

Defeating architectures for low-latency services : The case of L4S

Marius Letourneau : marius.letourneau@utt.fr

Contexte - Evolution de l'usage de l'Internet

- De nouveaux services à fortes exigences sur la latence



Les sources de la latence

- Temps de traitement des entités terminales et des middleboxes
- Temps d'acheminement des données dans le réseau :
 - La **taille** des files d'attente
 - La **réactivité** à la congestion

Solutions :

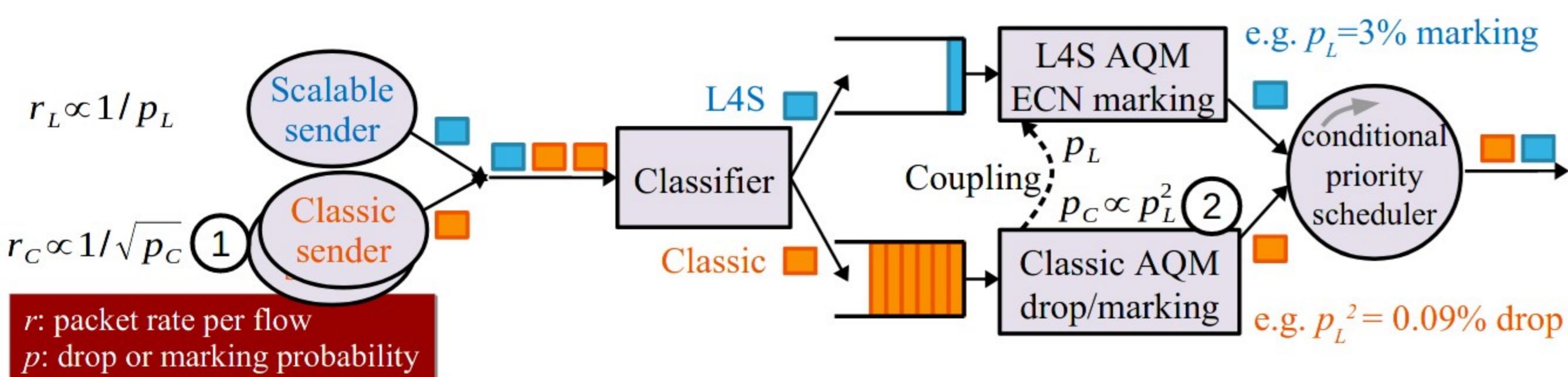
- Active Queue Management**
- Nouveaux algorithmes de contrôle de congestion**
- Explicit Congestion Notification**

Architecture L4S proposé par l'IETF

(Low Latency, Low Loss, Scalable throughput)

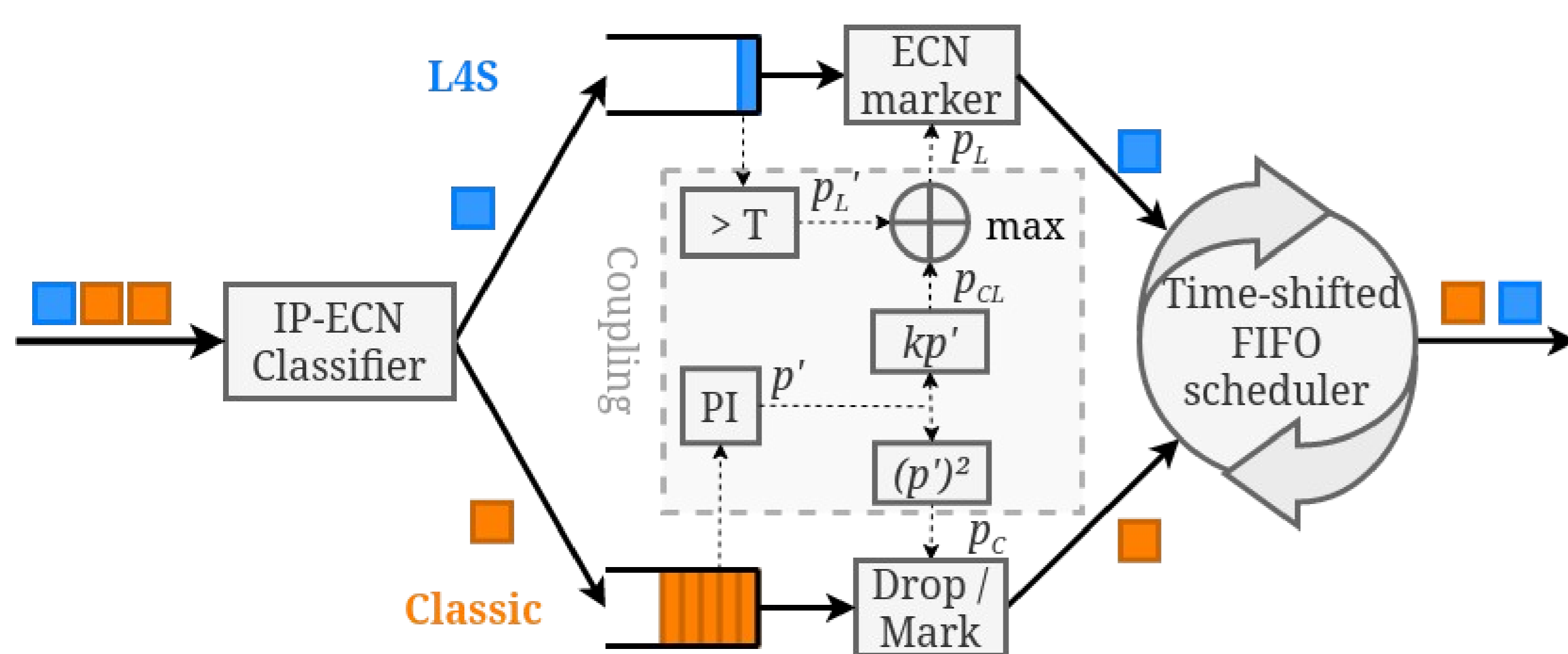
Principes généraux

- Réactivité : 2 files d'attente à probabilité de signalement différenciée
- Cohabitation : Couplage isolant la performance



Couplage des AQM

- p_x : probabilités de signalement
- Isolation entre flux classiques (C) et faible latence (L)
- Réactivité adapté à la congestion
- Prévient la famine de (C)



Problématique

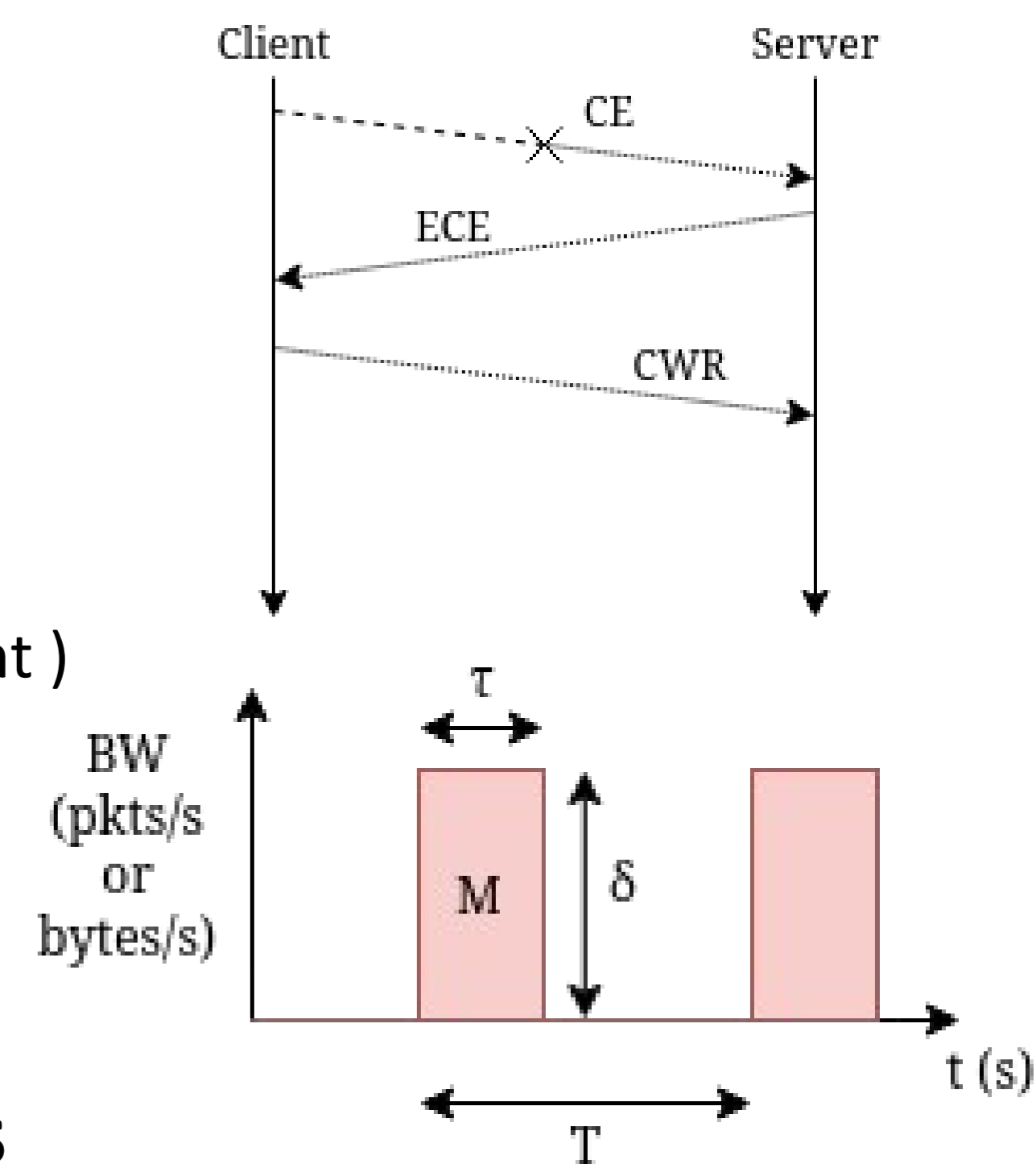
- Latence \Rightarrow nouvelle ressource à cibler (et il en faut peu !)
- AQM sensible au DoS (RFC7567) et L4S sensible aux bursts
- Quelles vulnérabilités ? Quels modèles d'attaques ?
- Quels impacts sur l'architecture et sur les autres participants ?
- Quelle détection et contre-mesures sans impacter la latence ?

Menace portée sur la latence dans L4S

Les « flux indésirables » :

- Implémentations fait-maison** (dysfonction) et / ou
- Détournements volontaires** (attaque)

- Flux malformés** :
 - Souvent légitimes
- Flux Unresponsive** :
 - Parfois légitimes
 - Surchargent les files d'attente
- Flux Misbehaving** :
 - Manipulation protocolaires (signalétique et/ou comportement)
 - Malformations délibérées



Contre-mesures actuelles

Solutions de l'IETF

- Flux malformés** :
 - Ordonnanceur réseau adapté
 - Traffic Shapping
 - Traffic Policing
 (Mais attention au *bufferbloat* !)
- Flux Unresponsive** :
 - Sacrifice de performances (débit, délais ou drop)
- Flux Misbehaving** :
 - Manipulations protocolaires : patches protocolaires, détecteur à état
 - Malformations délibérées : idem que pour flux malformés

À court terme

- Conception d'une attaque combinant les vulnérabilités identifiées :
 - En désactivant le *TCP Pacing* et le *fair-queuing* (sans être suspect)
 - Génération de *unresponsive ECN-capable flows*
 - Bursts* de paquets de manière occasionnelle (*low-rate DoS*)

À long terme

- Élaboration d'un **modèle mathématique** reliant la probabilité de signalement de congestion, l'évolution de la fenêtre de gestion et les dégâts induits
- Conception de **modèles de détection statistique** de ces attaques
- Intégration dans un **micro-service** de détection orchestrable
- Élaboration de contre-mesures utilisant la programmabilité réseau par une approche en micro-services