

La Prochaine Génération de Plateformes de Collecte de Données BGP

Thomas Holterbach
Université de Strasbourg

FRNOG
Vendredi 27 Septembre 2024

En collaboration avec:

Thomas Alfroy

Thomas Krenc

KC Claffy

Cristel Pelsser



Gérer BGP, c'est un peu comme conduire une voiture:
il faut **observer**, **analyser** et maîtriser les **facteurs extérieurs**



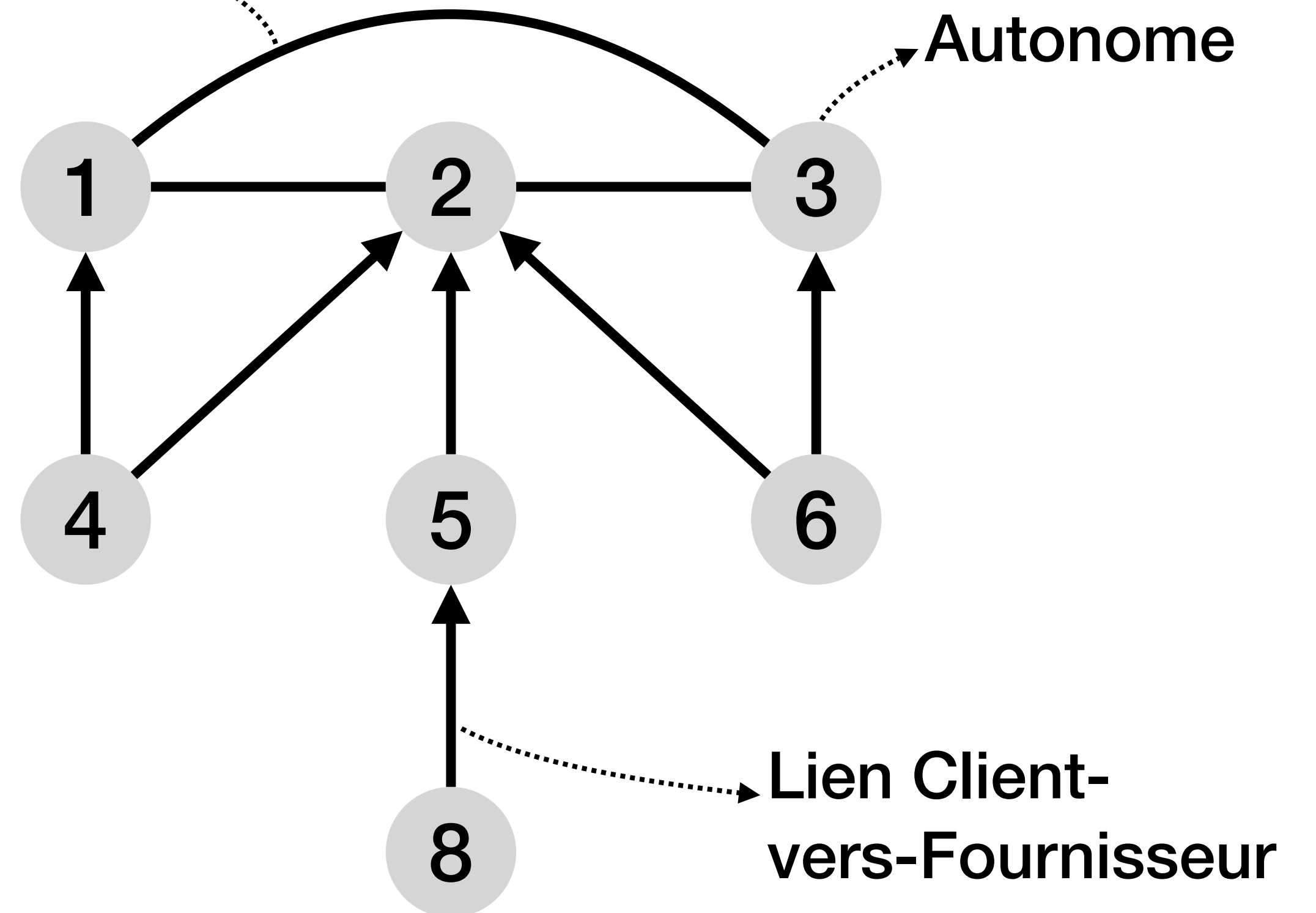
Heureusement, en voiture nous pouvons avoir une bonne visibilité



Pour obtenir de la visibilité sur BGP, il y a des archives publiques de routes BGP, maintenues par RIPE RIS, RouteViews et PCH

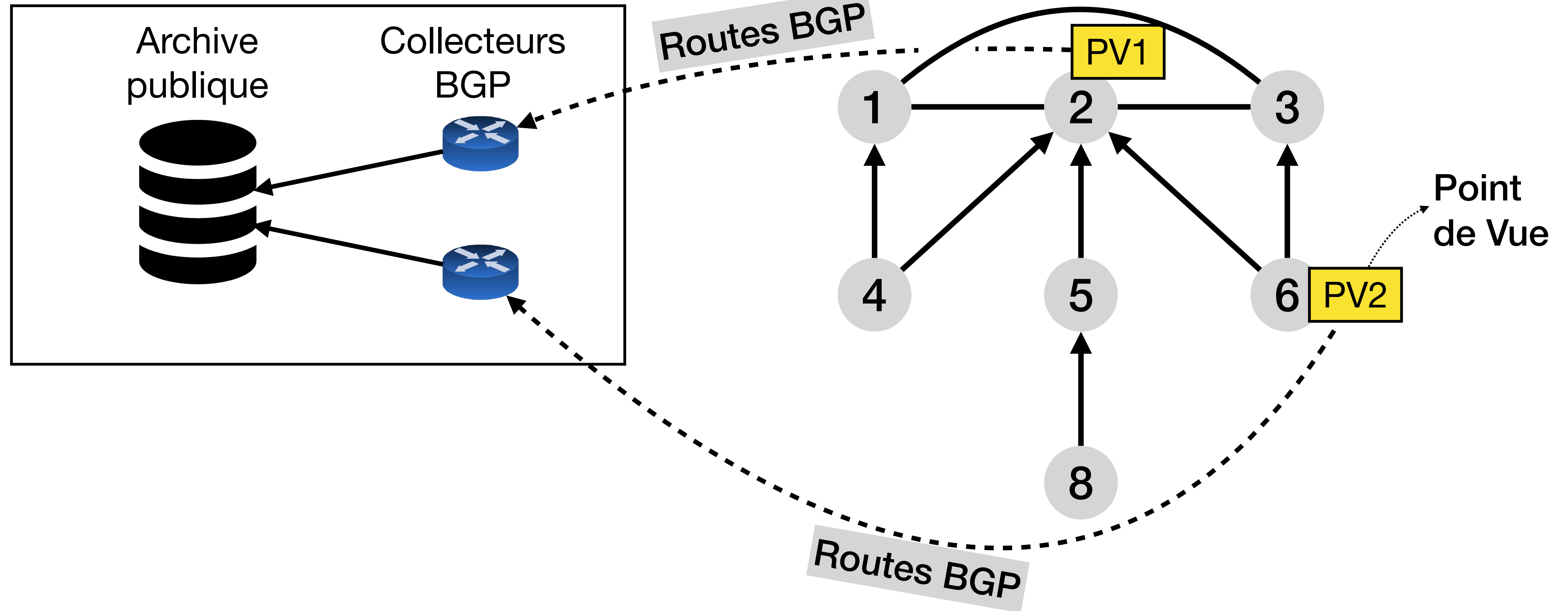
Lien peer-vers-peer

Systeme
Autonome



Pour obtenir de la visibilité sur BGP, il y a des archives publiques de routes BGP, maintenues par RIPE RIS, RouteViews et PCH

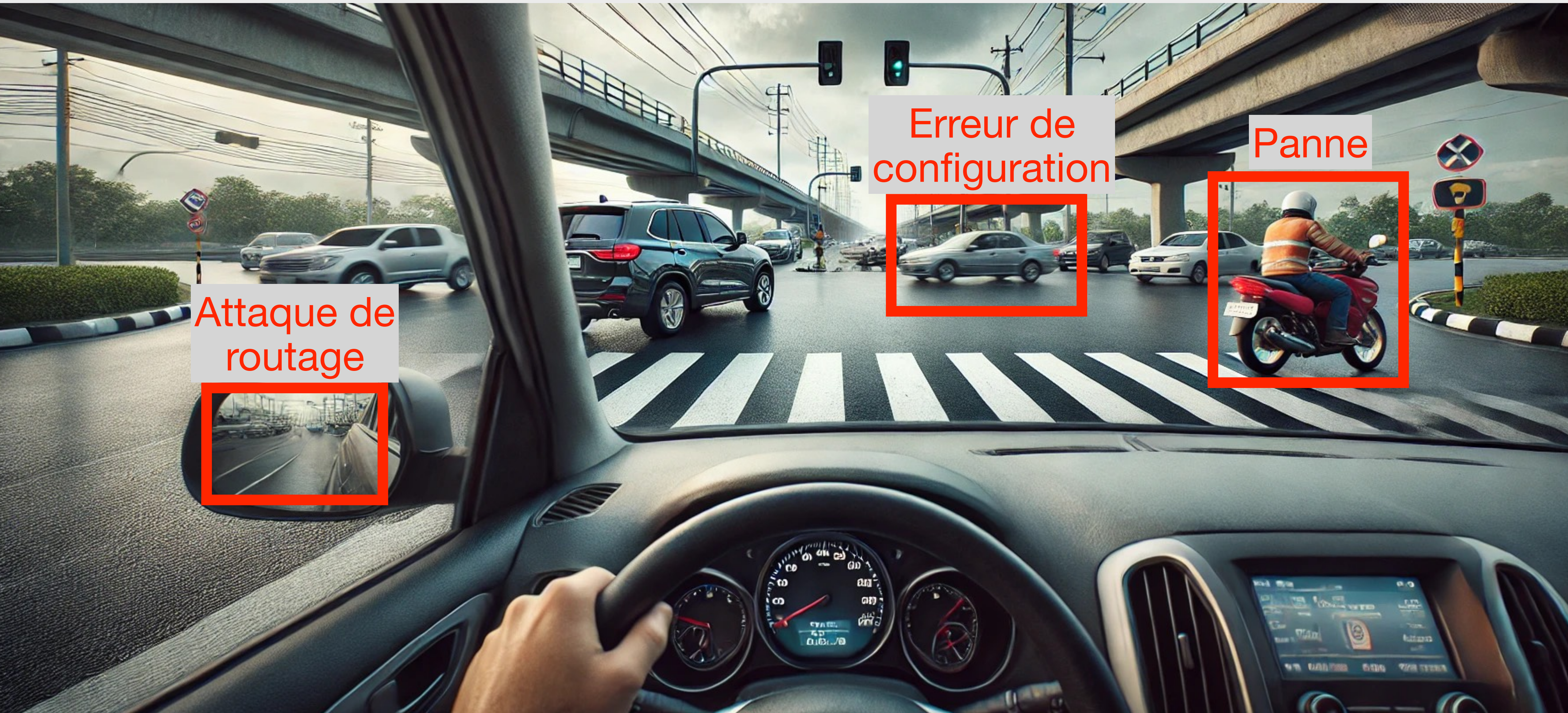
Plateforme de collection



Comme pour la conduite en voiture,
beaucoup de situations critiques peuvent survenir avec BGP



Comme pour la conduite en voiture,
beaucoup de situations critiques peuvent survenir avec BGP



Attaque de
routage

Erreur de
configuration

Panne

Heureusement, il existe des outils de surveillance BGP qui exploitent les archives de routes BGP pour détecter ces problèmes

Projets de recherche



Outils commerciaux



catchpoint.



1.2%

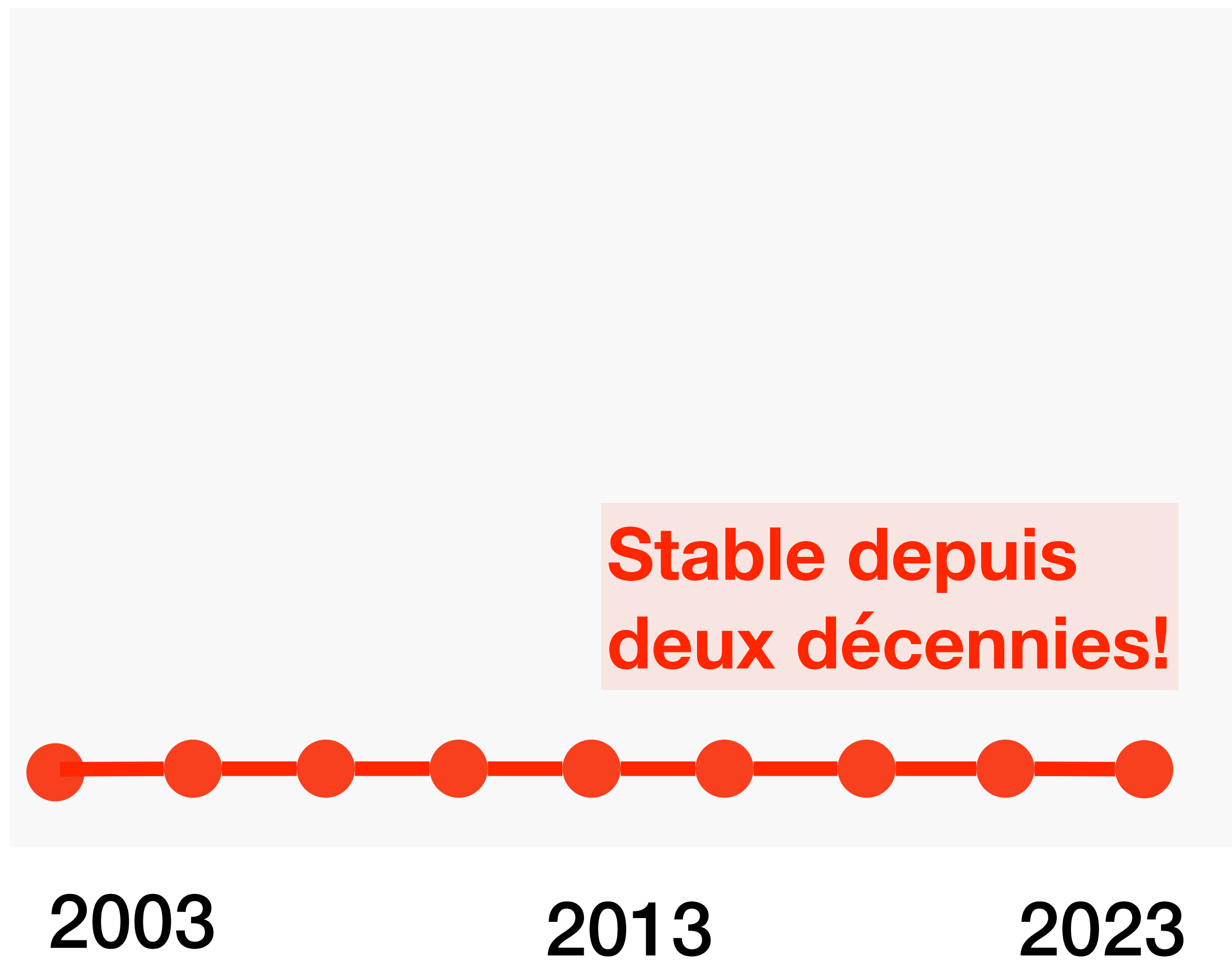
**% d'AS partageant
leur données BGP**
(RIS+RouteViews)

— **1.2%**

**% d'AS partageant
leur données BGP**
(RIS+RouteViews)

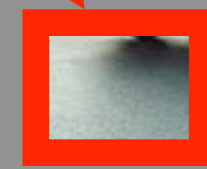
1.2%

100%



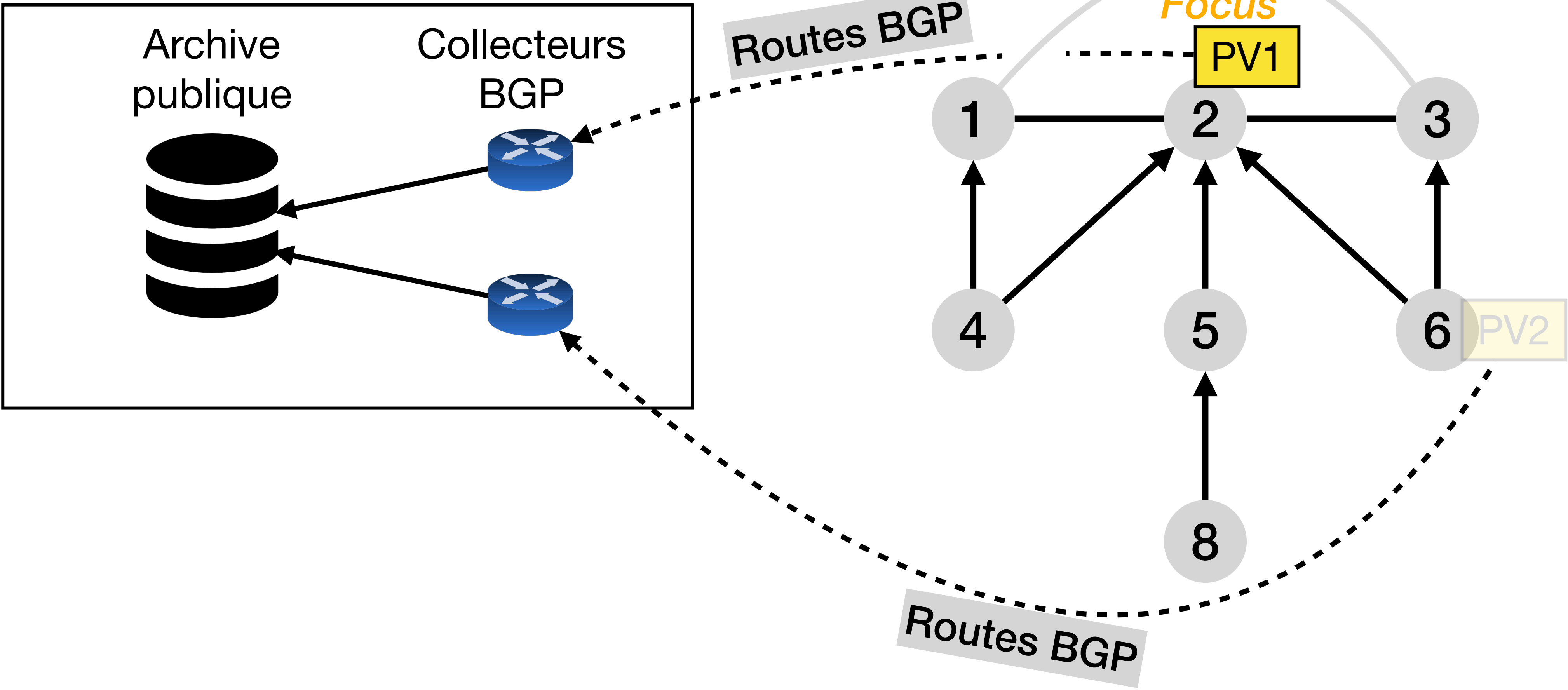
Heureusement, un point de vue a une large vue sur les informations BGP

1.2% de visibilité



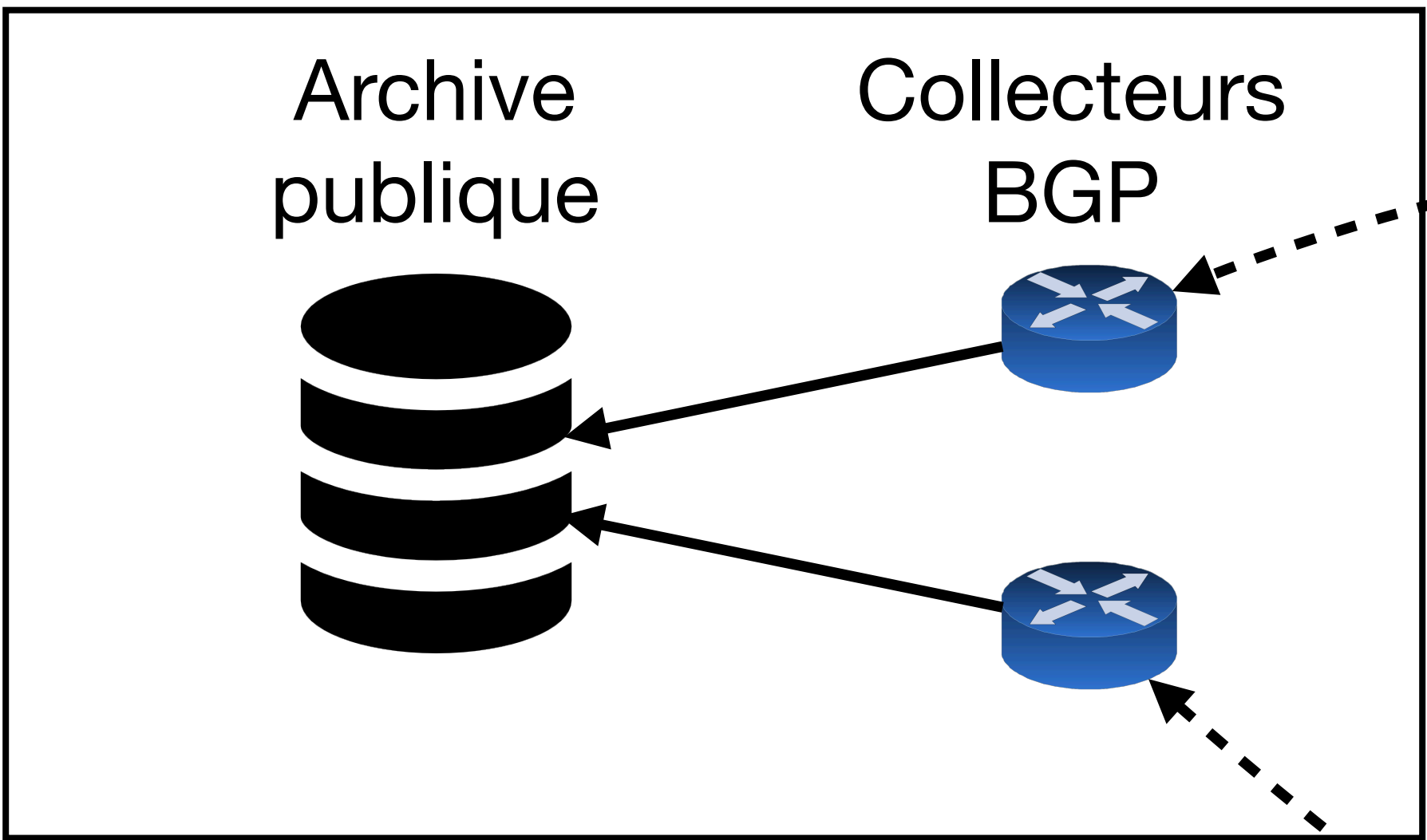
PV1 voit tout les liens sauf 1 — 3

Plateforme de collection

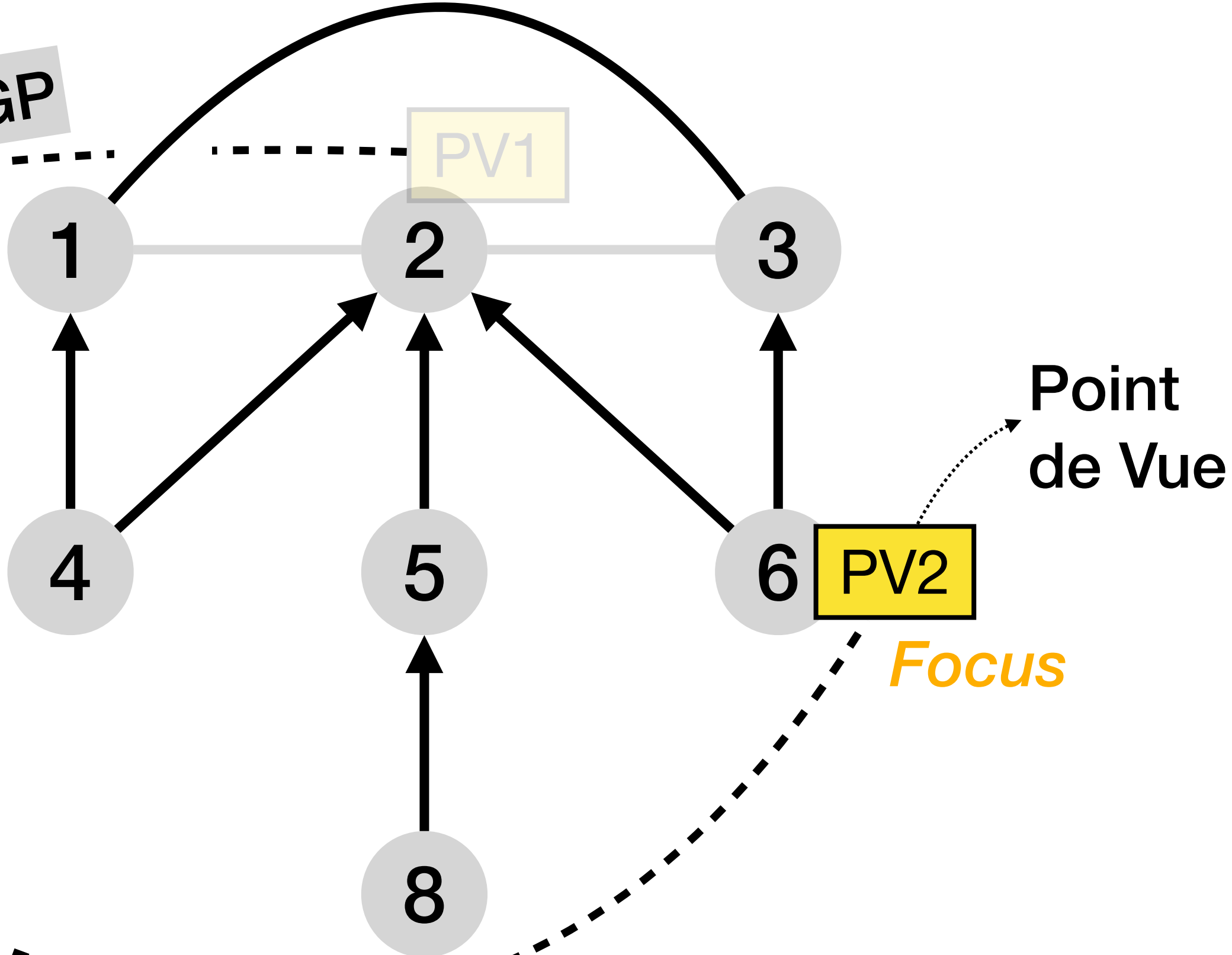


PV2 voit tout les liens sauf 1—2 et 2—3

Plateforme de collection



Routes BGP



Aujourd'hui, on ne sait pas a quel point
notre vue sur le routage BGP est complete

**10% de
visibilité?**



Aujourd'hui, on ne sait pas a quel point
notre vue sur le routage BGP est complete

20% de
visibilité?



Aujourd'hui, on ne sait pas a quel point
notre vue sur le routage BGP est complete

50% de
visibilité?



On mesure l'impact de la faible couverture de PV de RIS et RouteViews sur deux cas pratiques en utilisant des **simulations***

Cas pratique #1: Identification des liens de peer-to-peer

Cas pratique #2: Détection de “forged-origin” hijack

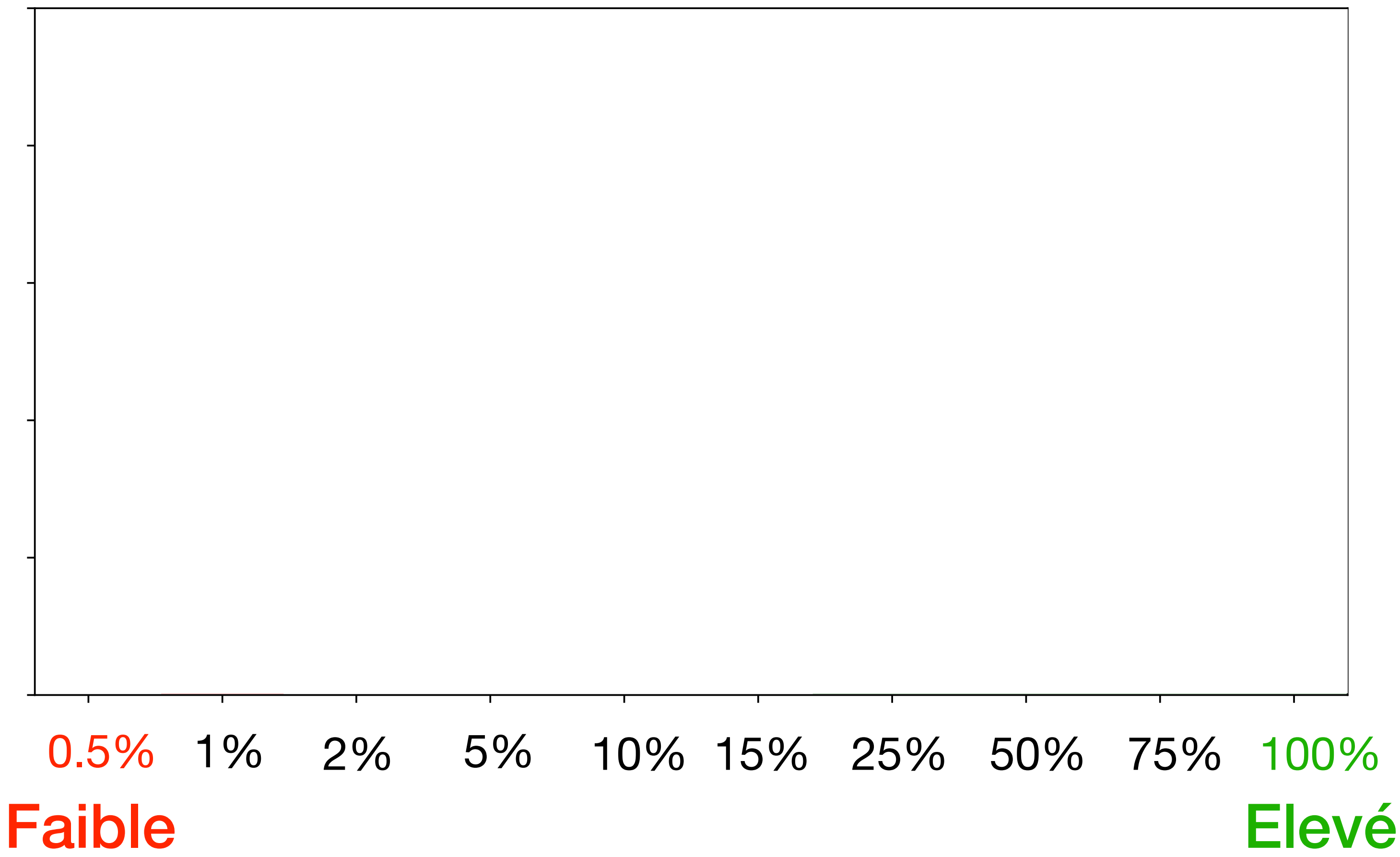
*Nos simulations utilisent c-bgp sur des topologies avec 6k ASes

On mesure l'impact de la faible couverture de PV de RIS et RouteViews sur deux cas pratiques en utilisant des **simulations***

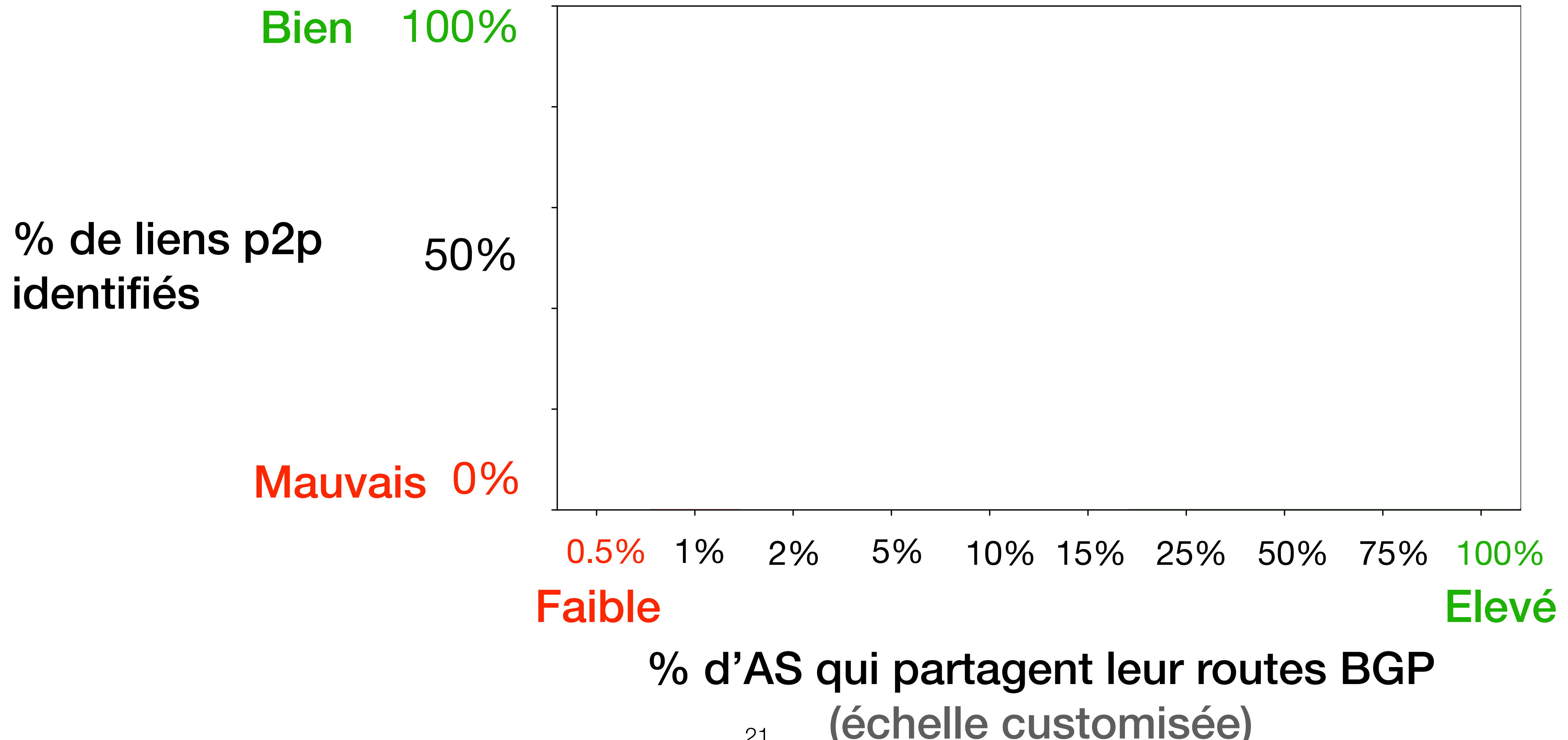
Cas pratique #1: Identification des liens de peer-to-peer

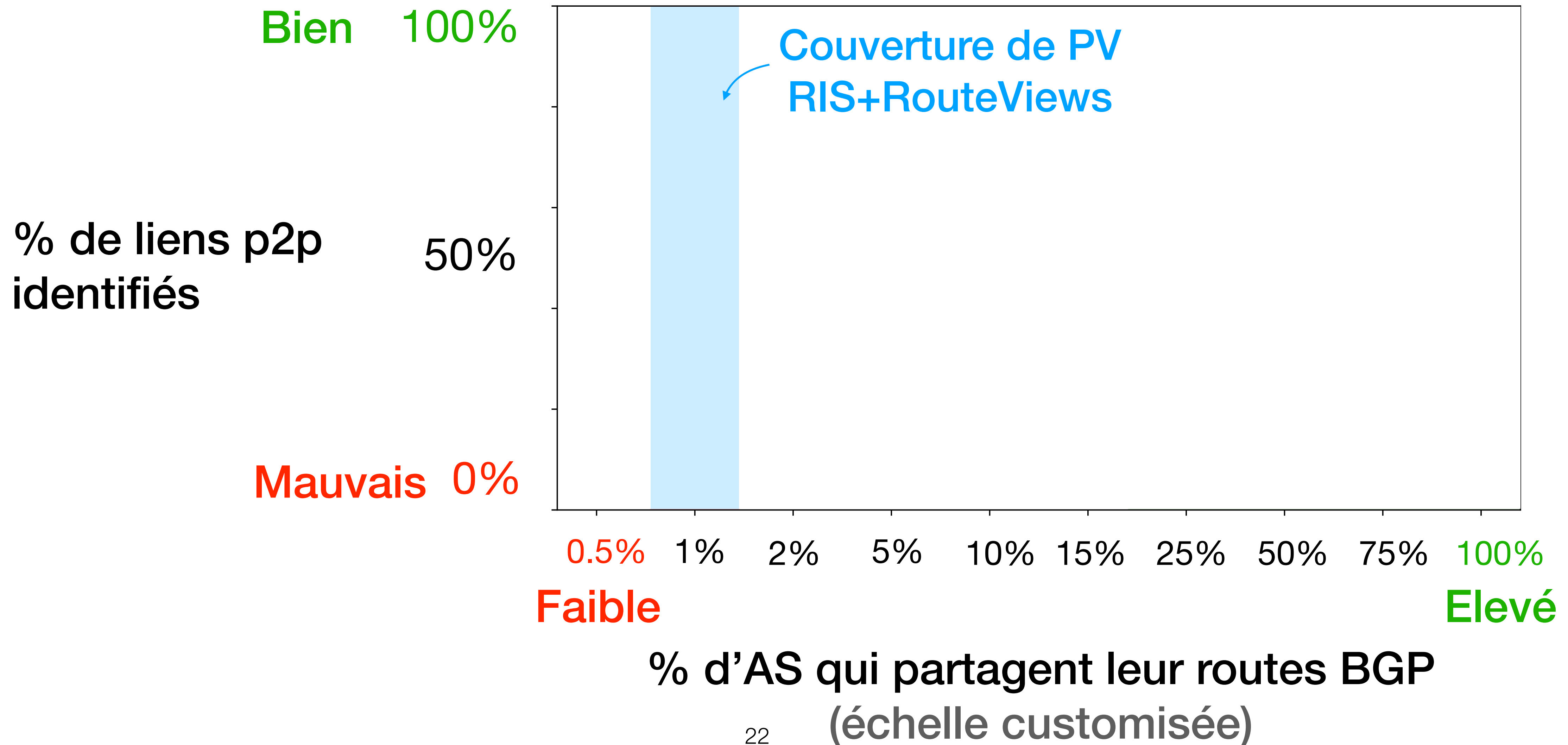
Cas pratique #2: Détection de “forged-origin” hijack

*Nos simulations utilisent c-bgp sur des topologies avec 6k ASes

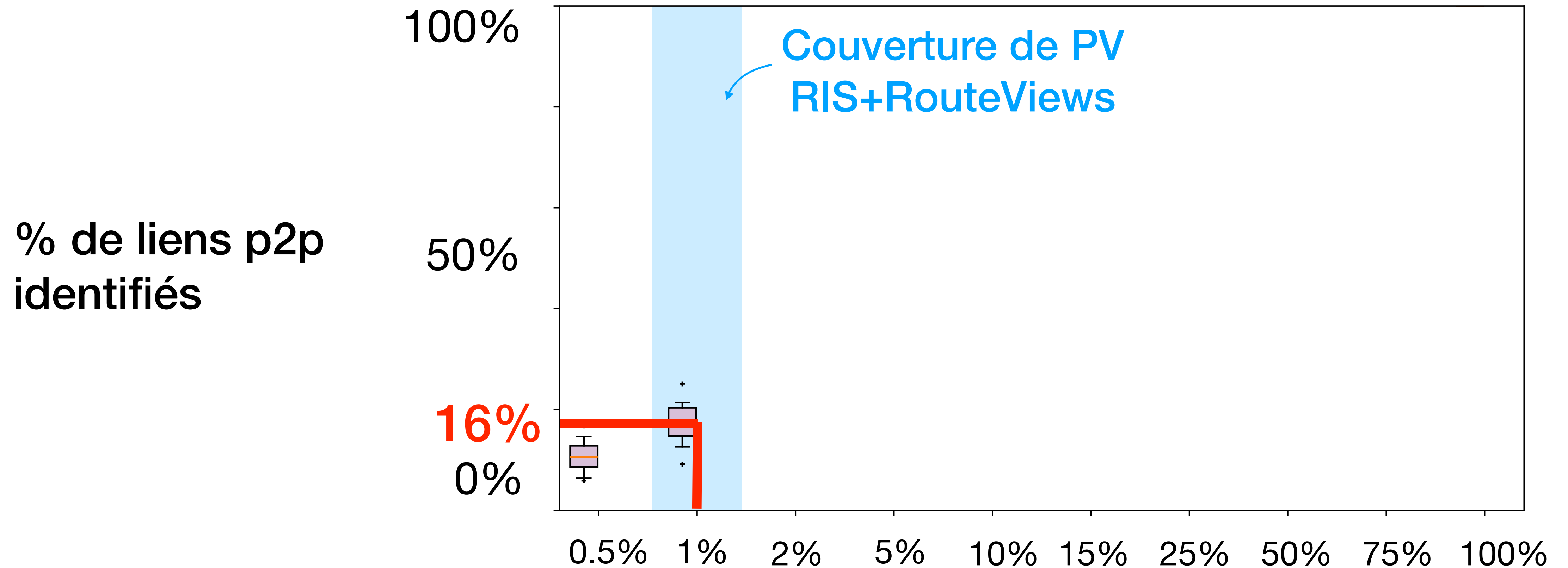


% d'AS qui partagent leur routes BGP
(échelle customisée)





Nos simulations montrent qu'on identifie ~16% des liens de p2p



Resultats de 10 simulations sur des "mini" Internets avec 6k ASes

% d'AS qui partagent leur routes BGP (échelle customisée)

Si l'objectif est d'identifier les liens p2p,
notre visibilité reste très limitée, à seulement 16 %

**16% de
visibilité**



On mesure l'impact de la faible couverture de PV de RIS et RouteViews sur deux cas pratiques en utilisant des **simulations***

Cas pratique #1: Identification des liens de peer-to-peer

Cas pratique #2: Détection de “forged-origin” hijack

*Nos simulations utilisent c-bgp sur des topologies avec 6k ASes

Si l'objectif est de détecter les forged-origin hijacks, notre visibilité est insuffisante, avec un taux de détection de 74 %

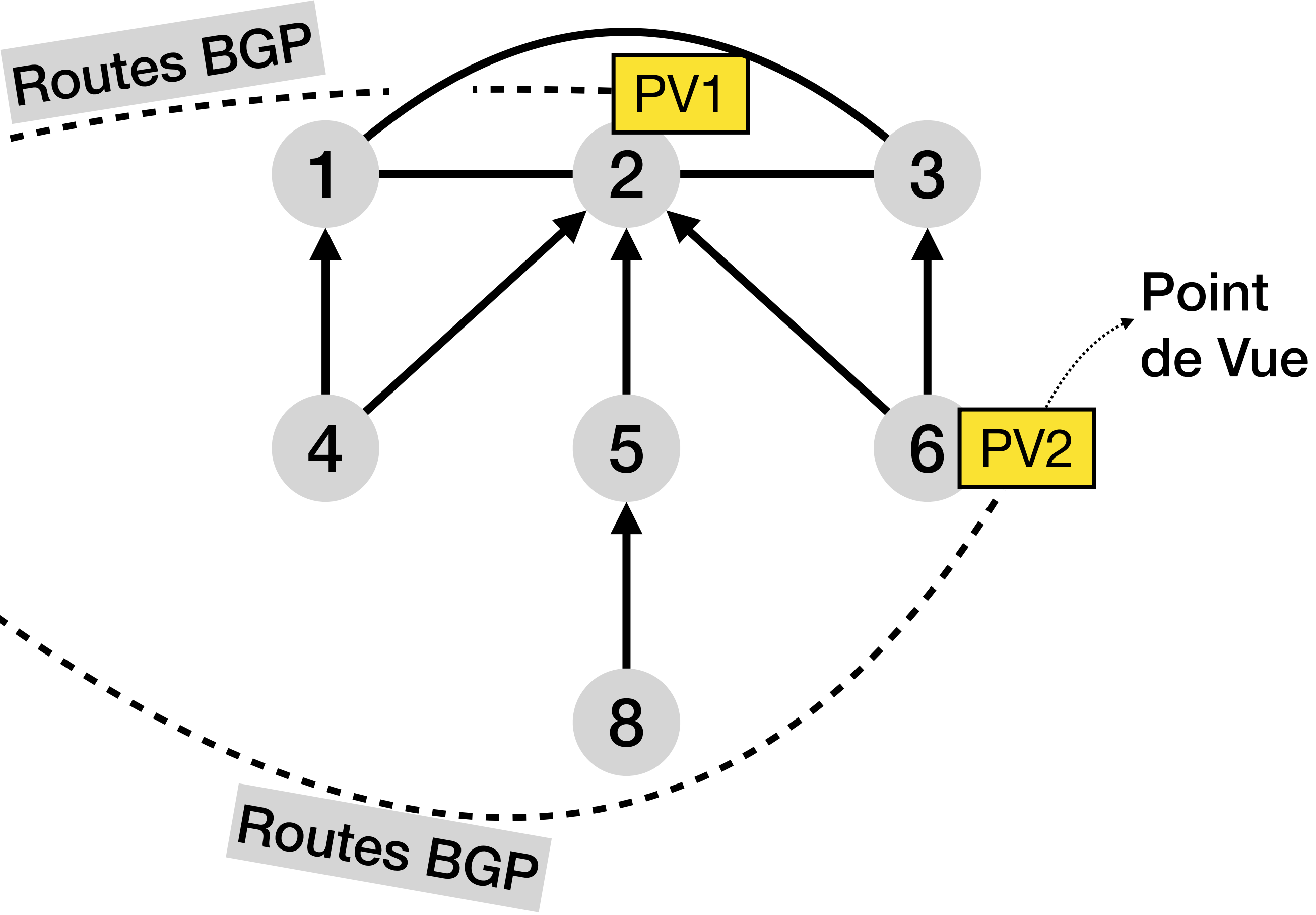
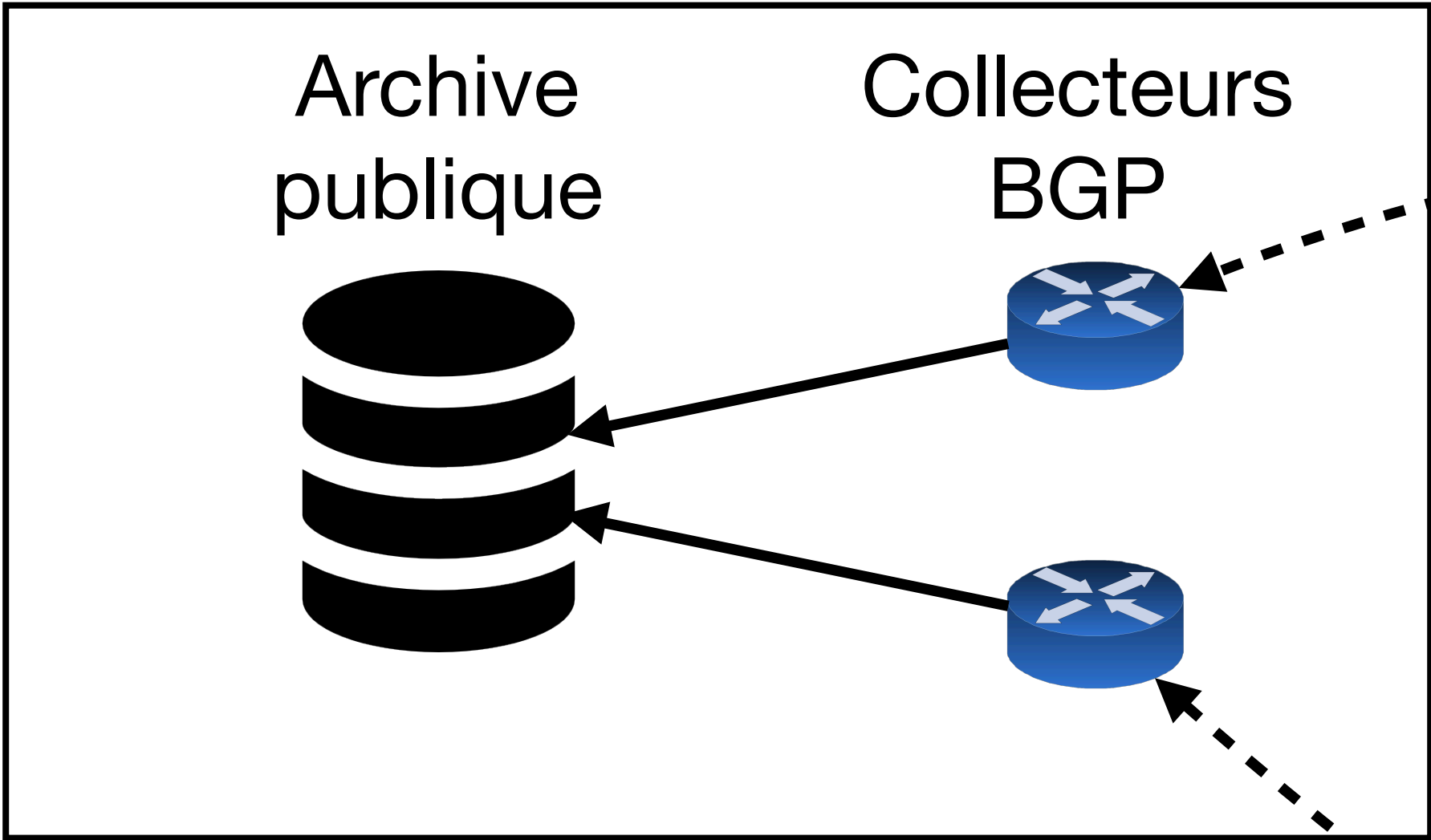
74% de
visibilité



Ne pourrions-nous pas simplement **augmenter**
le nombre de points de vue ?

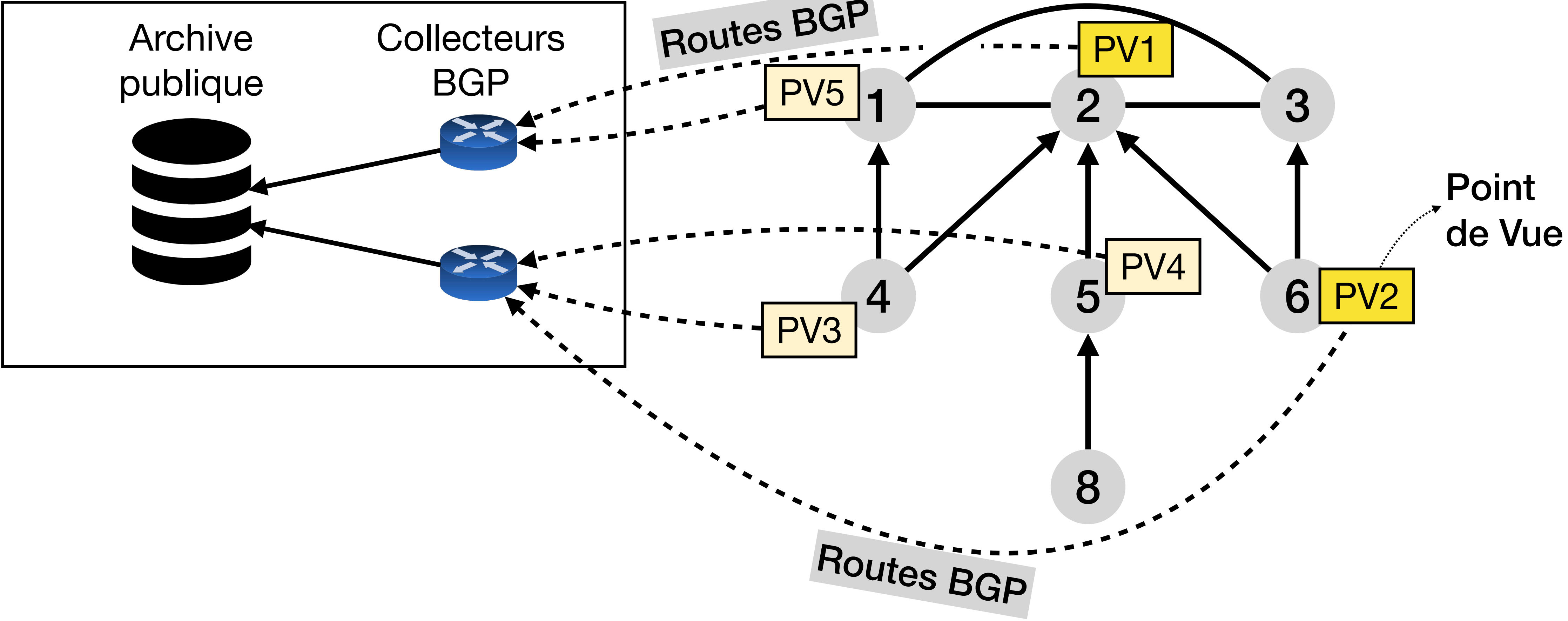
Ne pourrions-nous pas simplement **augmenter** le nombre de points de vue ?

Plateforme de collection

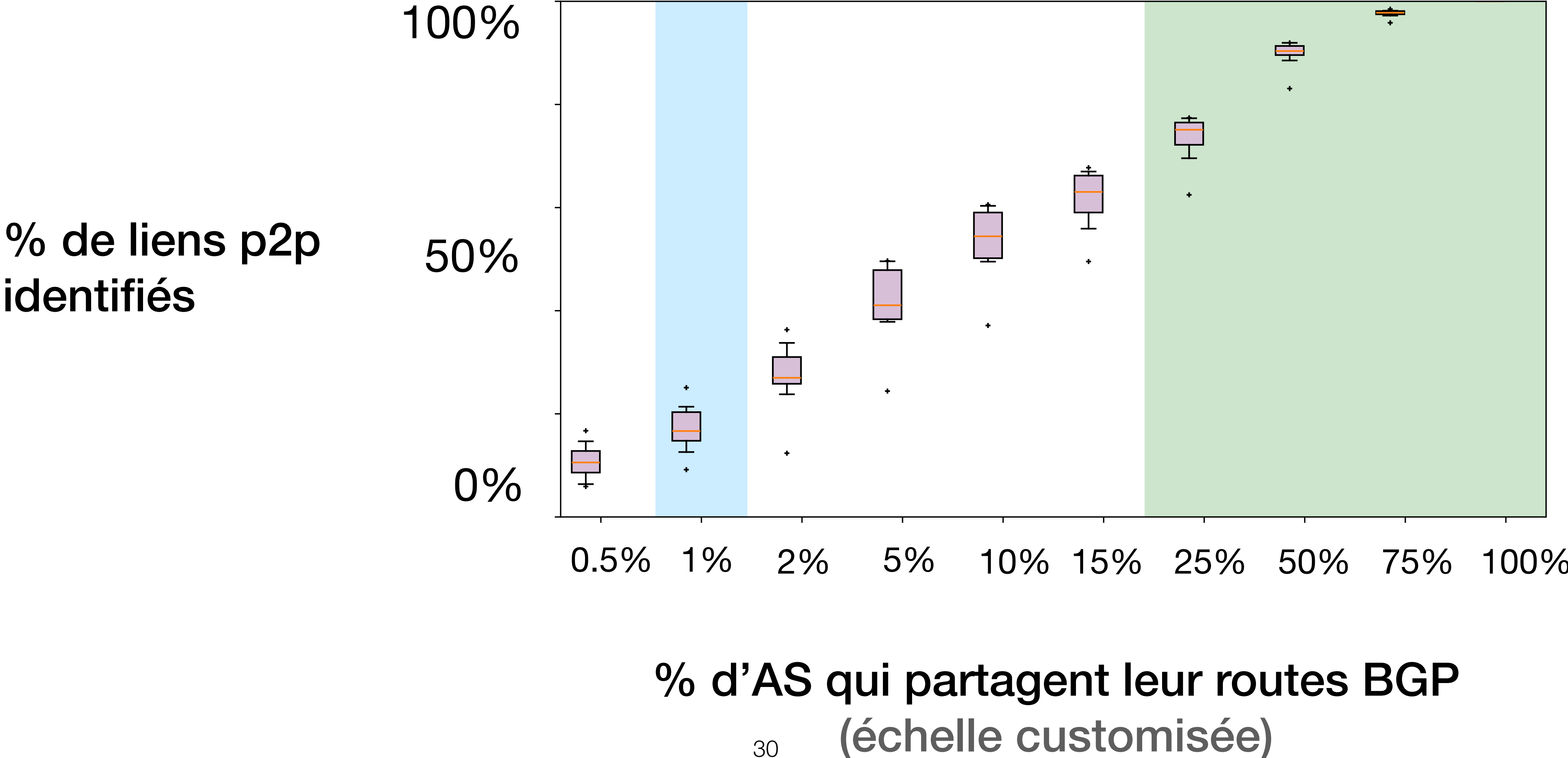


Ne pourrions-nous pas simplement **augmenter** le nombre de points de vue ?

Plateforme de collection



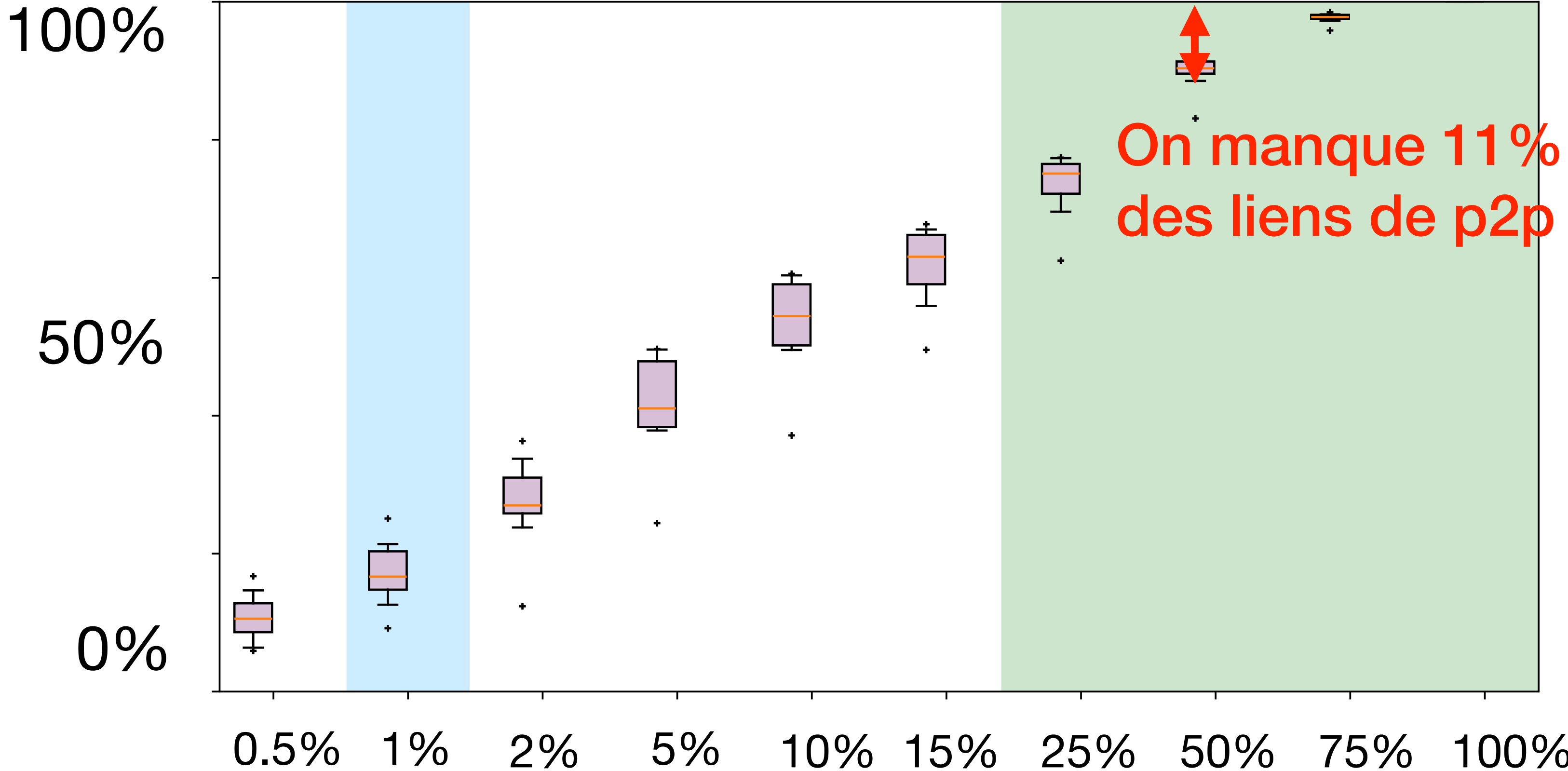
Nos simulations suggèrent
une couverture de PV **20x plus élevée**



Nos simulations suggèrent
une couverture de PV **20x plus élevée**

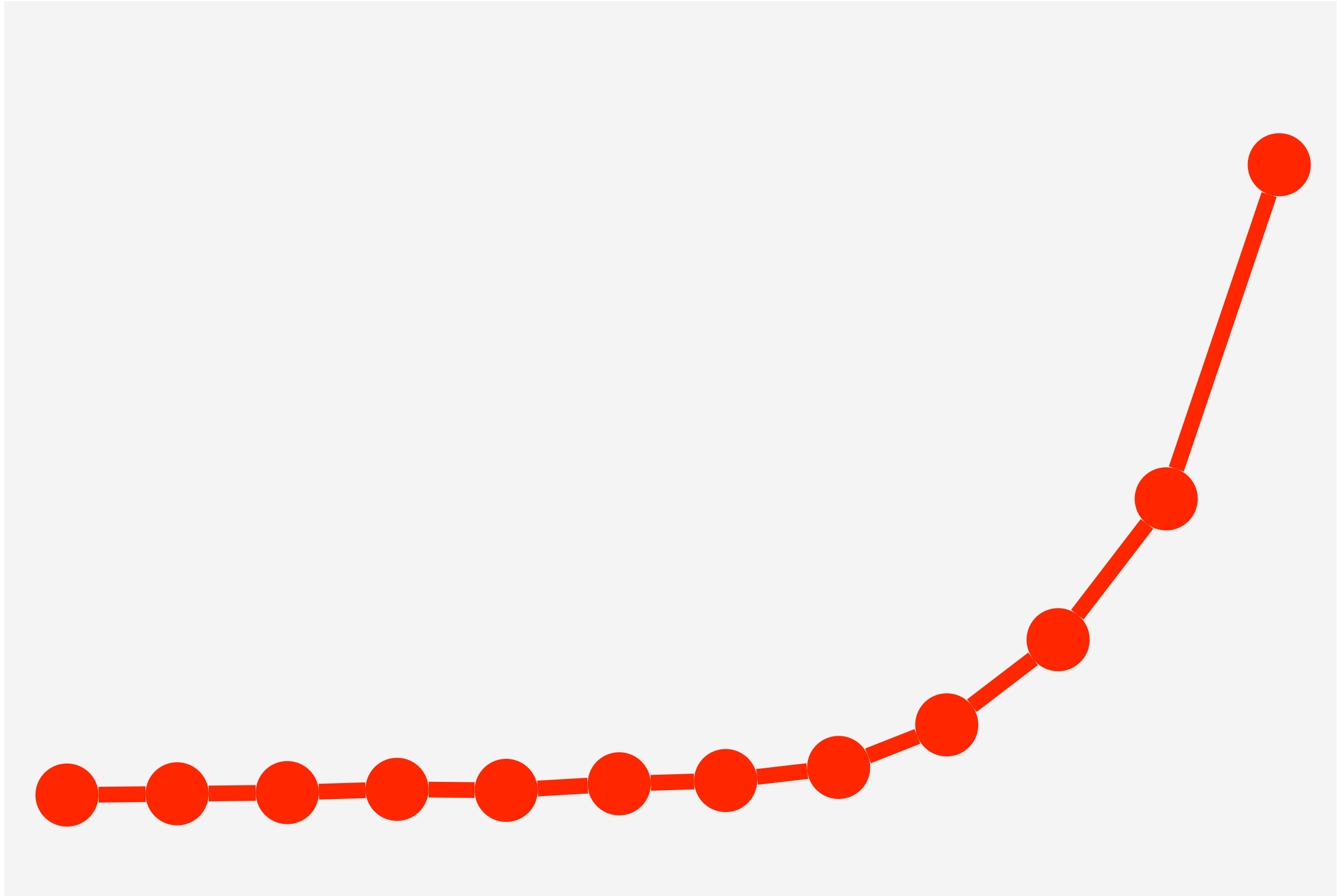
Couverture de VP
suggérée

% de liens p2p
identifiés

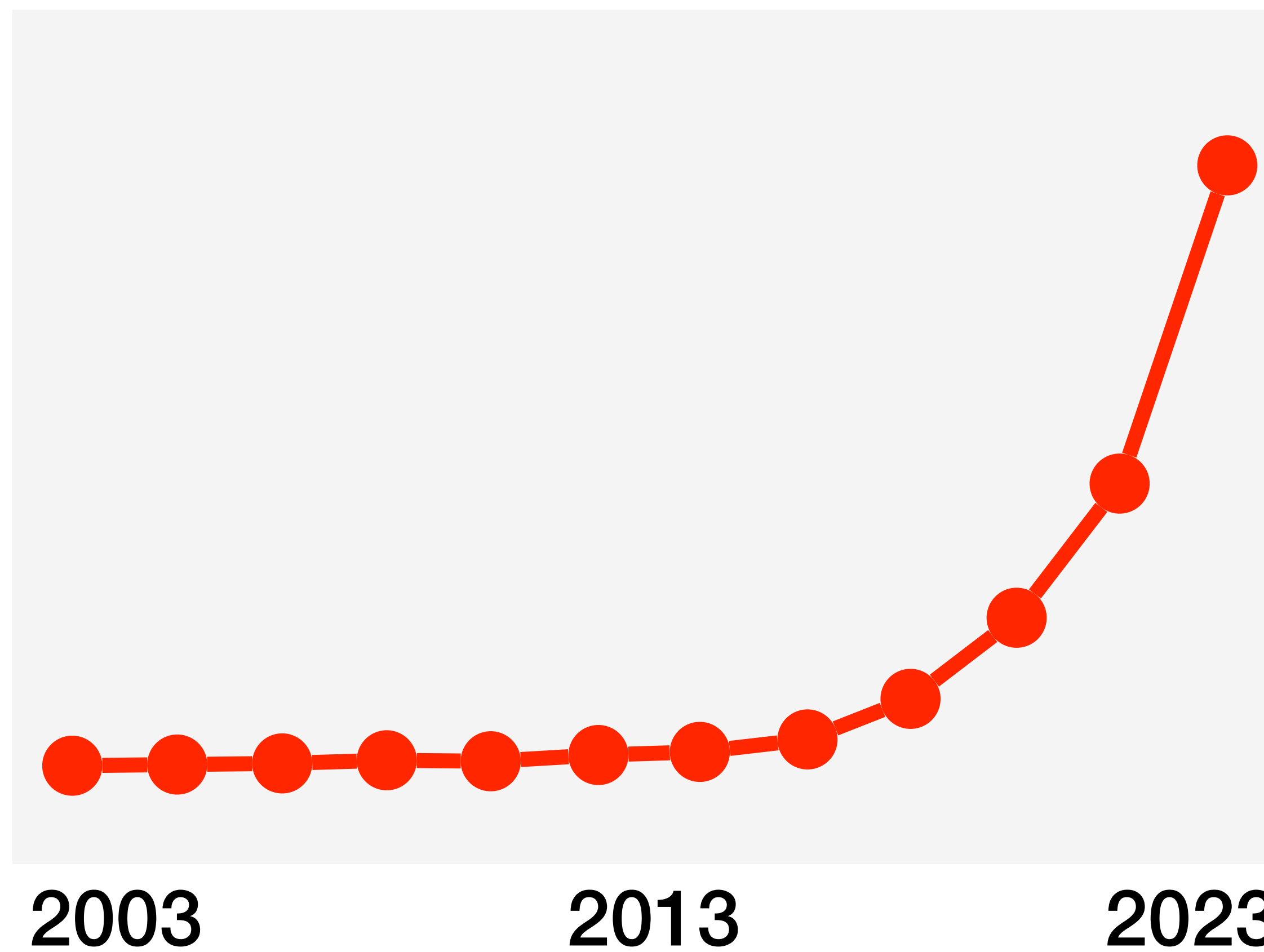


On manque 11%
des liens de p2p

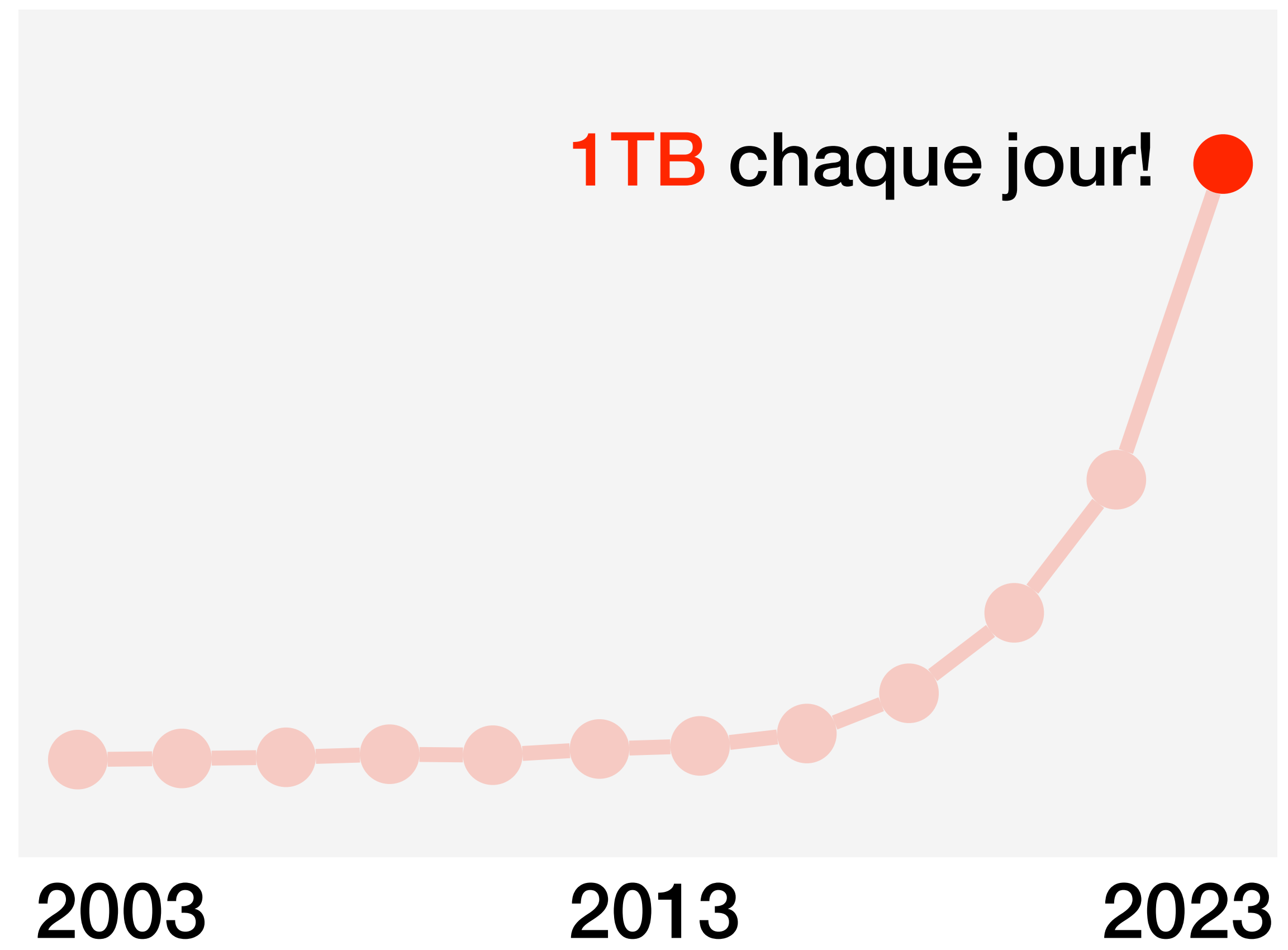
% d'AS qui partagent leur routes BGP
(échelle customisée)



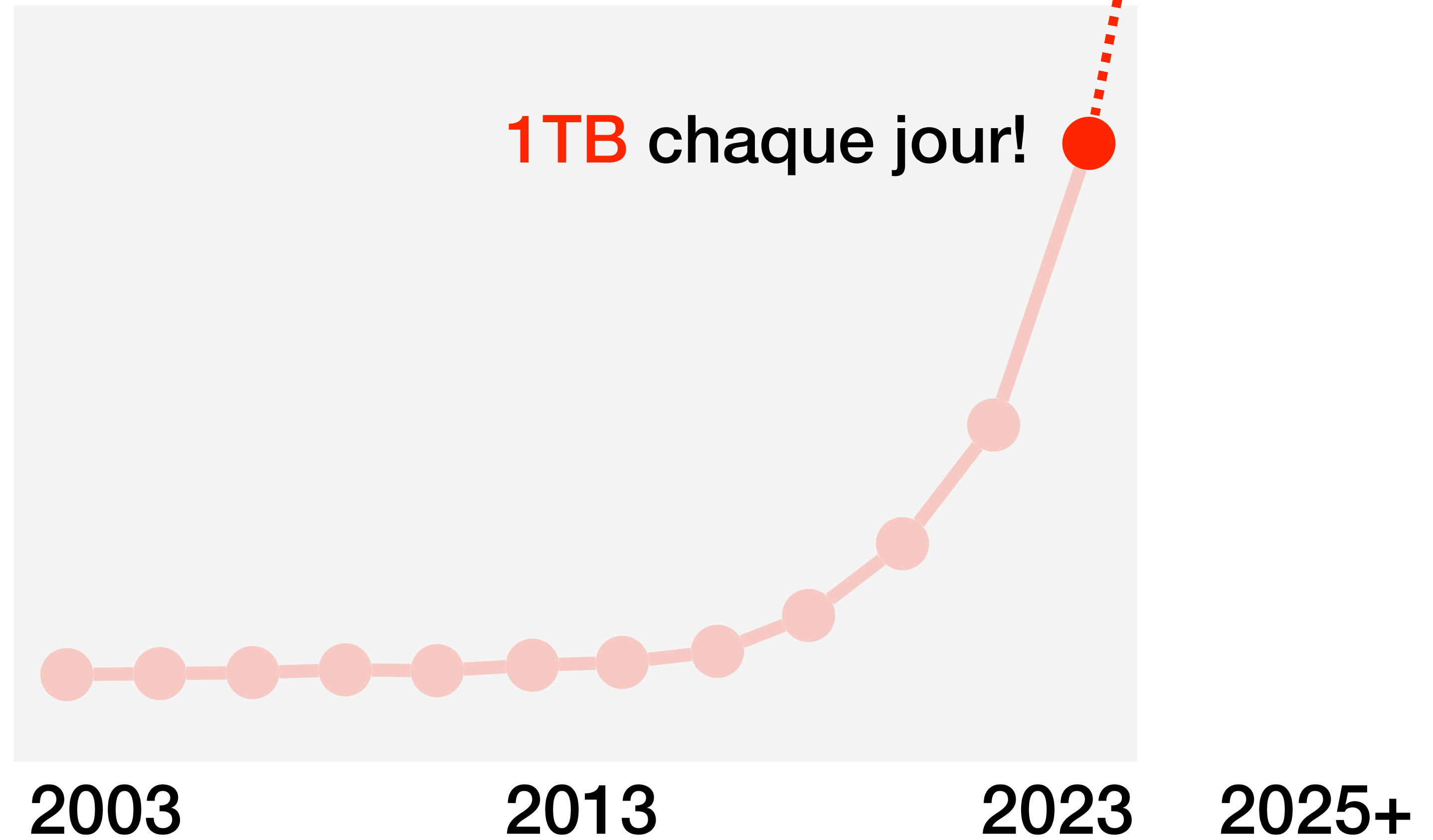
Nombre median de routes BGP collectées par RIS et RouteViews



Nombre median de routes BGP collectées par RIS et RouteViews



Nombre median de routes BGP collectées par RIS et RouteViews



Les plateformes publiques de collection de données BGP n'ont d'autres choix que de limiter leur couverture de PV

The screenshot shows a blog post on the RIPE Labs website. The header includes the RIPE Labs logo and a navigation menu. The article title is "Route Collection at the RIPE NCC - Where are we and where should we go?". The author is Emile Aben, and the post is dated 7 Oct 2020, with a 13-minute read time. The article is categorized under "ris", "events", and "routing". The main text begins with: "Over the past months we've been looking at our Routing Information Service (RIS) and thinking about how to make it best fit for purpose. Ahead of our upcoming RIPE NCC Open House on RIS, this post raises a set of open questions to our community aimed at starting a conversation about how we can keep RIS useful to you."

The screenshot shows a blog post on the RIPE Labs website. The header includes the RIPE Labs logo and a navigation menu. The article title is "RIPE NCC Measurement Data Retention Principles". The author is Robert Kisteleki, and the post is dated 22 Nov 2023, with a 6-minute read time. The contributors listed are Paul de Weerd. The article is categorized under "ris", "atlas", "tools", "community", and "measurements". The main text begins with: "RIPE Atlas and RIPE RIS both provide a wealth of Internet measurement data invaluable to both Internet researchers and network operators alike. But that's not to say that questions about the cost and value of storing this data don't come up from time to time. Here, we open up the discussion on whether change is called for."

Dans le meme temps, les utilisateurs n'ont souvent d'autres choix que d'échantillonner les données

Auriez-vous utilisé plus de données BGP si vous pouviez?*

**Survey conducted among authors of eight top research papers that sampled BGP data*

Dans le meme temps, les utilisateurs n'ont souvent d'autres choix que d'échantillonner les données

Auriez-vous utilisé plus de données BGP si vous pouviez?*

Seven researchers



Yes!



No

One researcher

*Sondage réalisé sur des auteurs de huit top papiers de recherche qui échantillonne les données BGP

GILL: La Prochaine Génération de Plateformes de Collecte de Données BGP



GILL
→



Plan

1. Les routes BGP sont souvent redondantes
2. Cette redondance permet une collecte *“overshoot-and-discard”*
3. ***GILL***: notre plateforme qui utilise la stratégie *“overshoot-and-discard”*

Plan

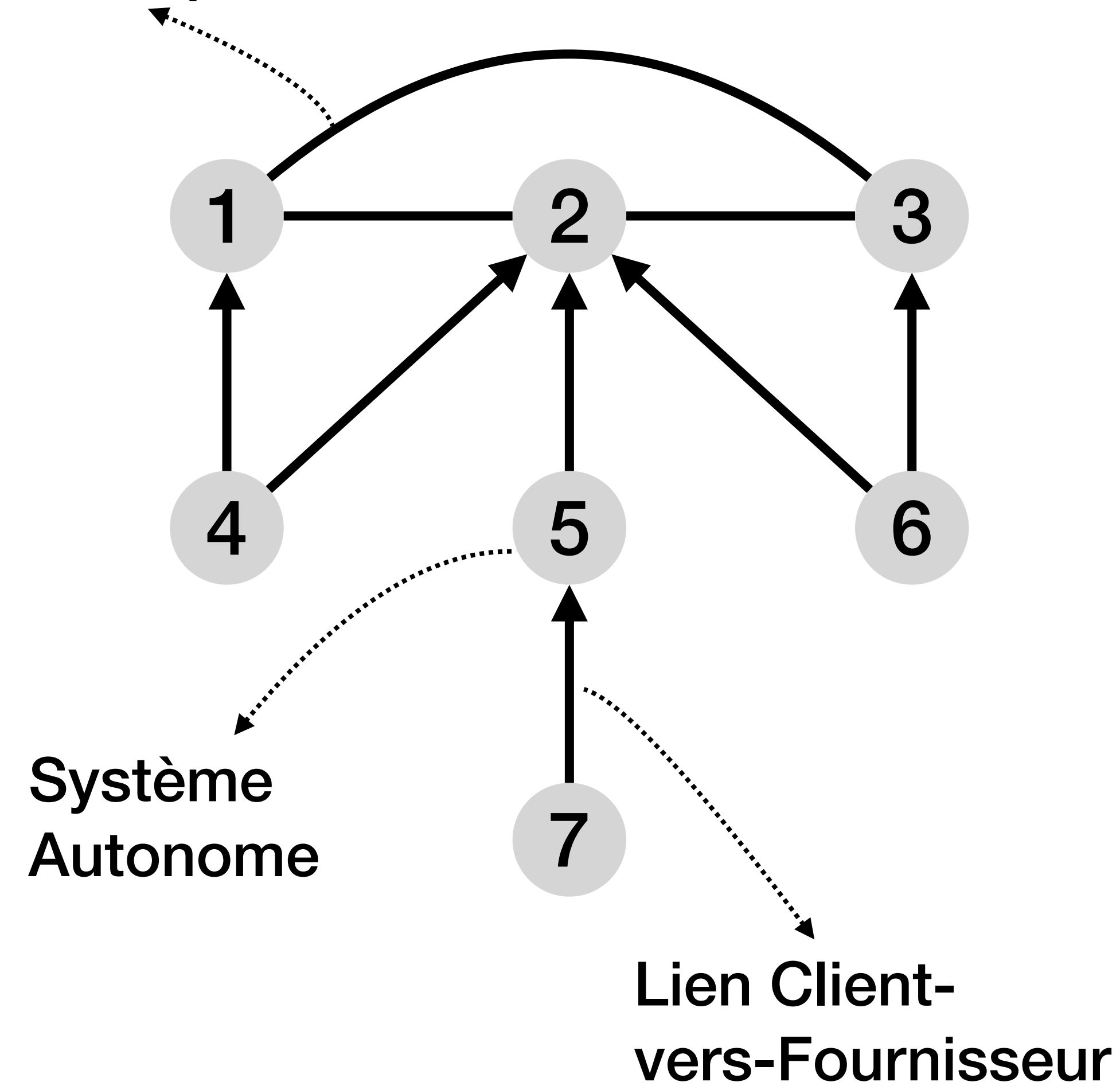
1. Les routes BGP sont souvent redondantes

2. Cette redondance permet une collecte *“overshoot-and-discard”*

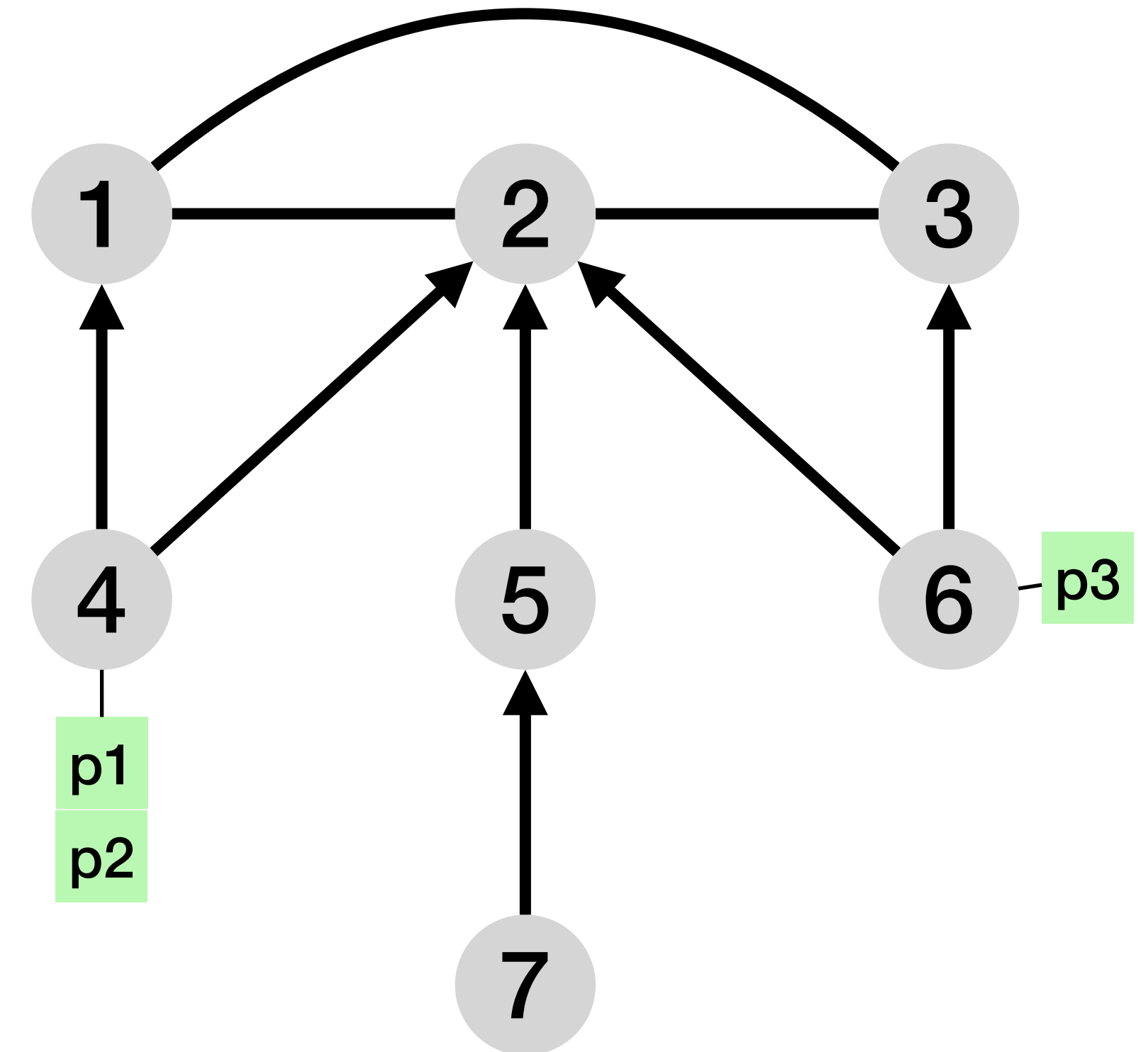
3. *GILL*: notre plateforme qui utilise la stratégie *“overshoot-and-discard”*

Les mises à jour de routes BGP peuvent être redondantes

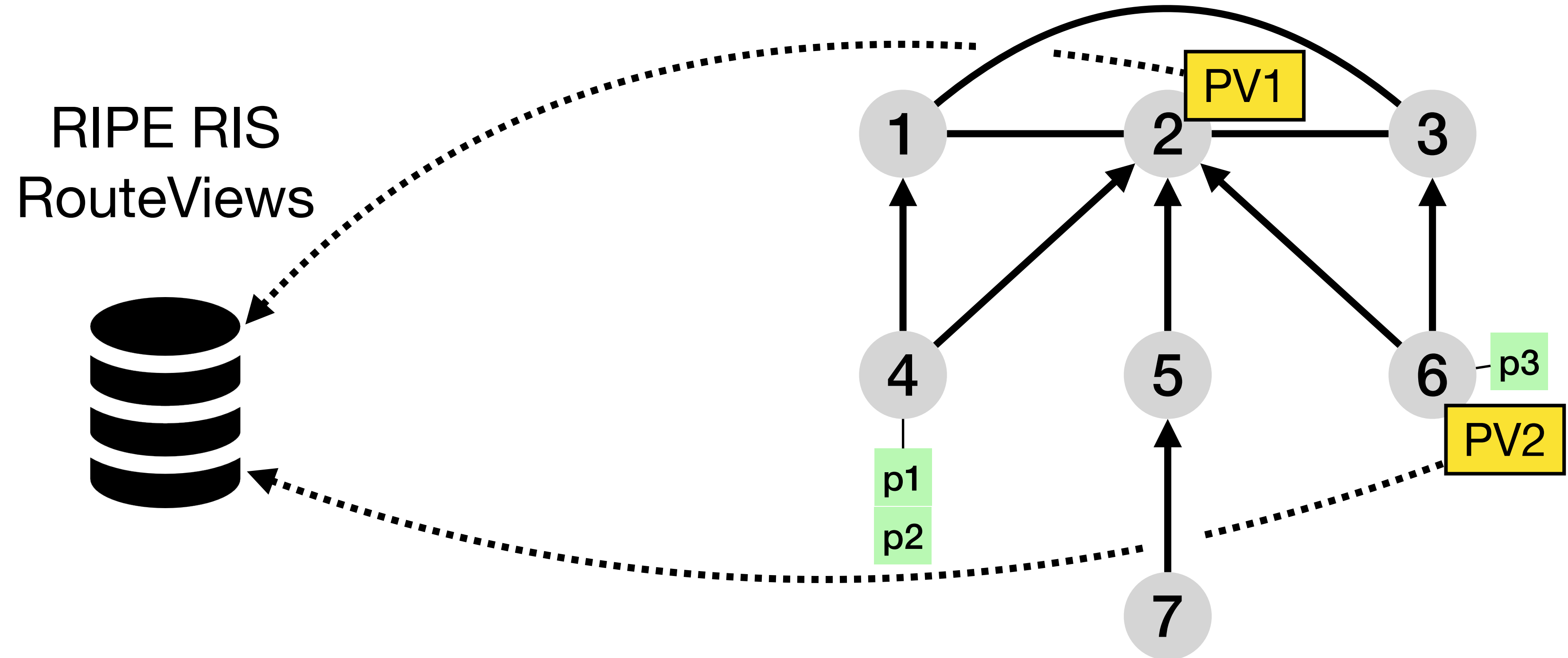
Lien peer-vers-peer



Les mises à jour de routes BGP peuvent être redondantes



Les mises à jour de routes BGP peuvent être redondantes

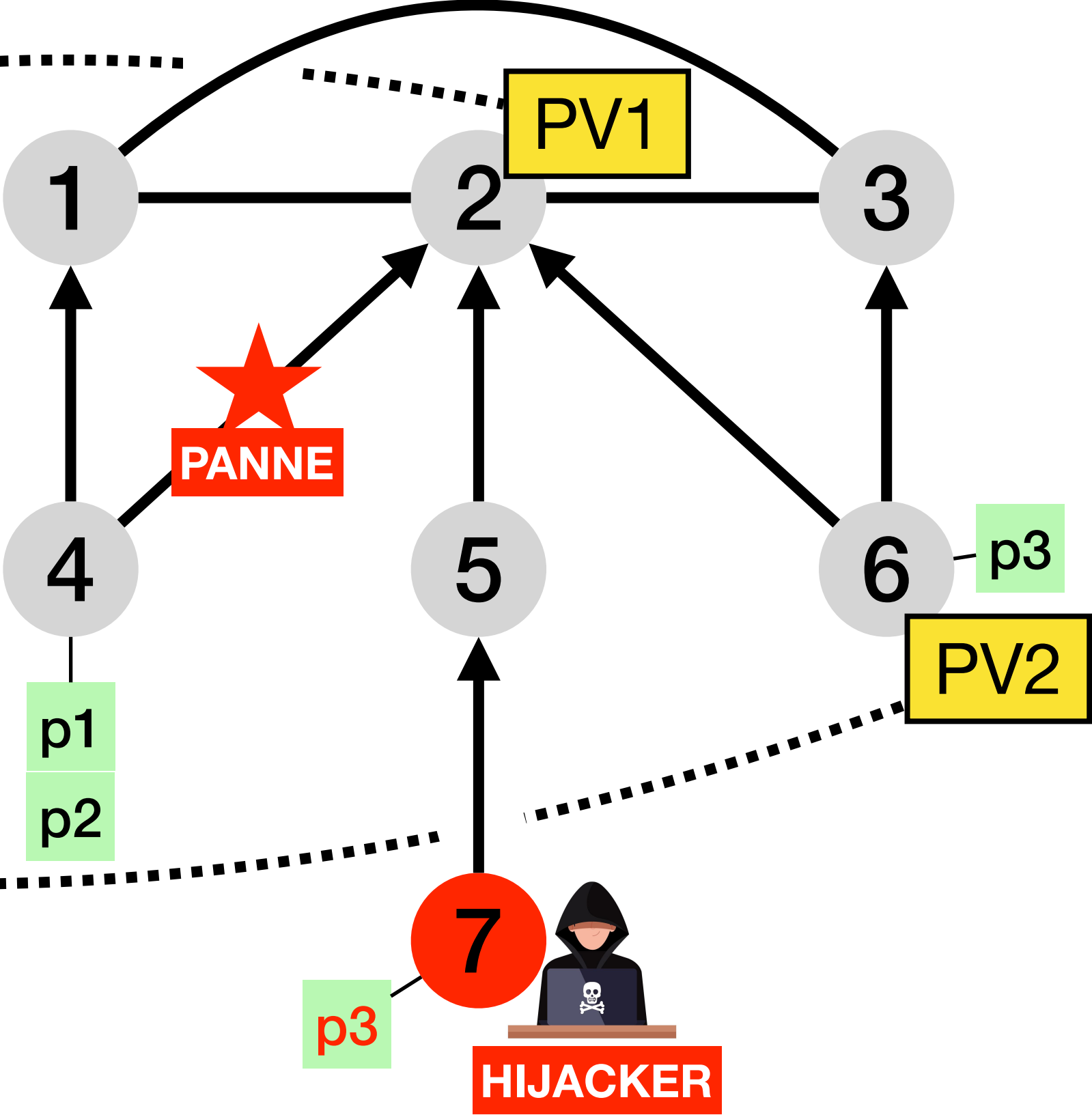
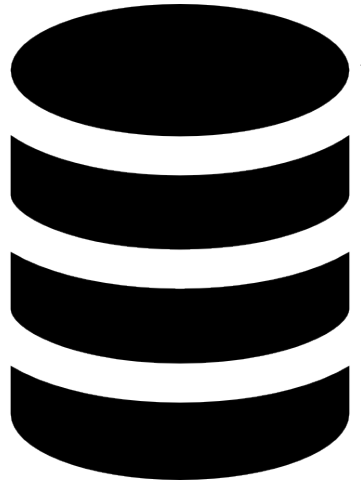


Les mises à jour de routes BGP peuvent être redondantes

Routes collectées

VP	prefix	AS path

RIPE RIS
RouteViews

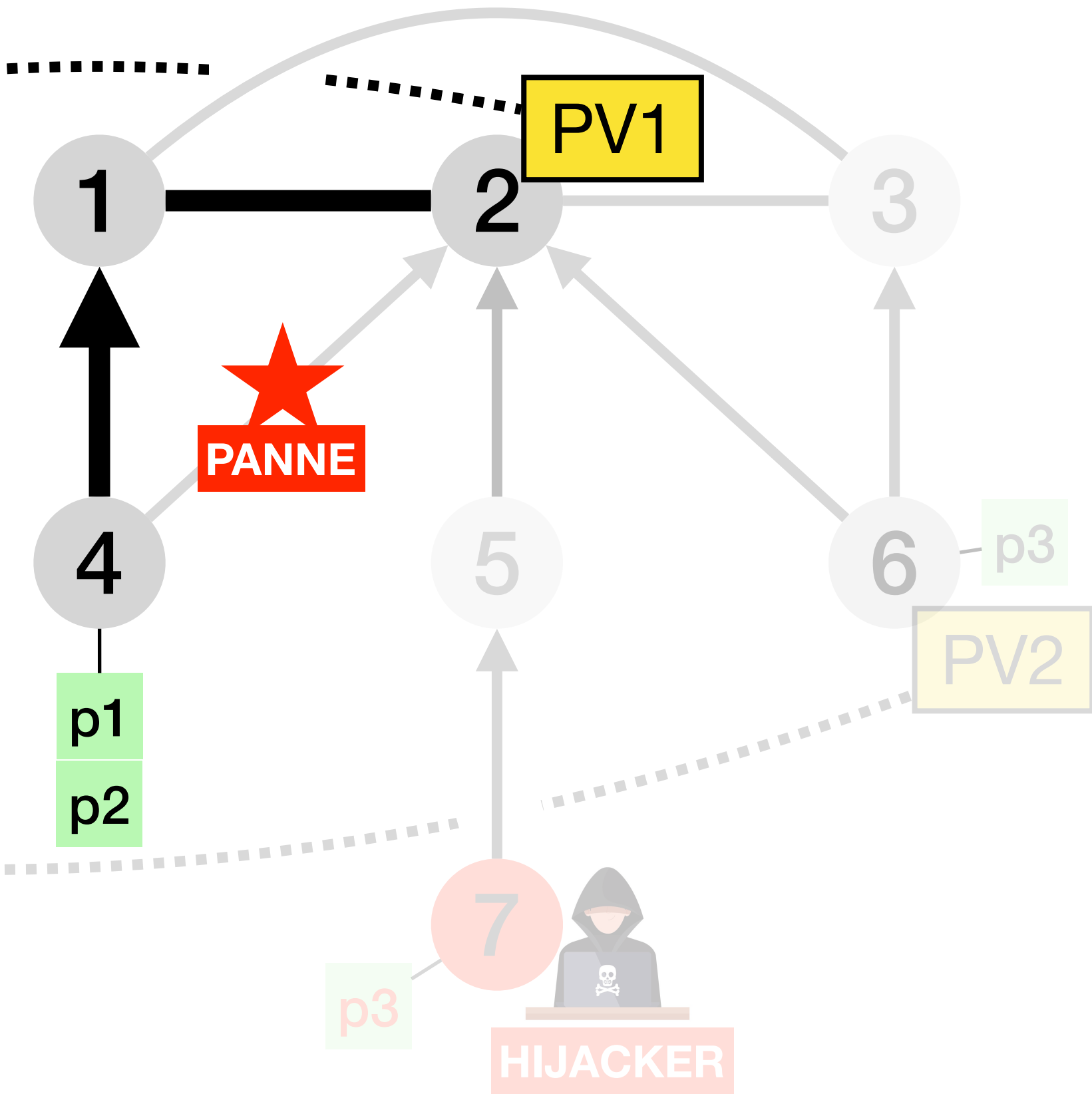
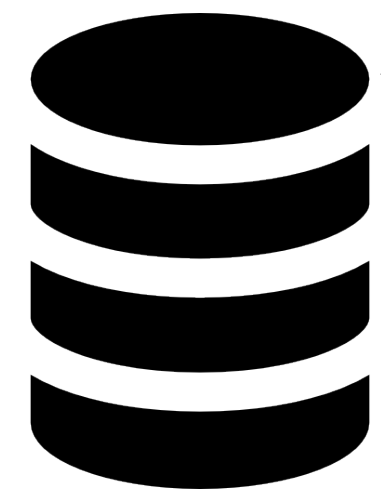


Les mises à jour de routes BGP peuvent être redondantes

Routes collectées

VP	prefix	AS path
PV1	p1	2 1 4
PV1	p2	2 1 4

RIPE RIS
RouteViews

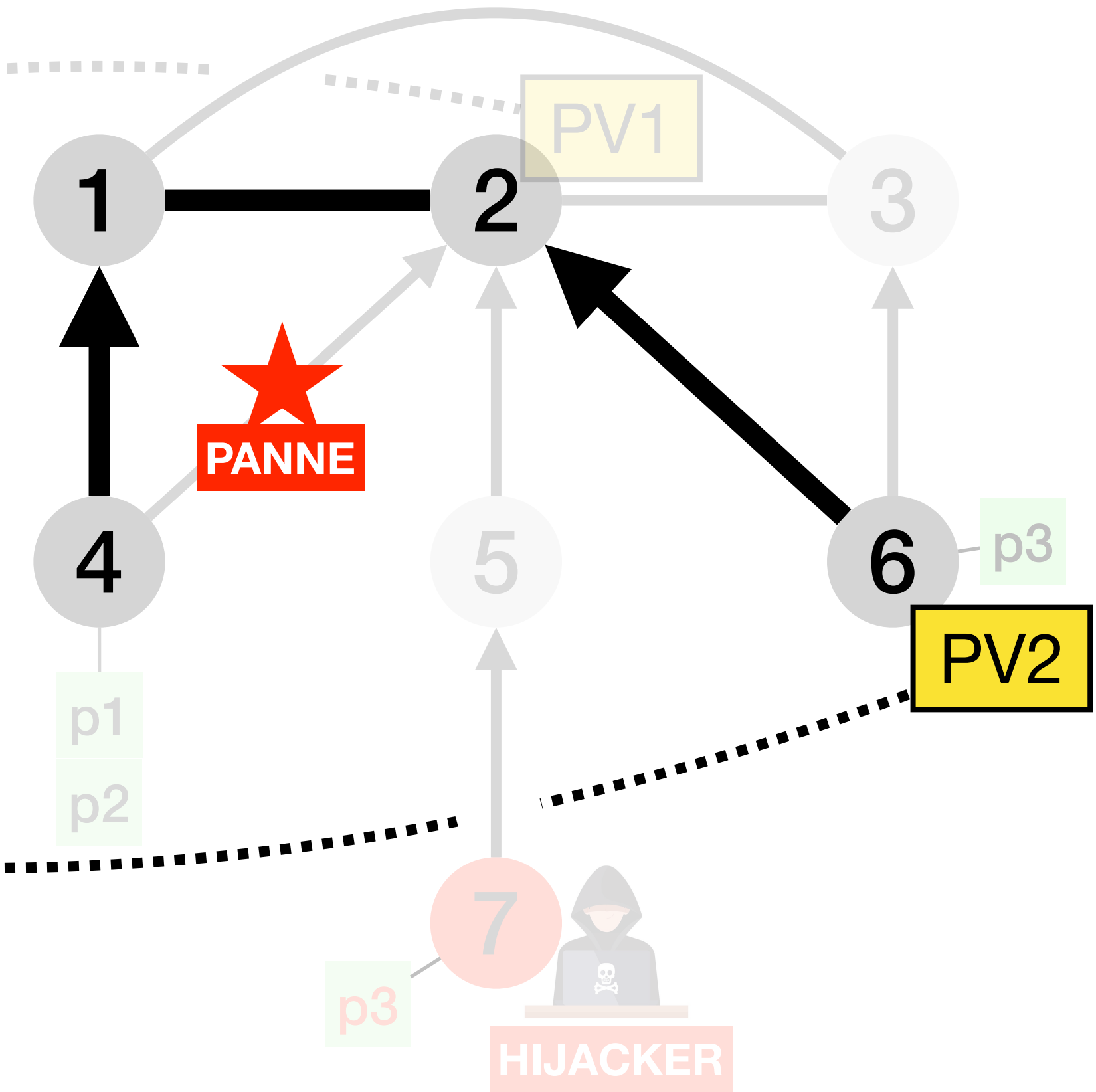


Les mises à jour de routes BGP peuvent être redondantes

Routes collectées

VP	prefix	AS path
PV1	p1	2 1 4
PV1	p2	2 1 4
PV2	p1	6 2 1 4
PV2	p2	6 2 1 4

RIPE RIS
RouteViews



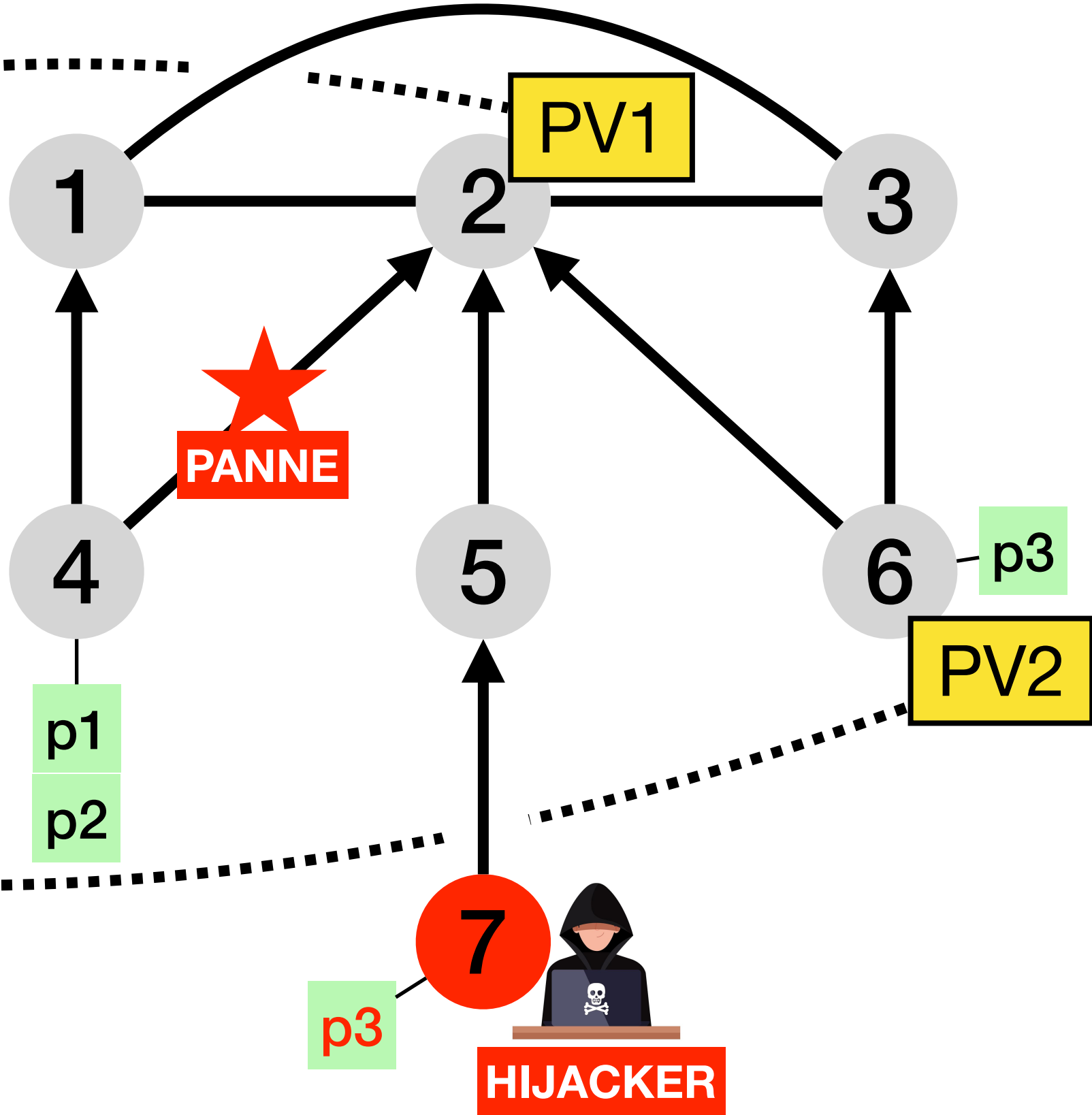
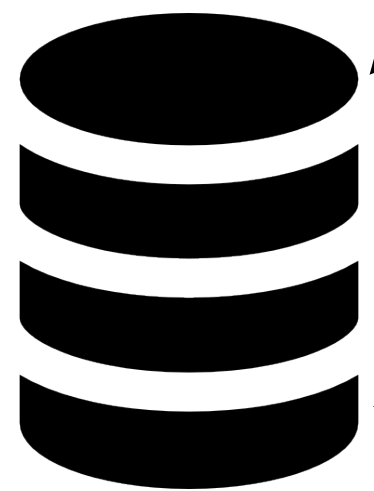
Les mises à jour de routes BGP peuvent être redondantes

Routes redondantes

PV1	p1	2 1 4
PV1	p2	2 1 4
PV2	p1	6 2 1 4
PV2	p2	6 2 1 4

Routes redondantes

RIPE RIS
RouteViews



Les mises à jour redondantes ne sont pas très utiles

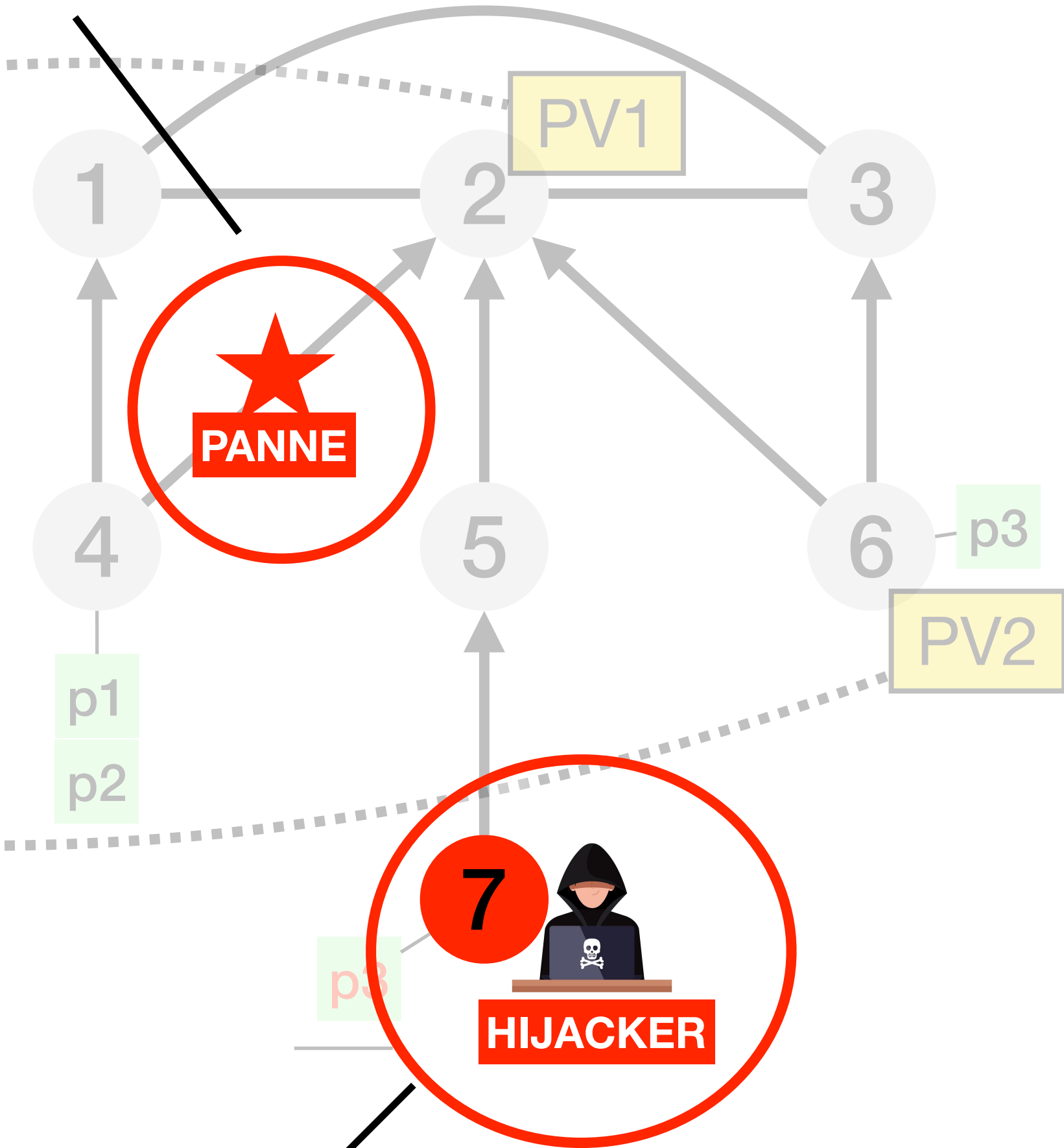
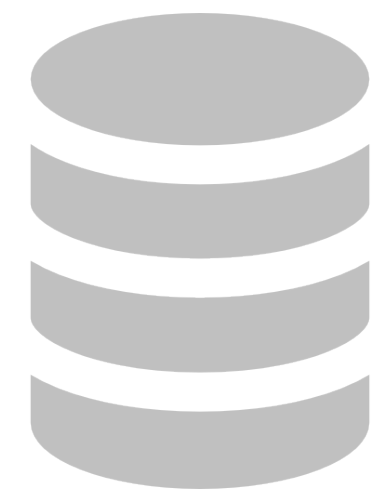
La panne est visible dans une direction seulement

Routes redondantes

		Path
PV1	p1	2 1 4
PV1	p2	2 1 4
PV2	p1	6 2 1 4
PV2	p2	6 2 1 4

Routes redondantes

RIPE RIS
RouteViews

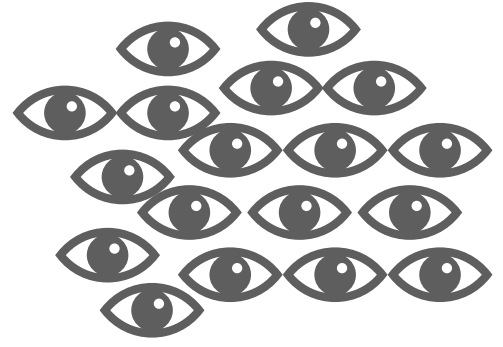


Le hijack n'est pas détecté

Plan

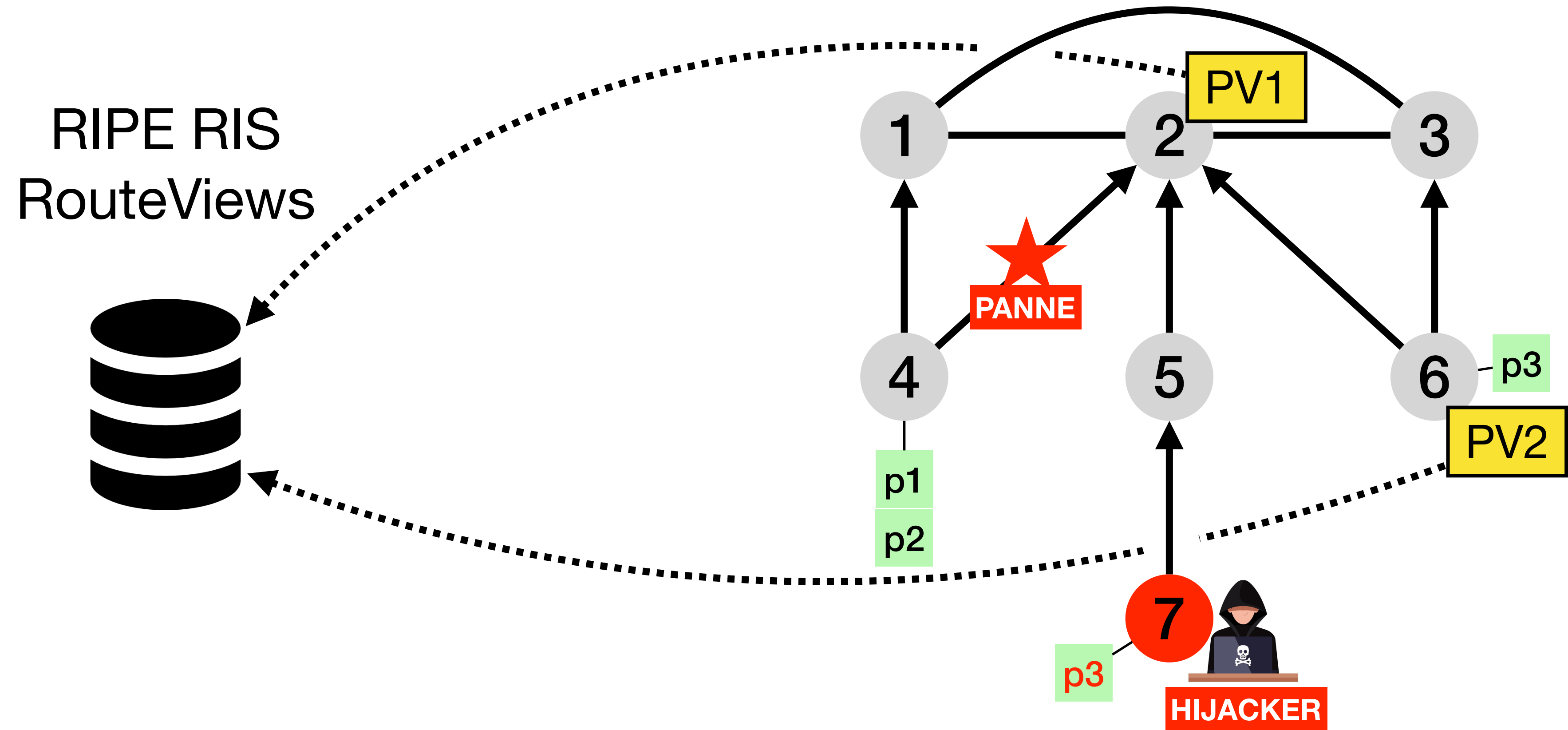
1. Les routes BGP sont souvent redondantes
- 2. Cette redondance permet une collecte “*overshoot-and-discard*”**
3. *GILL*: notre plateforme qui utilise la stratégie “*overshoot-and-discard*”

Le paradigme de collecte “overshoot-and-discard”

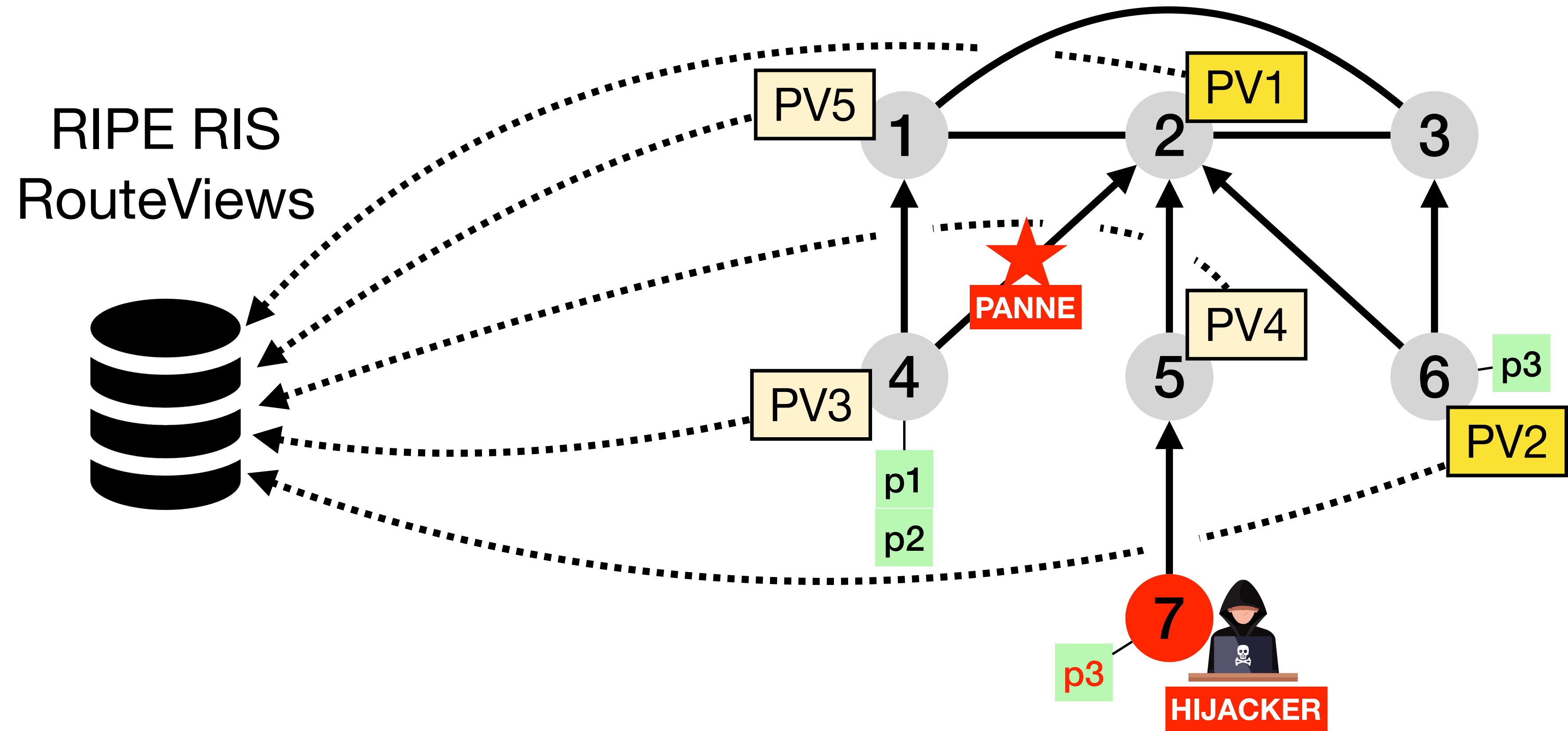


Overshoot: On collecte des données depuis autant de PVs que possible
Pour ne pas oublier des informations importantes

Overshoot: collecter des données depuis autant de PVs que possible



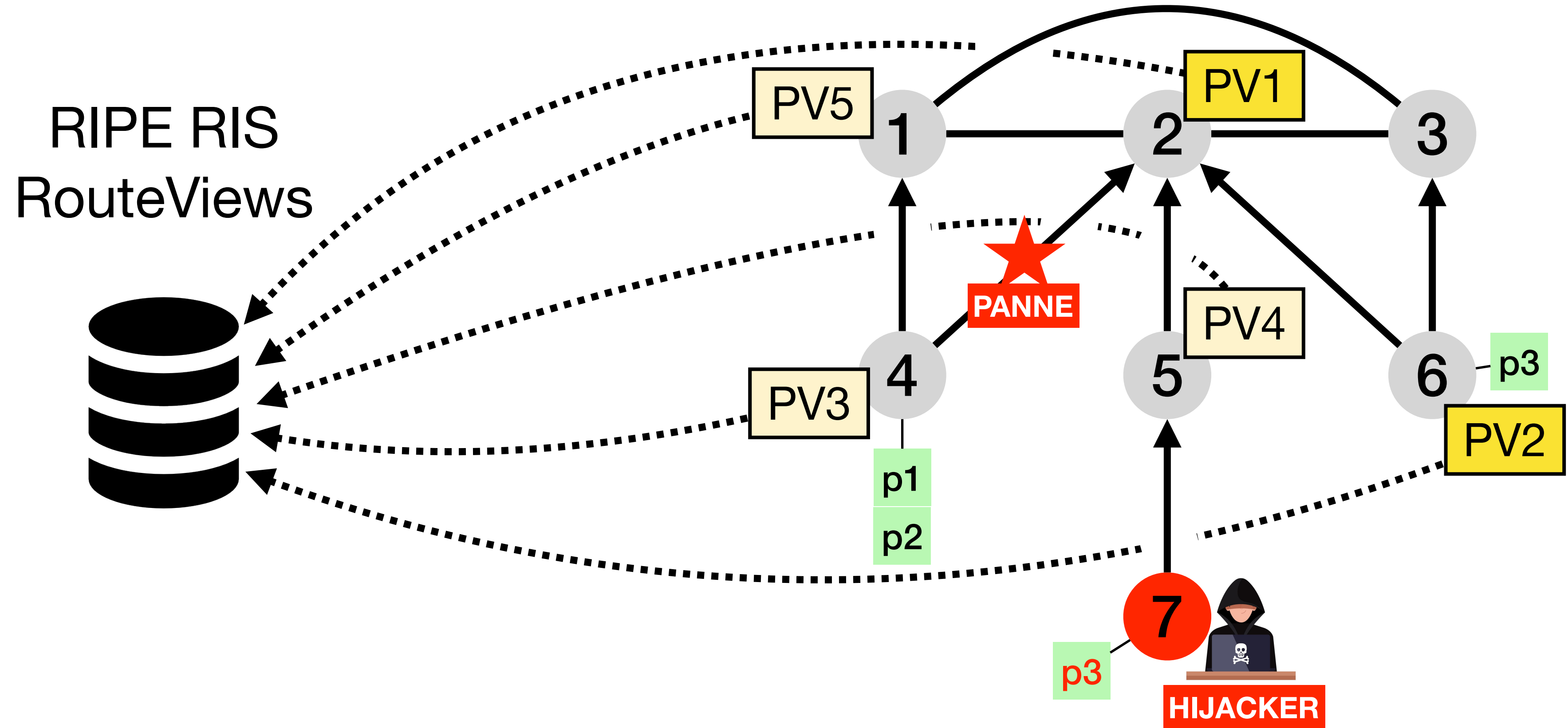
Overshoot: collecter des données depuis autant de PVs que possible



Overshoot: collecter des données depuis autant de PVs que possible
Pour éviter d'oublier des informations importants

Routes collectées

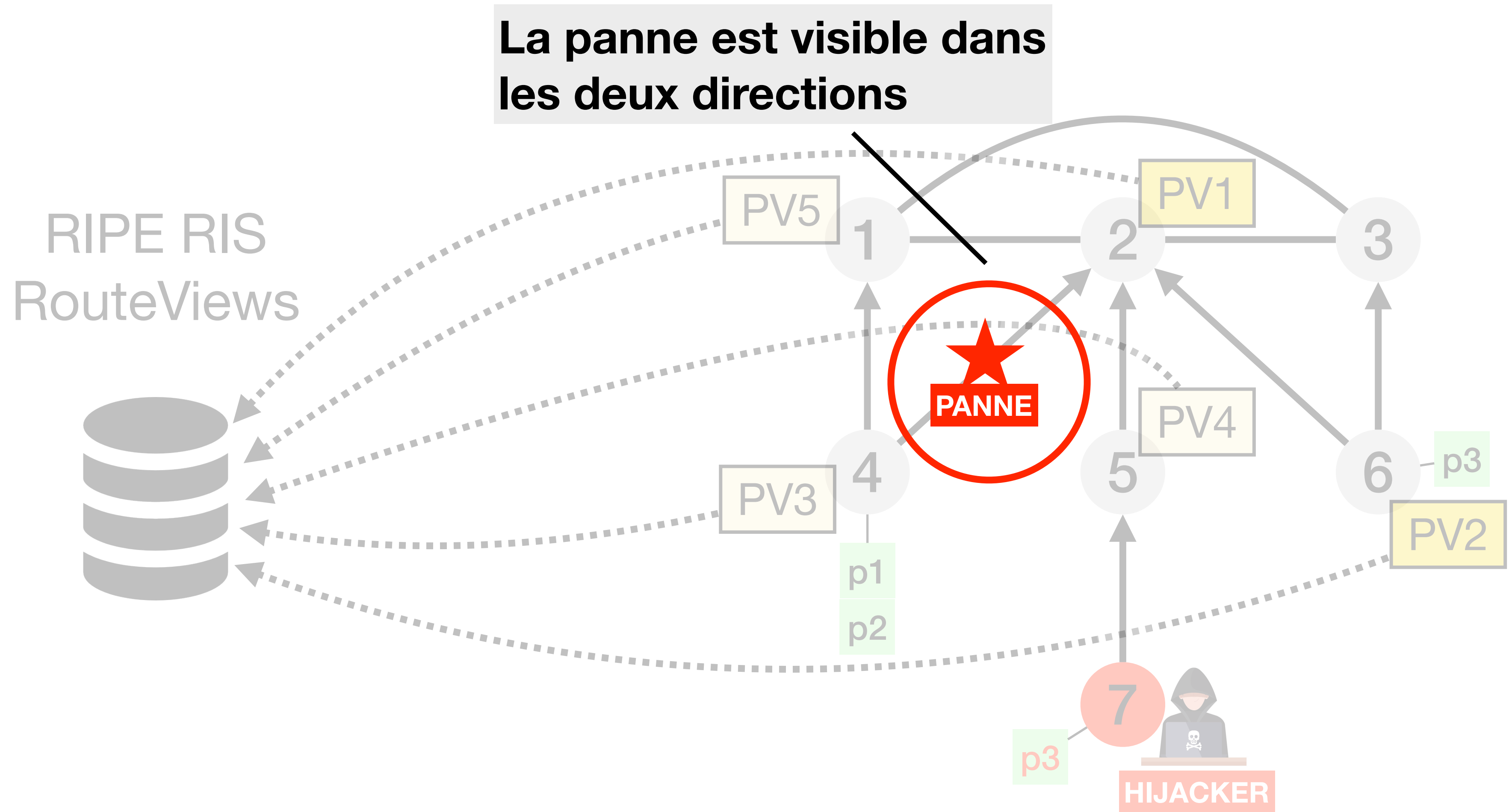
VP	prefix	AS path
PV1	p1	2 1 4
PV1	p2	2 1 4
PV2	p1	6 2 1 4
PV2	p2	6 2 1 4
PV3	p3	4 1 2 6
PV4	p3	5 7



Overshoot: collecter des données depuis autant de PVs que possible
Pour éviter d'oublier des informations importants

Routes collectées

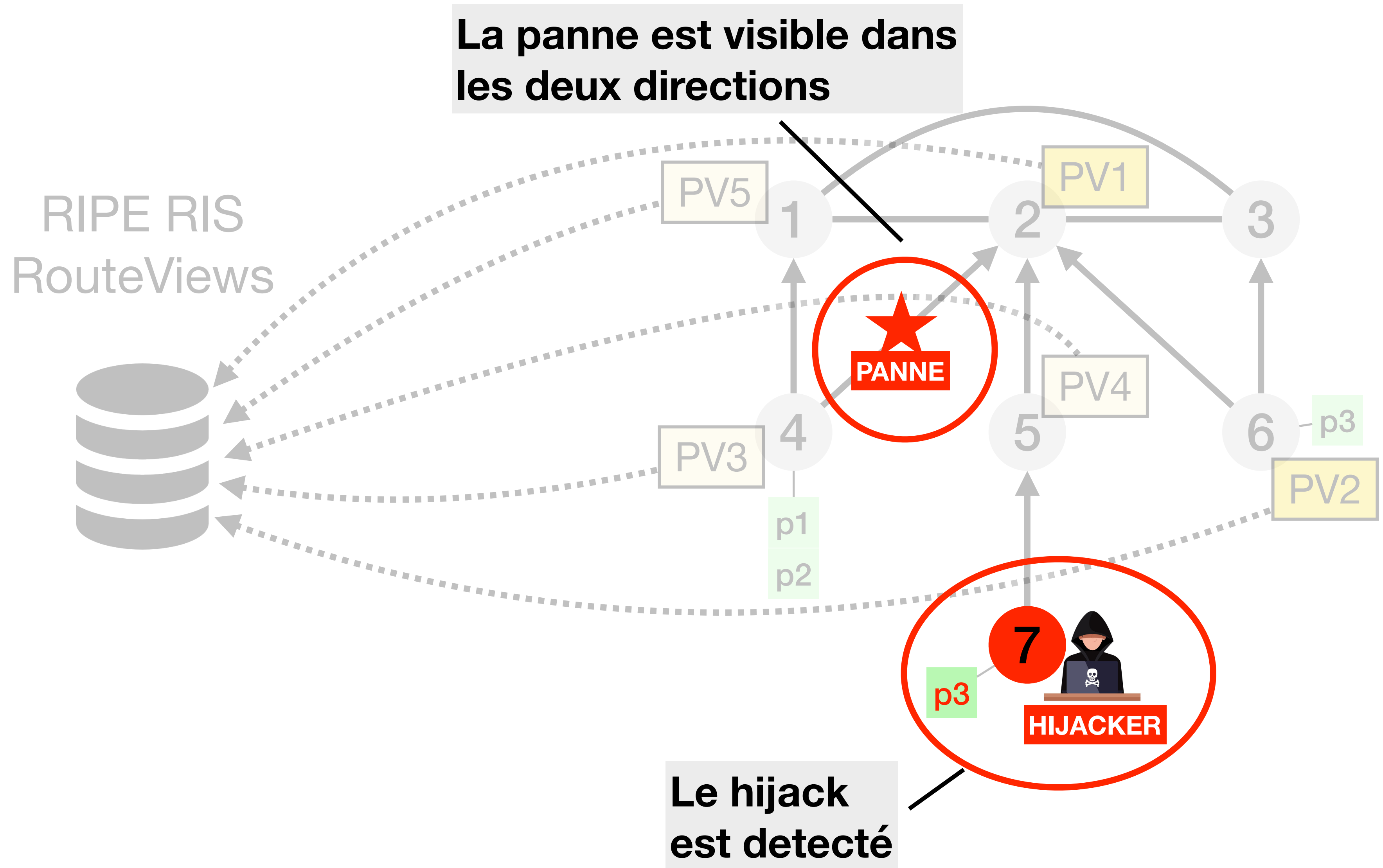
VP	prefix	AS path
PV1	p1	2 1 4
PV1	p2	2 1 4
PV2	p1	6 2 1 4
PV2	p2	6 2 1 4
PV3	p3	4 1 2 6
PV4	p3	5 7



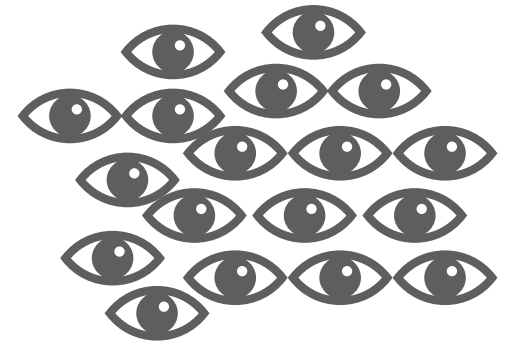
Overshoot: collecter des données depuis autant de PVs que possible
Pour éviter d'oublier des informations importants

Routes collectées

VP	prefix	AS path
PV1	p1	2 1 4
PV1	p2	2 1 4
PV2	p1	6 2 1 4
PV2	p2	6 2 1 4
PV3	p3	4 1 2 6
PV4	p3	5 7



Le paradigme de collecte “overshoot-and-discard”



Overshoot: On collecte des données depuis autant de PVs que possible
Pour ne pas oublier des informations importantes

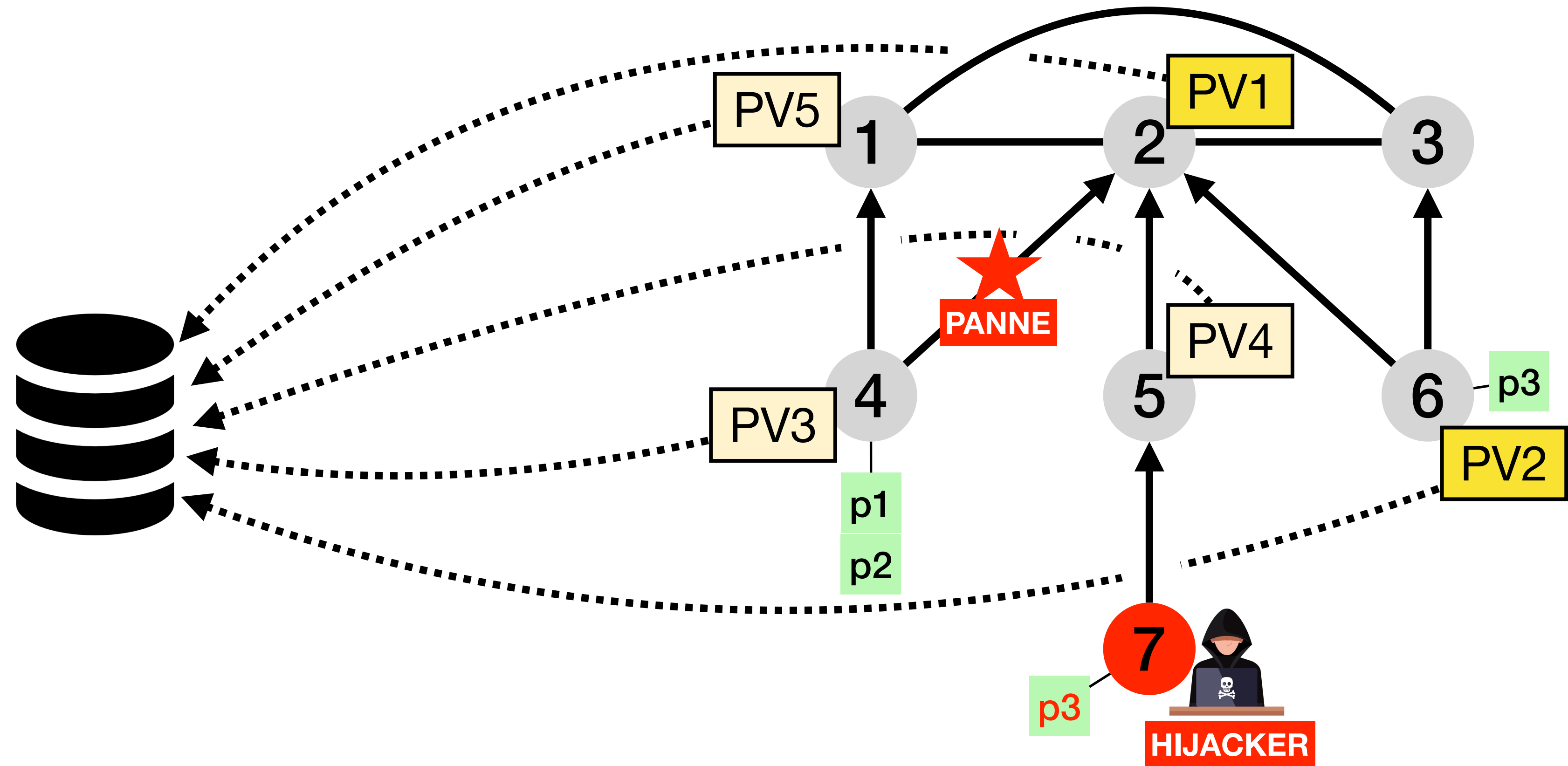


Discard: On filtre les routes BGP redondantes
Pour réduire le volume de données collecté

Discard: les routes BGP redondantes sont supprimées avec des filtres

Routes collectées

VP	prefix	AS path
PV1	p1	2 1 4
PV1	p2	2 1 4
PV2	p1	6 2 1 4
PV2	p2	6 2 1 4
PV3	p3	4 1 2 6
PV4	p3	5 7



Discard: les routes BGP redondantes sont supprimées avec des filtres

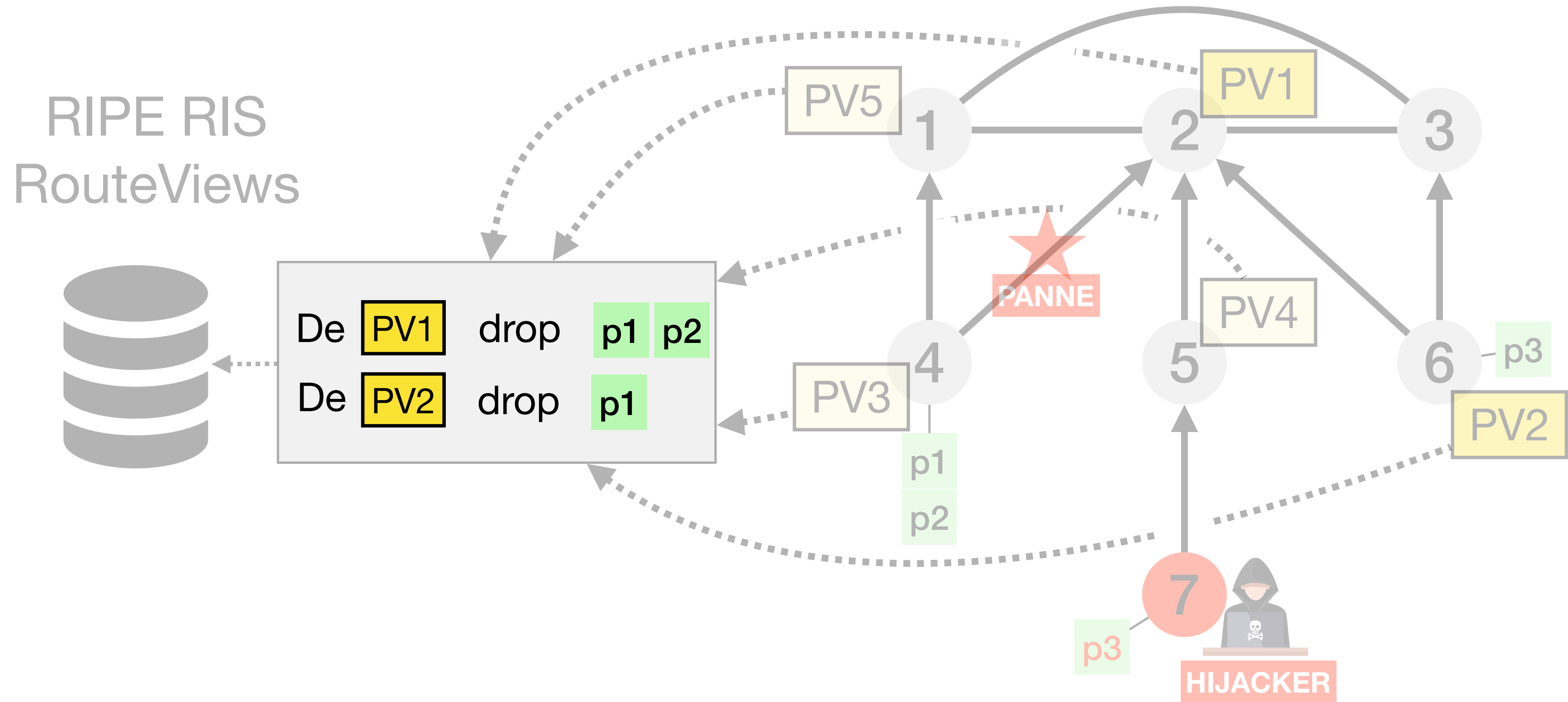
Routes collectées

VP	prefix	AS path
PV1	p1	2 1 4
PV1	p2	2 1 4
PV2	p1	3 2 1 4
PV2	p2	6 2 1 4
PV3	p3	4 1 2 6
PV4	p3	5 7

RIPE RIS
RouteViews



De **PV1** drop p1 p2
De **PV2** drop p1



Discard: les routes BGP redondantes sont supprimées avec des filtres

Routes collectées

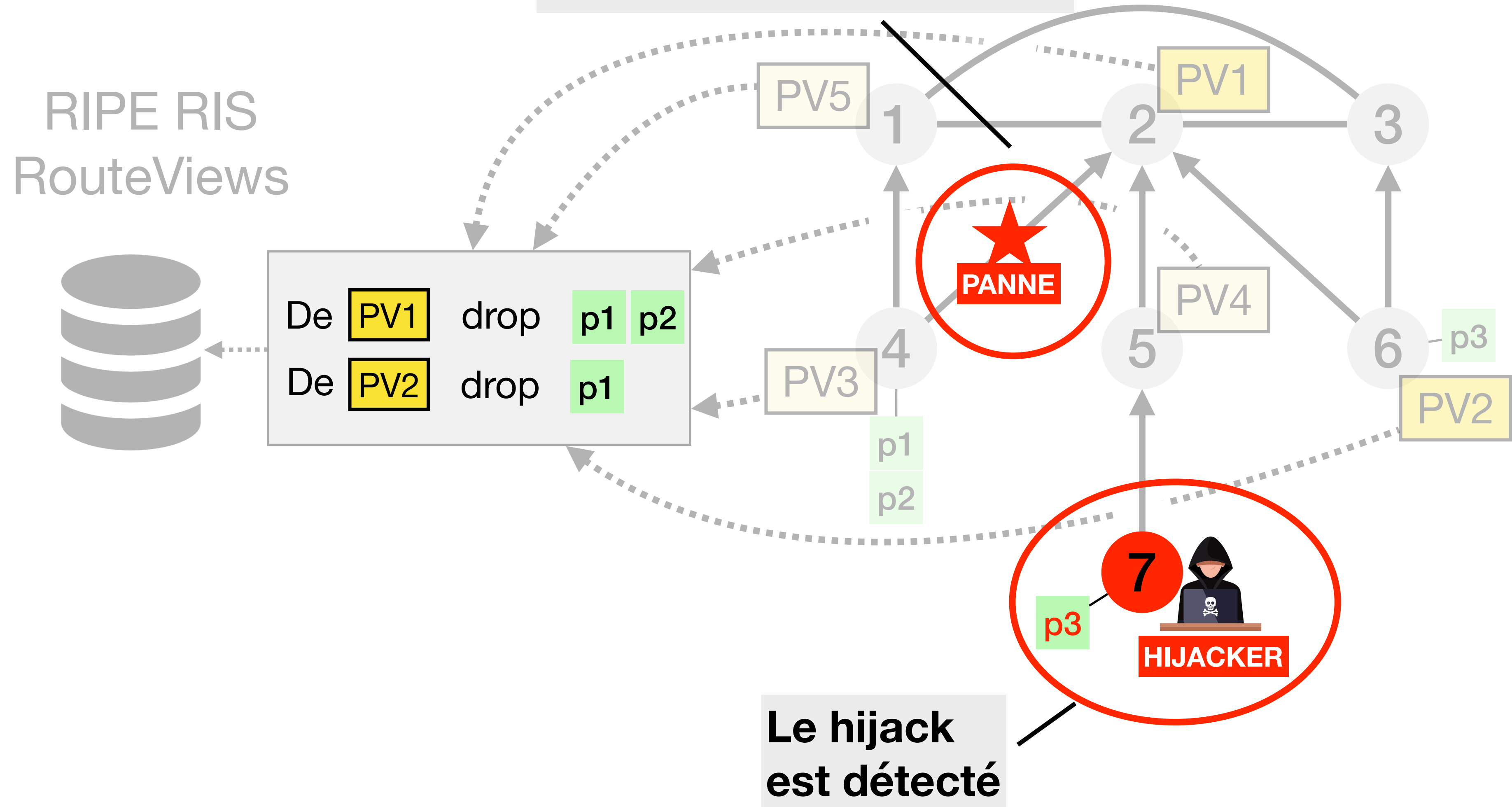
VP	prefix	AS path
PV1	p1	2 1 4
PV1	p2	2 1 4
PV2	p1	3 2 1 4
PV2	p2	6 2 1 4
PV3	p3	4 1 2 6
PV4	p3	5 7

RIPE RIS
RouteViews



De PV1 drop p1 p2
De PV2 drop p1

La panne est visible dans les deux directions



Le hijack est détecté

Plan

1. Les routes BGP sont souvent redondantes
2. Cette redondance permet une collecte *“overshoot-and-discard”*
3. ***GILL***: notre plateforme qui utilise la stratégie *“overshoot-and-discard”*

Nous avons adressé deux challenges fondamentaux pour developper GILL

Challenge #1: **Il n'y pas de consensus sur comment définir la redondance dans les données BGP**

***GILL* garde les routes BGP qui permettent de mieux reconstituer les routes supprimées**

**Imaginons que les routes BGP
sont des pixels**



GILL garde les routes BGP qui permettent de mieux reconstituer les routes supprimées

Imaginons que les routes BGP sont des pixels

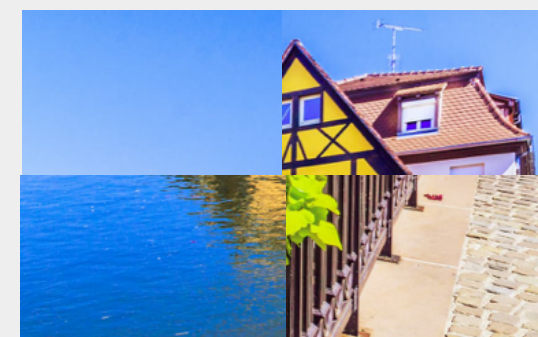


Deux sous ensembles possibles avec le même nombre de pixels

Option #1:



Option #2:



GILL garde les routes BGP qui permettent de mieux reconstituer les routes supprimées

Imaginons que les routes BGP sont des pixels

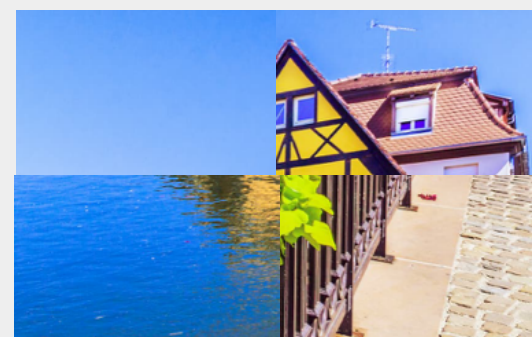


Deux sous ensembles possibles avec le même nombre de pixels

Option #1:

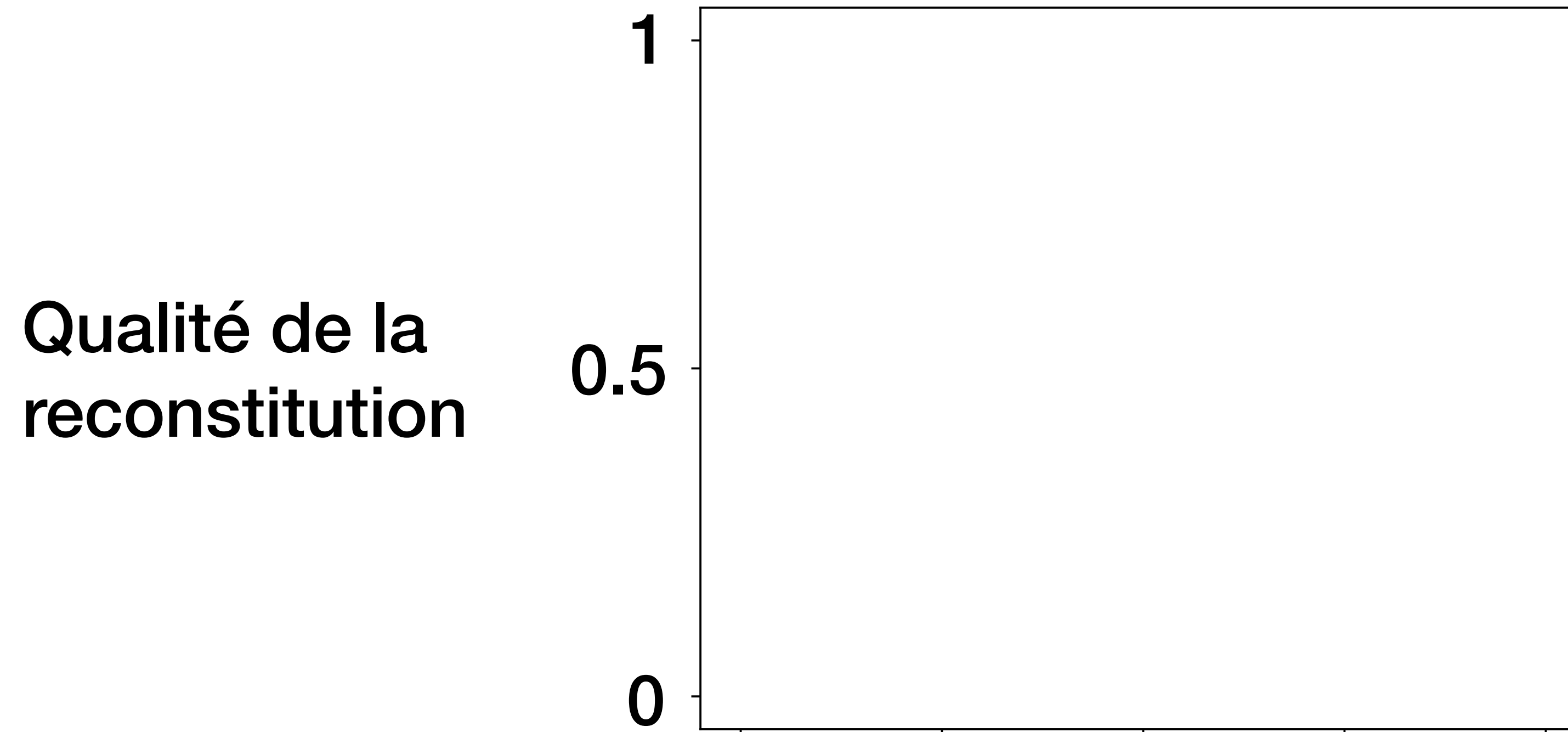


Option #2:

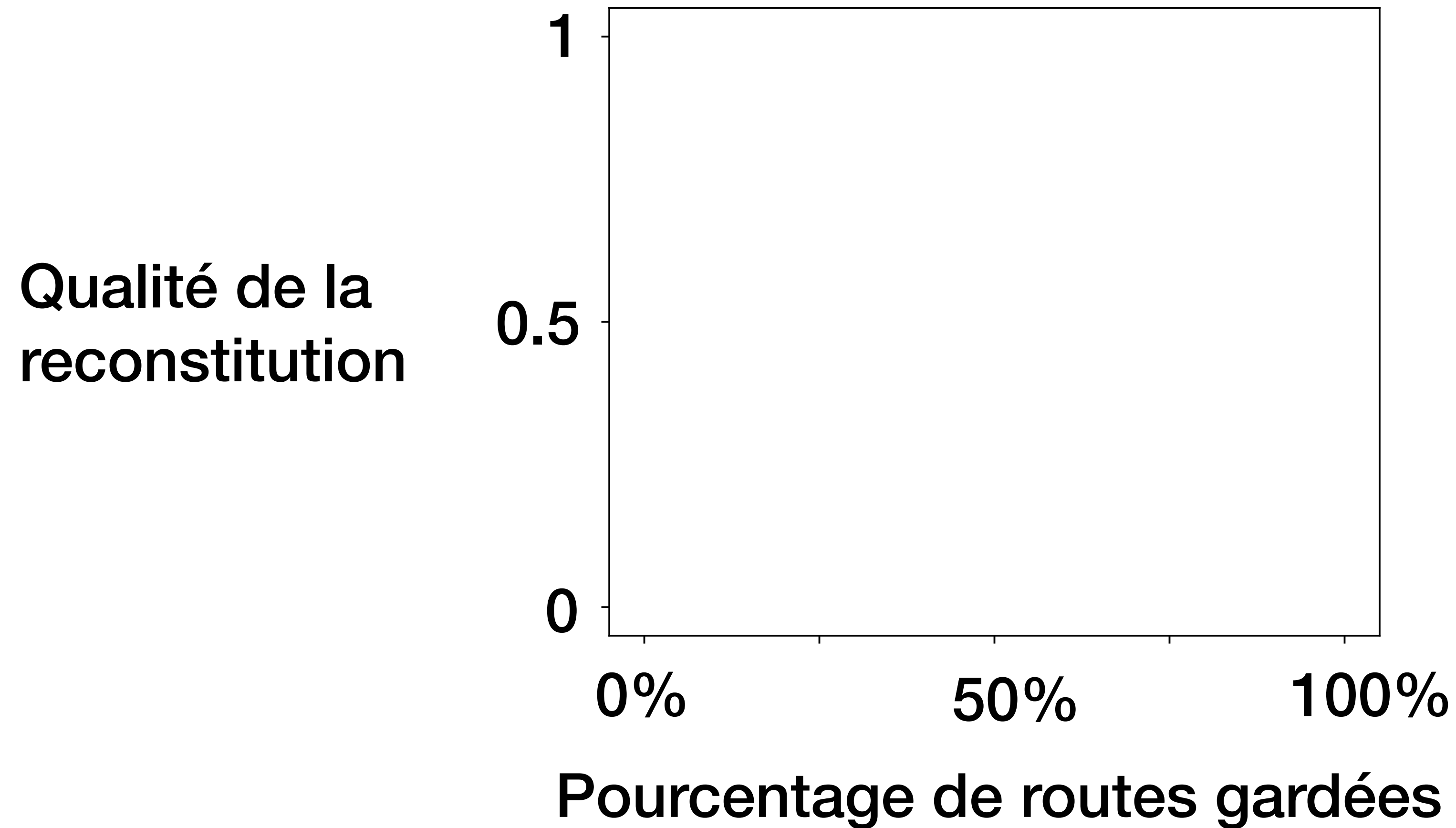


GILL va garder ces pixels “utiles”

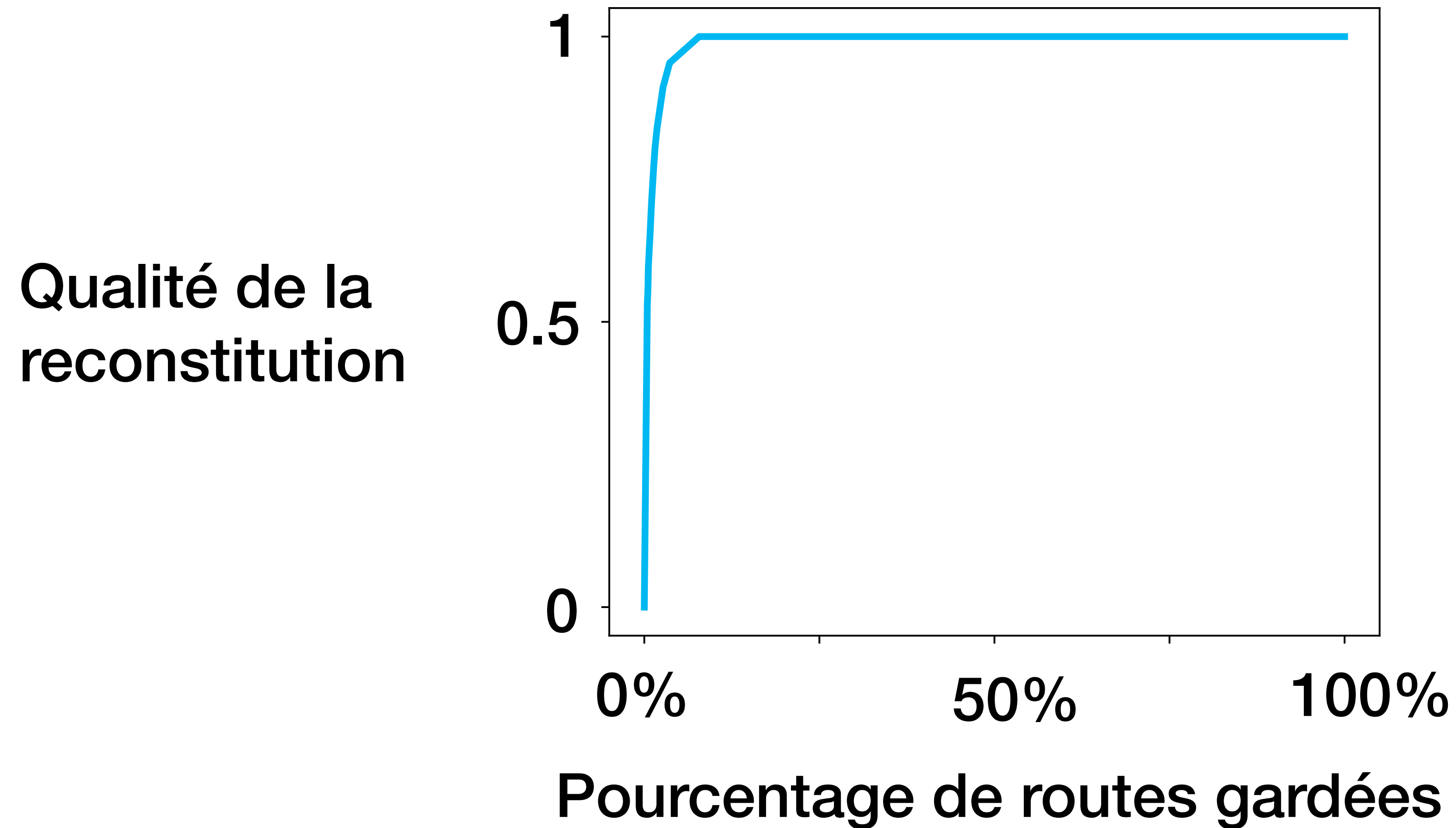
Bonne nouvelle: les routes BGP sont **fortement redondantes**:
on peut éliminer beaucoup de routes sans perdre de données critiques



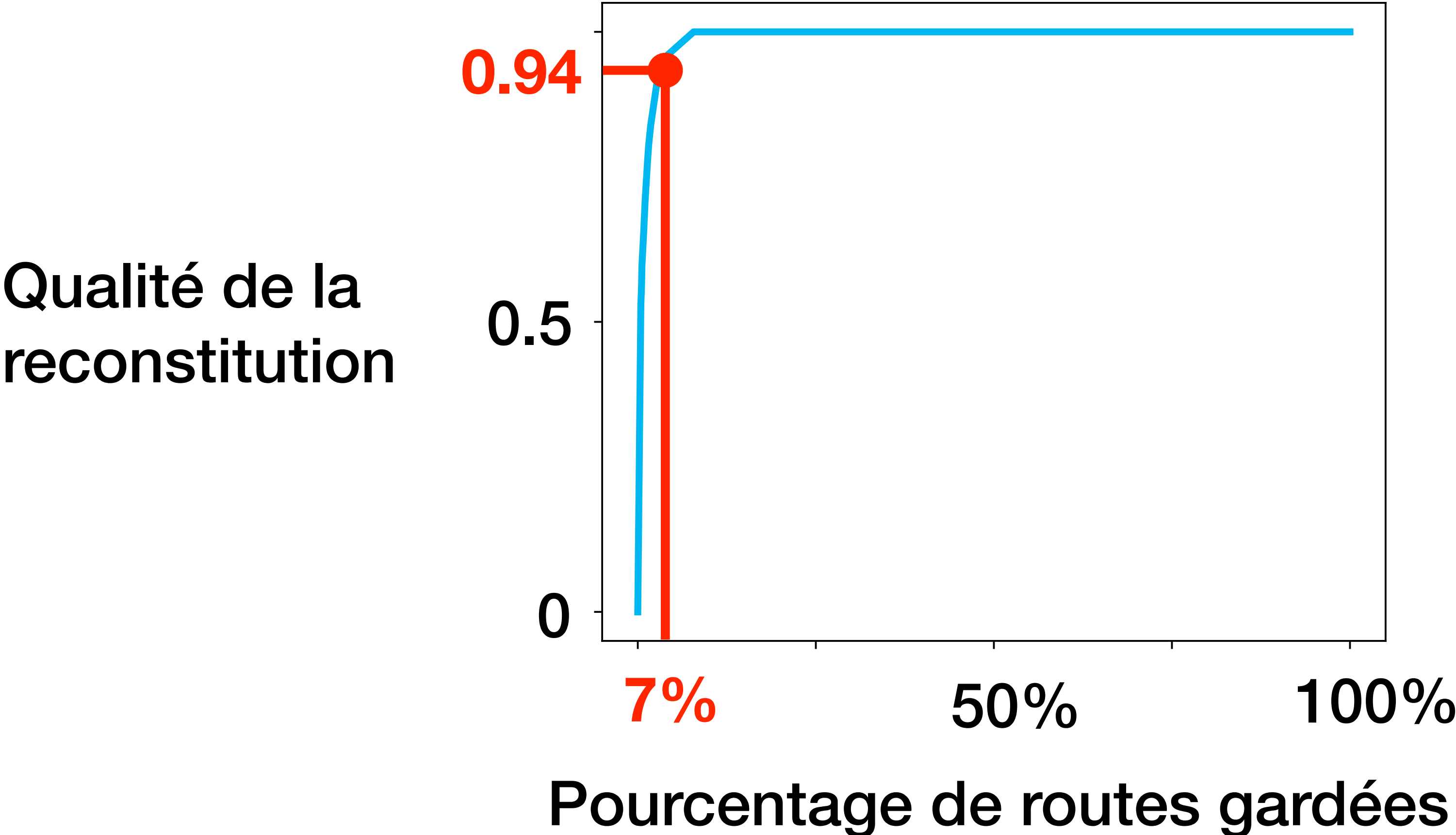
Bonne nouvelle: les routes BGP sont **fortement redondantes**:
on peut éliminer beaucoup de routes sans perdre de données critiques



Bonne nouvelle: les routes BGP sont **fortement redondantes**:
on peut éliminer beaucoup de routes sans perdre de données critiques

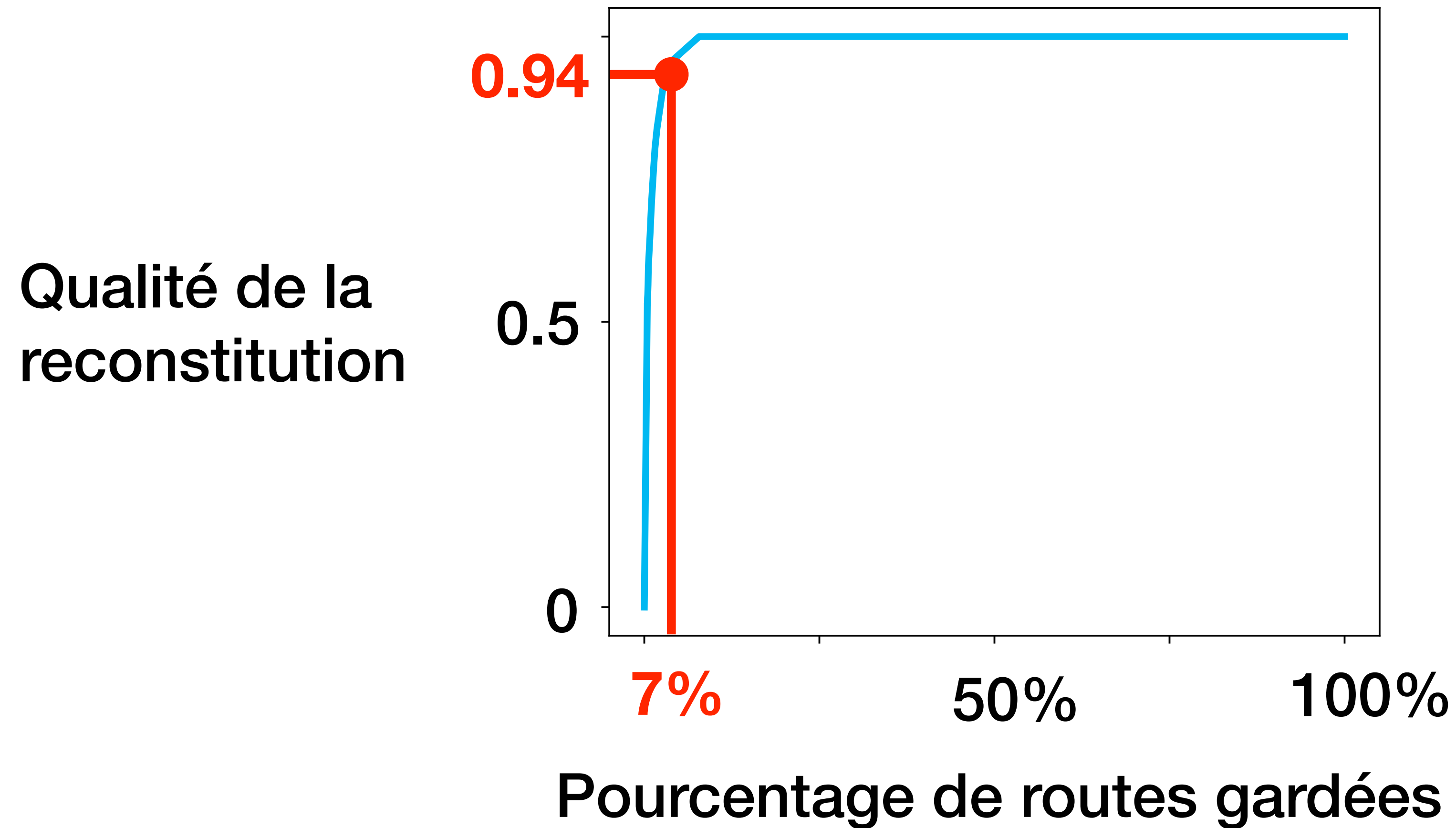


Bonne nouvelle: les routes BGP sont **fortement redondantes**:
on peut éliminer beaucoup de routes sans perdre de données critiques



On peut reconstituer
94% des routes
depuis **7%** d'entre elles

Bonne nouvelle: les routes BGP sont **fortement redondantes**:
on peut éliminer beaucoup de routes sans perdre de données critiques



On peut reconstituer
94% des routes
depuis **7%** d'entre elles

Avec des données réelles,
pas des simulations!

Nous avons adressé deux challenges fondamentaux pour developper GILL

Challenge #1: Il n'y pas de consensus sur comment définir la redondance dans les données BGP

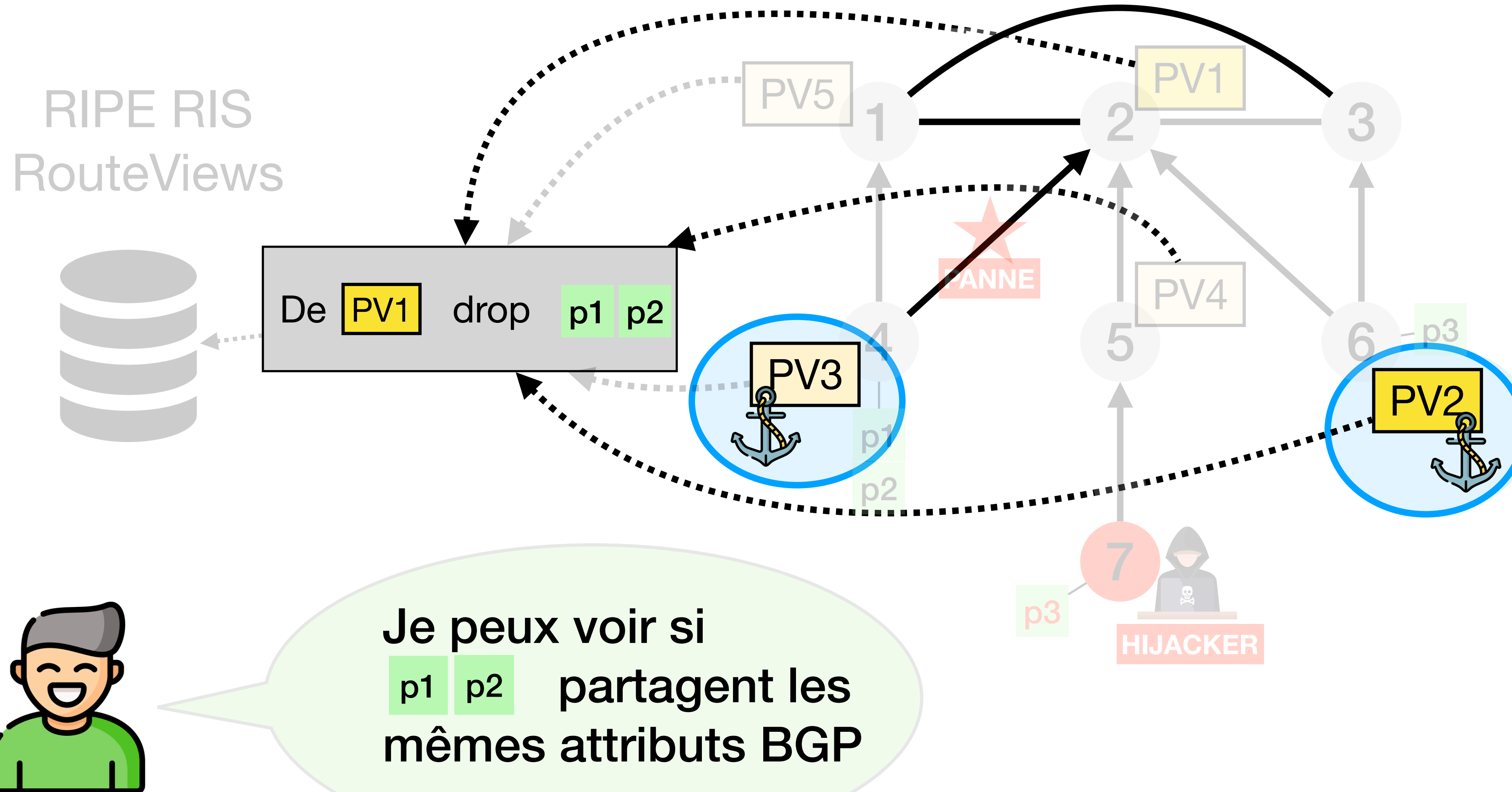
Challenge #2: **Comment garantir l'équité** sachant que les utilisateurs peuvent avoir des objectifs très variés

GILL identifie des PVs non redondants, appelés “ancre”, depuis lesquels il conserve toutes les données

GILL identifie des PVs non redondants, appelés “ancre”, depuis lesquels il conserve toutes les données

Routes collectées

VP	prefix	AS path
VP1	p1	2 1 4
VP1	p2	2 1 4
VP2	p1	6 2 1 4
VP2	p2	6 2 1 4
VP3	p3	4 1 2 6
VP4	p3	5 7



Un prototype de *GILL* tourne sur bgproutes.io

bgproutes.io

GILL
MVP
DFOH

GILL

Expanding BGP Data Horizons

List of peers

Click on any peer to get more information about it.
We have integrated peers from RIS and RouteViews to bootstrap GILL with some peers. However, it currently has a limited number of peers as it is still in prototype mode.

Use the form below to apply filters and select the peers you wish to view.

Peer ASN

Peer IP

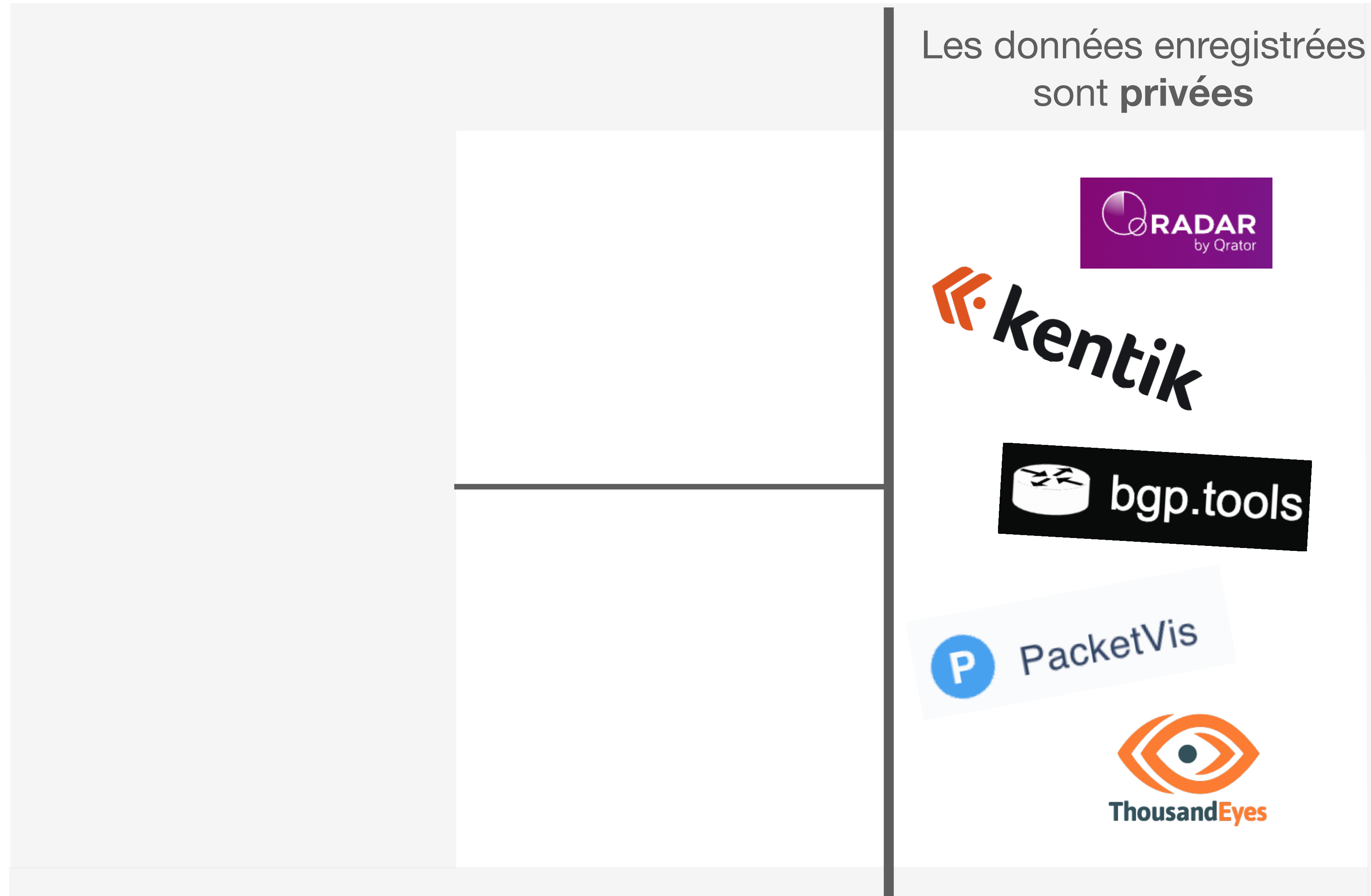
Only show the active peers

Organisation	ASN	IP address	Up since	Removed since	Peer origin
RGNET-IAD	3927	198.180.150.120	2024-09-14	Still active	GILL
RGNET-SEA	3130	147.28.0.5	2024-09-14	Still active	GILL
RGNET-DFW	4128	157.238.224.206	2024-09-14	Still active	GILL
WYBT-NET	59645	195.191.197.21	2024-09-14	Still active	GILL
BENJOJONET	206924	185.230.223.3	2024-09-14	Still active	GILL
NetDEF-US	207465	194.147.139.2	2024-09-14	Still active	GILL
SFMIX-MGMT	12276	198.35.53.242	2024-09-14	Still active	GILL
INTERNET2-BLIND	200055	192.250.20.21	2024-09-14	Still active	GILL

GILL à déjà une dizaine de peers
Et on va bientôt mirroring ceux de RIPE RIS et RouteViews

Vous pouvez peerer avec GILL!
Le processus est entièrement automatisé et réalisé en 5 min!

GILL se démarque des autres plateformes de collecte de données BGP



GILL se démarque des autres plateformes de collecte de données BGP



GILL se démarque des autres plateformes de collecte de données BGP



***GILL* a un impact positif sur de nombreuses études**

***GILL* a un impact positif sur de nombreuses études**

Impact sur le long terme

Simulations avec une couverture de 50%

x3 de liens de p2p identifiés

x2 de pannes qu'on peut localiser

+9% de BGP hijacks qu'on peut détecter

***GILL* a un impact positif sur de nombreuses études**

Impact sur le long terme

Simulations avec une couverture de 50%

x3 de liens de p2p identifiés

x2 de pannes qu'on peut localiser

+9% de BGP hijacks qu'on peut détecter

Impact sur le court terme

réplication d'études existantes avec nos algorithmes d'échantillonnages

+15% d'AS business relationships inférés

4x de précision pour l'inférence d'hijacks

***GILL* a un impact positif sur de nombreuses études**

Impact sur le long terme

Simulations avec une couverture de 50%

x3 de liens de p2p identifiés

x2 de pannes qu'on peut localiser

+9% de BGP hijacks qu'on peut détecter

Impact sur le court terme

réplication d'études existantes

+15% d'AS business relationships inférés

4x de précision pour l'inférence d'hijacks

Ces bénéfices sont possible sans utiliser plus données!

La Prochaine Génération de Plateformes de Collecte de Données BGP

<https://bgproutes.io>

