Les protocoles Peer-to-Peer :

leur utilisation et leur détection

Gabrielle Feltin
Guillaume Doyen
Olivier Festor
LORIA

PLAN

- Genèse et définitions
- Applications P2P
- Modèles P2P
- Napster ou le modèle hybride
- Gnutella ou le modèle pur
- Axes de recherche
- Sécurité et détection
- Conclusion

Genèse

- Internet a été conçu comme un système P2P
  - Libre échange des données
    - Sans firewall, sans NAT, sans connexion asymétrique
  - Applications telnet, ftp ouvertes à tous
  - Coopération
    - sans spam et sans abus de bande passante
- Usenet News, DNS, protocole de routage (RIP, OSPF) : vieux modèles de P2P
- Emergence du P2P = renaissance du modèle originel d'Internet, au niveau applicatif

Connaissance

- Logiciels P2P de type file sharing
  - Napster
  - Gnutella
  - Edonkey
  - Kazaa
  - BitTorent
- Echange possible de musique ou de film
  - Souvent de manière illicite
- Mais d'autres protocoles et logiciels P2P
  - Manière forte et équitable de **collaborer en vue accroître le potentiel du réseau**
    - Seti@home
    - Groove
    - Jxta

Définitions

- « **Peer-to-peer** computing is the **sharing of computers resources and services** by direct exchange **between systems** »
- « **Peer-to-peer** refers to a class of systems and applications that employ **distributed resources** to perform a critical function in a **decentralized manner** »
- Échange direct des ressources et services entre ordinateurs, chaque **élément** étant **client** et **serveur**
  - Utilisation maximale de la puissance du réseau
  - Elimination des coûts d'infrastructure
  - Exploitation du fort potentiel inactif en bordure de l'Internet

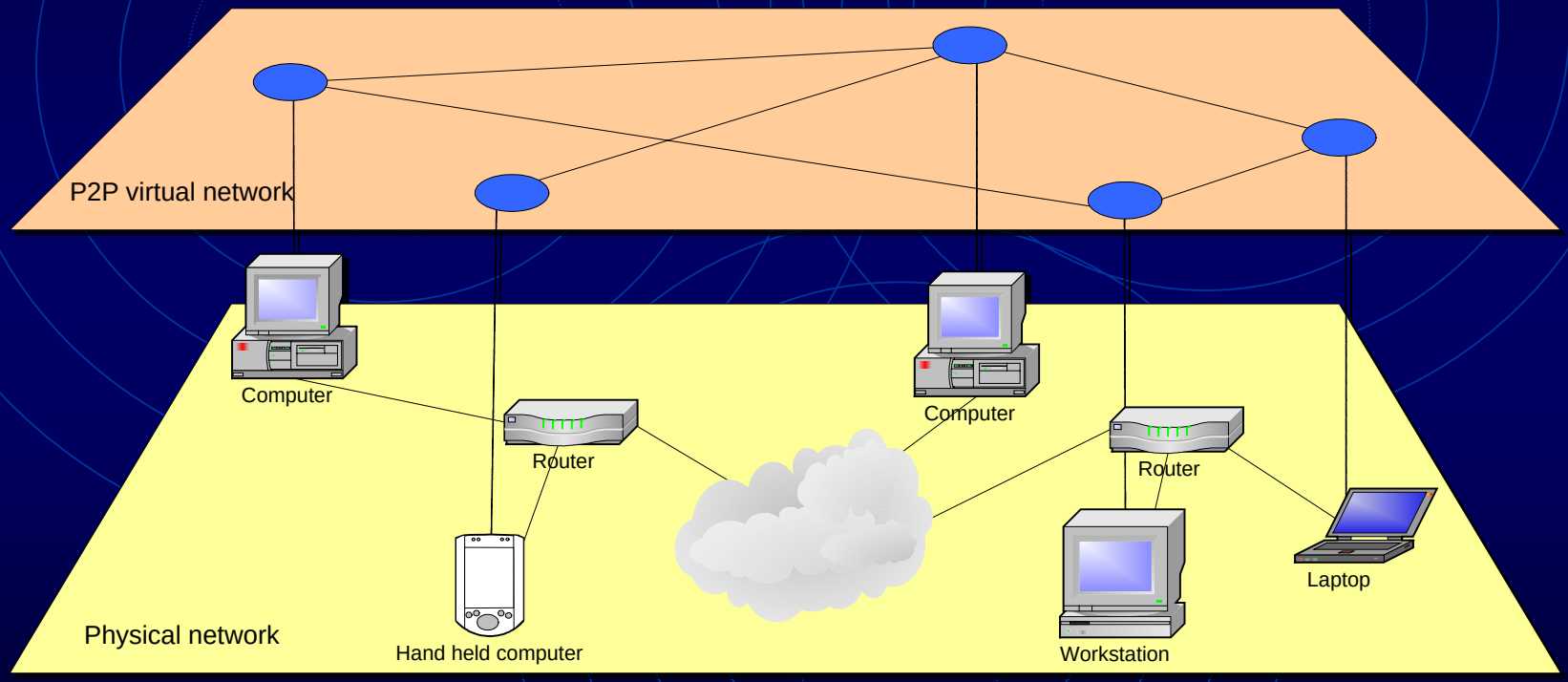
  ➔Retient l'attention de la recherche, des développeurs et des investisseurs

  ➔Article en collaboration avec la recherche

Définitions

- Eléments constituant un réseau P2P peuvent être de nature hétérogène
  - PC
  - PDA
  - Téléphone portable
- Réseau P2P présente une topologie virtuelle
- Nature « ad hoc »
  - Eléments constituants peuvent aller et venir
  - Topologie du réseau pas stable

Topologie virtuelle

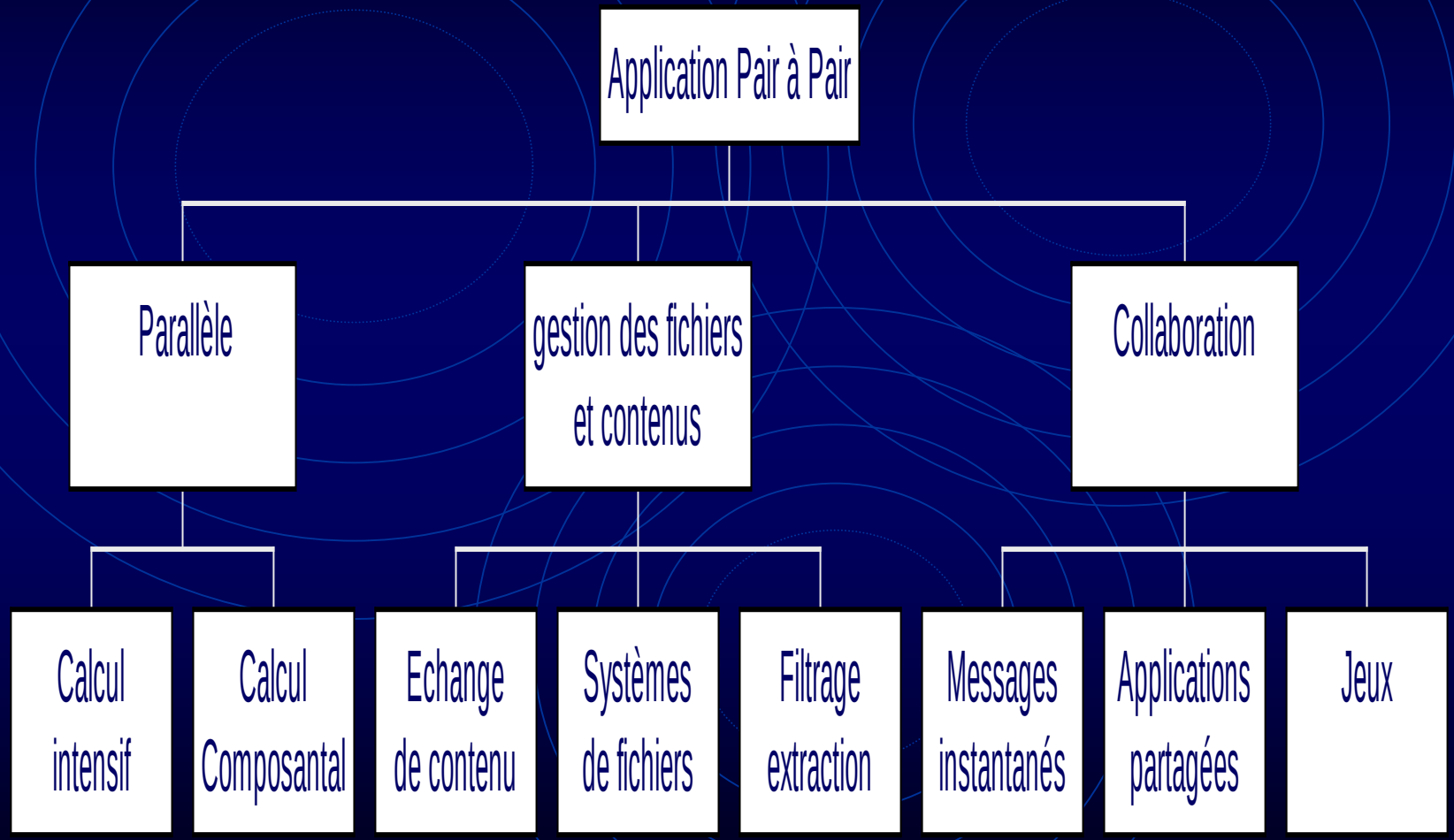


G. Feltin G. Doyen O. Festor

Objectifs

- Modèle P2P très général
  - ➔ Applications de nature différente, objectifs variés
  - Partage et réduction des coûts entre les différents peers
  - Fiabilité (pas d'élément centralisé)
  - Passage à l'échelle (évite les goulots d'étranglement)
  - Agrégation des ressources (puissance de calcul, espace de stockage)
  - Accroissement de l'autonomie, chacun à la responsabilité de partager ses ressources
  - Anonymat pouvant être assuré par des algorithmes de routage ne permettant pas le pistage d'une requête
  - Communication ad-hoc et exhaustive

Les applications



Applications parallèles

- Découper un gros calcul en petites unités sur un grand nombre de peers
- Utiliser les machines oisives d'un réseau pour effectuer les calculs
  - Calcul intensif : calcul d'une même opération munie de paramètres différents
    - SETI@Home, genome@Home
  - Calcul composantal : découpe un même calcul en petites unités indépendantes réassemblables pour effectuer le calcul complet
- Les grilles de calcul se rapprochent du P2P pour en utiliser l'architecture
    - Le Global Grid Forum (GGF) a rejoint en avril 2002 le P2P Working Group (Avaki, Lattice)
    - Les travaux portent sur le partage de mémoire et d'adressage global à très grande échelle

Gestion des fichiers et contenus

- Stocker et retrouver des informations sur différents éléments du réseau
- Echange de contenu
  - Napster, Gnutella, Morpheus, Kazaa
  - Freenet (anonymat des sources et intégrité des documents)
  - BitTorrent (transfert parallèle de plusieurs sources, possibilité arrêt et de reprise de transfert
- Etablir un système de fichiers distribué dans une communauté
  - PAST, OceanStore (plus de 6 millions d'utilisateurs), CFS
- Bases de données et tables de hachage distribuées
  - Mariposa, Chord

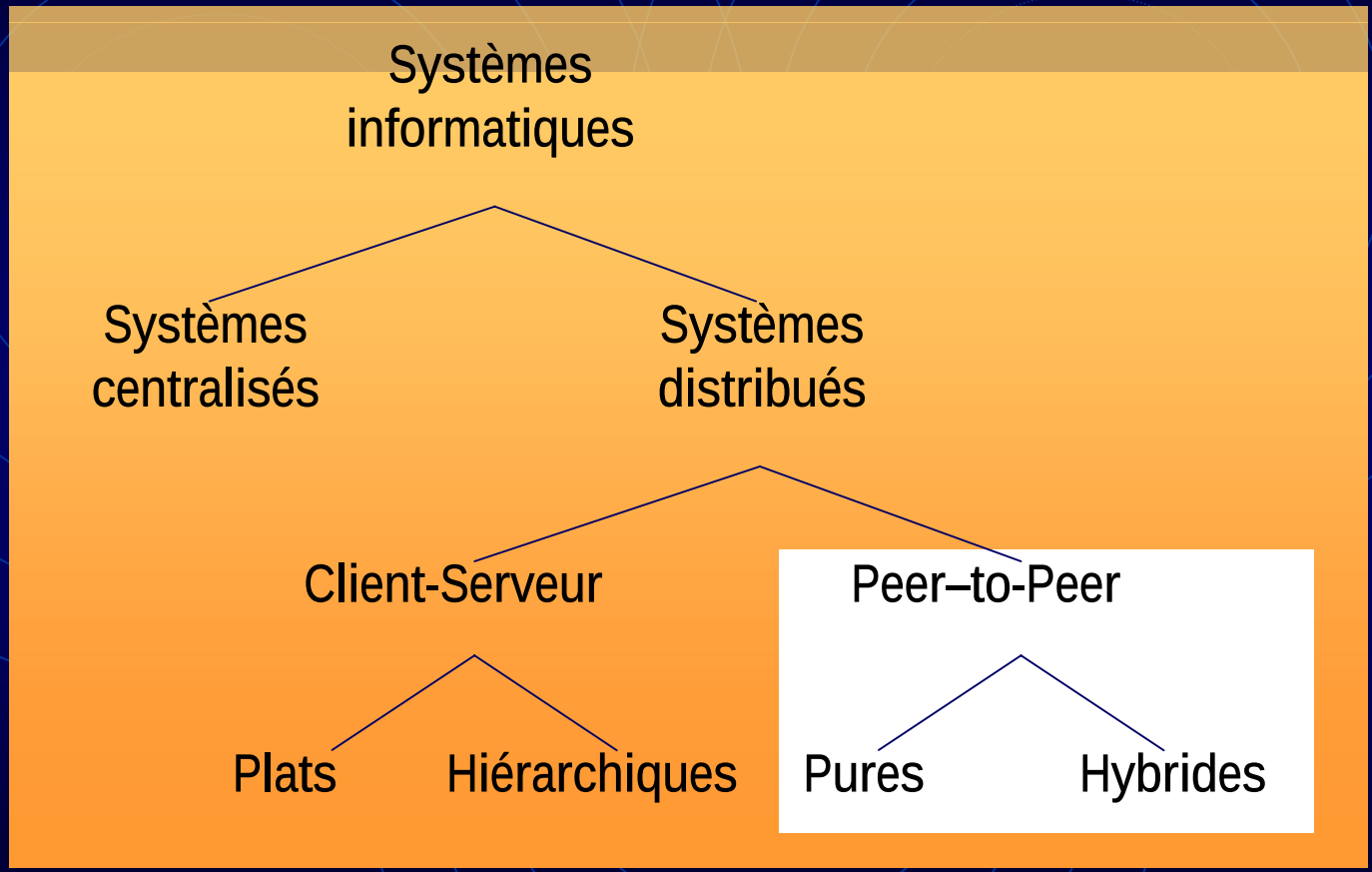
Collaboration

- Collaborer en temps réel entre usagers sans utiliser de serveur central
  - Messages instantanés
    - Yahoo
    - AOL
    - Jabber
  - Travail coopératif ou applications partagées, permettant de travailler de manière commune sur un projet distribué
    - Groove
    - Magi
    - Powerpoint distribué
    - Projet de CAO
  - Commerce électronique
  - Jeux en réseau, dont l'architecture est exempte de toute autorité centrale
    - DOOM

Plates-formes

- Infrastructures génériques pour développer des applications P2P
- Assurent les composants primaires du P2P:
  - Gestion des peers
  - Nommage
  - Découverte de ressources
  - Communication entre peers
  - Sécurité
  - Agrégation des ressources
- Les plates-formes
  - JXTA
  - .net
  - Anthill (Construite sur Jxta)

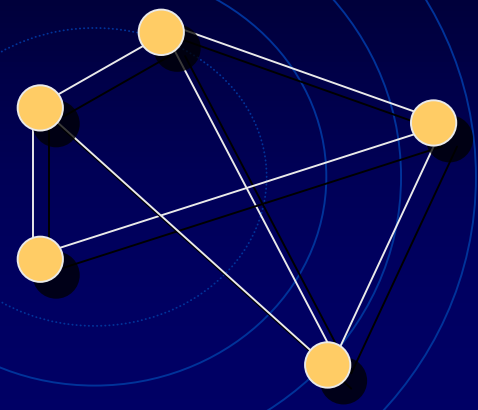
Taxonomie des systèmes informatiques

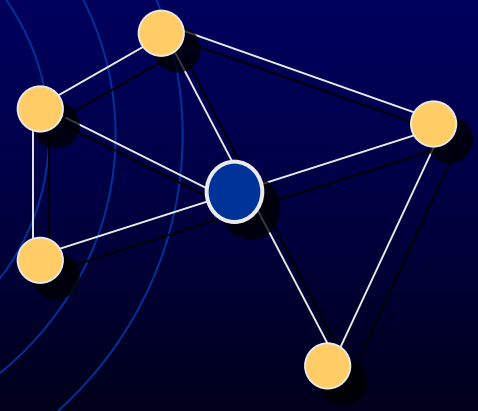


Classification des systèmes informatiques

Taxonomie des systèmes P2P

- Modèle pur
  - Pas de serveur centralisé
    - Gnutella
    - Freenet
- Modèle hybride ou centralisé
  - Un serveur est contacté pour obtenir des méta-informations
    - identité du peer sur lequel sont stockées les informations
    - Vérifier les crédentials de sécurité
  - Echange réalisée en P2P
    - Napster
    - Groove
    - Magi





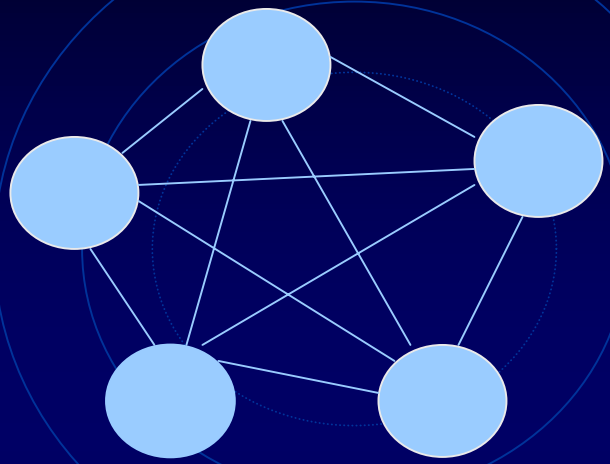
Taxonomie des systèmes P2P

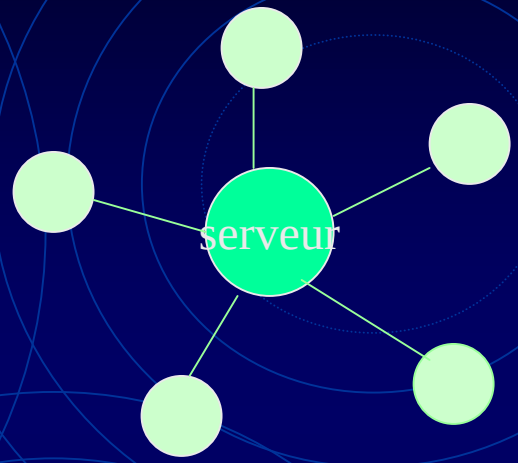
- Modèle super-peer, qui est un modèle hybride
  - Les super-peers contiennent des informations que les autres peers n'ont pas
  - Les autres peers ne consultent ces super-peers que s'ils ne peuvent trouver l'information autrement
  - Kazaa, FastTrack, …
- Classification applicative
- Classification technologique (stockage et contrôle des données, usage des ressources, contrôle de l'état global, contraintes de qualité de service)
- Classification architecturale (identité, découverte, authentification, autorisation)

Caractéristiques

- Localisation des fichiers dans un environnement distribué
- Meta-données ou index du réseau P2P
- Libre circulation des fichiers entre systèmes
- Mode de communication standard (TCP, HTTP)
- Capacité de connexion variable suivant les modèles
- Echanges d’informations non sécurisés
- Peers non sûrs
- Aucune vue globale du système

P2P contre Client/serveur





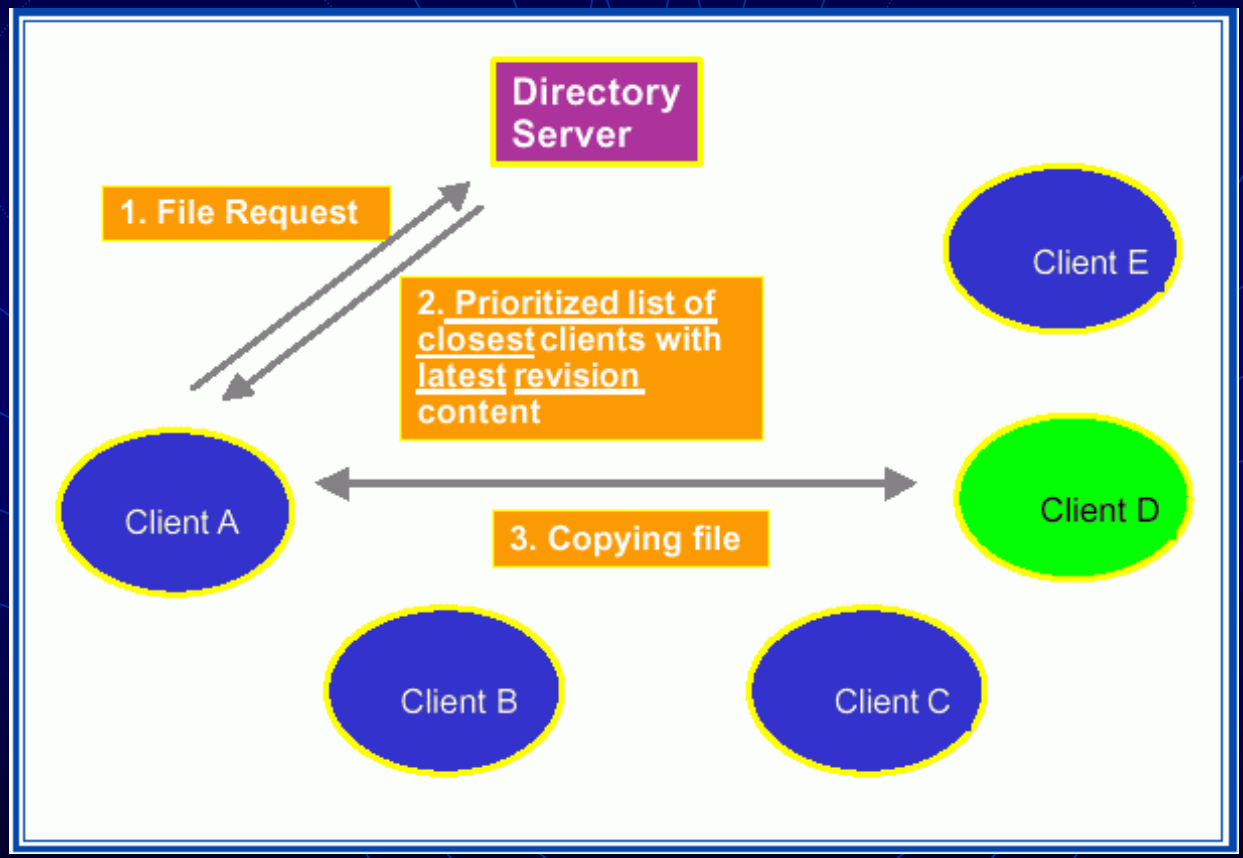
Auto-organisé
Evolution dynamique, ad-hoc
Découverte des peers
Flux distribué
Symétrie du réseau
Communication par messages
Adressage dynamique au niveau appli.
Entités autonomes
Attaques difficiles (mobilité, anonymat)

Management centralisé
Configuration statique
Consultation de tables
Flux centralisé
Asymétrie du réseau
Orienté RPC
Adressage statique @IP
Entités dépendantes
Attaques plus simples

Napster

- Partage de fichiers mp3
- Fondé en mai 1999 par Shawn Fanning et Sean Parker
- Arrêté en septembre 2001, après poursuite judiciaire
- Application phare : 40 millions de téléchargements, 160 000 utilisateurs en moyenne
- Répertoire centralisé pour les données administratives et les index des fichiers mp3 téléchargeables par les peers

Echanges dans Napster



Bilan Napster

Les limites

- Pas d'anonymat partout
  - Vous êtes connus du serveur…
  - … Et des peers sur lesquels vous téléchargez
- Limites habituelles d'un serveur central
  - Disponibilité
  - Passage à échelle
    - Saturation de la bande passante
    - Saturation du nombre de processus
  - Légal: facile à fermer
- Mauvaises informations du débit des peers pour ne pas être sollicités

Les avantages

- Avantages habituels d'un serveur central
  - Facile à administrer
  - Facile à contrôler, à fermer
- Evite les recherches coûteuses sur le réseau
  - Pas de routage
  - Planification de la gestion des utilisateurs
- Tolérance aux fautes
  - Par un sondage régulier des peers connectés, état cohérent
- Service novateur
  - Généralise le P2P
  - Généralise les procès contre le non-respect des droits d'auteur

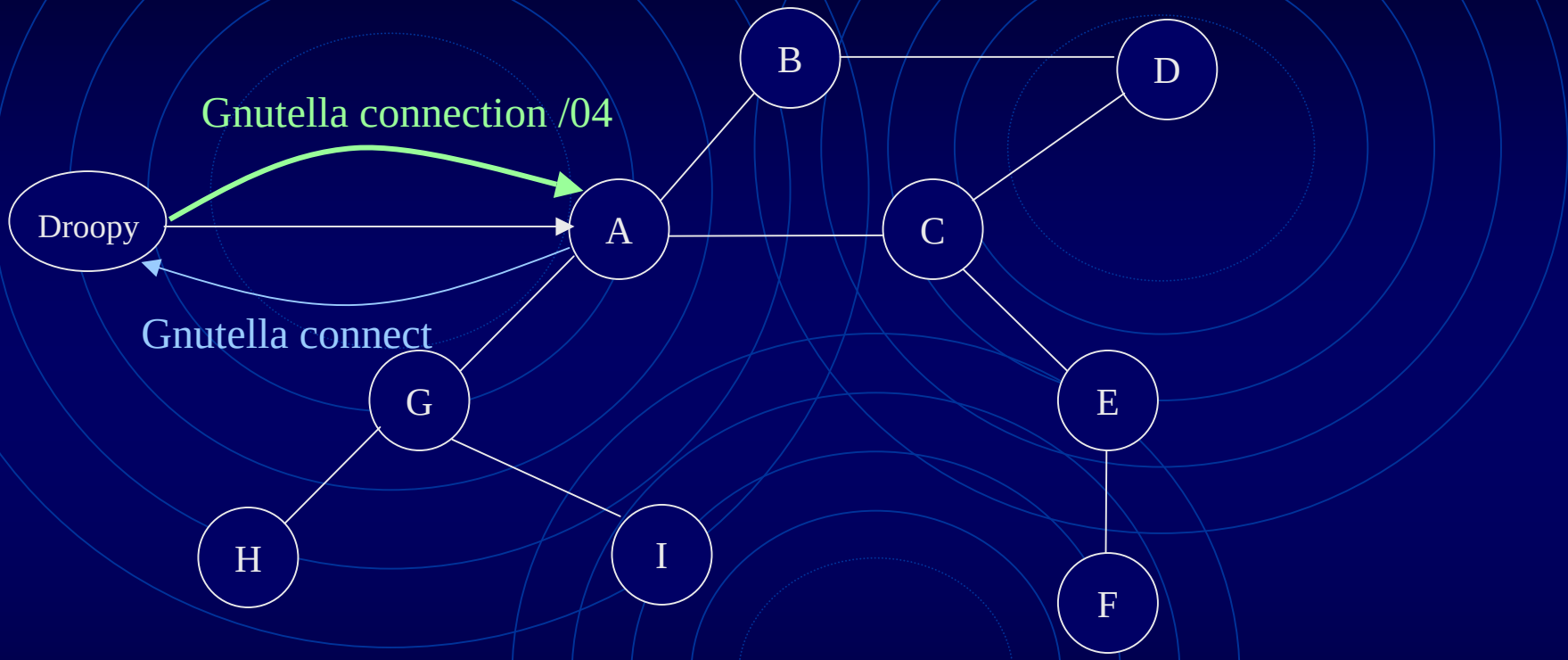
Gnutella

- Protocole de fichiers partagés
- Version 0.4 , en mars 2000, développé en une quinzaine de jours par Justin Frankel et Tom Pepper
- Plusieurs dizaines de milliers d'utilisateurs simultanés
- Extensions :
  - Limeware
  - ToadNode
  - BearShare

Gnutella: Protocole

- Réseau complètement décentralisé, modèle pur
- Servent = **Serv**eur + Client
  - Chaque élément joue à la fois le rôle de client et serveur
- Messages : informations émises par les servents à travers le réseau Gnutella
- Fonctionne au dessus de TCP/IP

Connexion d’un peer Gnutella



G. Feltin G. Doyen O. Festor

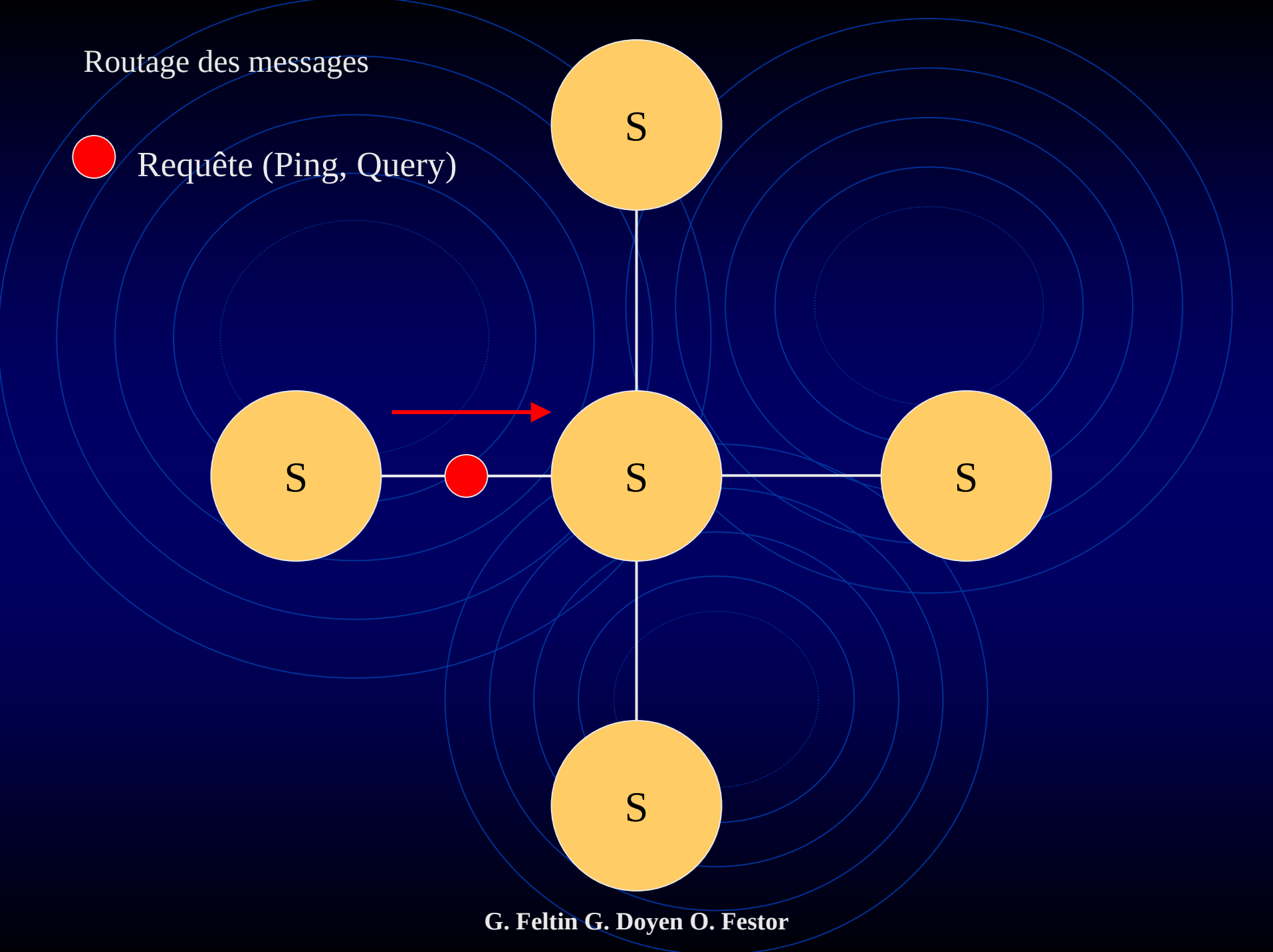
Les Messages Principaux

Message	Description
Ping (0x00)	Utilisé pour découvrir les autres servents sur le réseau Un servent qui reçoit un Ping doit répondre avec un (ou plusieurs) Pong
Pong (0x01)	Réponse à un Ping, contient : • Adresse IP + n° de port du servent • Le nombre et la quantité de données partagées
Query (0x80)	Utilisé pour la recherche d'un fichier
QueryHit (0x81)	Réponse à un Query
Push (0x40)	Permet de télécharger des données depuis un servent situé derrière un firewall

Si les deux servents sont derrière un firewall, le téléchargement est impossible

Routage des messages

Requête (Ping, Query)

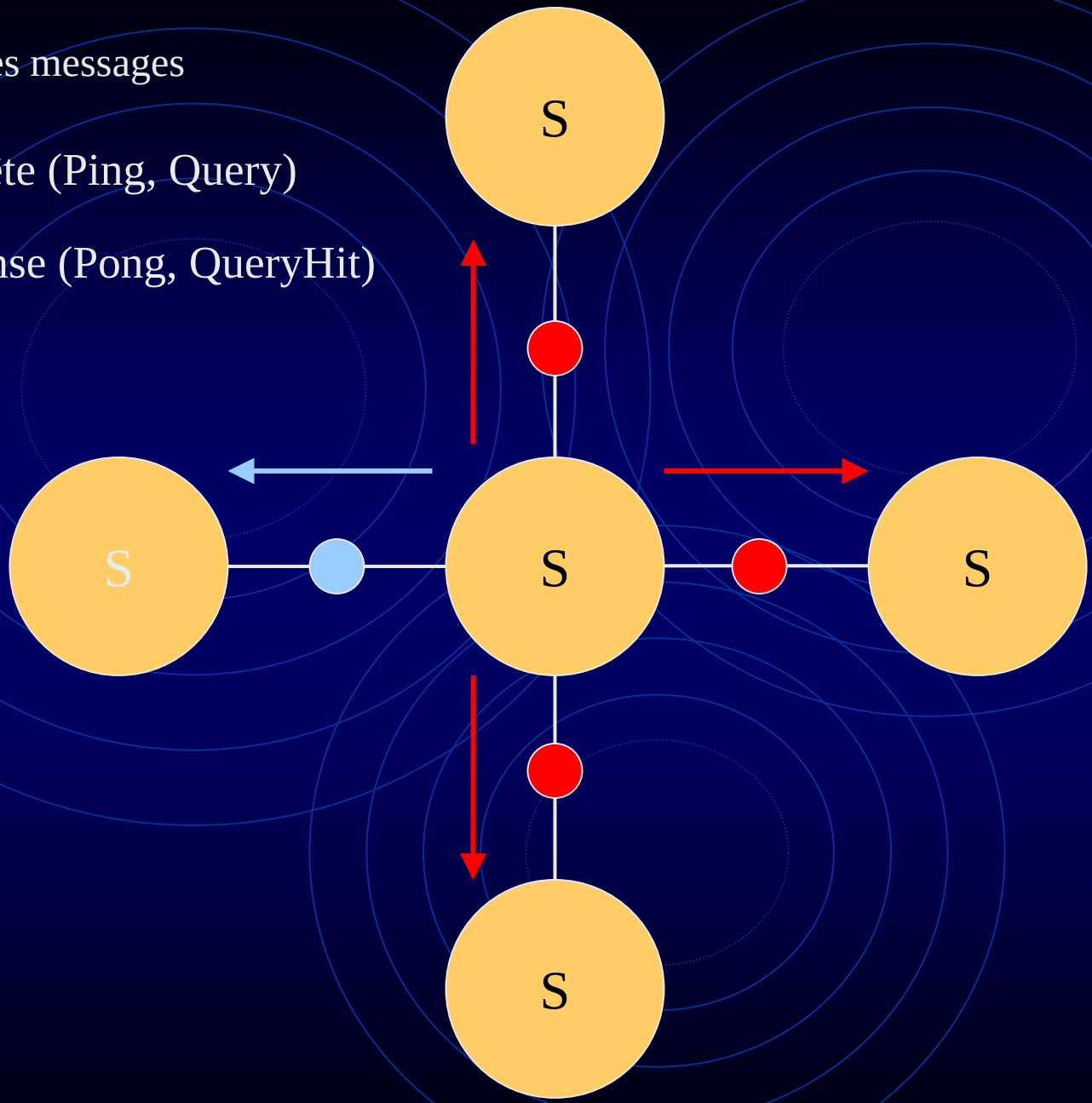


G. Feltin G. Doyen O. Festor

Routage des messages

Requête (Ping, Query)

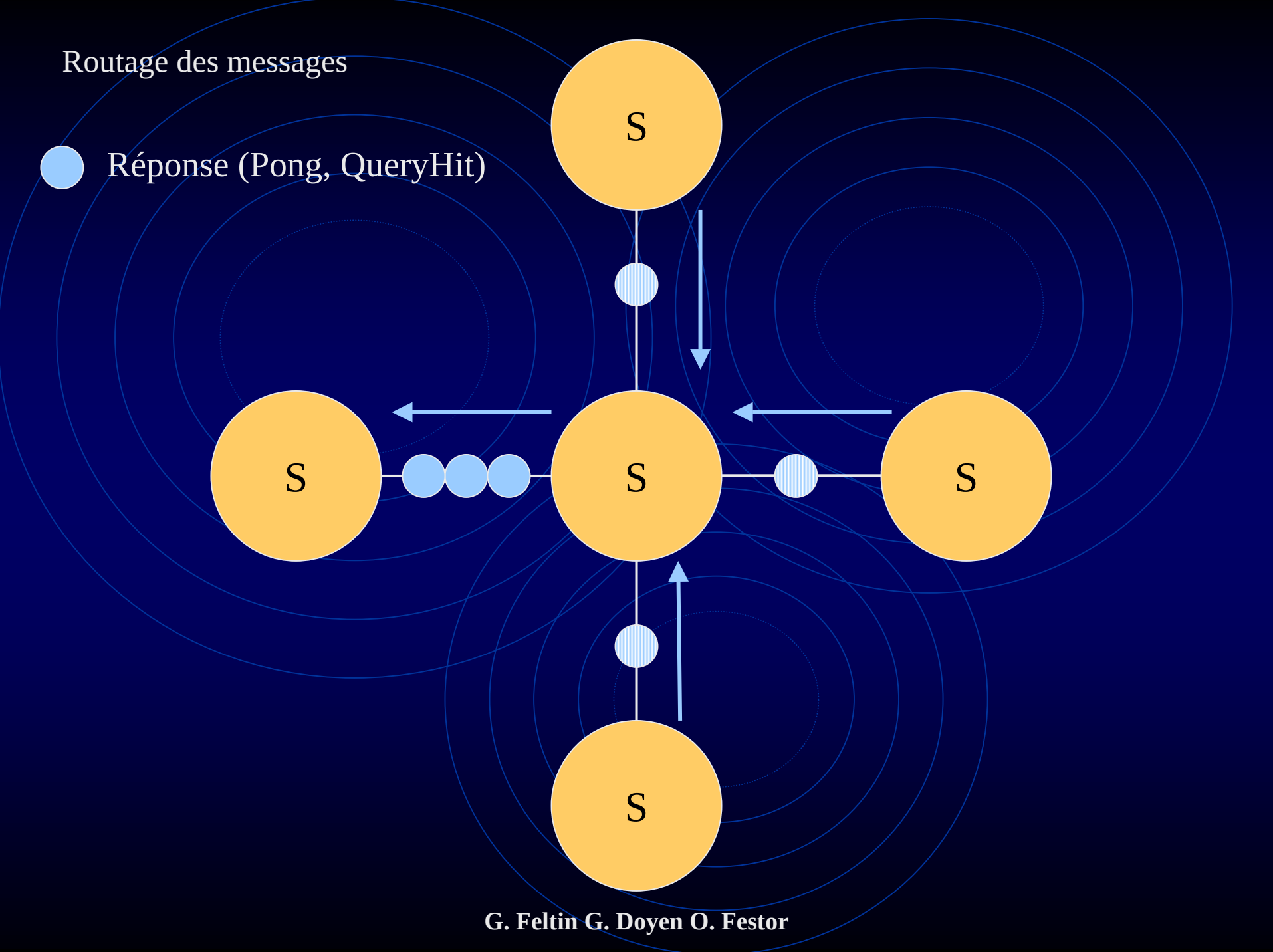
Réponse (Pong, QueryHit)



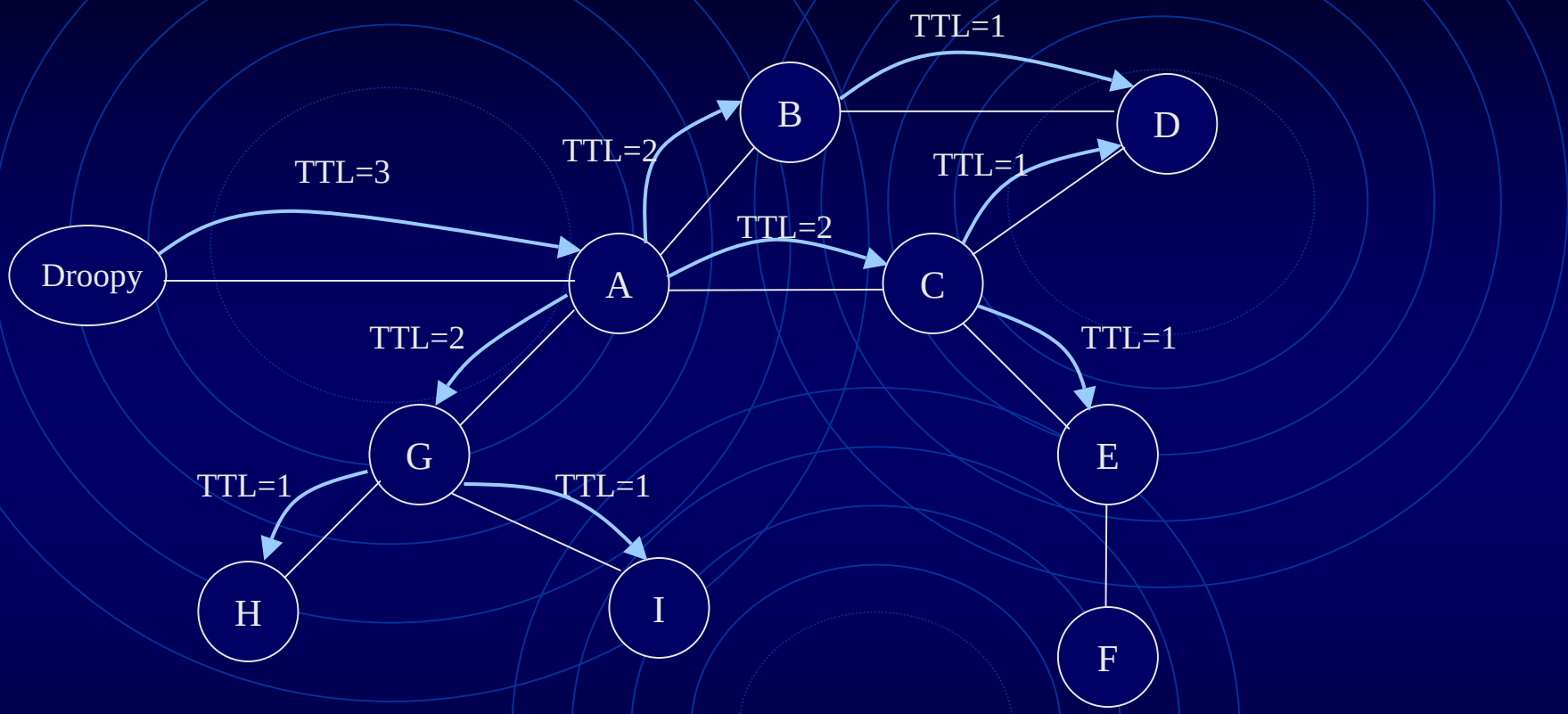
G. Feltin G. Doyen O. Festor

Routage des messages

Réponse (Pong, QueryHit)

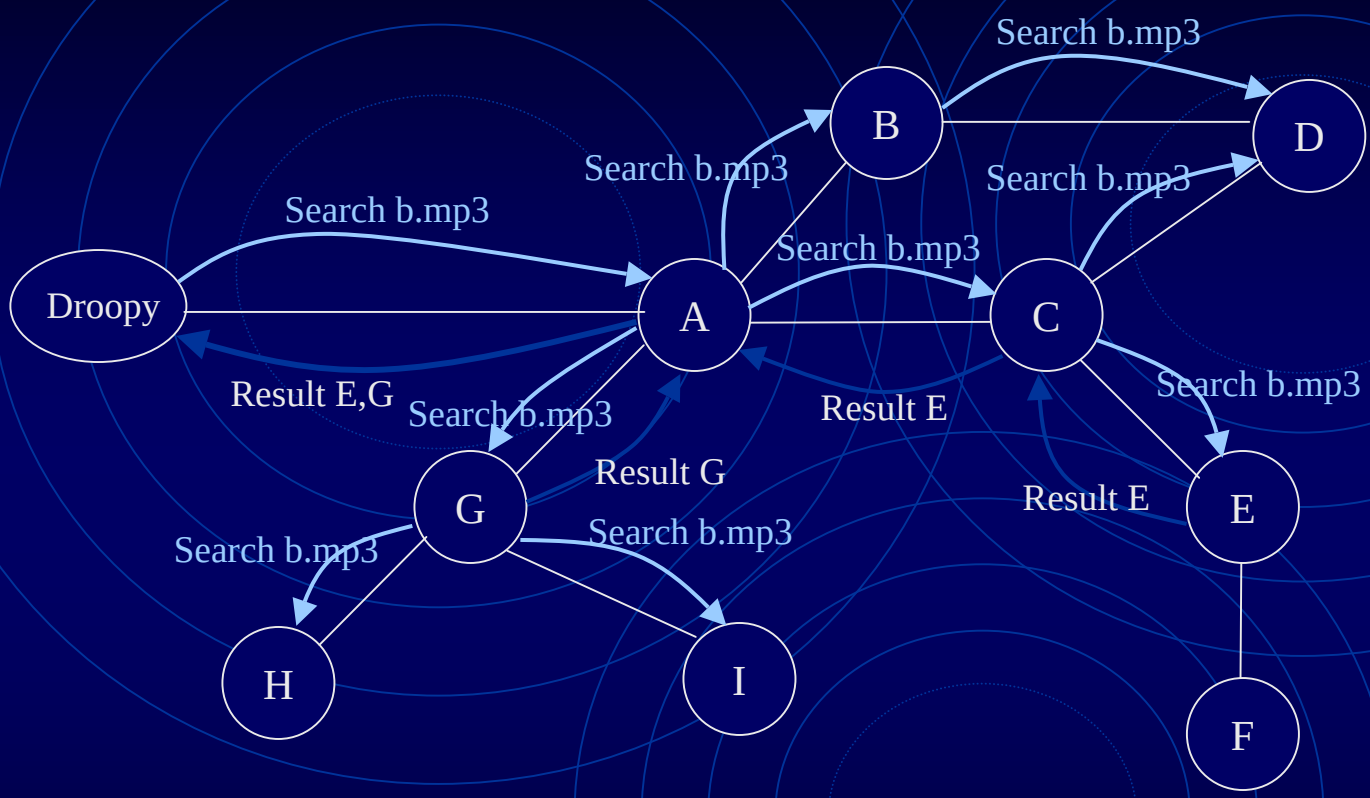


Mécanisme de routage (TTL=3)



Inondation

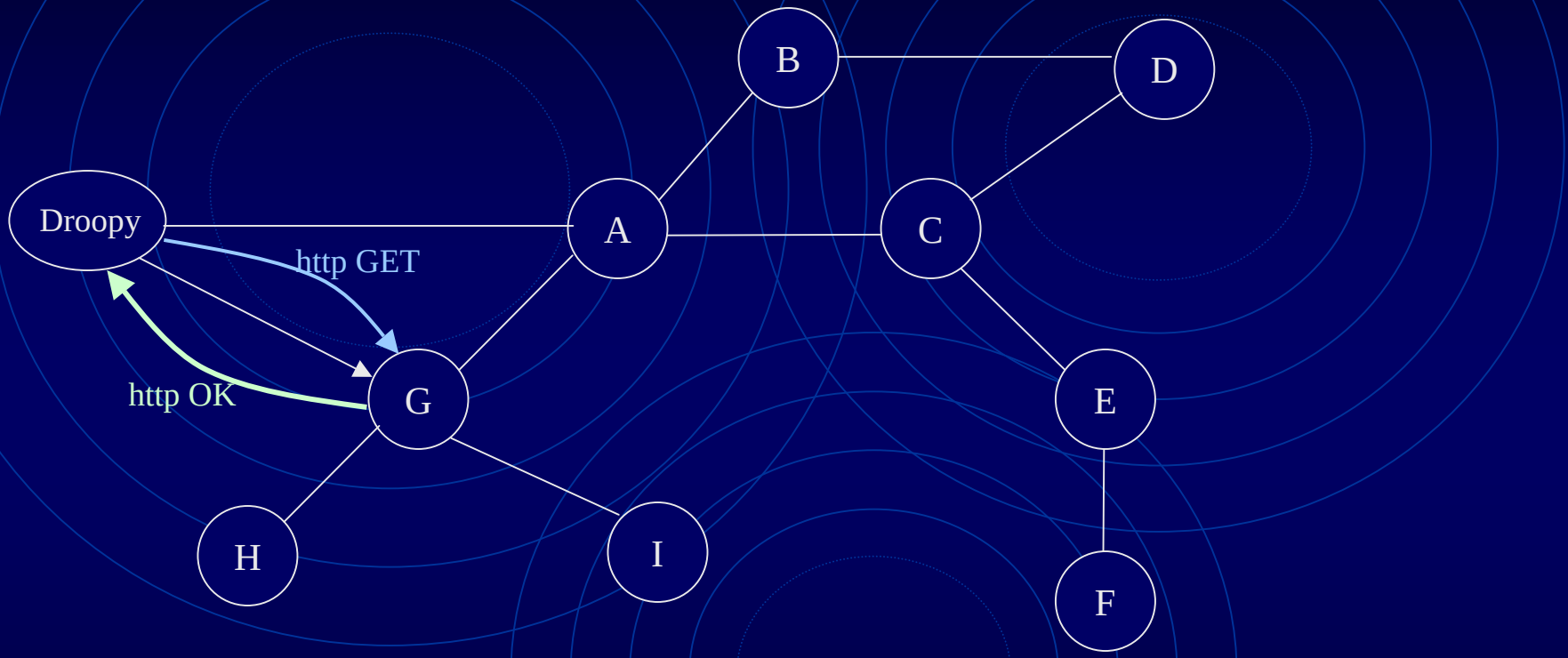
Recherche de données (query-query hit)



Réseau rapidement inondé par des ping-pong
Supporte mal la montée en charge du nombre d'utilisateurs
Avec un TTL à 7, seulement 25% des requêtes aboutiraient

G. Feltin G. Doyen O. Festor

Echange de fichiers



G. Feltin G. Doyen O. Festor

Bilan Gnutella

Limites

- Réseau rapidement inondé par des ping-pong
- Supporte mal la montée en charge du nombre d'utilisateurs
- Message push continuellement envoyé, si pas de réponse
- Manque de fiabilité dans ses requêtes

Avantages

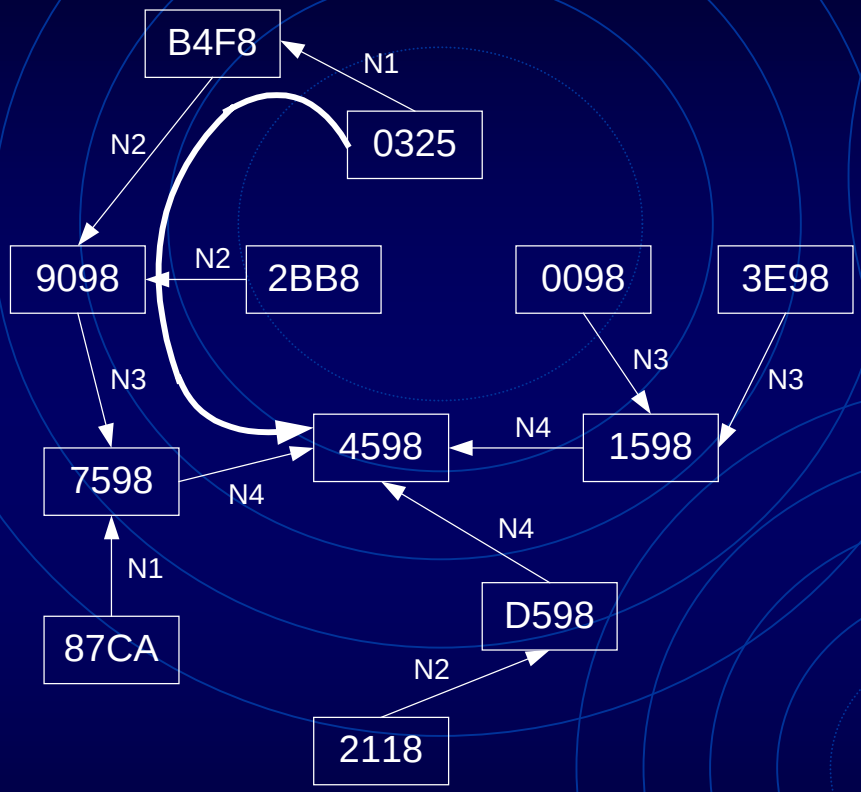
- Administration simple, car mutualisée
- Topologie évolutive
- Disponibilité du réseau, on ne peut arrêter

Orientation possible: les super-peers ou arbre de peers
Gnutella version 0.6 ou Kazaa

Recherche : localisation, routage et partage de fichiers

- Limitation du modèle pur, type Gnutella, dû à l'utilisation du TTL
- Fournir des solutions P2P de stockage, de recouvrement de données fiables
- Séparation entre:
  - problème de localisation et de routage (dans un environnement distribué dynamique)
  - application de partage de fichiers

Algorithme de Plaxton



(a)

Nommage des peers : fonction de hachage

	0	1	...	8	9
N1	xxx0	xxx1	...	B4F8	xxx9
N2	xx05	xx15	...	xx85	xx95
N3	x025	x125	...	x825	x925
N4	0325	1325	...	8325	9325

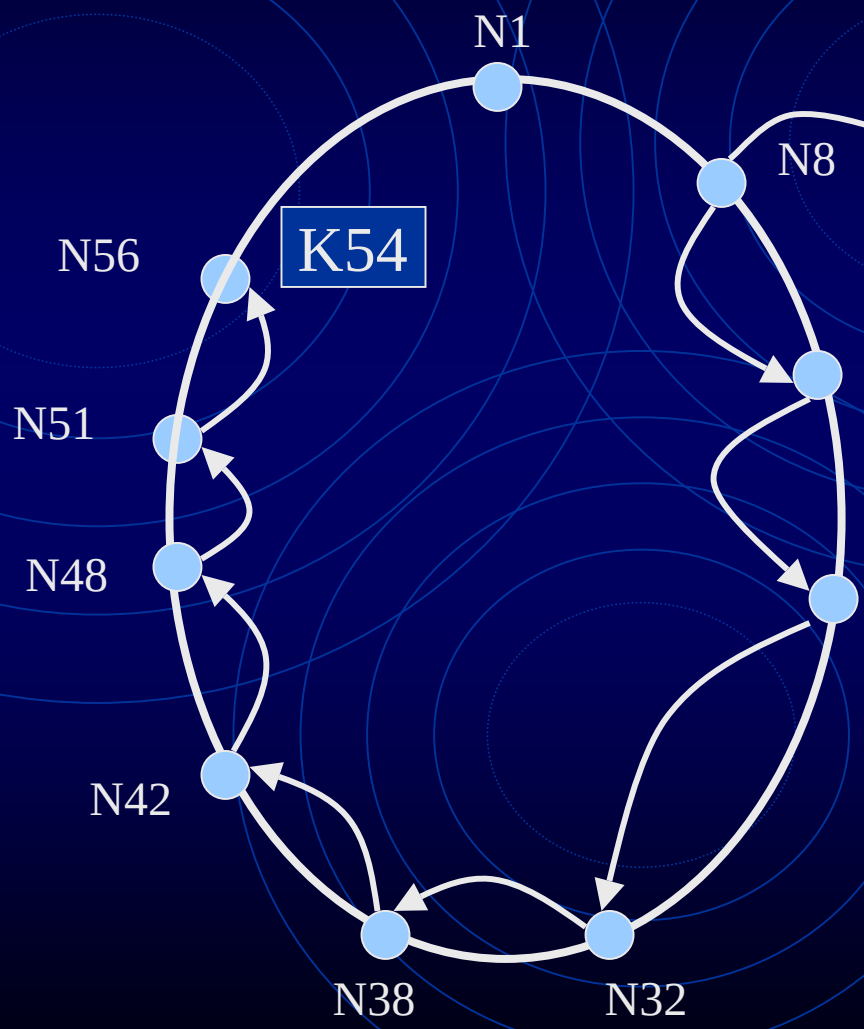
(b)

La localisation et le routage sont faits en même temps

Un système de N peers peut être joint en $\log_b(N)$ itérations

G. Feltin G. Doyen O. Festor

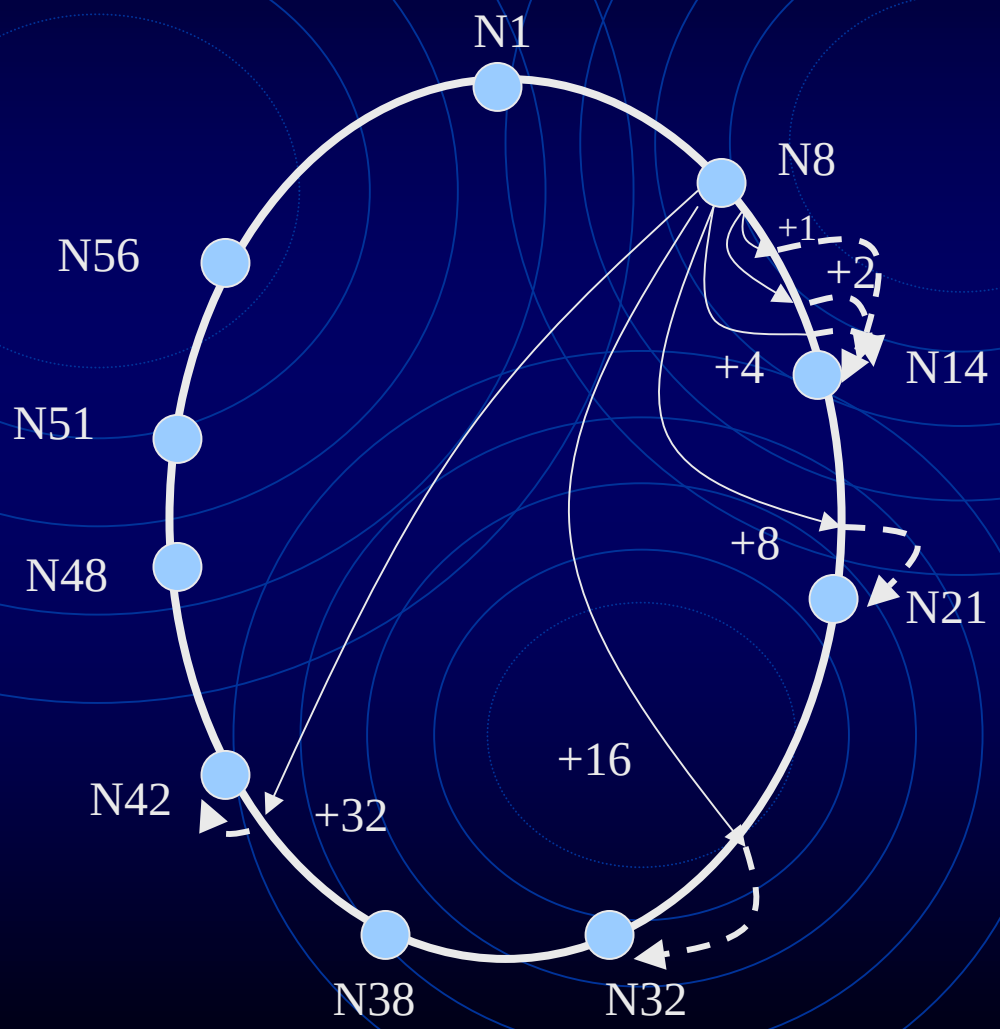
Chord :Acheminent d'une requête par parcours de l'anneau



Emploi de topologie connue:
Hypercube, anneau, tore
Hachage par @IP
Clés par ordre croissant
Intervalles de clés d'un nœud:
[clé(noeud actuel), clé(suivant)

G. Feltin G. Doyen O. Festor

Définition des fingers d'un noeud



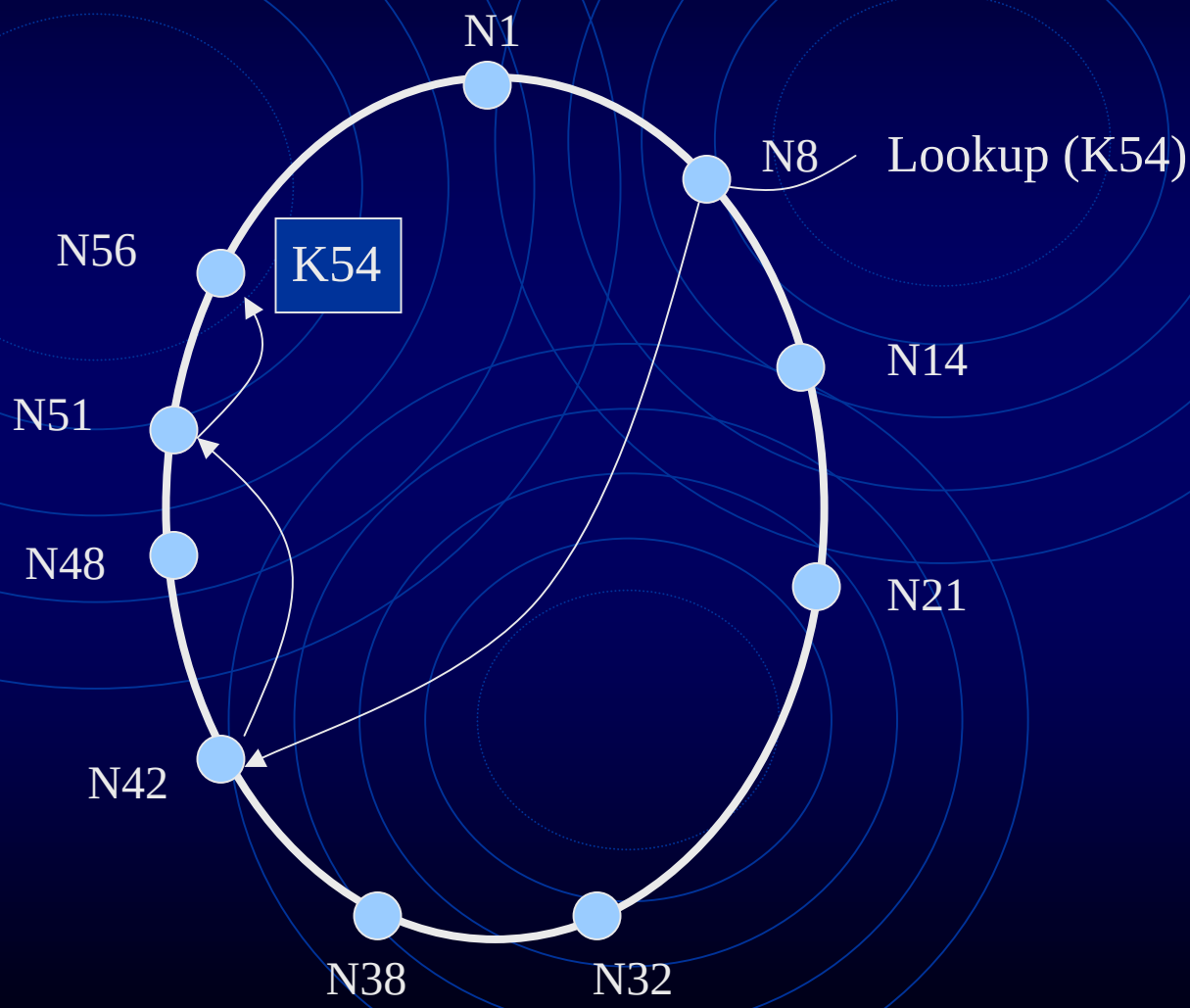
N8+1	N14
N8+2	N14
N8+4	N14
N8+8	N21
N8+16	N32
N8+32	N42

$N+2^{i-1}$ $1<i<m$

Clés $[0,2^m[$

G. Feltin G. Doyen O. Festor

Acheminement d’une requête en utilisant les fingers



G. Feltin G. Doyen O. Festor

CFS

- Application P2P de stockage de données à grande échelle
- Son architecture repose sur Chord pour le routage des messages
- Dhash (Distributed Hash) assure la fragmentation et le recouvrement des données (blocs de petite taille, contrairement à PAST ou OceanStore)
  - Permet d'utiliser des faibles espaces de stockage
  - Améliorer la sécurité des éléments stockés en les dispatchant
  - Equilibrer le trafic

Supervision

- Pas d’interface de supervision explicite
- A ce jour, minimum de gestion nécessaire au bon fonctionnement d’une application
  - Kazaa auto configure les peers participant au service pour organiser sa topologie autour des super-peers
  - CAN organise des mesures entre peers adjacents pour garantir une performance optimale
  - PAST utilise des cartes à puce pour contrôler l’accès des usagers à des données distribuées

Gestion des performances

- But : accroître le niveau de qualité d'une application intrinsèque
  - « The active virtual peer technology » permet d'effectuer la gestion de performance sur une application de type Gnutella
    - Restreindre les messages de signalisation
    - Paramétrer le routage en fonction de l'état des liens
    - Rediriger les requêtes de téléchargement
    - Contrôler et adapter la topologie virtuelle
  - MMAPPS (Market Management of Peer-to-Peer Services)
    - Mécanisme d'évaluation de la contribution
    - N'autorise l'accès aux ressources qu'en fonction des ressources fournies
- Rien pour l'administrateur de domaine, afin de contrôler les applications sauvages

Administration du P2P

- Contrôle du trafic, plutôt qu'une qualité de service aux usagers
- Assez compliqué, car il faut identifier ce type de trafic, les applications P2P n'utilisant pas un port spécifique
  - ➔ nécessaire d'inspecter les paquets jusqu'au niveau 3 à 7
  - ➔ Une fois l'identification d'un paquet effectuée, il faut pouvoir traiter l'ensemble du flux
  - ➔ nécessaire de pouvoir s'adapter rapidement aux changements
- Contrôler la bande passante P2P parmi l'ensemble du trafic, à différencier le traitement effectué en fonction des sources, destinations, date, profil des usagers

Les droits légaux des oeuvres

- La mise en ligne d'œuvres protégées sans autorisation vous expose à des poursuites
  - article L 3335-4 du code de la propriété intellectuelle
- Le téléchargement de copies illicites vous rend coupable de copies illicites et donc de contrefaçon, voire même de recel pour peu que vous ayez eu connaissance de l'origine frauduleuse des fichiers
  - Article 321-1 du code pénal

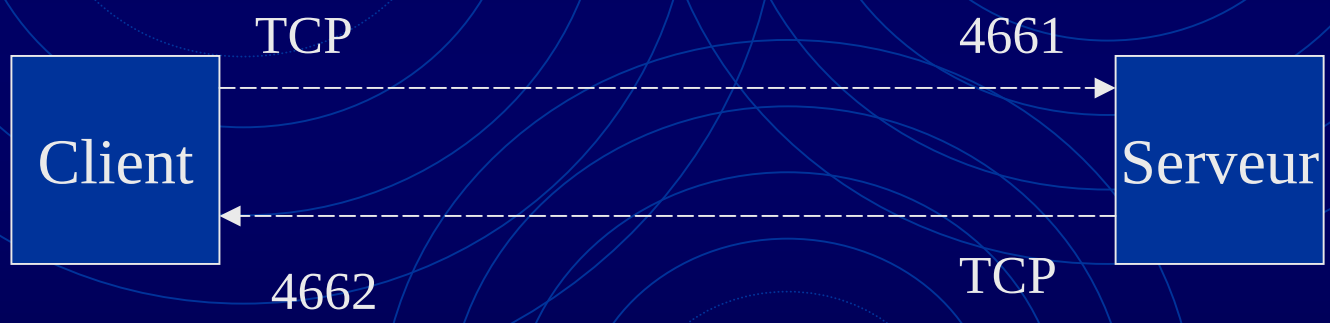
➔ Sensibilisation des utilisateurs et des directions

- Droit d'auteur
- Consommation de la bande passante, et oui, nous payons RENATER!
- Partage des données sur le poste de travail, on peut exporter tout le disque, voir les dossiers partagés sur Internet

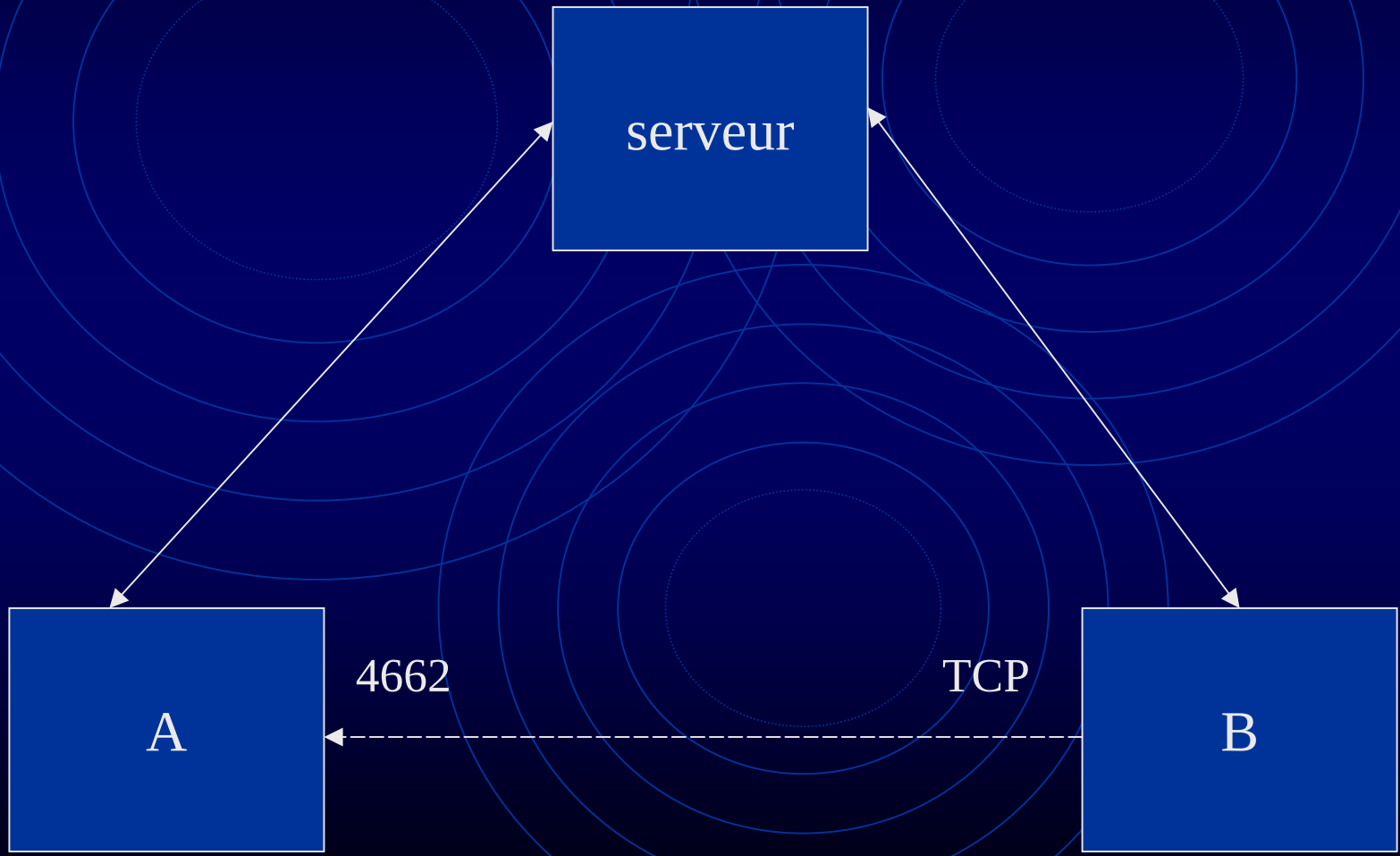
Traitement du P2P

- Problématique:
  - De nouveau les logiciels apparaissent très souvent
  - Certains sites ont les autorisations des auteurs
  - Et **surtout**, les logiciels P2P peuvent être utilisés pour:
    - des chargements de logiciels
    - Partage de fichiers distribués (bien plus rapide que ftp)
    - Travail collaboratif
    - Recherche sur le P2P

Fonctionnement : Connexion à un serveur (E-Donkey)

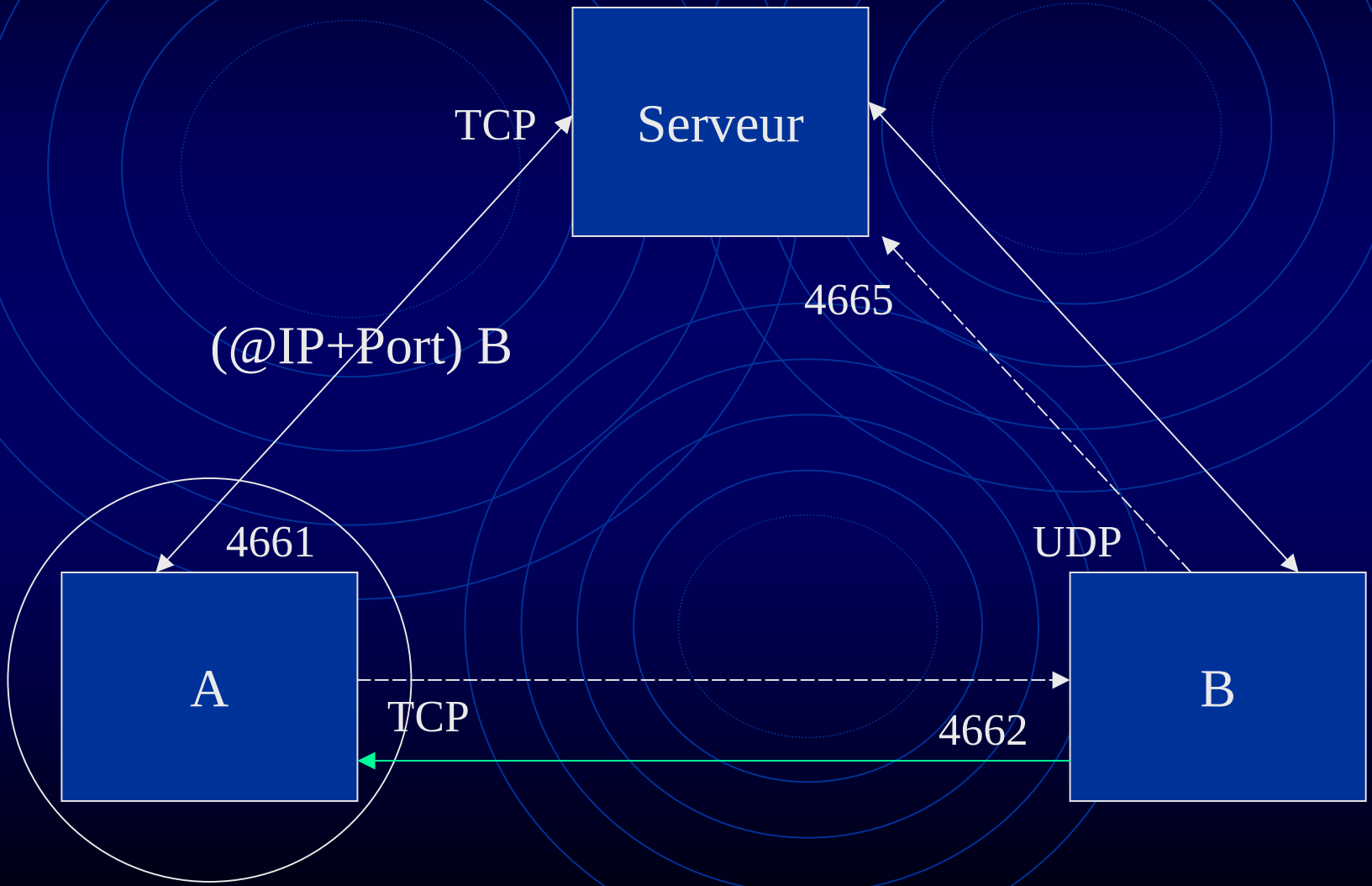


A a un ID fort: peer to peer en natif



G. Feltin G. Doyen O. Festor

A a un ID faible



G. Feltin G. Doyen O. Festor

Filtrage des ports

- En entrée, pratiquement toujours fait
- En sortie, on ne peut pas tout bloquer, car beaucoup d'applications dynamiques

412	Direct Connect	6346 à 6347	Gnutella
1214	Kazaa/Morpheus	6881	Groove Napster/WinMX
4662 à 4665	eDonkey	6881 à 6889	BitTorent

- Mais fermer tous les ports P2P :
  - risque de tunneling http ou icmp
  - Utilisation de protocole crypté ou de SSH ?

➔Difficulté d'identifier le trafic

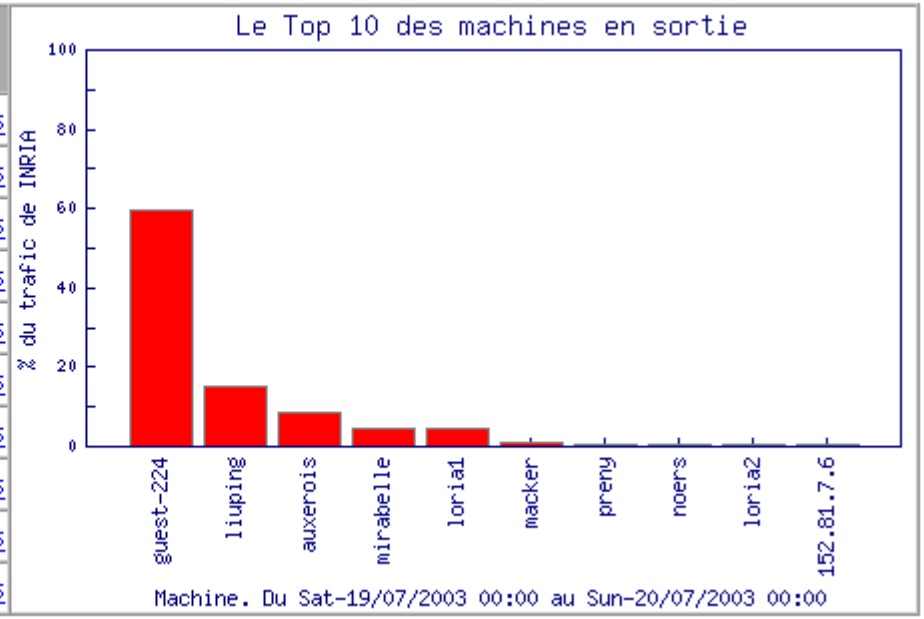
Filtrage du trafic

- Securing your network against Kazaa (Ftwall) Chris Lowth -Linux Journal
  - Netfilter ou iptables avec l'option QUEUE
  - Flitrage en sortie
- QoS sur le trafic P2P

Détection avec NetMet

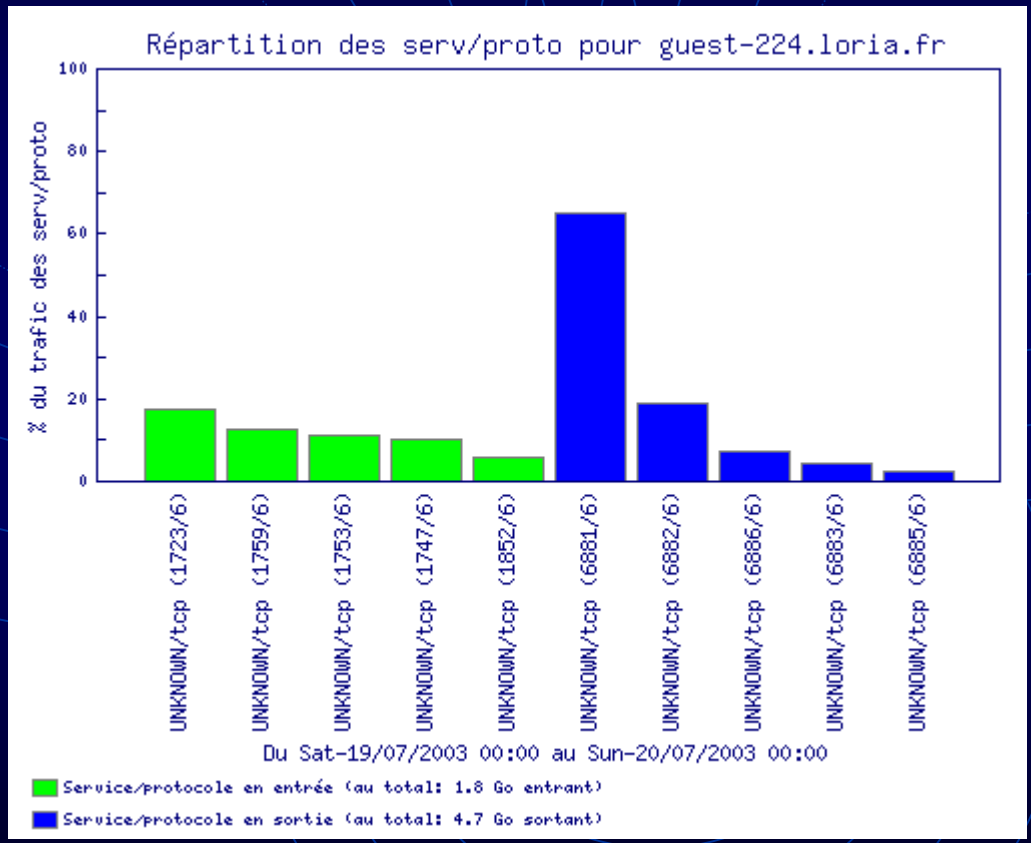
Outil de métrologie basé sur l'analyse des flux, comme NetMet, fait ressortir Rapidement le trafic P2P

Host	Cumul (octets)	Cumul (%)	
guest-224.loria.fr	4.7 Go	59.49	Détails
liuping.loria.fr	1.2 Go	15.05	Détails
auxerois.loria.fr	691.7 Mo	8.79	Détails
mirabelle.loria.fr	366.7 Mo	4.66	Détails
loria1.loria.fr	346.6 Mo	4.40	Détails
macker.loria.fr	87.6 Mo	1.11	Détails
preny.loria.fr	56.1 Mo	0.71	Détails
noers.loria.fr	38.3 Mo	0.49	Détails
loria2.loria.fr	36.8 Mo	0.47	Détails
152.81.7.6	34.6 Mo	0.44	Détails



G. Feltin G. Doyen O. Festor

Détail de NetMet : BitTorent



G. Feltin G. Doyen O. Festor

Détection par snort

• Utilisation d'un IDS (Intrusion Detection System) comme **snort** permet de repérer certains trafic P2P : Napster, Gnutella, BitTorent, FastTrack/Kazaa/Morpheus

SID	1432	**message**	P2P GNUTella GET
Signature	alert tcp $HOME_NET any -> $EXTERNAL_NET !80 (msg:"P2P GNUTella GET"; flow:to_server,established; content:"GET "; offset:0; depth:4; classtype:policy-violation; sid:1432; rev:4;)		
Summary	This event is generated when activity by Peer-to-Peer (p2p) clients is detected.		
Impact	Informational event. Unauthorized use of a p2p client may be in progress.		
Detailed Information	This event indicates that use of a p2p client has been detected. This may be against corporate policy. p2p clients connect to other p2p clients to share files, commonly music and video files but can be configured to share any file on the local machine. This activity may not only use bandwidth but may also be used to transfer company confidential information to unauthorized hosts external to the protected network bypassing other security measures in place.		
Affected Systems	Any host using a p2p client.		
Attack Scenarios	This is indicative of the use of a p2p client.		

Sécurité d’un réseau P2P

- Réseau P2P constitué de peers inconnus

Potentiellement dangereux

➔ Mise en œuvre de mécanismes de sécurité

- Cryptage des données avec clés multiples
- Sandboxing (exécuter une application dans un environnement clos)
- Gestion des droits d’utilisation
- Facturation
- Protection des hôtes par des pare-feux
- IPV6 authentification et intégrité

Conclusion

- Connaissance des protocoles P2P
  - Passage à l'échelle, routage
  - Encore du travail pour la supervision
- Connaissance des applications
  - Génome humain
- Sensibilisation des utilisateurs
- L'Internet de demain ?
  - Mobilité, sans fil, bande passante, puissance des machines, domotique
  - Applications P2P
    - passage à échelle (pas d'engorgement des serveurs)
    - résilience en cas d'attaque massive
  - Pushing Peer-to-Peer - Simsom Garfinkel http://www.technologyrewiev.com/articles/wo_garfinkel1003003.asp