

MOSAICO:

Multi-layer Orchestration for Secured and low-Latency applications

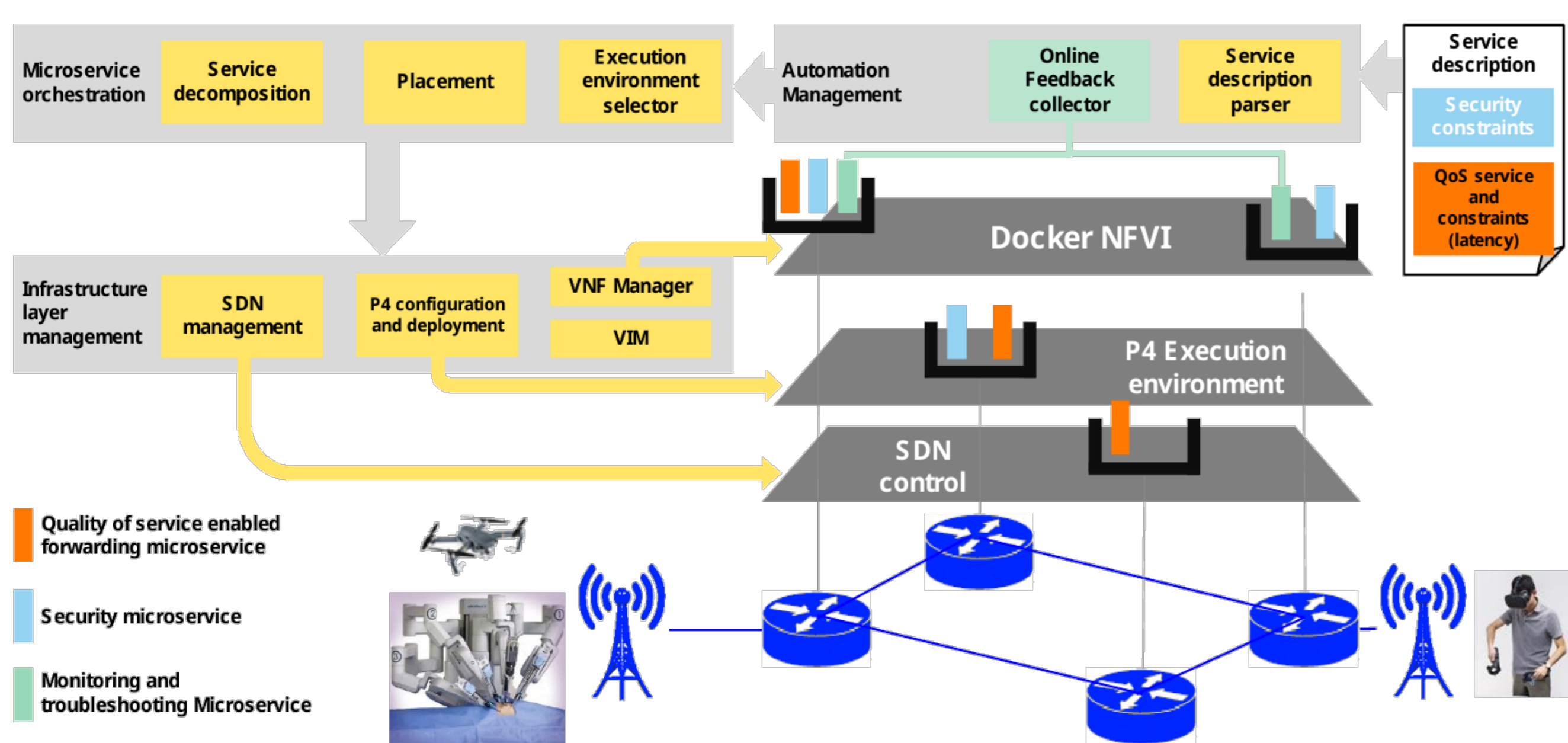
Marius Letourneau : marius.letourneau@utt.fr

Contexte

Evolution de l'usage de l'Internet

- De **nouveaux services** ont de **fortes exigences sur la latence** et poussent à créer de **nouvelles classes de trafic**
Exemples : *Cloud Gaming, usine 4.0, Internet haptique etc..*
- La **programmabilité des réseaux**, la virtualisation de fonctions réseaux (NFV) et le **Software Defined Networking** ont permis d'accroître les performances du trafic sur Internet
- Nouvelles évolutions : le découpage de fonctions réseaux en micro-services

L'architecture Mosaico



Objectifs : répondre au besoin de faible latence en offrant des solutions pour :

- Identifier les **fonctions réseaux** faible latence à convertir en micro-services
- Définir des **solutions d'orchestration** permettant la gestion de micro-services déployés dans un milieu technique hétérogène
- Appréhender le **placement optimal** des micro-services
- Assurer la **robustesse** de la solution face à des comportements malveillants

Les sources de la latence

La latence vient essentiellement :

- Du **temps de traitement** des entités terminales et des middleboxes
- Du **temps d'acheminement** des données dans le réseau

Vis à vis du temps d'acheminement

deux problèmes :

- La **taille** des files d'attente
- La **réactivité** à la congestion

Solutions :

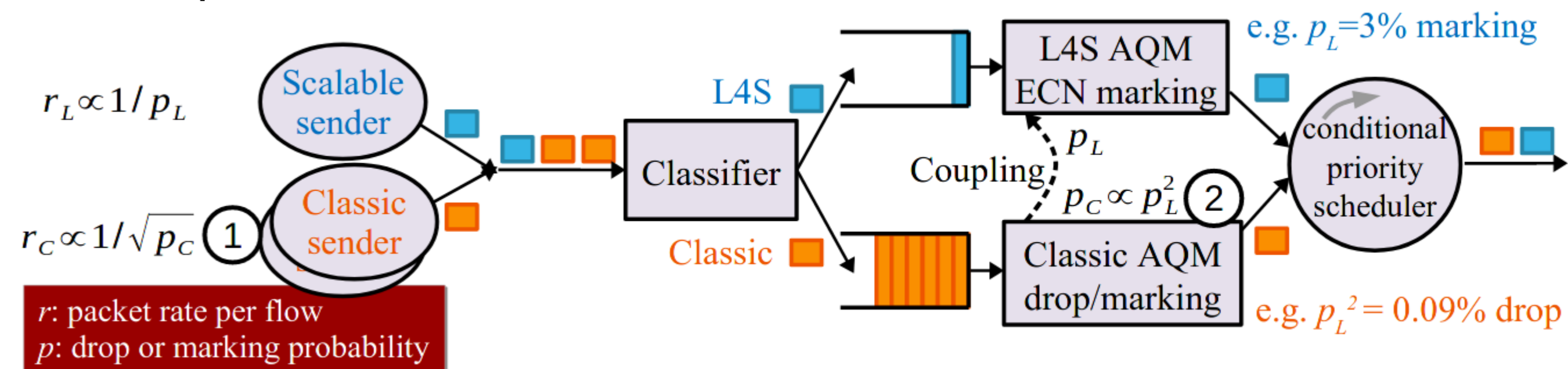
- **Active Queue Management**
- Nouveaux algorithmes de **contrôle de congestion**
- **Explicit Congestion Notification**

Architecture L4S

Une architecture standardisée par l'IETF qui combine ces solutions

(**L4S** : Low Latency, Low Loss, Scalable throughput)

- **Réactivité** : 2 files d'attente à probabilité de signalement différencié
- **Cohabitation** : Couplage pour isoler la performance de chaque file d'attente



Les attaques possibles sur la latence

Il existe des flux déviants que l'on appelle les *misbehaving flows*. Ils peuvent venir de deux facteurs :

- **Implémentations fait-maison** (dysfonction)
- **Détournements volontaires** (attaque)

Attaques visant la latence

- Low-Rate DoS : vise à **déclencher le ralentissement** de l'émission des entités distantes et à **saturer les files d'attente** des routeurs
- Manipulation des **algorithmes de contrôle de congestion** (*Hacked ACK*)
- Manipulation des **signaux de congestion** (*Hacked ECN*)

À court terme :

- Quid de la robustesse de l'architecture L4S : l'IETF et le projet européen RITE ont déjà identifié des vulnérabilités
- Étude de l'impact du trafic déviant (*misbehaving*) sur l'architecture L4S
- Étude de l'impact réciproque de la stratégie de couplage des classes de trafic standard et low-latency
- Évaluation de la résistance aux différentes attaques identifiées dans l'état de l'art sur l'Internet faible latence

À court terme :

- Conception de modèles de détection statistique de ces attaques
- Intégration dans un micro-service de détection
- Élaboration de contre-mesures utilisant la programmabilité et les micro-services pour s'en prémunir