Systèmes pair à pair, Cours Master 2, 2018

Michel Habib
habib@irif.fr
http://irif.fr/~habib

5 février 2018

Stéganographie

- Passage caché d'un message en clair
- Le dernier bit d'une image = une page de texte
- Très utilisé depuis l'antiquité (encre sympathique, premières lettres des mots des paragraphes ou de chapitres, un vers sur deux en poésie ...)

Un message stéganographié peut aussi être crypté !

Malgré l'intelligence artificielle il restera du travail pour les humains !

https://mars.nasa.gov/multimedia/resources/mars-posters-explorers-wanted/

Définition

COMMISSION GENERALE DE TERMINOLOGIE ET DE TECHNOLOGIE
Vocabulaire de l'informatique
poste à poste, Domaine : Informatique.
Synonyme : pair à pair,
Définition : Se dit du mode d'utilisation d'un réseau dans lequel chaque utilisateur est en mesure de mettre certaines ressources de son ordinateur à la disposition des autres.
Note : Chaque ordinateur peut faire office de serveur.
équivalent étranger : peer-to-peer (P2P, P-to-P).

Le modèle pair-à-pair va bien plus loin que les applications de partage de fichiers. Il permet en effet de décentraliser des services et de mettre à disposition des ressources dans un réseau. Tout nœud d'un réseau pair-à-pair peut alors proposer des objets et en obtenir sur le réseau. Les systèmes pair-à-pair permettent donc de faciliter le partage d'informations. Ils rendent aussi la censure ou les attaques légales ou pirates plus difficiles. Ces atouts font des systèmes pair-à-pair des outils de choix pour décentraliser des services qui doivent assurer une haute disponibilité tout en permettant de faibles coûts d'entretien.
Toutefois, ces systèmes sont plus complexes à concevoir que les systèmes client-serveur.

Toutefois, les systèmes pair-à-pair décentralisés ont plus de difficultés que les systèmes client-serveur pour diffuser l'information et coordonner l'interconnexion des nœuds, donc assurer des faibles délais aux requêtes.
C'est pourquoi sont apparus des systèmes pair-à-pair qui imposent une structure entre les nœuds connectés, afin de garantir des délais de communication faibles : il s'agit des systèmes décentralisés structurés. Ces systèmes utilisent des réseaux d'interconnexion pour relier les nœuds.
Réseaux d'interconnexion virtuels au dessus de l'Internet.

Réseau d'overlay

Chaque système pair-à-pair se construit à partir d'un réseau d'interconnexion virtuel entre pairs au dessus d'Internet.
Remarque : Internet est aussi un réseau d'overlay au dessus du réseau téléphonique.

Nécessité du passage à l'échelle dans le cadre des réseaux pair-à-pair

- Passage à l'échelle est une formule un peu vague qui vient des physiciens, avec la notion échelle de grandeur (x 100).
- Un système pair-à-pair qui fonctionne bien, via internet et les échanges entre internautes peut être très rapidement utilisé par des millions d'utilisateurs en quelques jours.
- Or il est difficile de faire ces tests lors de la conception d'un système informatique.

Les systèmes pair-à-pair ont ainsi pu se passer de serveurs pour assurer une répartition de la charge parmi les nœuds en terme :

- de trafic de contrôle et envoyé par chaque nœud, ce qui revient à limiter le nombre de nœuds auxquels est connecté chaque nœud ;
- de nombre de requêtes transmis à un nœud ;
- de responsabilité pour l'accès aux objets partagés dans le réseau.
- Enfin, ces systèmes permettent souvent d'utiliser un routage proche de celui du graphe dont ils s'inspirent, diminuant ainsi le nombre de messages de requêtes transitant dans le réseau.

Architecture centralisée

Dans cette architecture, un client (un logiciel utilisé par les membres) se connecte à un serveur qui gère les partages, la recherche, l'insertion d'informations, bien que celles-ci transitent directement d'un utilisateur à l'autre.
Certains considèrent que de telles architectures ne sont pas pair-à-pair, car un serveur central intervient dans le processus. D'autres leur répondent que les fichiers transférés ne passent pas par le serveur central. C'est la solution la plus fragile puisque le serveur central est indispensable au réseau. Ainsi, s'il est supprimé, à la suite d'une action en justice par exemple, comme ce fut le cas avec Napster et Audiogalaxy, tout le réseau s'effondre.

Architecture décentralisée

Une telle architecture permet de résister à de telles attaques puisque le logiciel client ne se connecte pas à un unique serveur mais à plusieurs. Le système est ainsi plus robuste mais la recherche d'informations est plus difficile. Elle peut s'effectuer dans des systèmes décentralisés non-structurés, comme Gnutella, où la recherche nécessite un nombre de messages élevé, proportionnel au nombre d'utilisateurs du réseau (et exponentiel suivant la profondeur de recherche).

Dans les systèmes décentralisés structurés, une organisation de connexion est maintenue entre les nœuds. La plupart est basée sur les tables de hachage distribuées (DHT), permettant de réaliser des recherches en un nombre de messages croissant de façon logarithmique avec le nombre d'utilisateurs du réseau, comme CAN, Chord, Freenet, GNUnet, I2P, Tapestry, Pastry et Symphony.

Architecture décentralisée hiérarchique

Une autre solution a été envisagée, consistant en l'utilisation de super-nœuds, éléments du réseau choisis en fonction de leur puissance de calcul et de leur bande passante, réalisant des fonctions utiles au système comme l'indexation des informations et le rôle d'intermédiaire dans les requêtes.
Cette solution, rendant le système un peu moins robuste (les cibles à attaquer dans le réseau pour que le système devienne inopérant sont moins nombreuses que dans un système de type Gnutella, par exemple), est employée dans les systèmes FastTrack, comme KaZaA. Les nœuds du réseau peuvent alors devenir super-nœuds et vice-versa, selon les besoins du système ou de leur propre choix.
De la même façon, le système eDonkey2000 utilise des serveurs fixes, plus vulnérables car moins nombreux et moins souple que les super-nœuds FastTrack.

Partage de fichiers

- Très utilisé (eDonkey ou eMule (protocole originel eDonkey), Gnutella (utilisé par Limewire), FastTrack (utilisé par KaZaA), ...
  mais aussi BitTorrent (un protocole de communication, de transfert et de partage de fichiers en pair à pair)
  ...),
- Téléphonie (skype)
- Diffusion de versions de Linux ou mise à jour de logiciels par exemple pour Console de Jeux.
- 30-70 % du traffic Internet.
- Nombreux fichiers et nombreux utilisateurs.
- Fichiers volumineux.
- Forte volatilité de la population des utilisateurs.

Autres applications

- Bitcoin ou les monnaies électroniques
- Serveurs de clés de cryptographie

Faire un exemple avec 6 processeurs et la distribution d'une vidéo décomposable en 5 paquets ,
montrant que le pair à pair diminue le temps total de la diffusion, car les processeurs vont s'échanger en parallèle des fichiers.

Grandes applications "incontestées" et incontestables des sytèmes pair à pair

- Skype (réseau téléphonique)
- Le système Bitcoin (échange d'argent virtuel non centralisé la validation des transactions est assurée par le système pair-à-pair et est transparente). Première application d'un consensus distribué.
- Mise-à-jour de logiciels ... (BitTorrent est indispensable pour l'échange de gros fichiers tels que des mises à jour systèmes : RedHat et Eclipse l'utilisent.)

Principes de BitTorrent

- Toutes les Δ secondes ($\Delta = 10$), un pair évalue ce que lui ont donné les 5 pairs (avec qui il échange).
- Il élimine de sa liste de 5, celui qui lui a donné le moins (le maillon faible).
  Il choisit un nouveau pair aléatoirement parmi ses voisins, et recommence l'échange avec ses 5 pairs. (Ceci permet aux nouveaux de s'intégrer dans l'échange)
- On télécharge d'abord les fichiers les plus rares (en inspectant les pairs voisins).
- Au démarrage au moins un pair (la source) possède tous les paquets de l'objet à télécharger.

Une variante au démarrage la source ne propose que quelques paquets.

- Avalanche une variante proposée par Microsoft, basée sur le network coding.
- Quelle fut la raison de l'échec de cette variante ?
- A ce jour BitTorrent n'a pas vraiment de concurrent.

Problèmes

- Optimiser le trafic :
  - Moins de trafic de contrôle (50 % pour Gnutella).
  - Plus de localité dans les échanges de données.
- Ethique :
  - Interdire l'échange de certains fichiers (copyright, pédophilie).
  - Encourager le don d'upload.
  - Anonymat, résister aux attaques
- Droit :

  Etre conforme aux lois Hadopi 1, 2, 3 . . .

Réseau Virtuel

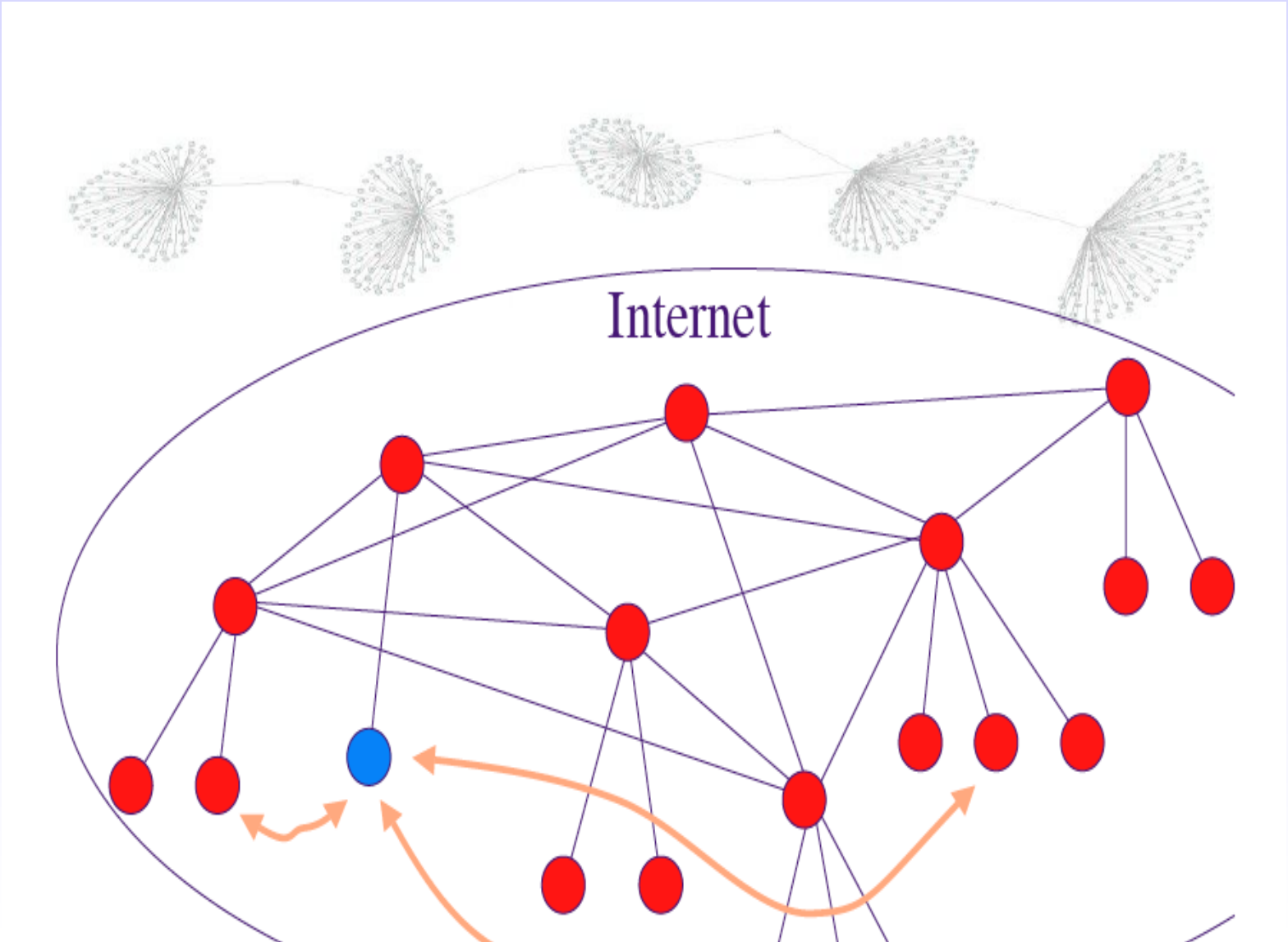
Routage

Chaque pair possède un petit carnet d'adresses (pas nécessairement petit) ;
Routage glouton entre source et destination.

Problème

Chemins de routage longs
petit-mondisation : ajout de raccourcis de manière distribuée

Entre pairs



Routage glouton dans un réseau virtuel

Hypothèse : chaque nœud dispose d'un oracle indiquant un voisin qui rapproche de la destination via :

- une approximation de la distance à la destination (étiquetage de distance, ...)
- Propriétés de graphes géométriques (triangulation Delaunay, graphes de Yao, ...)
- Routage glouton : le message est redirigé vers le voisin qui rapproche le plus de la destination

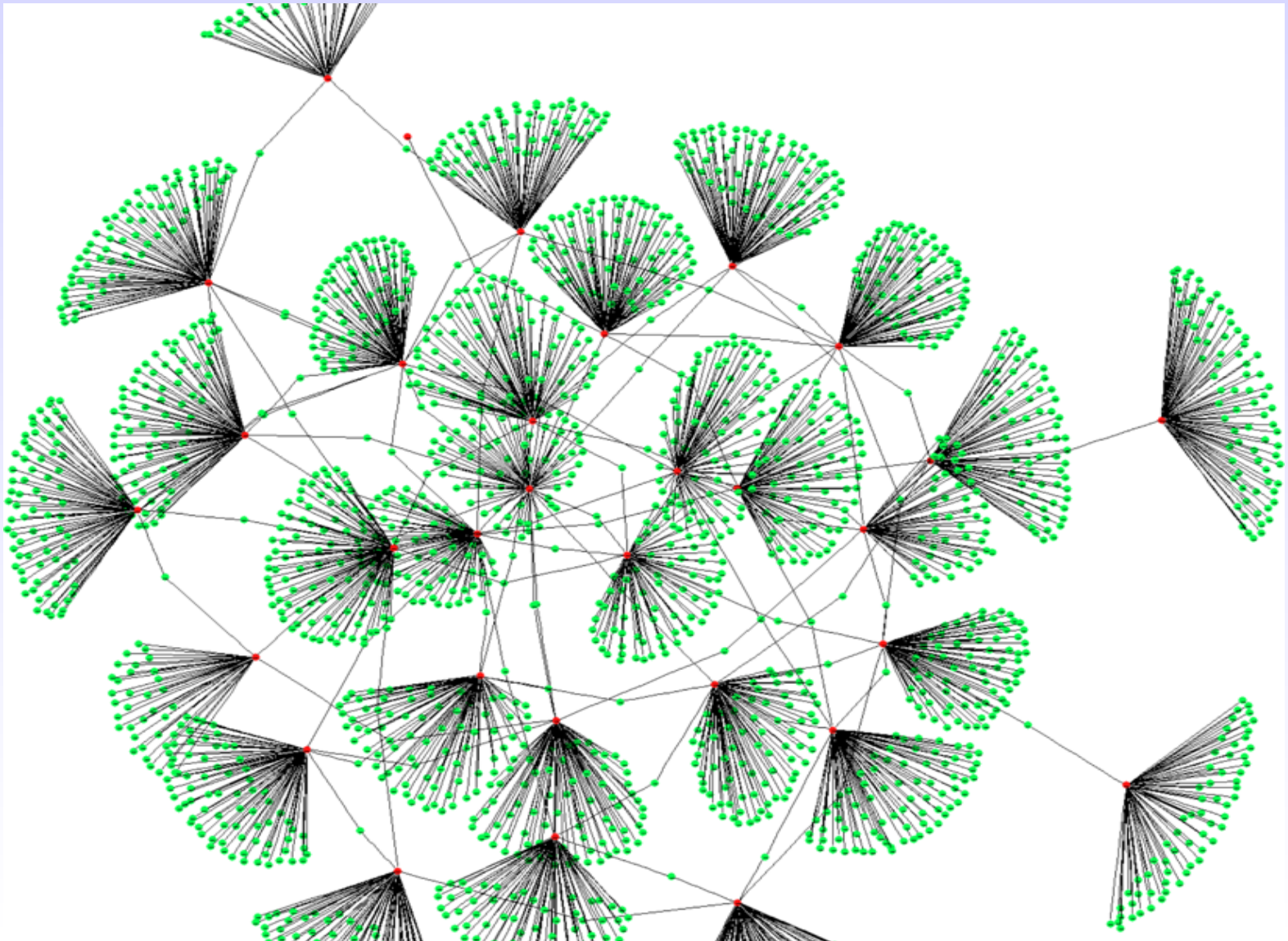
Thèmes

- Tables de hachage distribuées et routage :
  - Ettiquetage des noeuds, routage compact.
  - Indexation par mots clé.
  - Réseau logique versus réseau physique.
- Liens entre pair à pair et ad hoc :
  - Optimisation de l'inondation.
  - Incitation à la coopération.
  - Fragilité par rapport aux attaques malveillantes
- Ethique :
  Mécanismes d'interdiction de fichier.

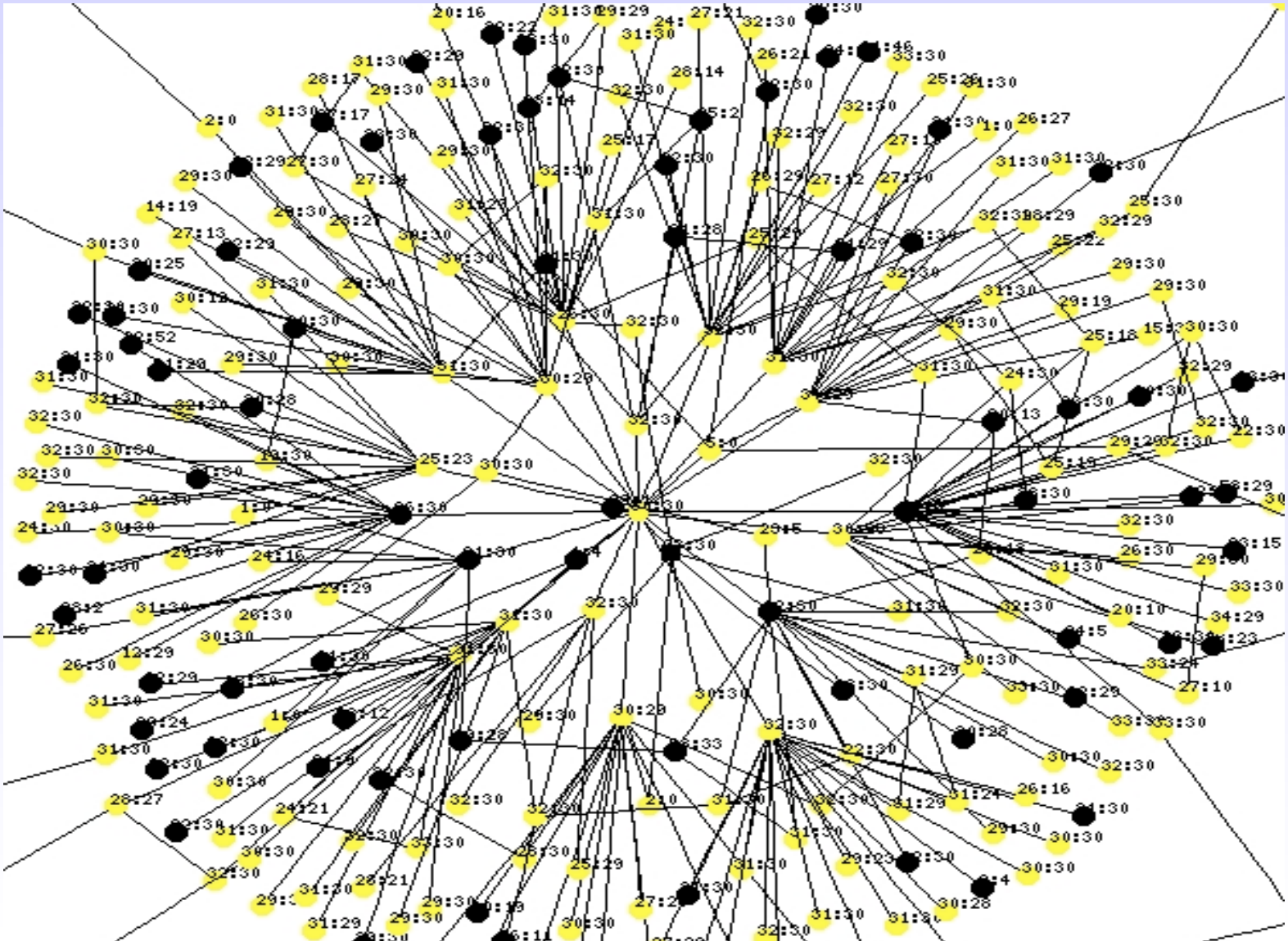
Résultats

- DHT sur de Bruijn
- Explorations de réseaux (Gnutella, eDonkey)
- Résultats théoriques sur le routage (tables compact versus facteur d'élongation, routage glouton petit monde).
- Utilisation de DHT pour les réseaux ad-hoc hiérarchiques.
- Diffusion d'un fichier (problème du bloc manquant, diffusion optimale entre N pairs).

Pairs et super pairs



Super pairs seulement



DHT de Bruijn

Résistance à la dynamicité par la redondance.
$O(k)$ contacts par noeud, routage en $O(logN)$.
Ou bien $O(klogN)$ contacts, routage en $O(logN/loglogN)$.

Exploration de Gnutella

- But premier : optimiser l'inondation.
- Redondances dans le voisinage à deux sauts (Non)
- Pairs et Super-pairs
- Super-pairs seulement

Perspectives

- Indexation par mots clés avec des DHTs (gestion des collisions).
- Protocole BitTorrent et dilemme du prisonnier itéré.
- Borne théoriques sur le routage compact appliquées aux DHTs.
- Thèmes connexes :
  - Estimation des distances dans Internet.
  - Théorie des jeux (tit for tat multi-joueurs).
  - Aspects légaux.

- Grande difficulté de l'analyse scientifique d'un système P-2-P
- Nécessité d'arguments probabilistes et statistiques (la mesure du plus mauvais cas, ne correspond à rien dans l'analyse de ces systèmes).
- Mais aussi la mise en œuvre de simulations (par exemple pour BitTorrent).

Réseaux d'interconnexion

- Connexion manuelle par opérateur (le modèle est le graphe complet)
- Autocommutateurs electromécaniques (modèle est un graphe Butterfly ?)
- Autocomutateurs électroniques. Le modèle est un réseau d'interconnexion qui vérifie :
  Graphe connexe de degré borné, ayant un petit diamètre et le plus grand nombre de sommets
  Pour les valeurs $\Delta = 3$, $diam = 2$, le graphe ayant le nombre maximum de sommets est le graphe de Petersen à 10 sommets.
- Ce modèle a servi pour les autocomutateurs des réseaux de téléphonie et pour les satellites.

Reseaux d'interconnexion

- Réseau d'overlay. Graphe abstrait (pas de hardware)
  - connexe
  - le degré est borné (contrainte moins forte)
  - Le graphe est dynamique (retrait ou ajout de pair)

- Au début le pair-à-pair était utilisé pour le partage des fichiers (mise à jour des noyaux Linux)
  Echanges de Musique, vidéos
- Mais maintenant : aussi Voix sur IP (Skype) , TV, streaming
- Mais les idées et techniques développées dans les systèmes pair-à-pair pourraient être essentielles pour les applications sur la grille de calcul.

Attaque d'un réseau pair-à-pair

Un logiciel malveillant ou malicieux (malware)
peut prendre le controle d'un réseau pair-à-pair .

Microsoft a essayé Avalanche un concurrent de BitTorrent, soit-disant basé sur le Network Coding.
Il devait être 20 fois plus rapide que BitTorrent, mais n'est jamais sorti !

Conclusions

Pour faire un système pair à pair, il faut :

1. Définir un protocole de transfert de fichiers efficace sur Internet (au dessus de TCP ou UDP). (Incluant une décomposition en paquets)
2. Choisir une structure de réseau virtuel
3. Définir des protocoles de nommage, ajout et retrait de pairs dans le système
4. Choisir un mode de gestion des fichiers partagés (une table de hachage distribuée)
5. Les trois derniers points ne sont pas indépendants !

La question cruciale :

Comment associer à une adresse IP un identifiant unique sommet d'un réseau virtuel ?