé publique du nœud
- Signé par une clé *de réseau* unique S_r

Génération du certificat

Certificat généré par un pourcentage des autres membres du réseau :

- Distribution équitable de l'autorité
- Mais personne n'a une vue globale du réseau (taille)

Principe de la cryptographie à seuil

Principe

- Le réseau possède un couple de clés (S_r, P_r)
- P_r est connue de tous
- S_r est fragmentée sur l'ensemble des nœuds
- Le chiffrement d'un message avec la clé privée demande la coopération de t nœuds
- **Aucun nœud ne connaît toute la clé privée à un instant**

Nombre fixe

[Kong *et al.*, 01]

Contrôle d'accès matérialisé par un *certificat* généré par l'accord d'un *nombre fixe* de pairs.

[Desmedt, 97], [Rabin, 98]

Papiers généraux : signer une donnée par la coopération de t entités parmi n, t et n fixés à l'initialisation

Ratio fixe mais avec serveur

[Saxena *et al.*, 03]

Extension à l'accord d'un *ratio fixe* de membres, mais utilisation d'un serveur de comptage.

[Frankel *et al.*, 97]

Modification de t et n à la volée :

1. $(t, n) \rightarrow (t, t)$ *(Poly-to-Sum)*
2. $(t, t) \rightarrow (t', n')$ *(Sum-to-Poly)*

Corruption possible si un attaquant parmi les t
Évaluation de la taille du réseau ?

Ratio fixe sans serveur

Contrôle d'accès

Contrôle d'accès par un *ratio fixe* des membres *sans serveur*

Système de cryptographie à seuil adaptative

Modification de t et n à la volée pour maintenir un *ratio fixe* mais sans connaître la taille du réseau.

Fonction RSA homomorphique

Fragmentation de rang 0

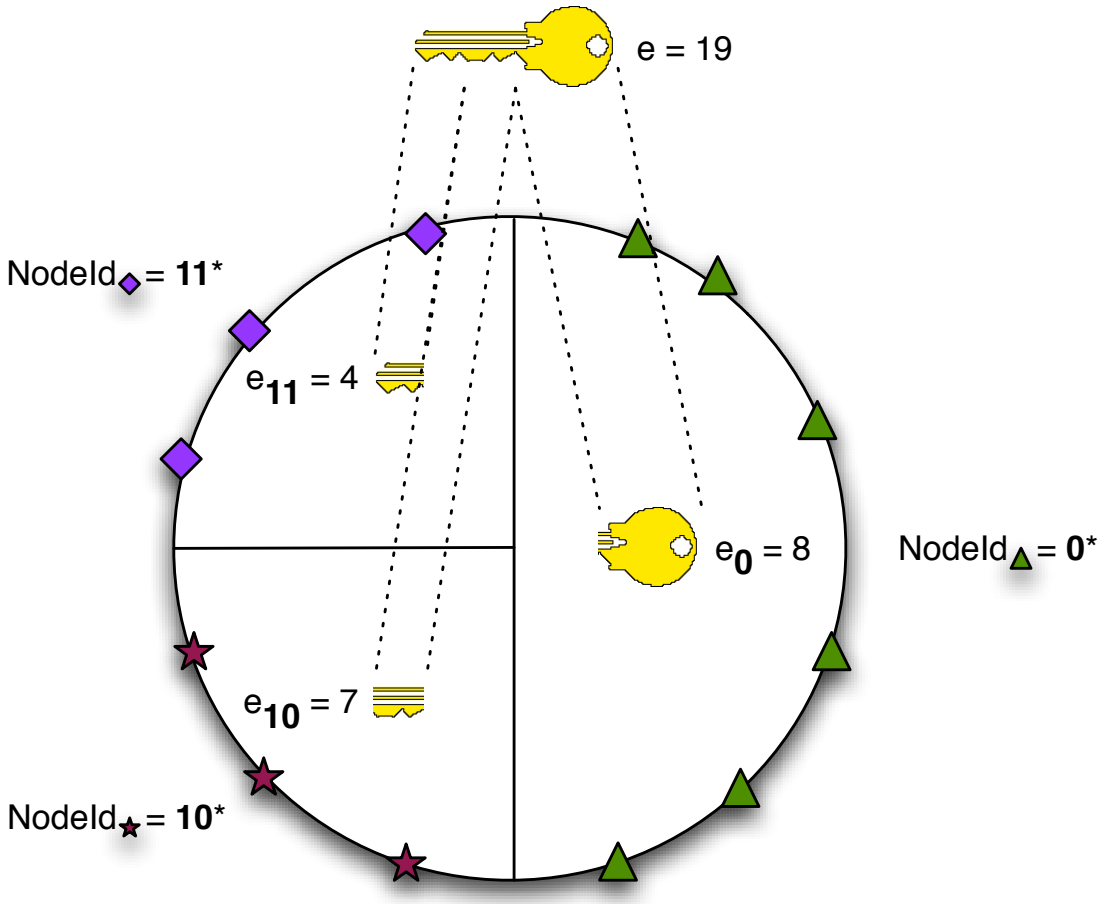
Soit $S_r = (e, n)$ la clé secrète du réseau
Soient e_0, e_1 tels que $e = e_0 + e_1$ (+ arithmétique)
Alors $m^e[n] = m^{e_0+e_1}[n] = (m^{e_0}[n] \times m^{e_1}[n])[n]$

Exemple

$(e, n) = (19, 187)$
$e_0 = 8, e_1 = 11$ tels que $19 = 8 + 11$
$m = 18$
Alors $18^{19}[187] = (18^8[187] \times 18^{11}[187])[187] = 52$

$\Rightarrow$ On répartit les fragments e_i et on itère récursivement au fur et à mesure de la croissance du réseau

Fragmentation de la clé



Fonctionnement du système

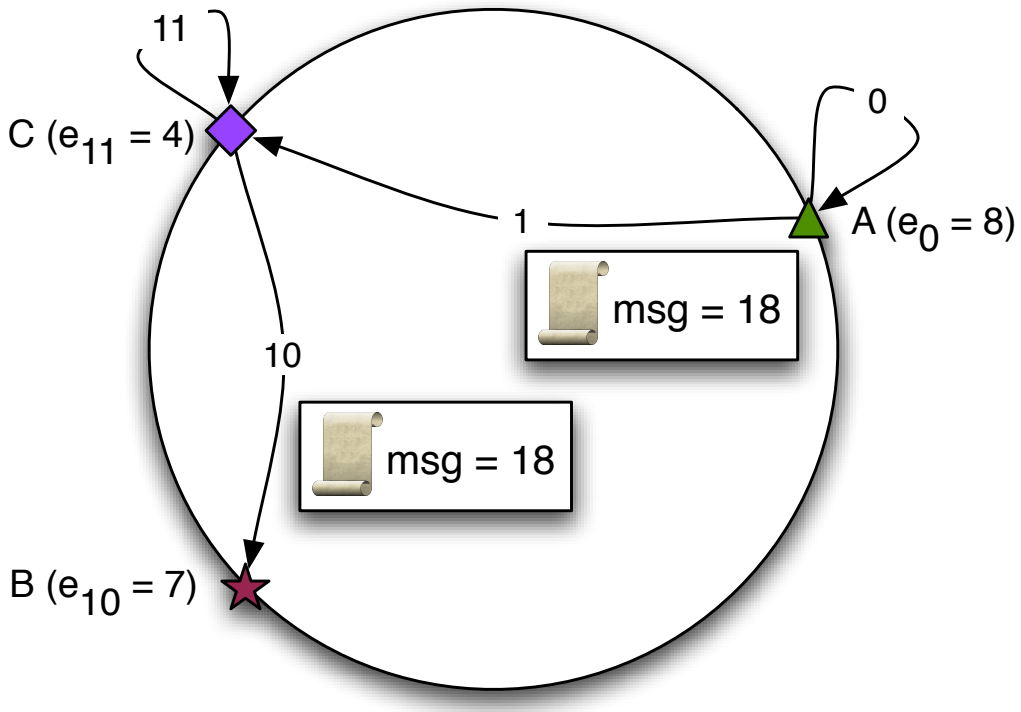
Valeurs du système

- t est le ratio de nœuds à contacter pour certifier un nouveau membre
- $\mathcal{G}_{min}$ (resp. $\mathcal{G}_{max}$) est la taille minimale (resp. maximale) d'un groupe de fragmentation
- $\frac{1}{\mathcal{G}_{max}} < t < \frac{1}{\mathcal{G}_{min}}$

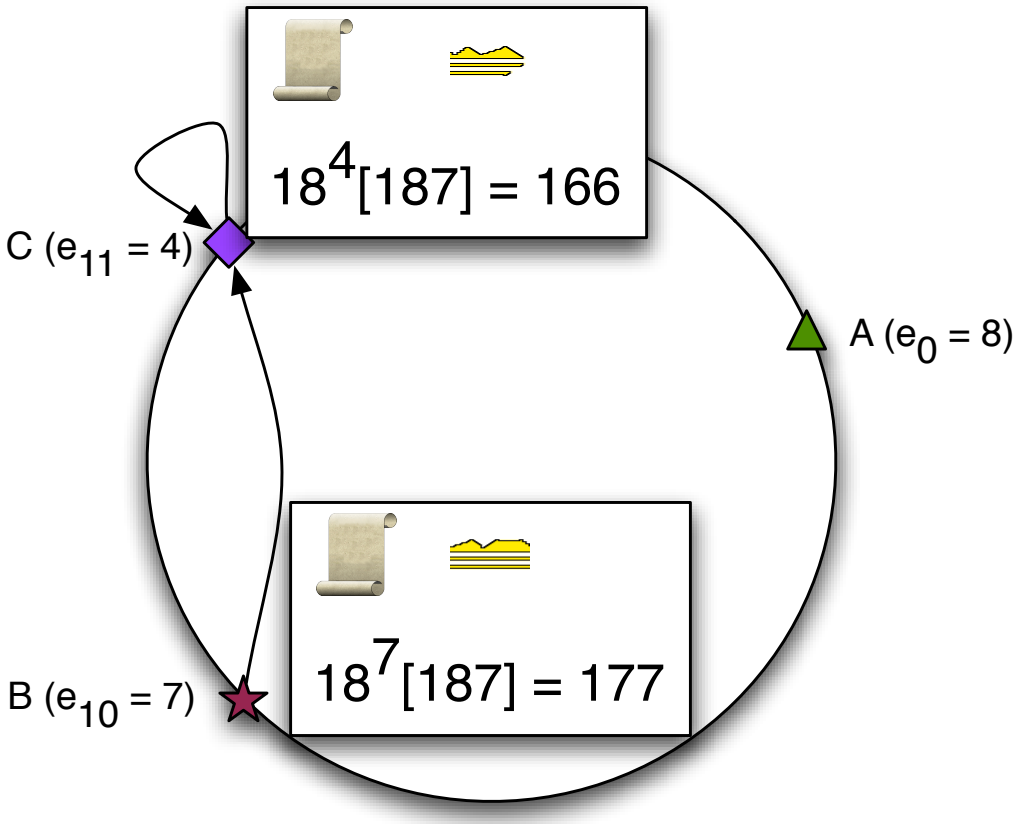
Remarque

Le nombre de nœuds du réseau n'intervient pas

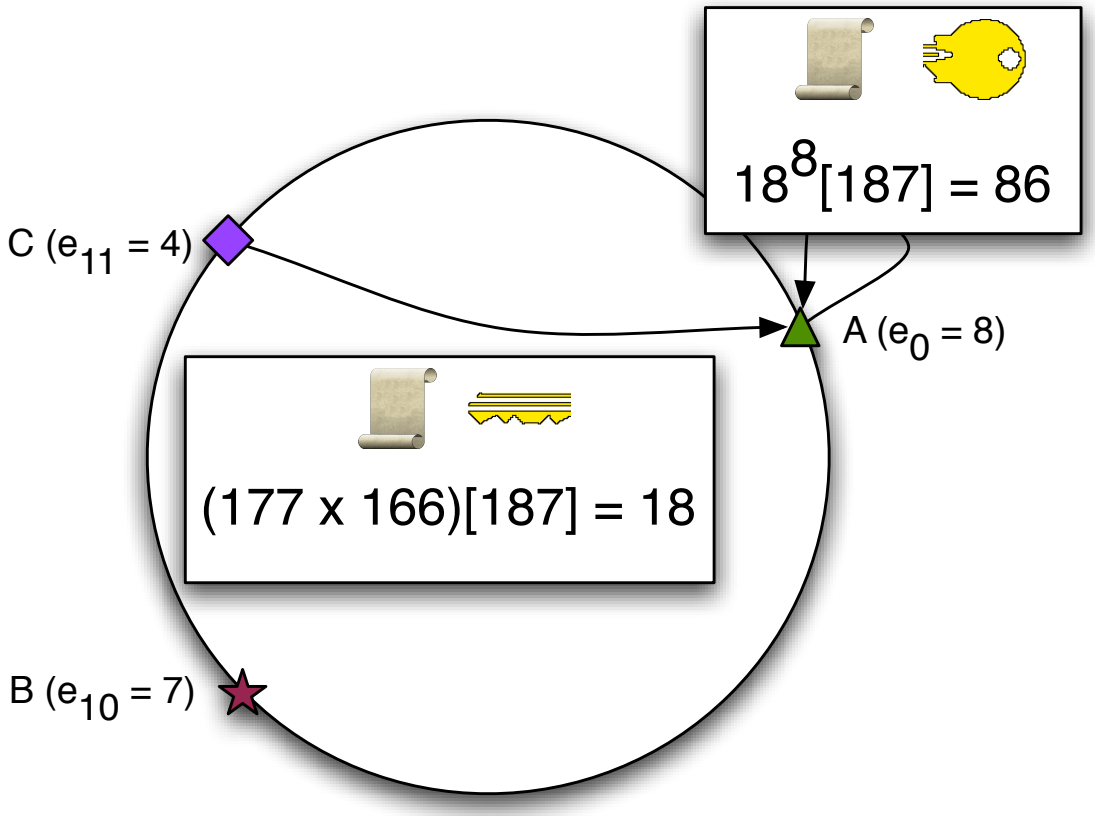
Chiffrement distribué



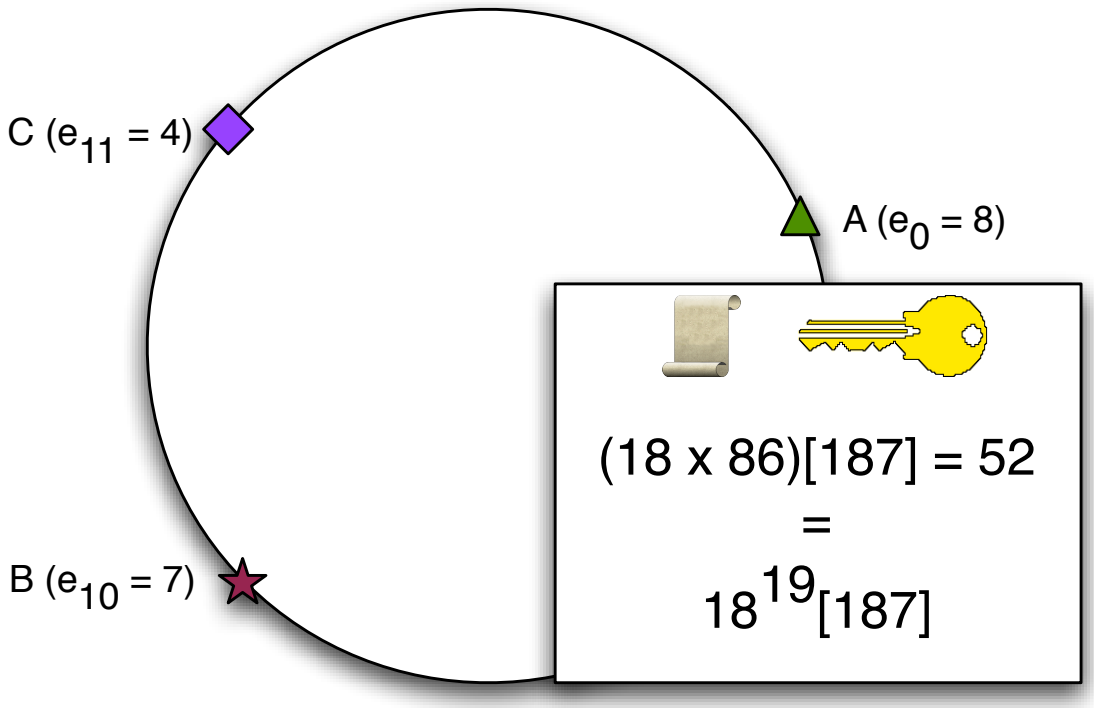
Chiffrement distribué



Chiffrement distribué



Chiffrement distribué



Tolérance aux nœuds malveillants

Problème des nœuds malveillants

Un nœud malveillant peut :

- Truquer le chiffrement par son fragment
- Truquer une multiplication intermédiaire

$\Rightarrow$ Détection seulement par le nœud initiateur, avec P_r

Solution

Demander chaque chiffré intermédiaire à k nœuds.

Gestion de la clé de réseau

La clé de réseau est fragmentée de manière adaptative pour maintenir le seuil
$\Rightarrow$ Protocoles distribués de gestion des fragments.

Invariant vérifié

1. La somme des fragments vaut la clé de réseau
2. Chaque nœud connaît tous les membres de son groupe

Rafraîchissement de deux fragments

Principe

Modifier deux fragments de la clé afin de rendre une ancienne version inutile, tout en conservant la clé du réseau inchangée (après une exclusion par exemple)

Fonctionnement

1. Demande de rafraîchissement à un autre groupe quelconque
2. Échange d'une valeur Δ
3. Soustraction/Addition de cette valeur au fragment

Fragmentation d'un fragment

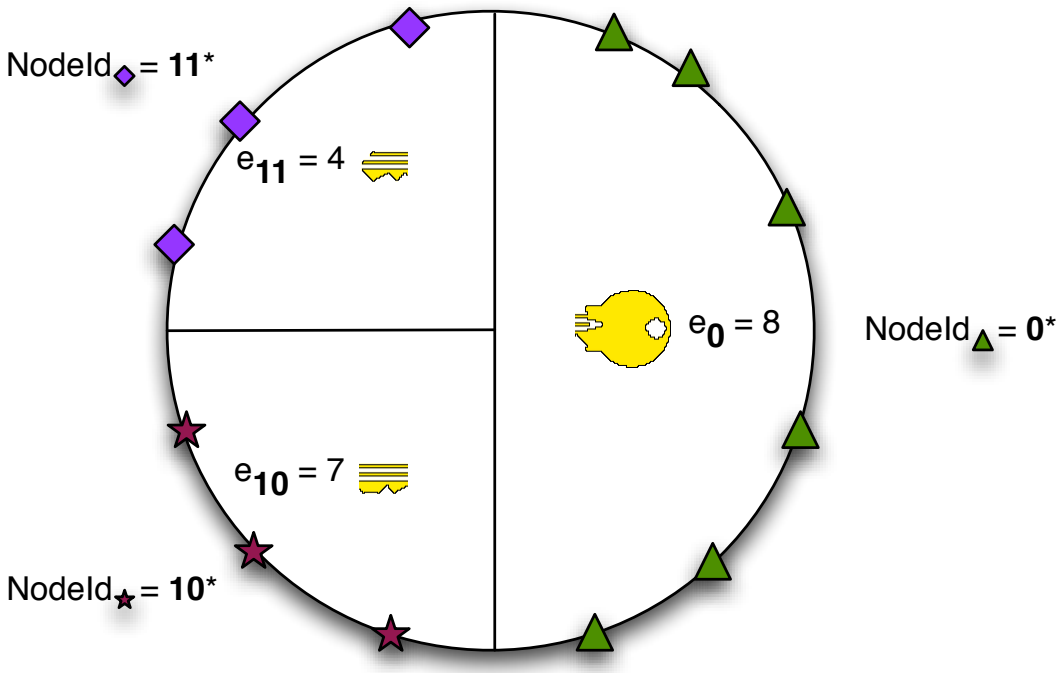
Principe

Diviser 1 fragment en 2 parties quand un groupe de fragmentation contient plus de G_{max} membres

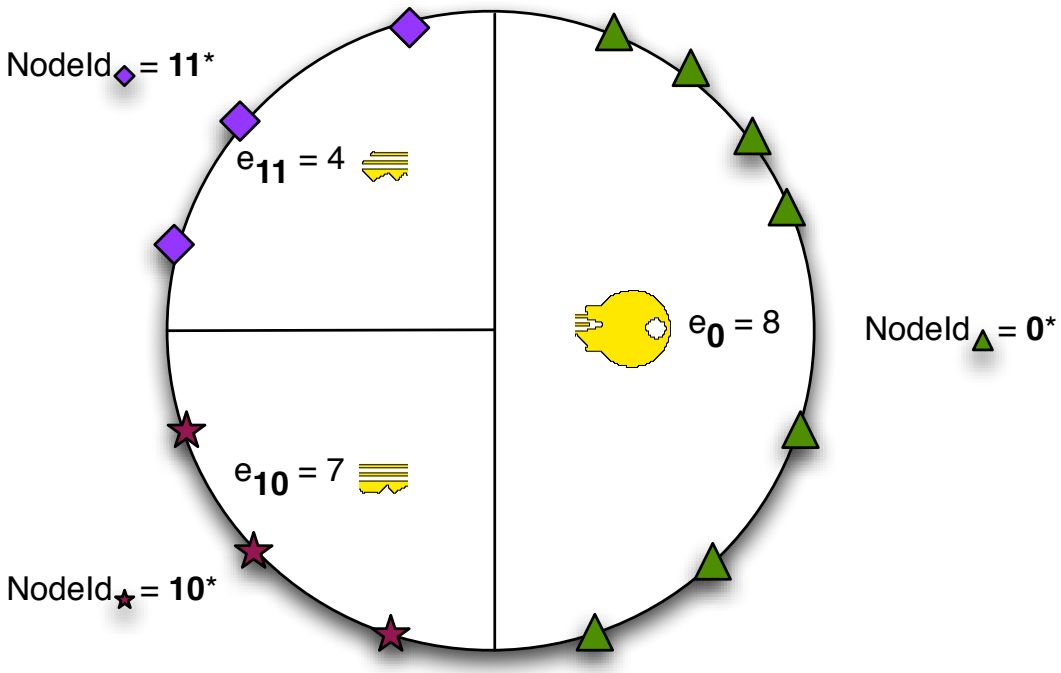
Fonctionnement

1. Accord sur la valeur des nouveaux fragments
2. Entrée dans un des deux groupes créés
3. Rafraîchissement des fragments

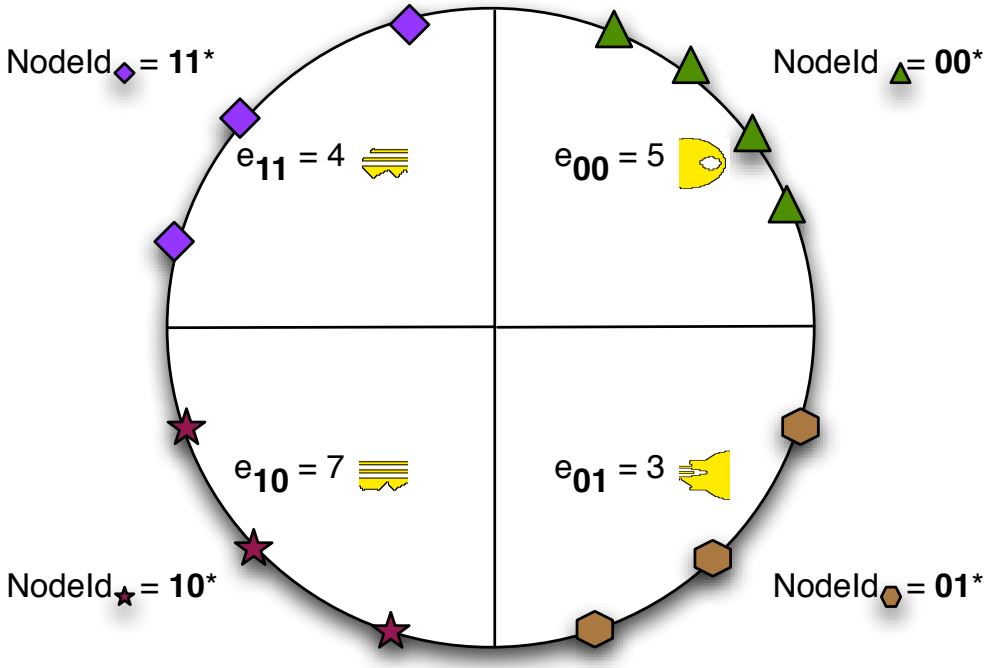
Fragmentation d'un fragment



Fragmentation d'un fragment



Fragmentation d'un fragment



Fusion de deux fragments

Principe

Réunir 2 groupes de fragmentation quand l'un des deux possède moins de G_{min} membres

Fonctionnement

1. Demande de fusion au groupe adjacent
2. Calcul du nouveau fragment somme
3. Entrée des membres des deux groupes dans le nouveau groupe

Obtention d'un fragment

Principe

Fournir à un nouveau membre le fragment du groupe auquel il doit appartenir et l'insérer dans ce groupe.

Fonctionnement

1. Interrogation d'un membre du groupe
2. Récupération du fragment et de la liste des membres
3. Annonce de l'arrivée à tous les membres

Discussion

Sécurité du système

- Pour certifier un nouveau membre, $t\%$ des membres actuels doivent être d'accord
- Pour reconstituer la clé secrète, il faut obtenir tous les fragments (Sybil attack)
- Les protocoles sont conçus pour tolérer des nœuds malveillants

État du travail

Travail réalisé :

- Architecture permettant le contrôle d'accès
- Protocole de certification distribuée
- Protocoles de maintenance de la clé de réseau

Travaux en cours/futurs :

- Détection de nœuds ne se conformant pas au protocole (IDS)
- Exclusion de ces nœuds
- Définition de protocoles pour assurer la confidentialité et/ou l'intégrité

Contrôle d'accès distribué à un réseau Pair-à-Pair

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong

Supélec, équipe SSIR (EA 4039)

15 juin 2007