Vers un Radar pour l'Internet

Matthieu Latapy*, Fabien Viger*,†,
Benjamin Orgogozo*, Damien Bobillot*

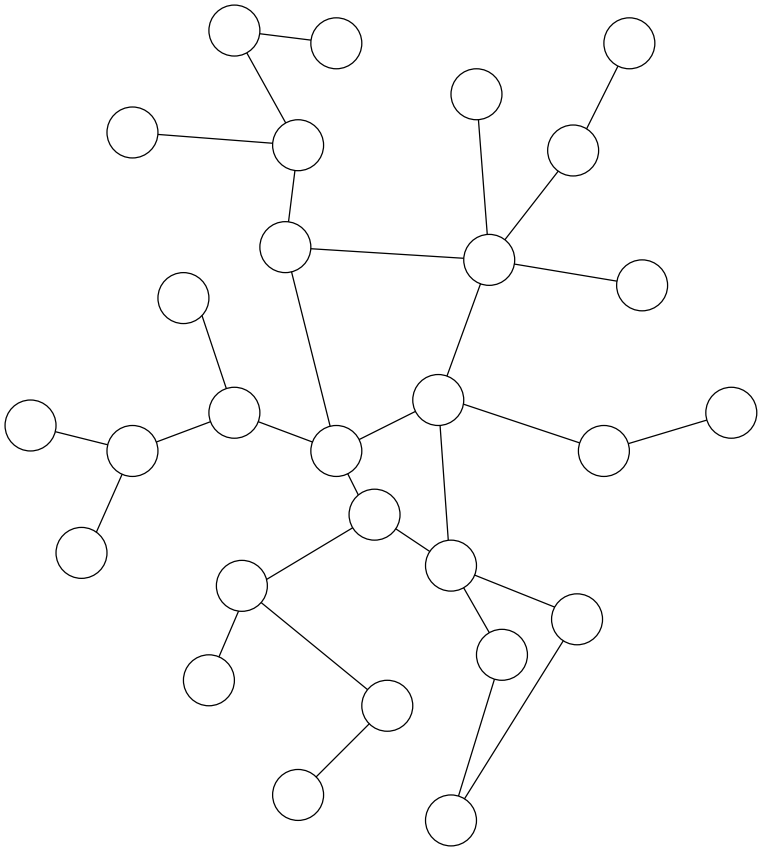
* LIAFA, CNRS et Université Paris 7

† LIP6, CNRS et Université Paris 6

13 Octobre 2005

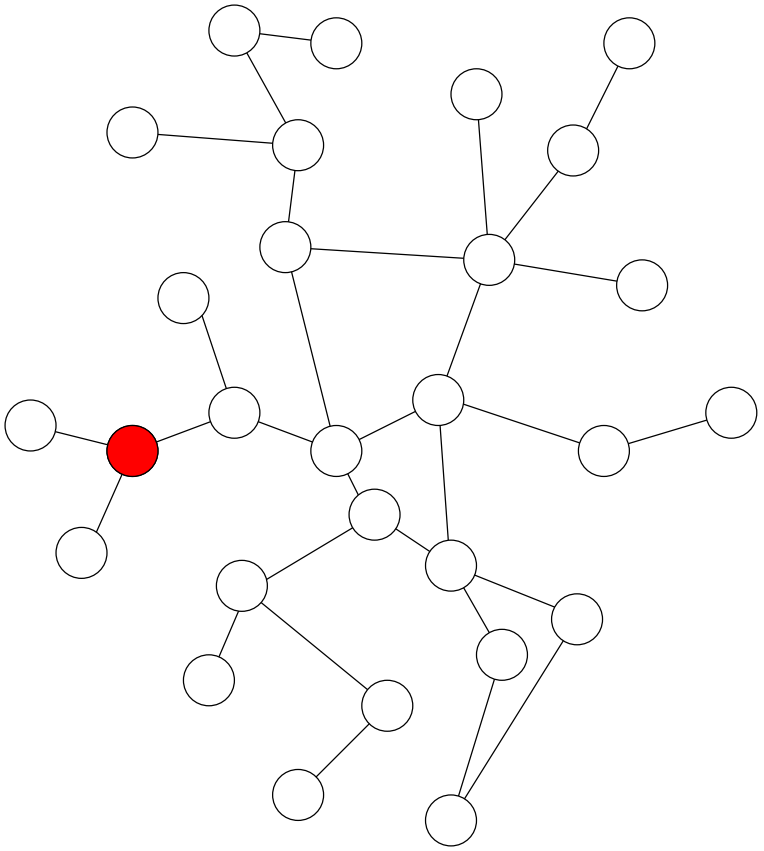
Le Radar, en théorie

Introduction



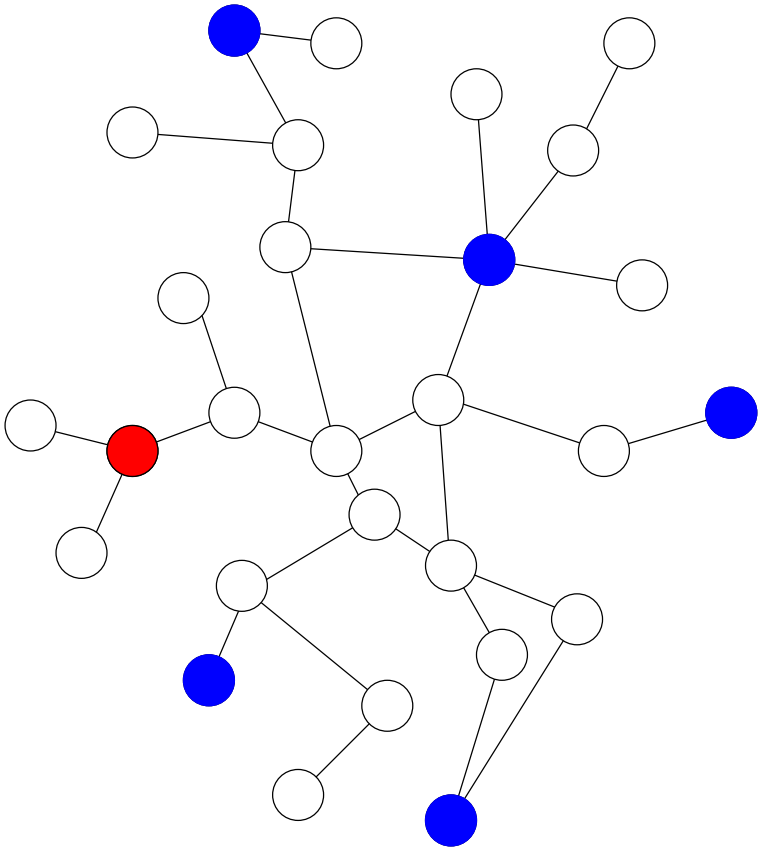
On se donne :

- ◇ 1 source



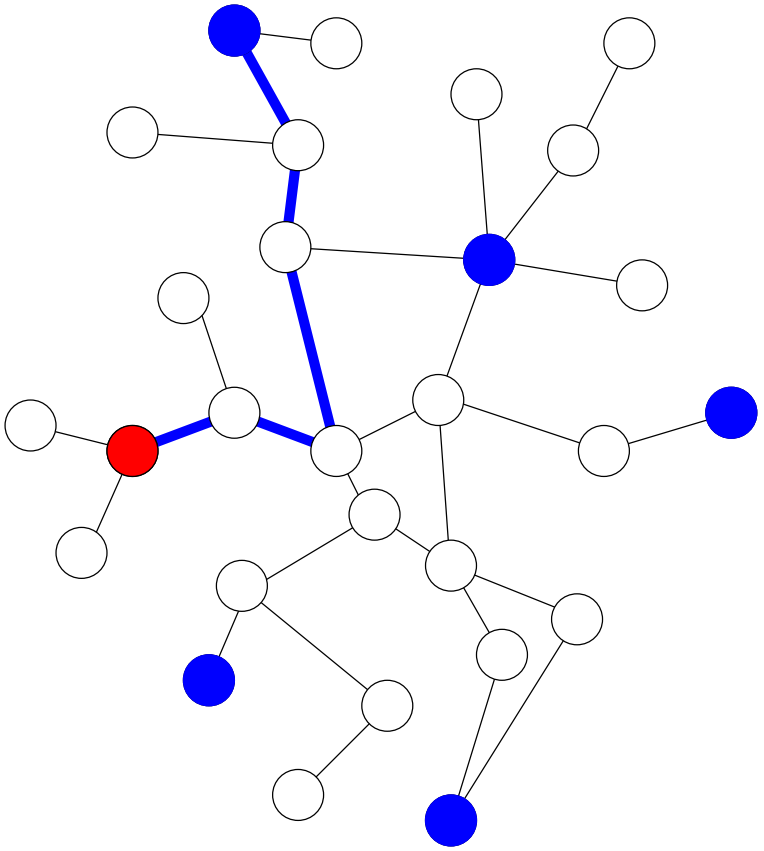
On se donne :

- ◇ 1 source
- ◇ Un ensemble d'adresses IP destinations D



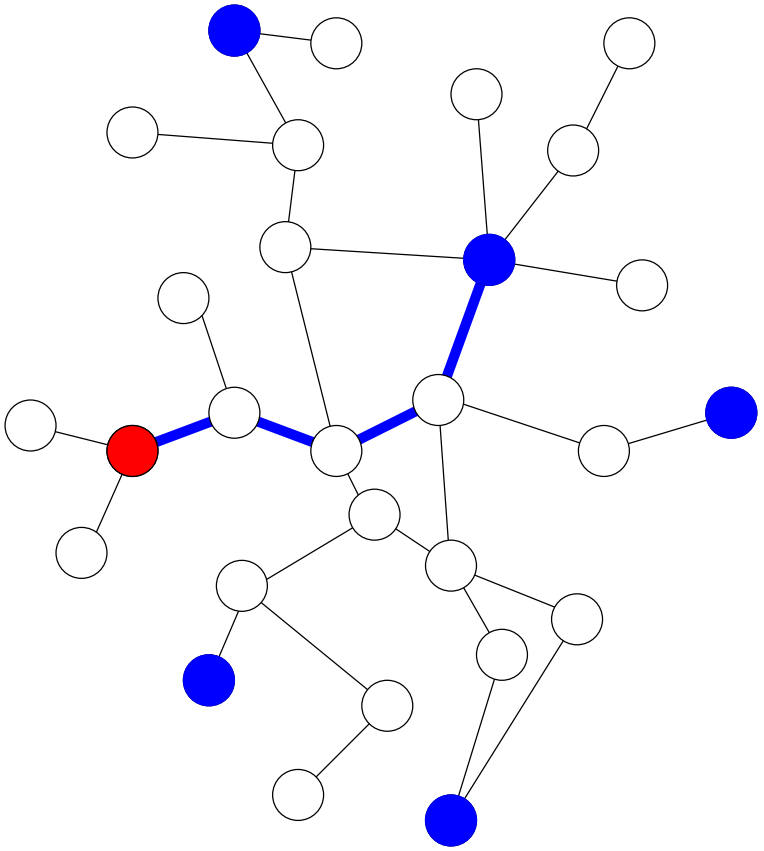
On se donne :

- ◇ 1 source
- ◇ Un ensemble d'adresses IP destinations D
- ◇ Des passes complètes : durée T_p, intervalles Δ_T.



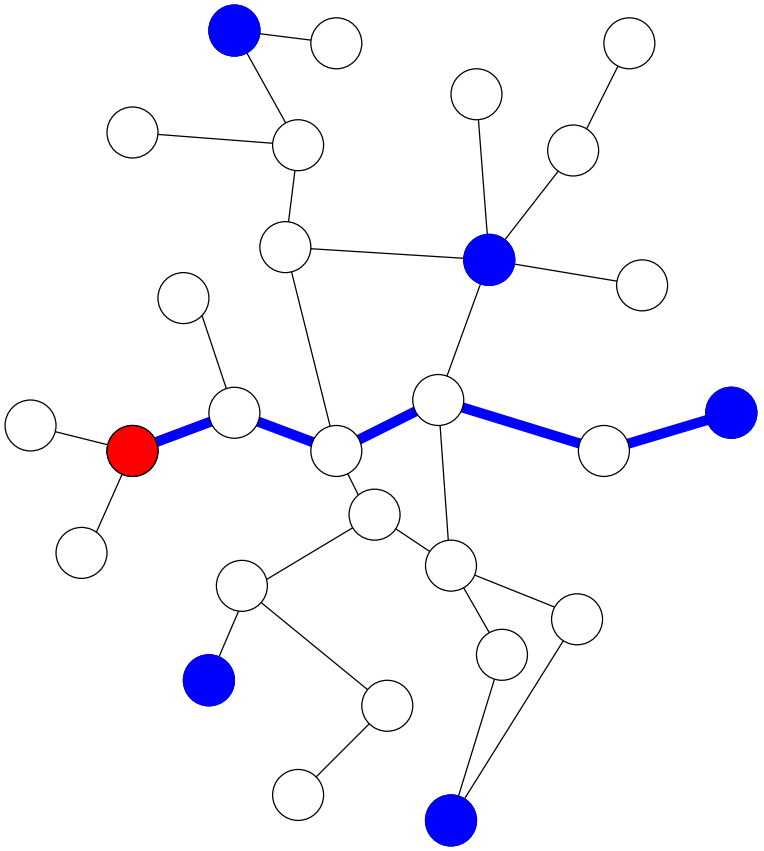
On se donne :

- ◇ 1 source
- ◇ Un ensemble d'adresses IP destinations D
- ◇ Des passes complètes : durée T_p, intervalles Δ_T.



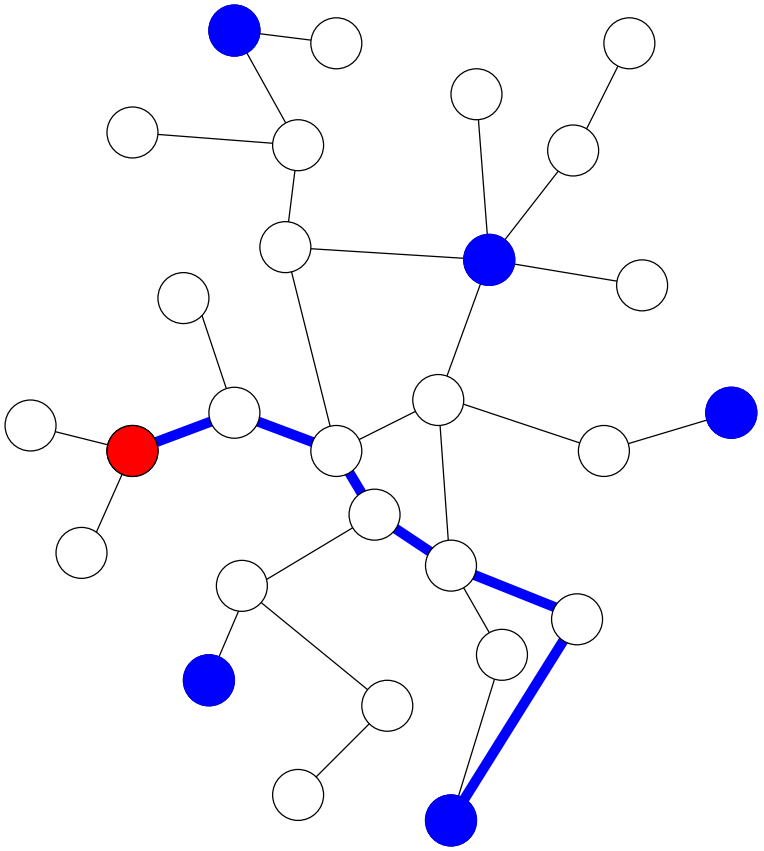
On se donne :

- ◇ 1 source
- ◇ Un ensemble d'adresses IP destinations D
- ◇ Des passes complètes : durée T_p, intervalles Δ_T.



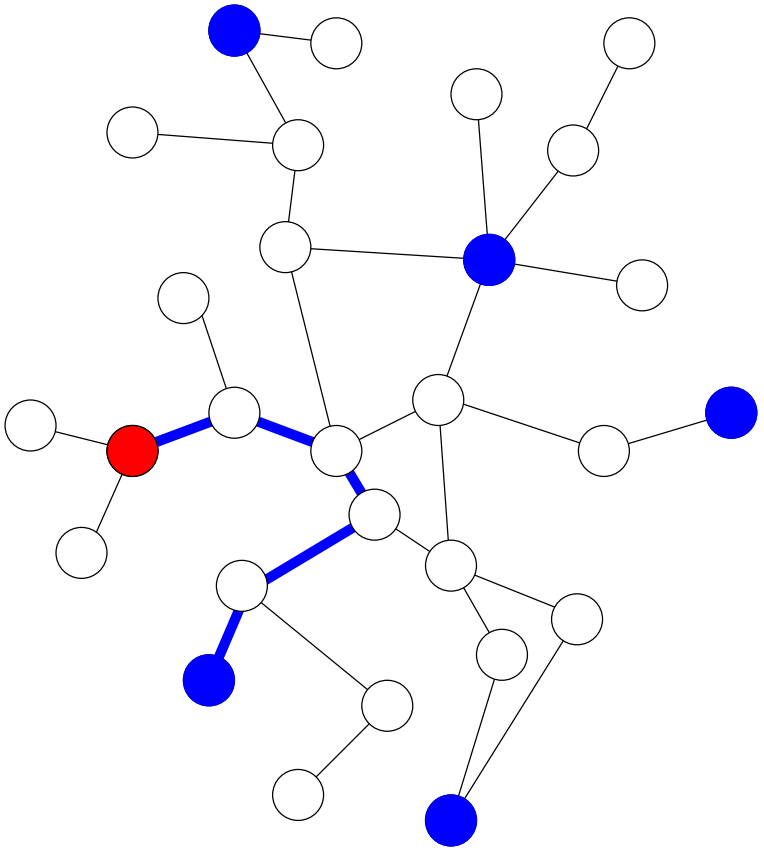
On se donne :

- ◇ 1 source
- ◇ Un ensemble d'adresses IP destinations D
- ◇ Des passes complètes : durée T_p, intervalles Δ_T.



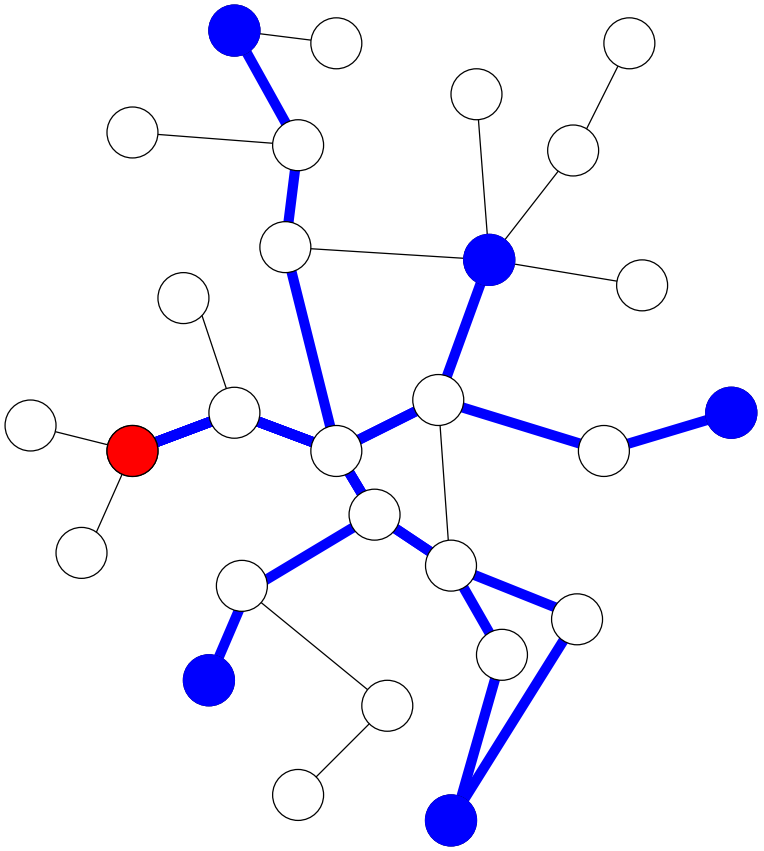
On se donne :

- ◇ 1 source
- ◇ Un ensemble d'adresses IP destinations D
- ◇ Des passes complètes : durée T_p, intervalles Δ_T.



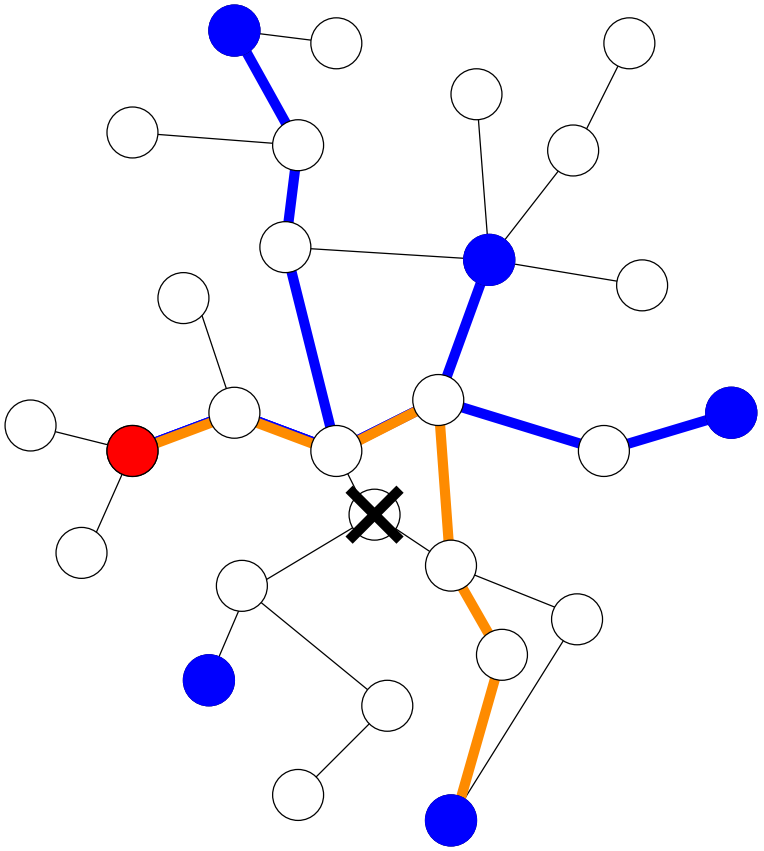
On se donne :

- ◇ 1 source
- ◇ Un ensemble d'adresses IP destinations D
- ◇ Des passes complètes : durée T_p, intervalles Δ_T.
- ◇ Après *assez* de passes, on a "tout vu"



On se donne :

- ◇ 1 source
- ◇ Un ensemble d'adresses IP destinations D
- ◇ Des passes complètes : durée T_p, intervalles Δ_T.
- ◇ Après *assez* de passes, on a "tout vu"



⇒ Changement = Anomalie

Partie I

Tour d'horizon

Objectifs
Plan d'attaque

Objectifs

Tour d'horizon

- ▷ Détection d'anomalies : pannes, attaques, congestions, autres (?)
- ▷ Aide visuelle au monitoring réseau

  - ◇ **Temps réel** : on devra pouvoir *contrer* l'attaque ou *réparer* la panne rapidement (quelques minutes).
  - ◇ **Non-invasivité** : le Radar ne doit pas induire de surcharge réseau
  - ◇ **Simplicité** et **compatibilité** pour un déploiement aisé.

Le Radar n'est pas, *a priori*, un outil de diagnostic détaillé.

Plan d'attaque

Tour d'horizon

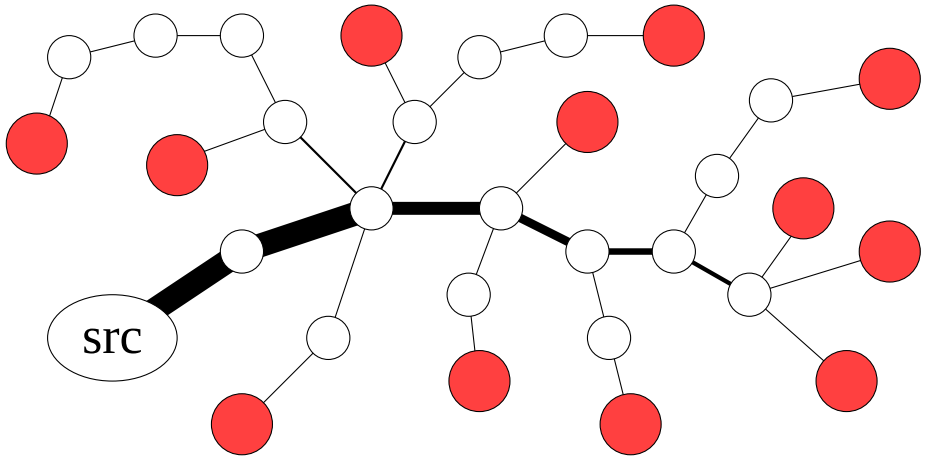
- ▷ Implémentation provisoire
- ▷ Étude prospective : que voit-on ?
- ▷ Analyse des données, étude de la dynamique, simulations d'attaques, optimisations
- ▷ Définition des outils de mesure et d'analyse finaux
- ▷ Mise en route

Partie II

Implémentation

- ▷ Source = un simple ordinateur connecté à Internet
- ▷ $100 \leq |D| \leq 60000$ adresses IP destinations
- ▷ outil `traceroute` (builtin)
- ▷ Durée d'une passe : $7s \leq T_p \leq 4h$
- ▷ Temps d'action $\rightarrow 1$ mois (13000 passes)

`traceroute` complets → redondance



Méthodes alternatives :

- ◇ Itérations sur les **arêtes** plutôt que sur les **routes**
- ◇ `traceroute` "par arbre"

Méthodes mixte : On sonde chaque arête une fois par passe, et on effectue un `traceroute` complet si on détecte un changement.

En pratique :

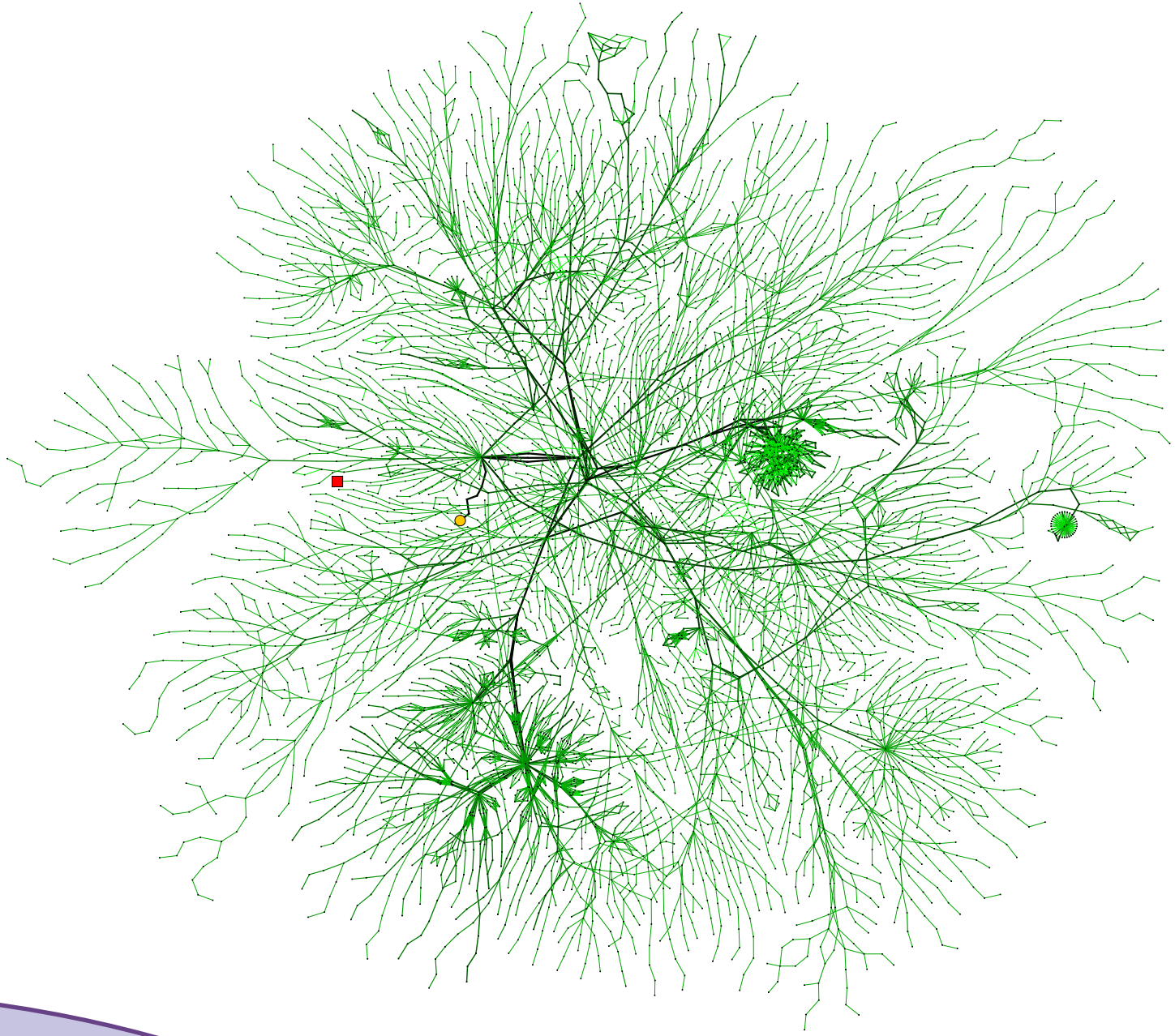
- ▷ 3 fois moins de paquets envoyés par passe
- ▷ Passes 3 fois plus rapides
- ▷ Et pourtant, d'avantages d'arêtes observées !

Partie III

Étude prospective

Ce que voit le Radar : image statique

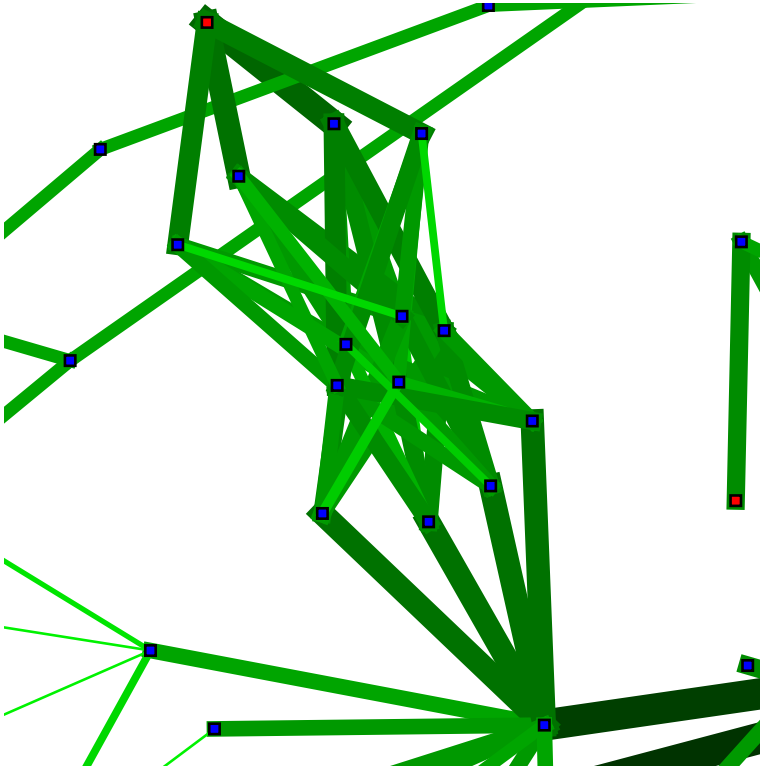
Étude prospective



Étape nécessaire avant de s'interesser au comportement dynamique de la topologie.

▷ Présence de structures non-triviales :

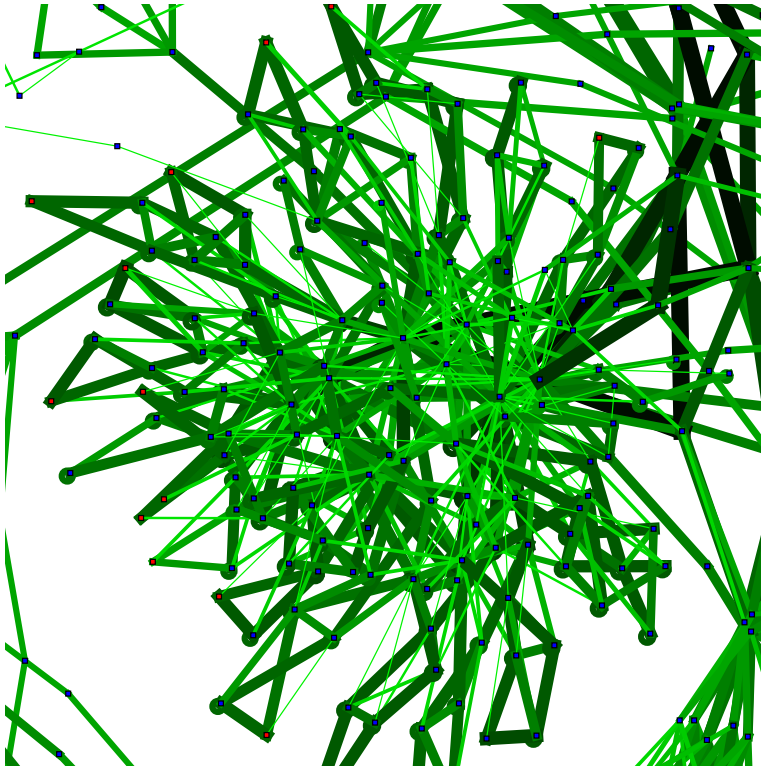
◇ k-cliques



Étape nécessaire avant de s'interesser au comportement dynamique de la topologie.

▷ Présence de structures non-triviales :

- ◇ k-cliques
- ◇ boucles, cliques



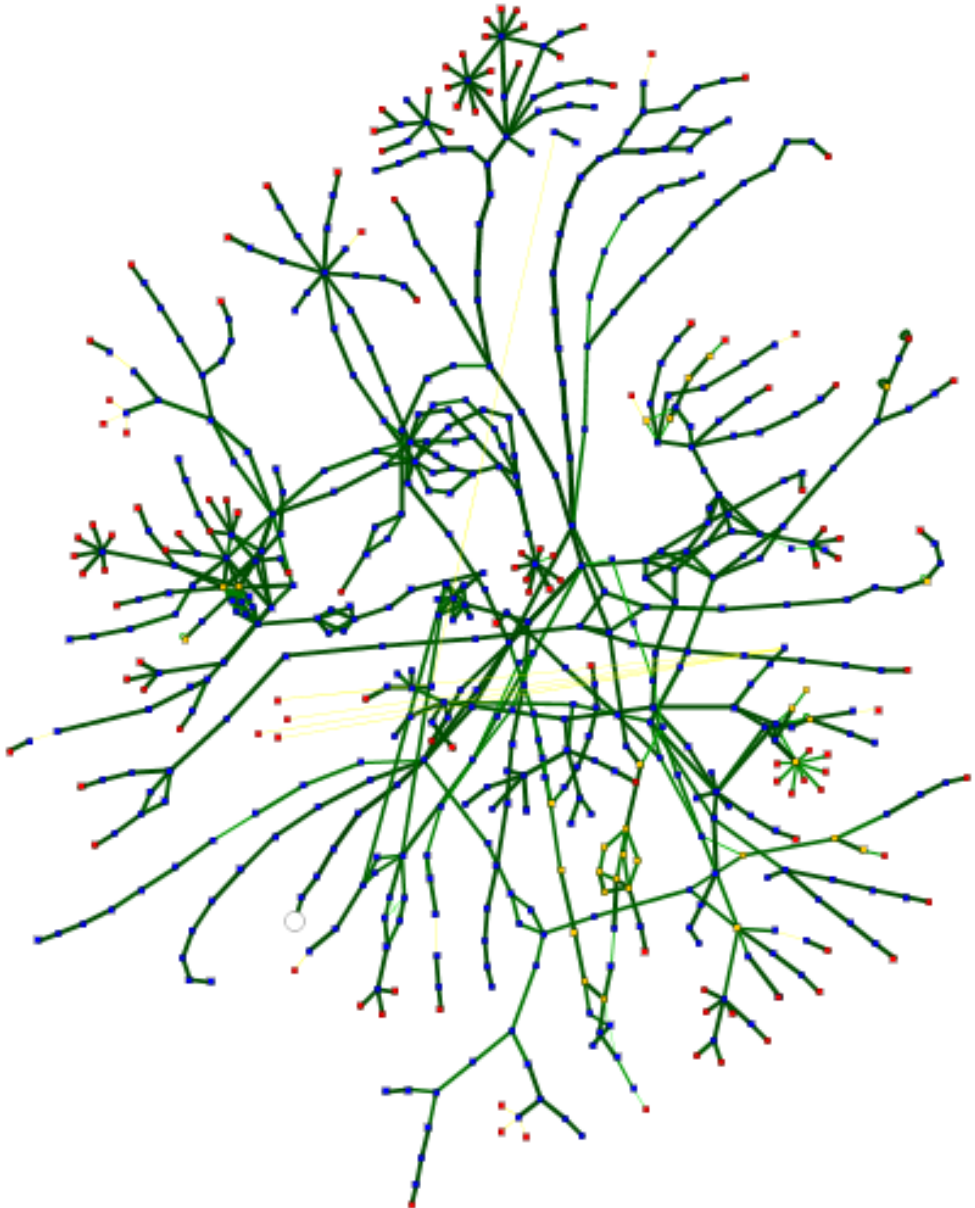
Étape nécessaire avant de s'interesser au comportement dynamique de la topologie.

▷ Présence de structures non-triviales :

- ◇ k-cliques
- ◇ boucles, cliques
- ◇ cycles

Ce que voit le Radar : dynamique

Étude prospective



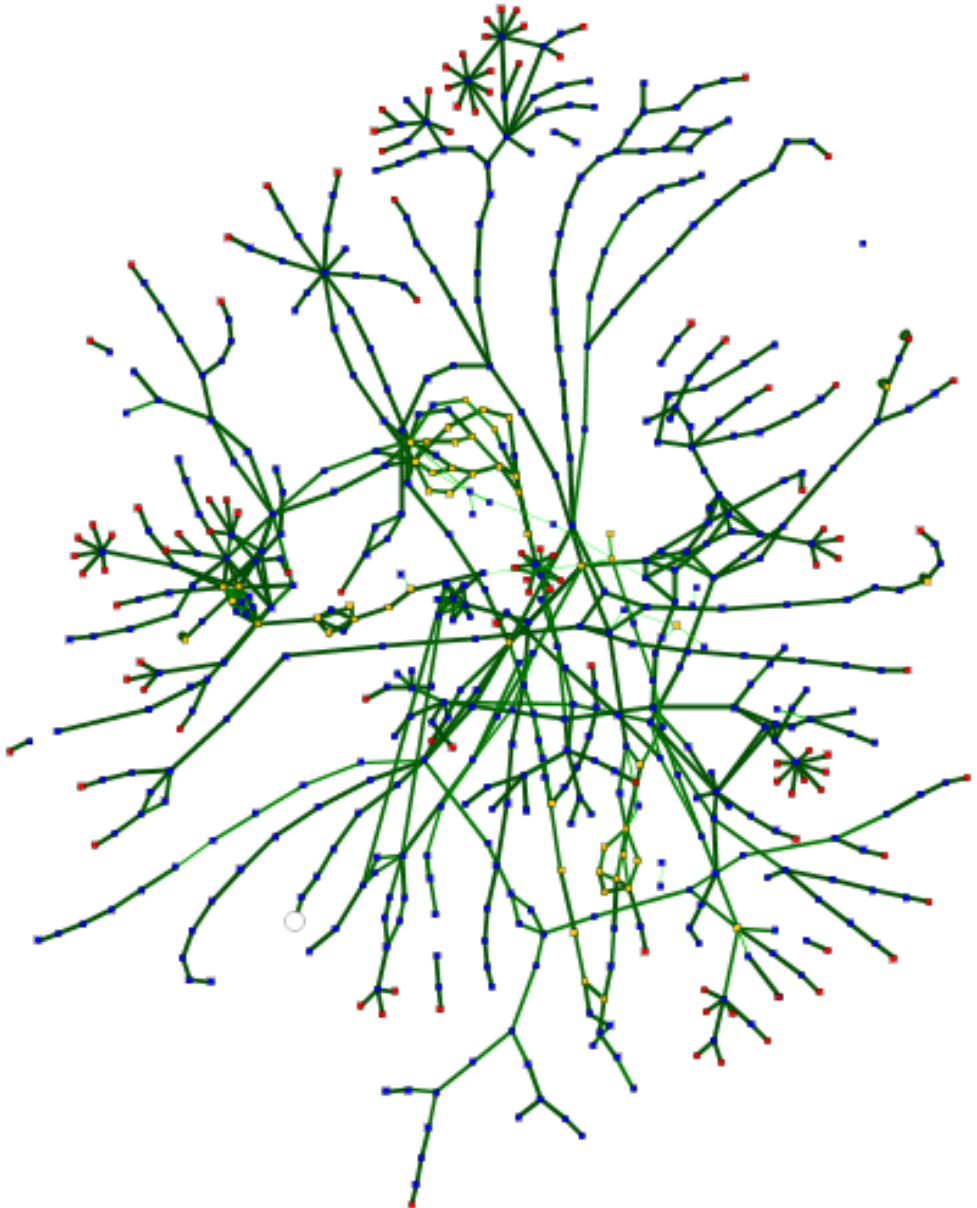
Différents **phénomènes** dynamiques apparaissent :

- ◇ Routeurs paresseux
- ◇ Load-balancing
- ◇ Changement de routage
- ◇ Anomalie ponctuelle
- ◇ Anomalie à long terme

[Passe 1/5]

Ce que voit le Radar : dynamique

Étude prospective



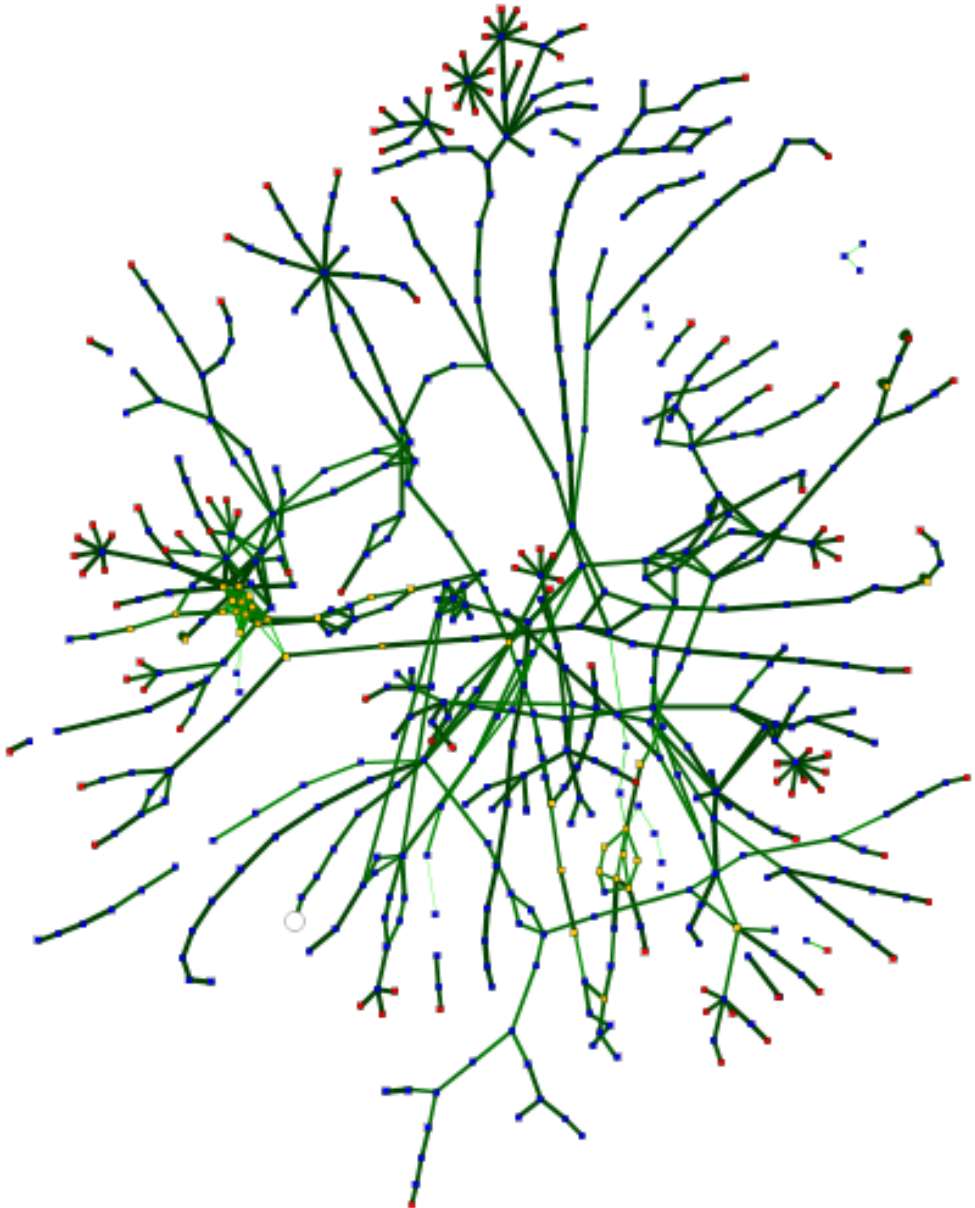
Différents **phénomènes** dynamiques apparaissent :

- ◇ Routeurs paresseux
- ◇ Load-balancing
- ◇ Changement de routage
- ◇ Anomalie ponctuelle
- ◇ Anomalie à long terme

[Passe 2/5]

Ce que voit le Radar : dynamique

Étude prospective



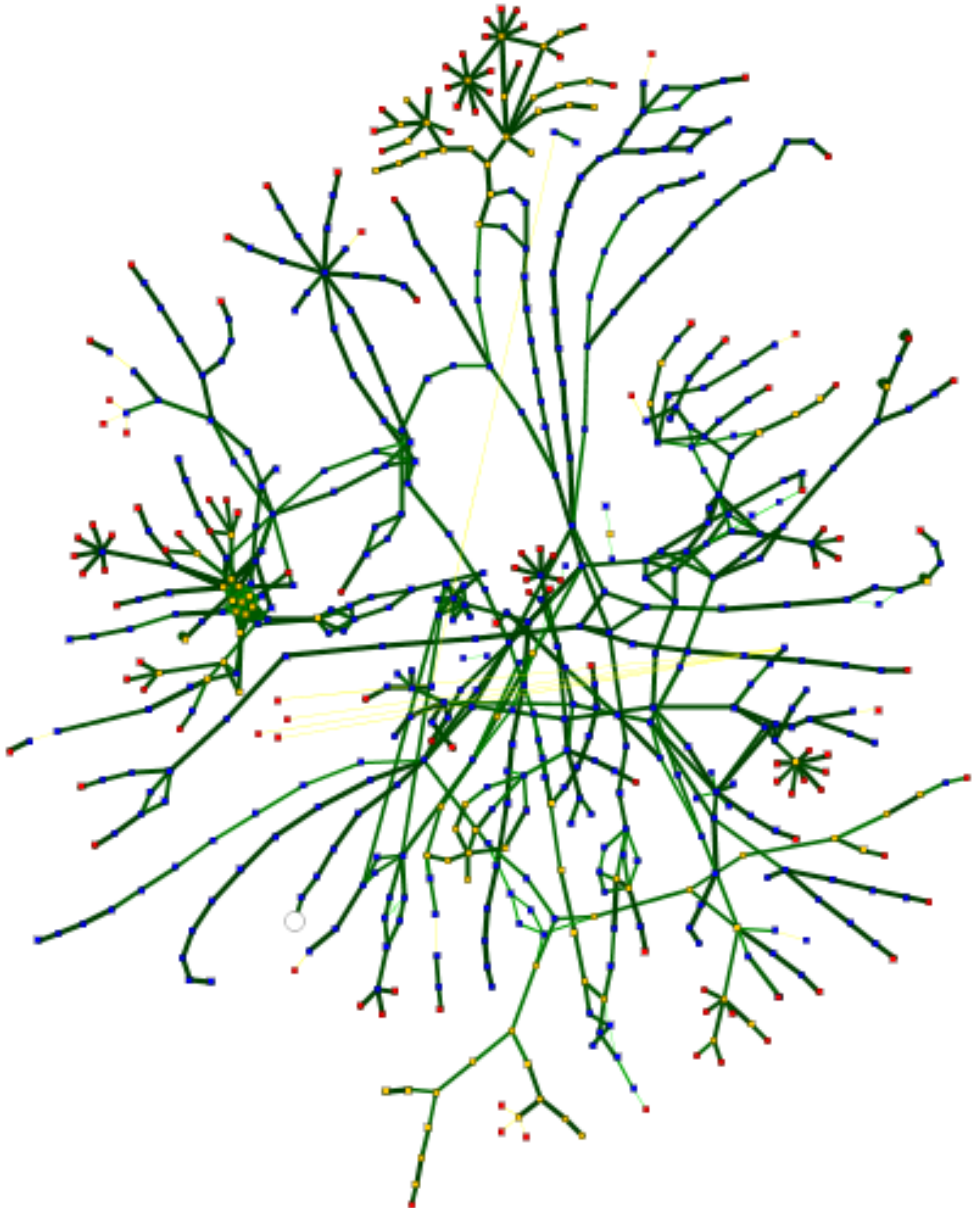
Différents **phénomènes** dynamiques apparaissent :

- ◇ Routeurs paresseux
- ◇ Load-balancing
- ◇ Changement de routage
- ◇ Anomalie ponctuelle
- ◇ Anomalie à long terme

[Passe 3/5]

Ce que voit le Radar : dynamique

Étude prospective



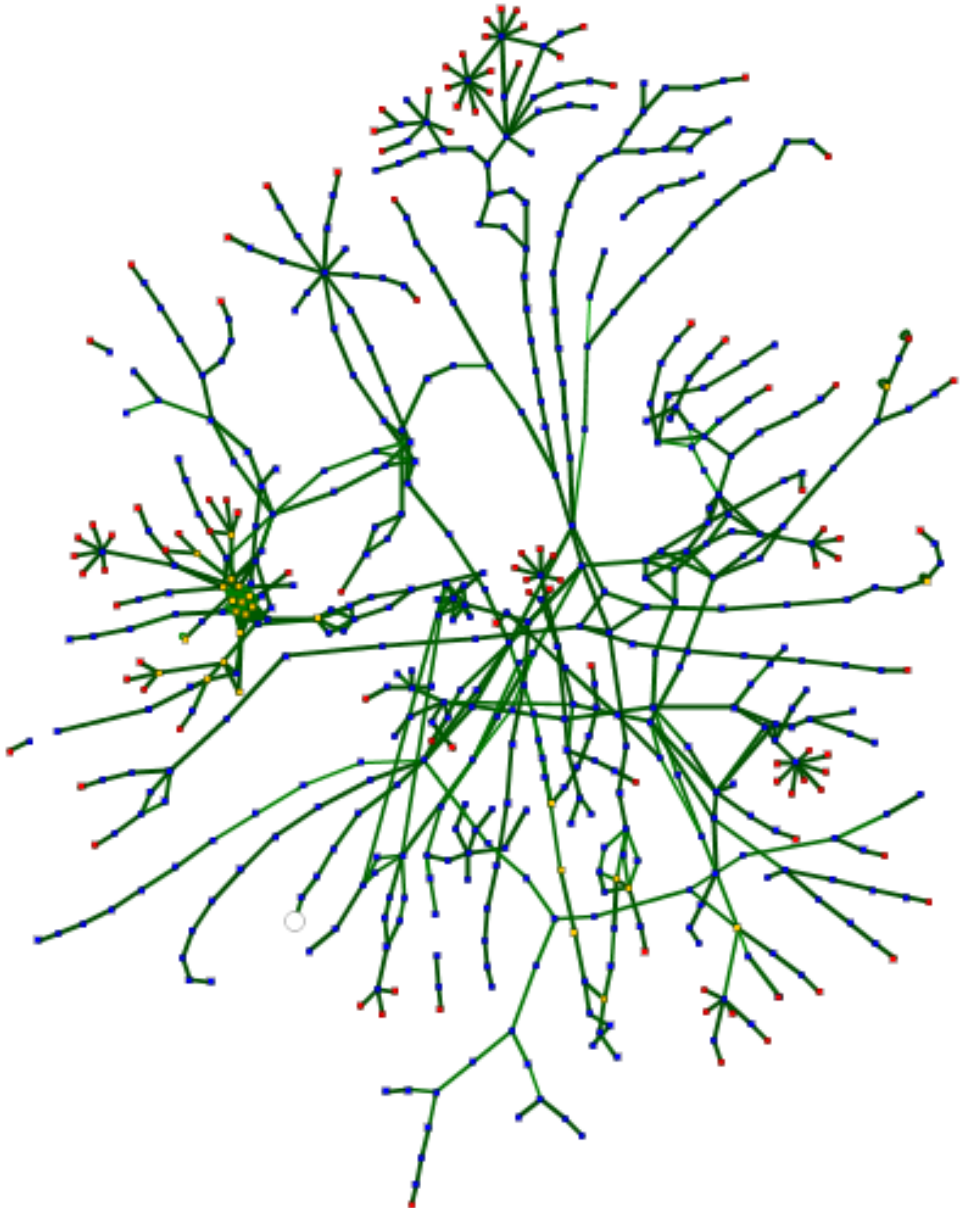
Différents **phénomènes** dynamiques apparaissent :

- ◇ Routeurs paresseux
- ◇ Load-balancing
- ◇ Changement de routage
- ◇ Anomalie ponctuelle
- ◇ Anomalie à long terme

[Passe 4/5]

Ce que voit le Radar : dynamique

Étude prospective



Différents **phénomènes** dynamiques apparaissent :

- ◇ Routeurs paresseux
- ◇ Load-balancing
- ◇ Changement de routage
- ◇ Anomalie ponctuelle
- ◇ Anomalie à long terme

[Passe 5/5]

Identification des phénomènes dynamiques

Étude prospective

Définir des **statistiques** sur les graphes pour isoler et détecter automatiquement ces phénomènes.

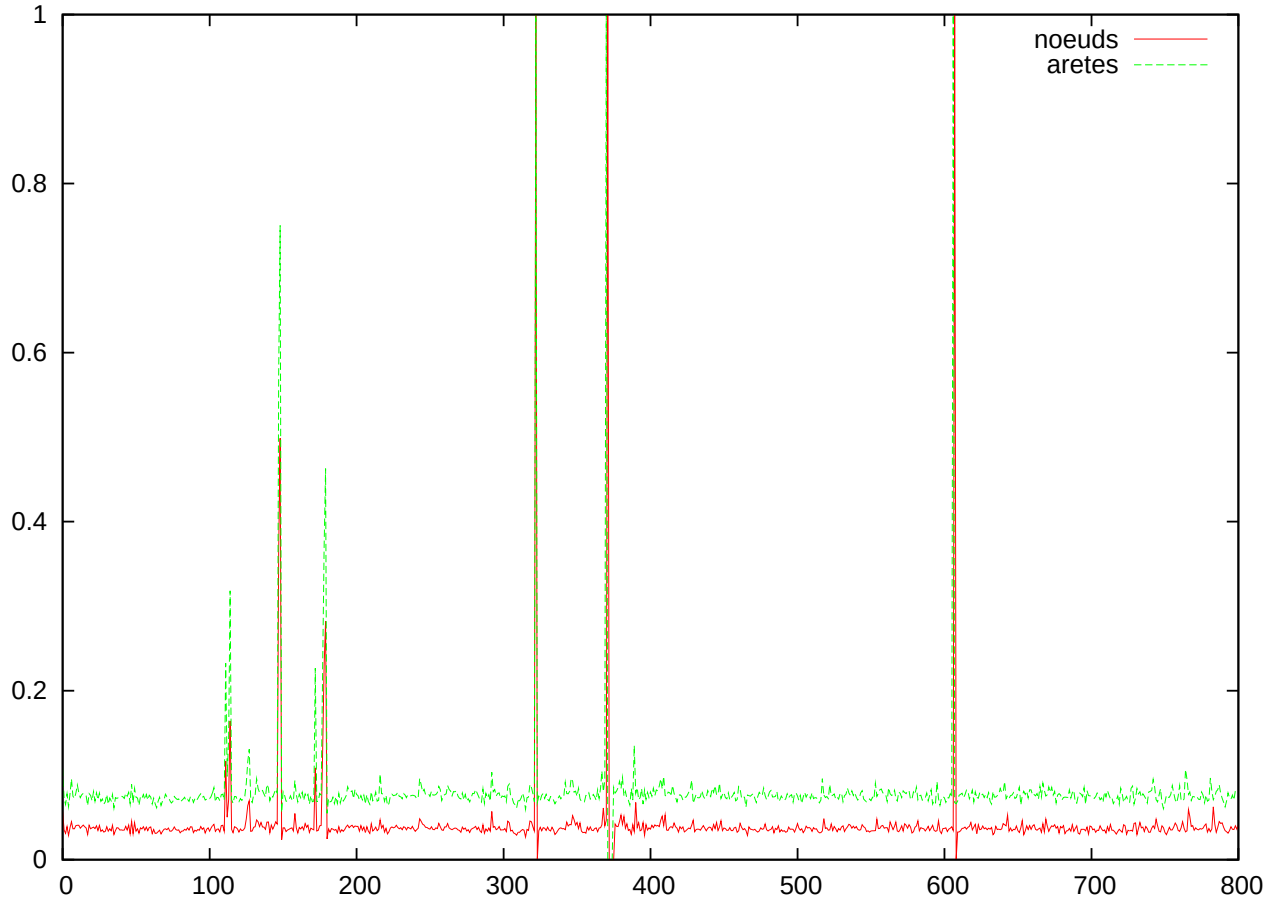
- ◇ Apparition/disparition d'arêtes/de noeuds
- ◇ "Spectre de clignotement" des arêtes
- ◇ Changement de distance d'un noeud
- ◇ Arêtes transverses
- ◇ RTT (Round-Trip Time)
- ◇ ?

Partie IV

Analyse des données

Stats : différences des graphes successifs

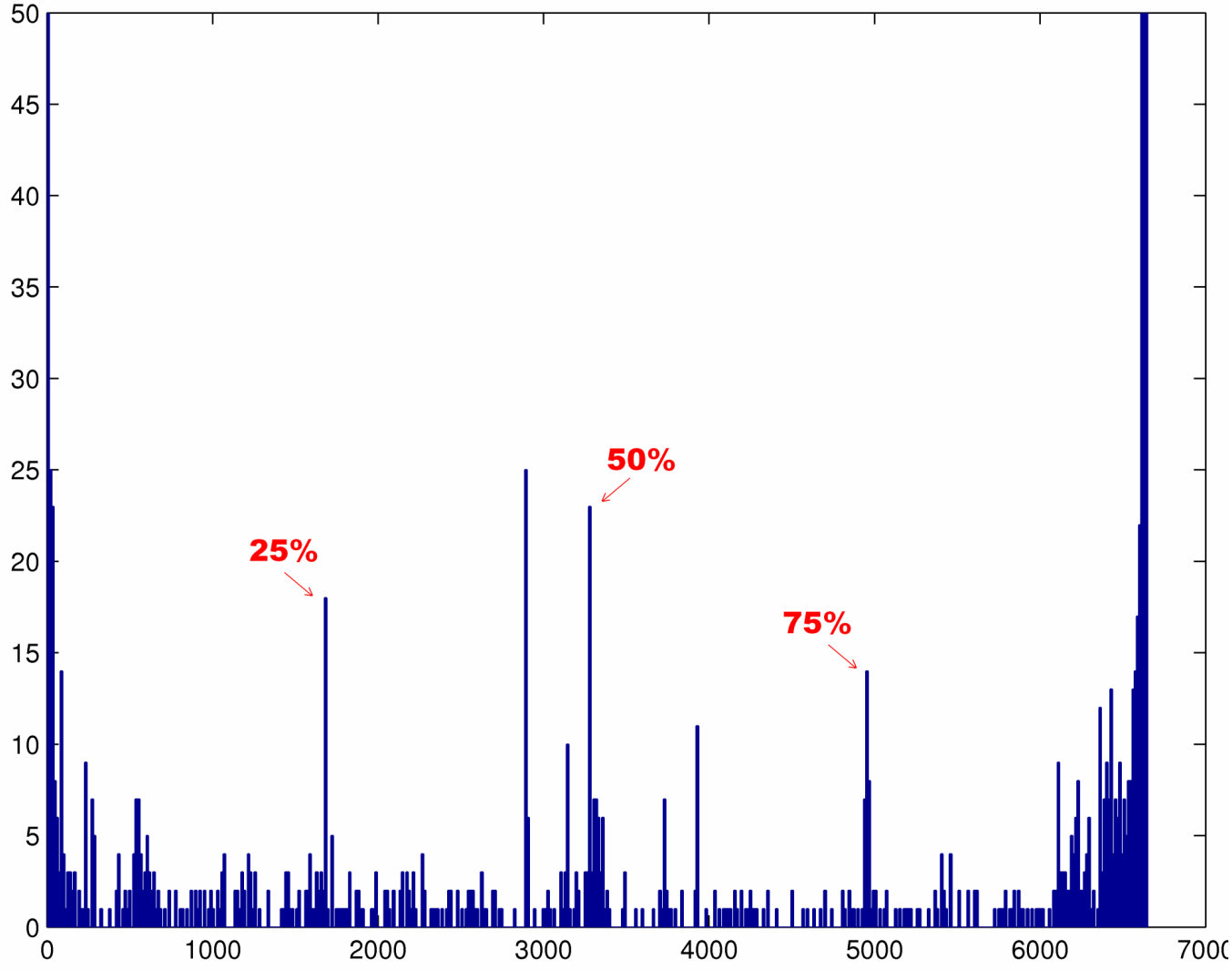
Analyse des données



$$\Delta_{g_t,g_{t+1}} = 4\%, \quad \Delta_{g_0,g_{last}} = 22\%, \quad \Delta_{g_t,G_\infty} = 57\%$$

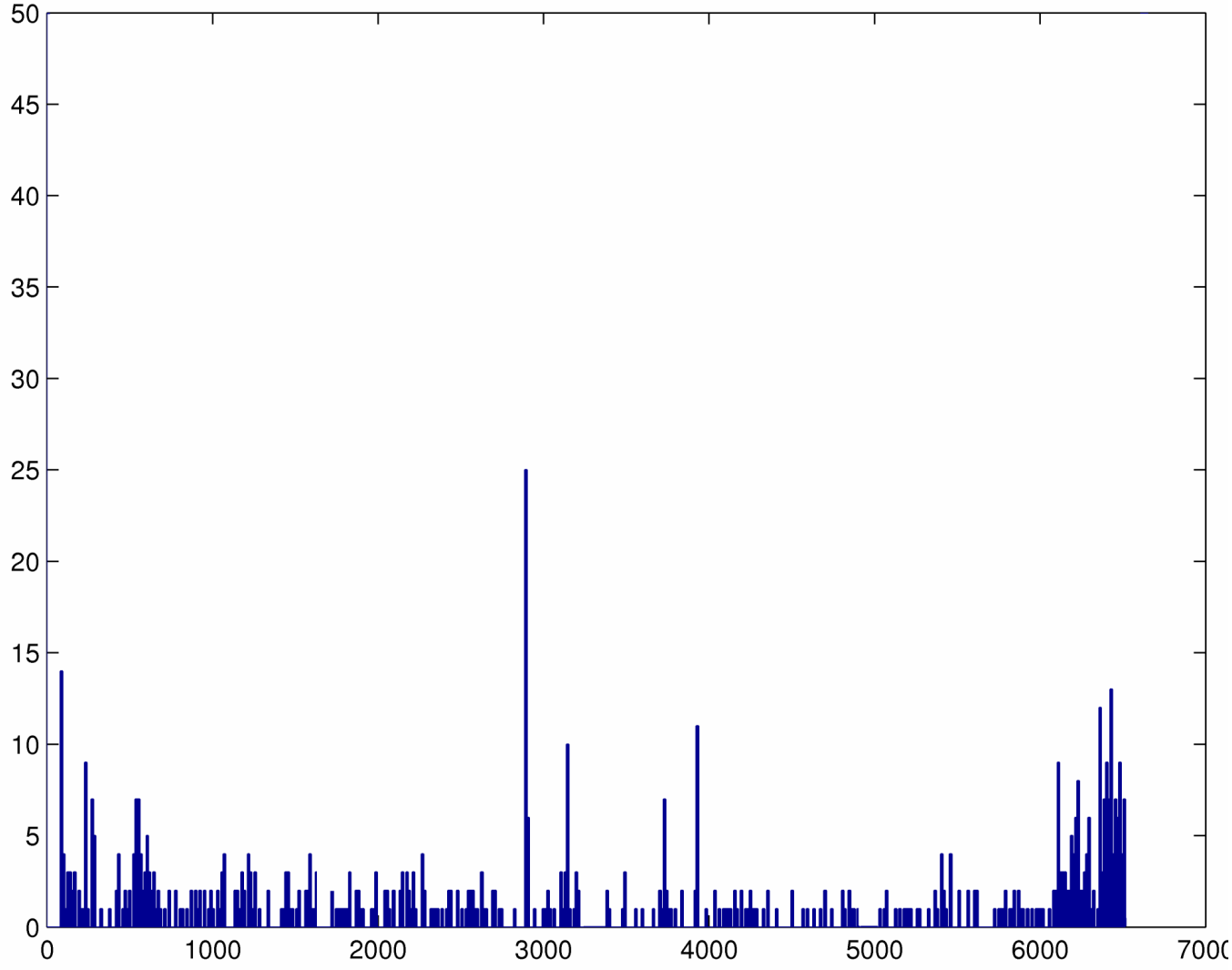
Stats : fréquence d'apparition

Analyse des données



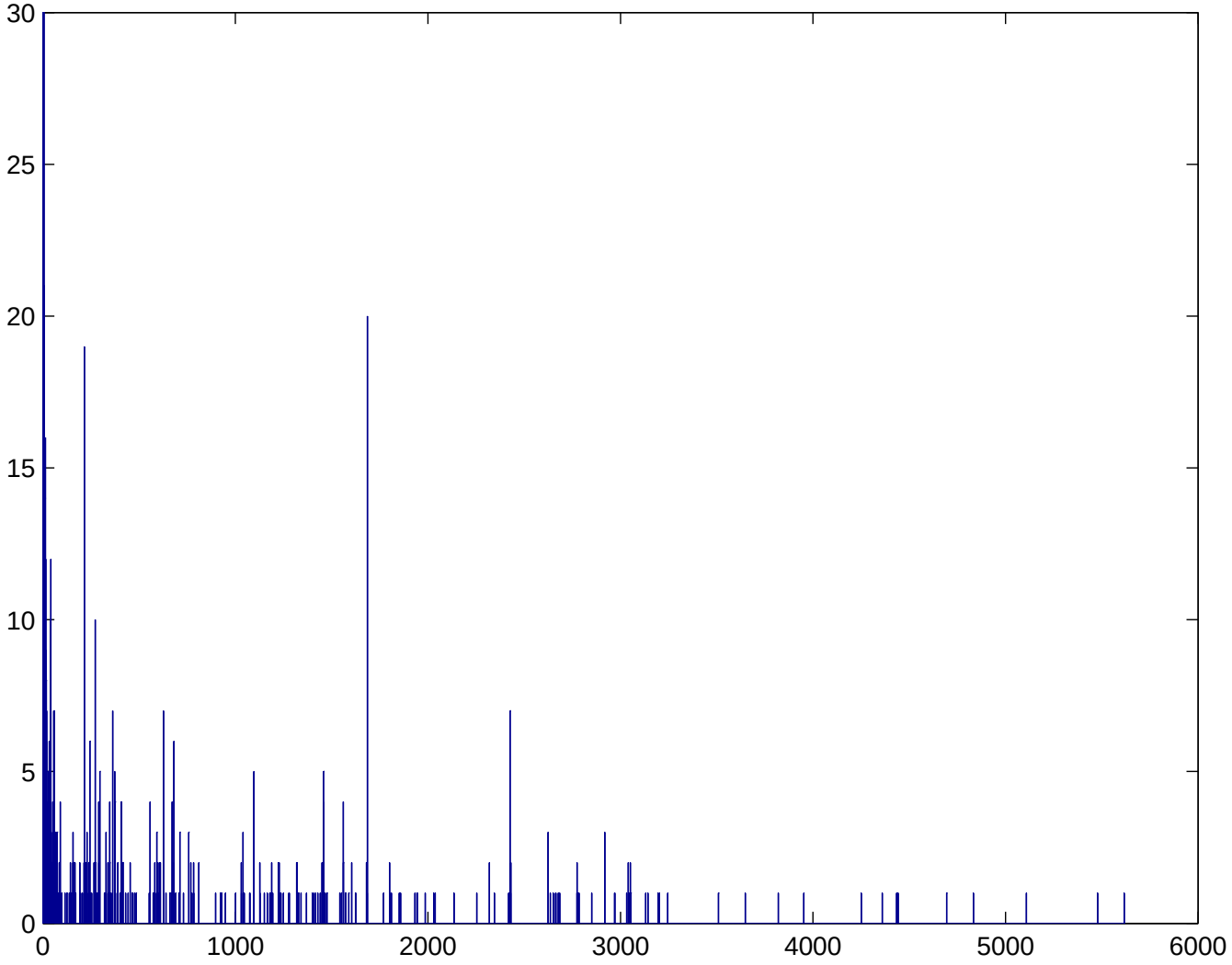
Stats : fréquence d'apparition

Analyse des données



Stats : Spectre de clignotement

Analyse des données



Encore en friche

Analyse de données

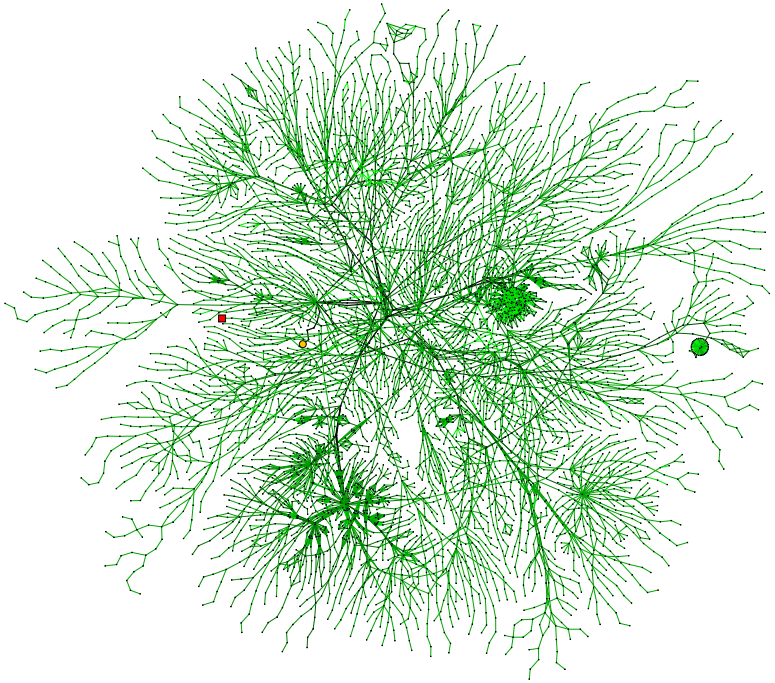
- ▷ Notions d'entropie ou de mesures de la complexité
- ▷ Calibrations à l'aide de simulations d'attaques
- ▷ Trouver d'autres grandeurs dynamiques intéressantes
- ▷ Évaluer la ou les bonnes résolution(s) temporelle(s)

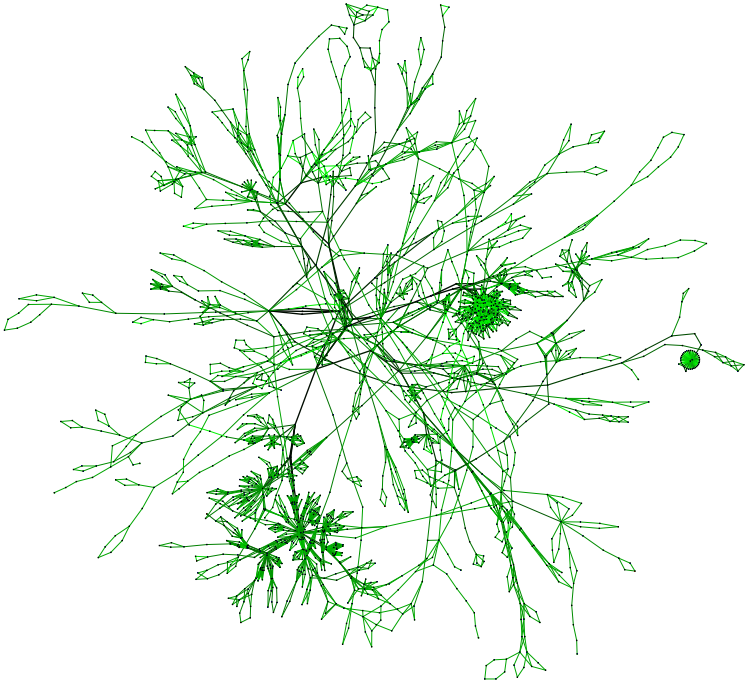
Partie V

Réductions de graphe

Réductions de graphe

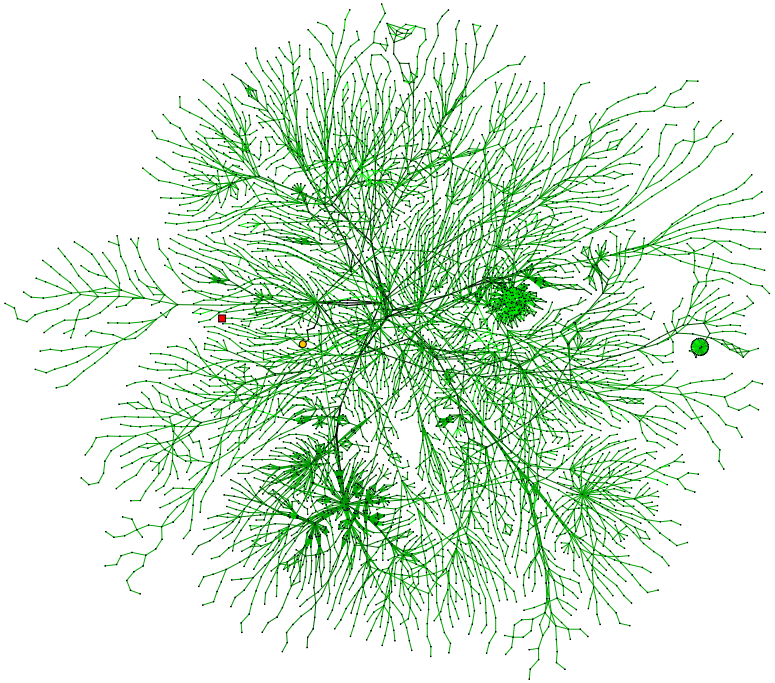
Réduction du graphe : Enlever les feuilles

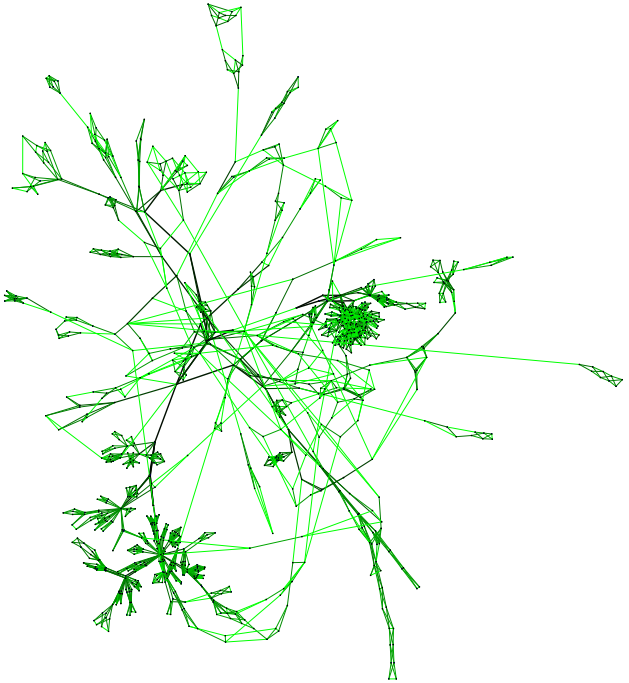




Réductions de graphe

Réduction du graphe : Raccourcir les branches





Réductions de graphe

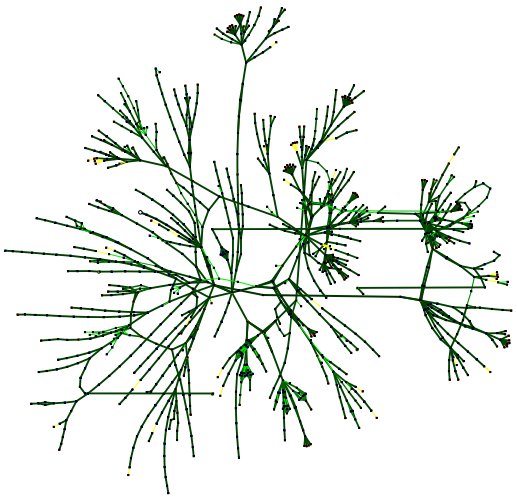
Réduction du graphe ...

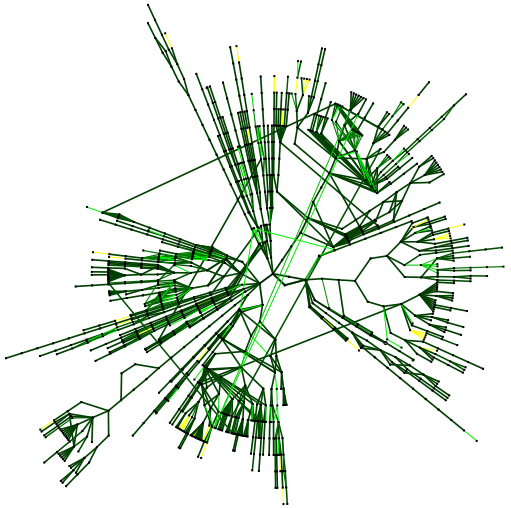
- ◇ Enlever les feuilles
- ◇ Raccourcir les branches
- ◇ Fusionner des noeuds (interfaces d'un unique routeur)
- ◇ Regrouper les cliques en un unique noeud
- ◇ etc..

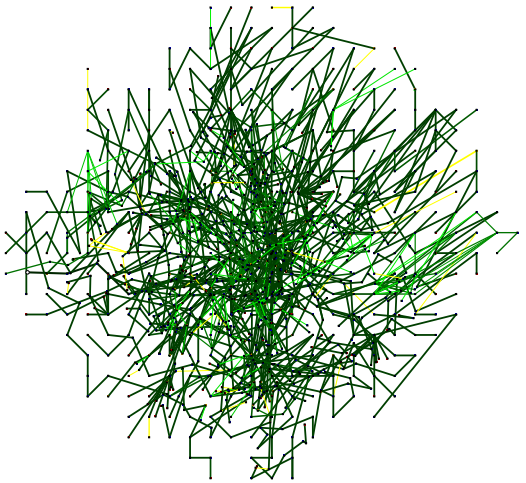
... Mais sans perdre trop d'information !

▷ Les réductions peuvent également aider à la détection automatique

Réorganisations du graphe







Le grâal : placement géographique ?

Bilan : jeune...

- Ce qui a été réalisé :
  - Implémentation provisoire
  - Optimisations de la politique de scan
  - Observations, statiques et dynamiques
  - Premiers traitements automatiques des données

Bilan : jeune...

▷ Ce que l'on peut en tirer :

- ◇ En termes pratiques, le radar tient ses promesses : simple, rapide et économe en ressources.
- ◇ La complexité de la topologie `IP` – statique ou dynamique – ne peut être négligée.
- ◇ La visualisation est en elle-même un outil à part entière, permettant à la fois de surveiller le réseau en temps réel mais aussi de comprendre quelles sont les conséquences d'un défaut de service sur le routage.
- ◇ La détection automatique d'anomalies est encore loin d'égaler l'expertise humaine

Bilan : jeune... mais prometteur !

- ▷ Outils : Monitoring (assisté ?) + Détection automatique
- ▷ Développements futurs :
  - ◇ Parallélisme
  - ◇ Intégration de mesures de qualité de service (RTT)
  - ◇ Plateformes permettant de simuler des pannes ou attaques d'envergure.

Merci pour votre attention