

Réseaux sans fil de nouvelle génération : architectures spontanées et optimisations inter-couches

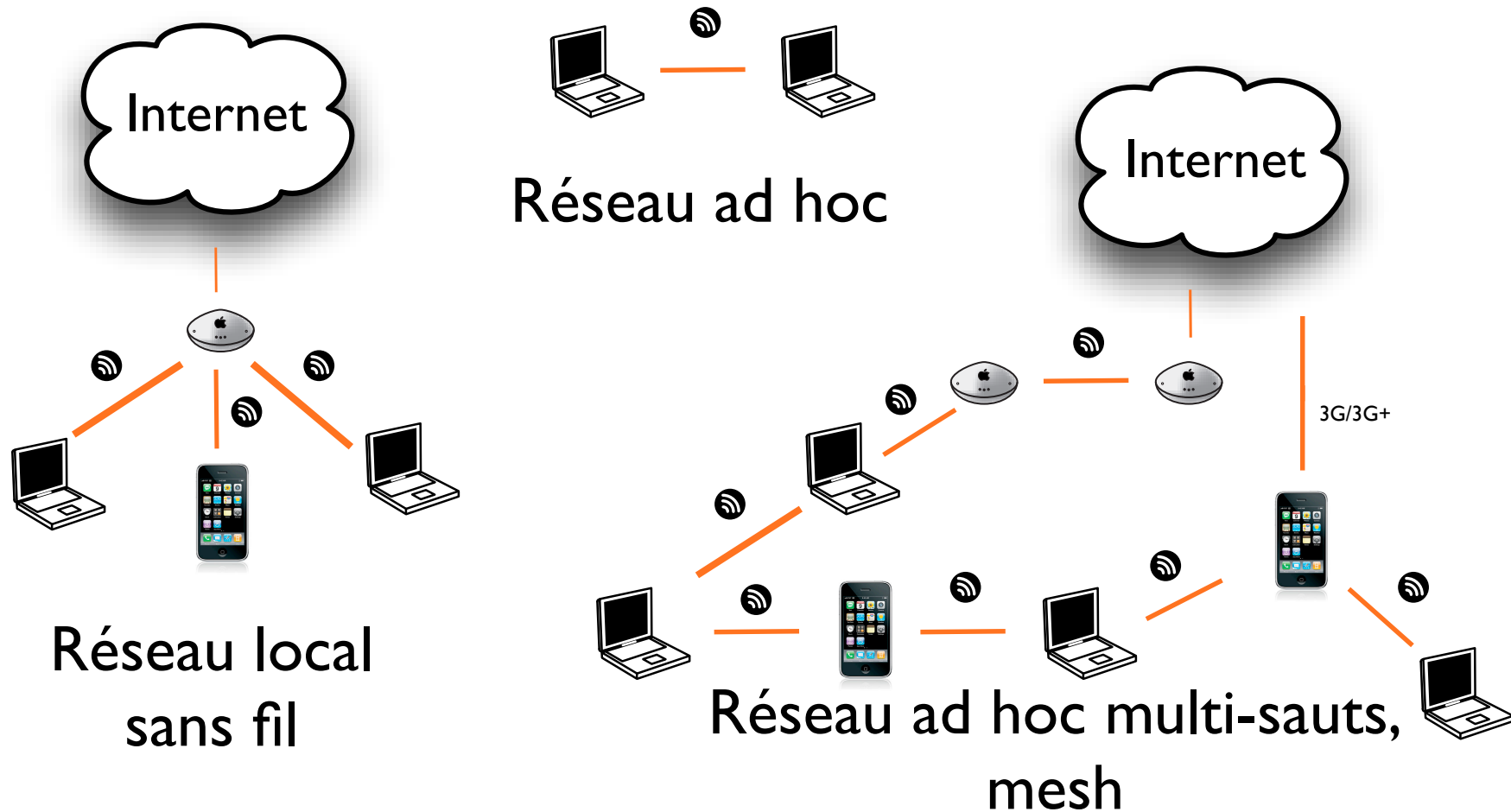
Yan Grunenberger

Travaux effectués dans l'équipe Drakkar
sous la direction d'Andrzej Duda et Franck Rousseau

Mercredi 3 décembre 2008



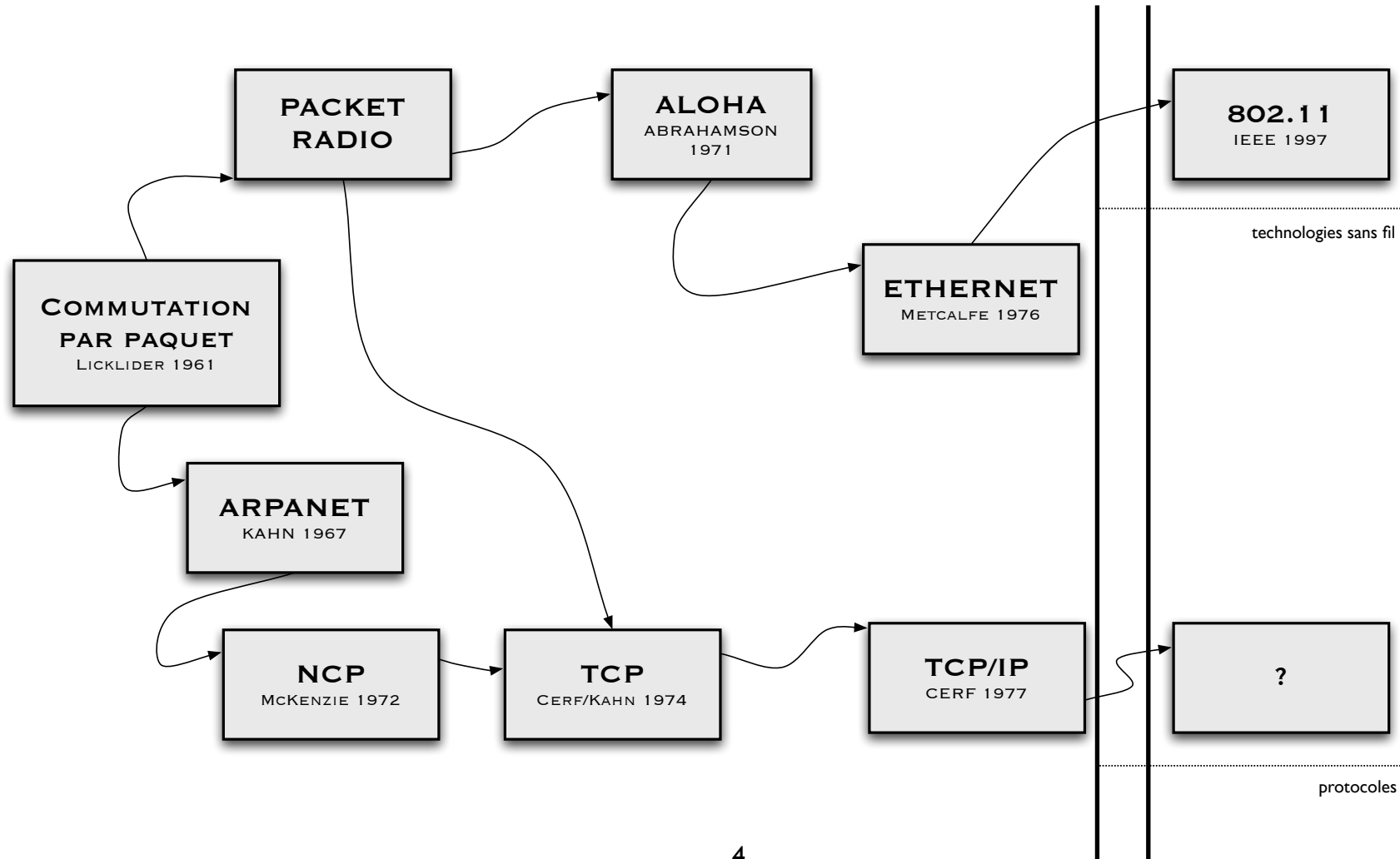
Réseaux sans fil de nouvelles générations



Sommaire

- Histoire des réseaux
- Architecture en couche
 - ◆ Autopsie des réseaux WiFi
- Virtualisation du réseau
 - ◆ Segmentation temporelle
 - ◆ Outil générique de manipulation de paquet
 - ◆ Mise en application au cas de mobilité
- Conclusions et perspectives

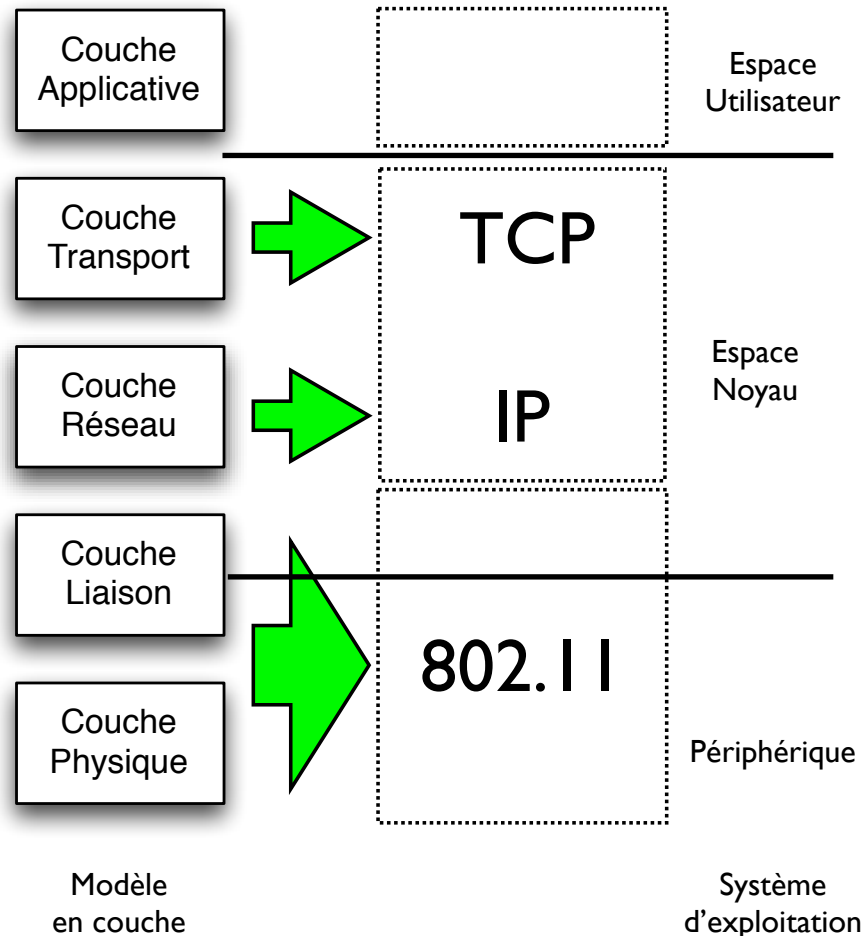
Historique



Historique

- Evolution rapide du réseau
 - ◆ mais stagnation depuis Ethernet - TCP/IP
- Renouveau avec les technologies sans fil
 - ◆ 802.11 évolution sans fil d'Ethernet
 - ◆ brise les hypothèses historiques
 - ◆ remet en cause l'architecture

Situation de TCP/IP



- Élément enkysté dans les systèmes d'exploitations actuels
 - ◆ prisonnier en espace noyau
- Composant central de l'architecture en couche
 - ◆ ne peut donc être modifié !
- Doit-on remettre en cause le modèle ?

Autopsie : physique

Couche
Applicative

Couche
Transport

Couche
Réseau

Couche
Liaison

Couche
Physique

- Communication half-duplex
 - ◆ Emission OU réception
- Chaque transmetteur voit ses congénères comme des sources d'interférences (pas de transmissions simultanées)
- Multiples modulations physiques
 - ◆ Couche de compatibilité nécessaire pour pouvoir se comprendre (ex : PLCP)

Autopsie : liaison

Couche
Applicative

Couche
Transport

Couche
Réseau

Couche
Liaison

Couche
Physique



- Offre une méthode d'accès CSMA/CA utilisant la Distributed Coordination Function
 - ◆ Basée sur le principe que les hôtes voient le même état
 - ◆ Responsable d'une anomalie de performance en cas de débit multiple
 - ❖ Solutions : choix dynamique de la fenêtre de contention : ex. Idle Sense

Autopsie : phys/liaison

Couche
Applicative

Couche
Transport

Couche
Réseau

Couche
Liaison

Couche
Physique

- La norme 802.11 ne permet d'assumer qu'un seul rôle
 - ◆ connexion ad hoc OU à un point d'accès
- Pourtant, plusieurs réseaux peuvent cohabiter sur le même canal
 - ◆ Multi-rôle de niveau 2
 - ❖ Connexion simultanée à 2 points d'accès

Autopsie : réseau

Couche
Applicative

Couche
Transport

Couche
Réseau

Couche
Liaison

Couche
Physique



- Repose sur l'utilisation du paquet IP
 - ◆ adressage IP pas forcément pertinent en sans fil (ex : adressage géographique)
 - ◆ routage traditionnel suivant le nombre de saut plus valide en sans fil
 - ❖ nouvelles générations de protocoles (OLSR, AODV)
 - ❖ approche inter-couches

Autopsie : transport

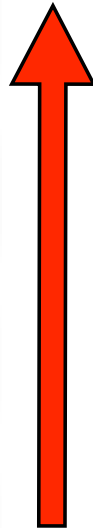
Couche
Applicative

Couche
Transport

Couche
Réseau

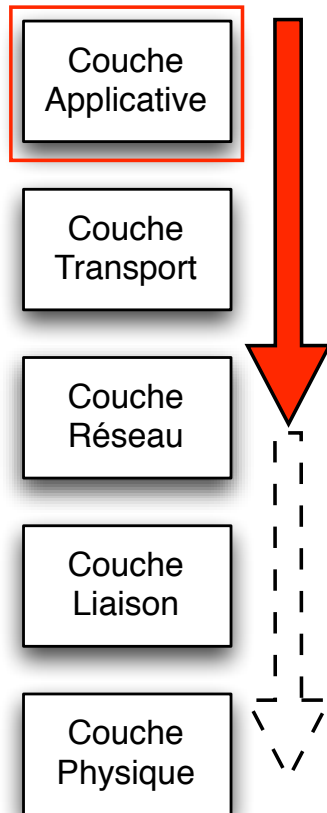
Couche
Liaison

Couche
Physique



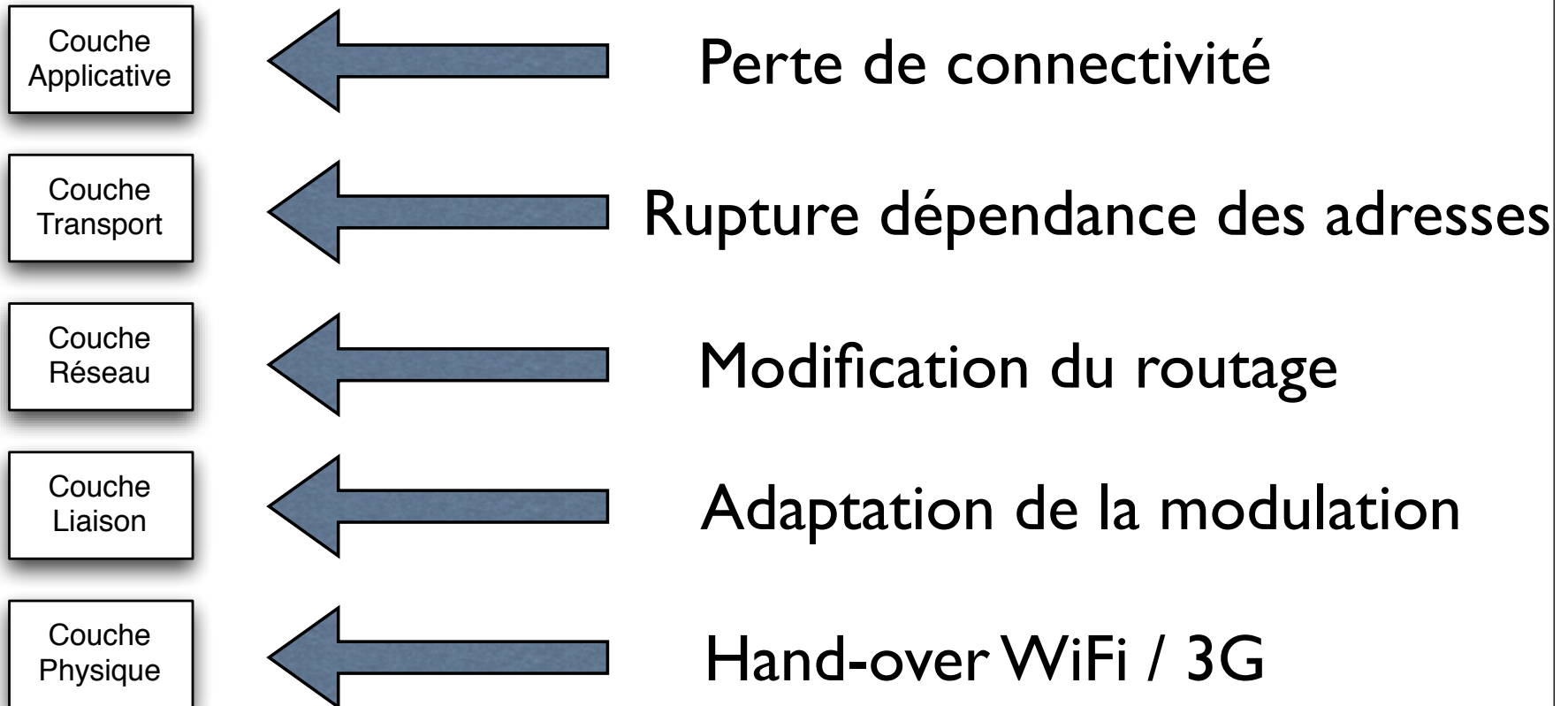
- Repose sur l'utilisation de TCP
 - ◆ TCP interprète toute perte de segment comme un signe de congestion...
 - ◆ ... fondamentalement inadapté au réseau sans fil !
- Connectivité de bout en bout entre 2 adresses IP
 - ◆ Confusion Adresse/Identifiant ?

Autopsie : application



- Les applications ne peuvent exprimer leur besoin à la pile réseau de manière parfaite
 - ◆ exemple : QoS au niveau IP doit être traduite en une QoS au niveau 802.11
- Les applications n'ont pas conscience des événements agissant sur les couches inférieures
 - ◆ exemple : la mobilité est un problème pour les applications de flux temps réel (VoIP)

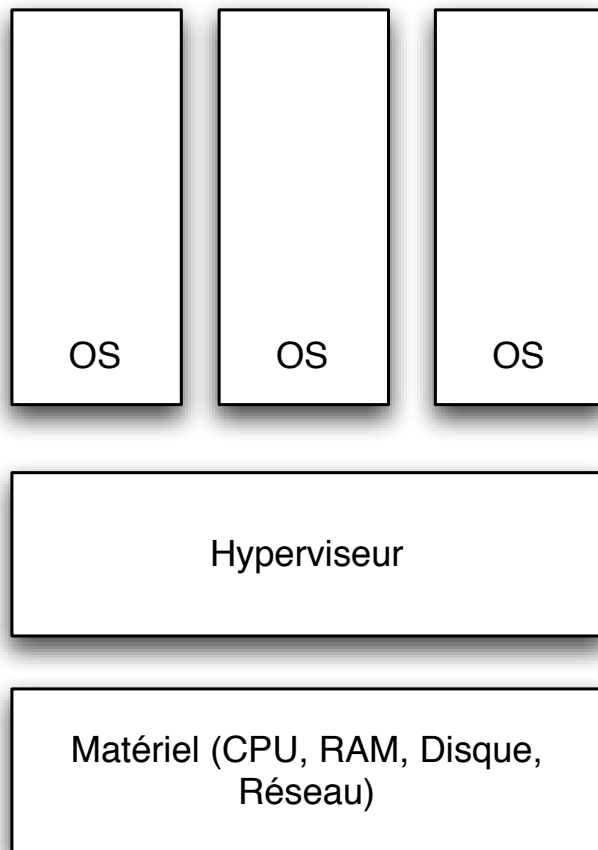
Application à la mobilité



Bilan sur le modèle en couche

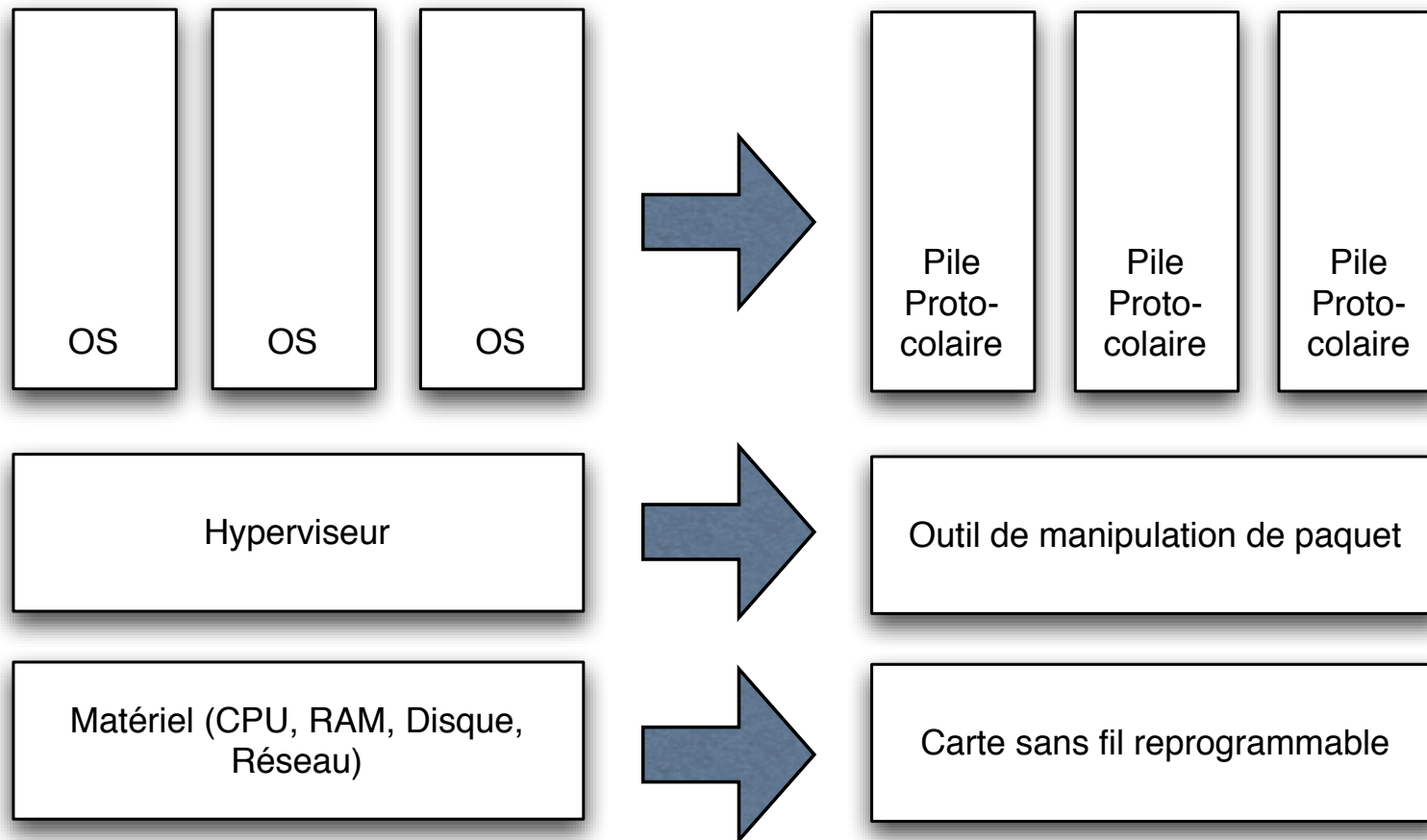
- Fondamentalement inadapté au médium sans fil
 - ◆ adaptation de la pile protocolaire nécessaire
 - ◆ approche globale et non plus localisée

Idée : analogie avec la virtualisation



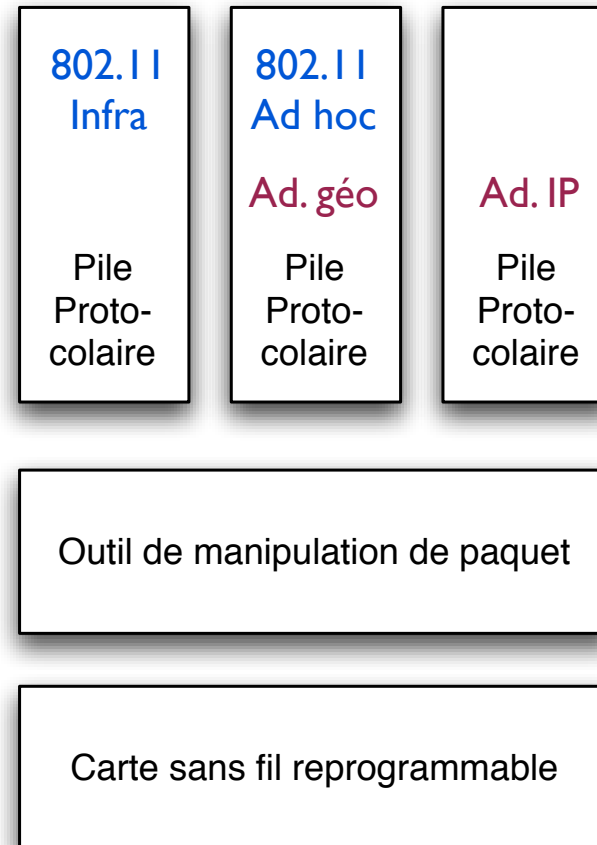
- Principe : faire fonctionner sur une seule machine un ou plusieurs systèmes d'exploitation
- Hyperviseur : noyau système ultra léger

Virtualisation Réseau



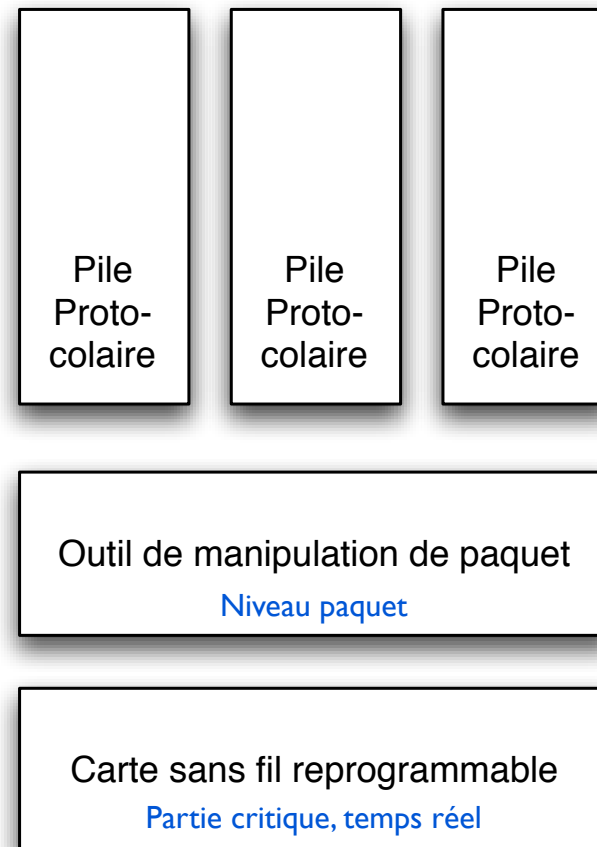
Exemples envisagés

- A l'échelle du paquet...
 - ◆ Une pile peut fonctionner en point d'accès, une autre en mode ad-hoc (802.11)
 - ◆ Utiliser un adressage IP traditionnel et un adressage géographique en parallèle
- A l'échelle du symbole ?



Comment ?

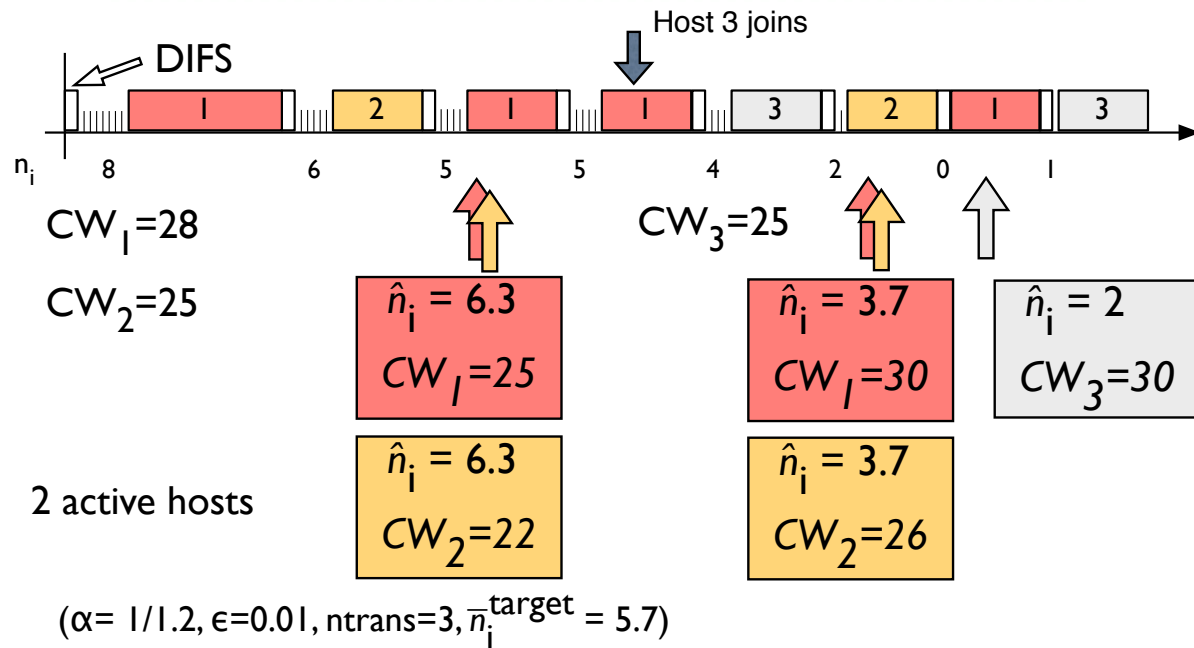
- “Matériel” : Carte sans fil programmable
- Echelle temporelle : le symbole - temps réel
- “Hyperviseur” : Outil de manipulation de paquet
- Echelle temporelle : le paquet



1ère contribution : évaluation d'une plateforme programmable temps réel

- Objectif : Evaluer à quel point on peut modifier la partie basse du modèle proposé
 - ◆ Idle Sense conçu par notre équipe
- Permet d'évaluer la souplesse dans les couches contraintes

Idle Sense, principes



Prérequis

- Matériel offrant une couche MAC programmable
 - Carte Intel centrino à micrologiciel
- Accès et manipulation
 - du comptage des slots
 - de la fenêtre de contention

Implémentation

- Idle Sense repose sur l'utilisation d'Additive Increase/Multiple Decrease (AIMD)
- Paramètres d'AIMD obtenus précédemment par simulation
- Cependant
 - Pas de division sur la plateforme, pas de flottant

Implémentation

- Adaptation de l'algorithme original

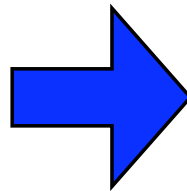
$$n_i^{\text{target}} = 3.91$$

$$\frac{1}{\alpha} = 1.0666$$

$$\epsilon = 6.0$$

$$\beta = 0.75$$

$$\gamma = 4$$



$$n_i^{\text{target}} = 4$$

$$\alpha = 1 - 1/16$$

$$\epsilon = 6$$

$$\beta = 1$$

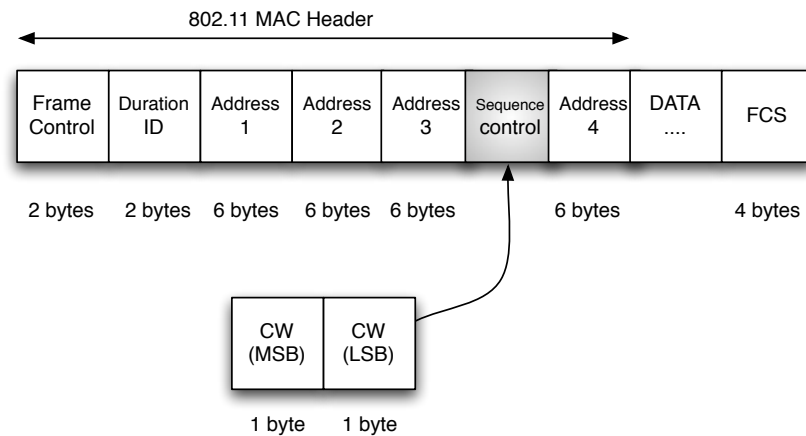
$$\gamma = 4$$

Implémentation

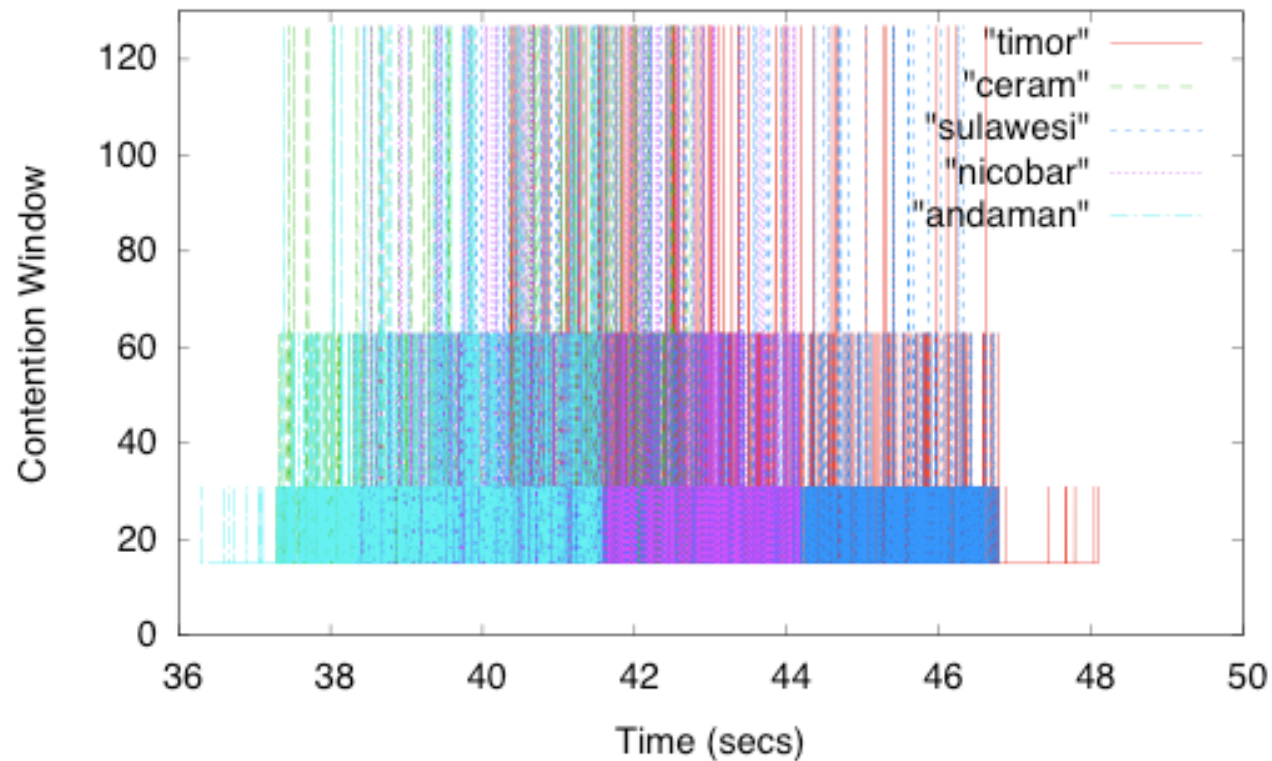
- Idle Sense doit disposer d'un générateur aléatoire quelconque
- Celui de 802.11 n'utilise que des puissances de deux avec un registre à décalage
- Modification du générateur aléatoire nécessaire

Débogage

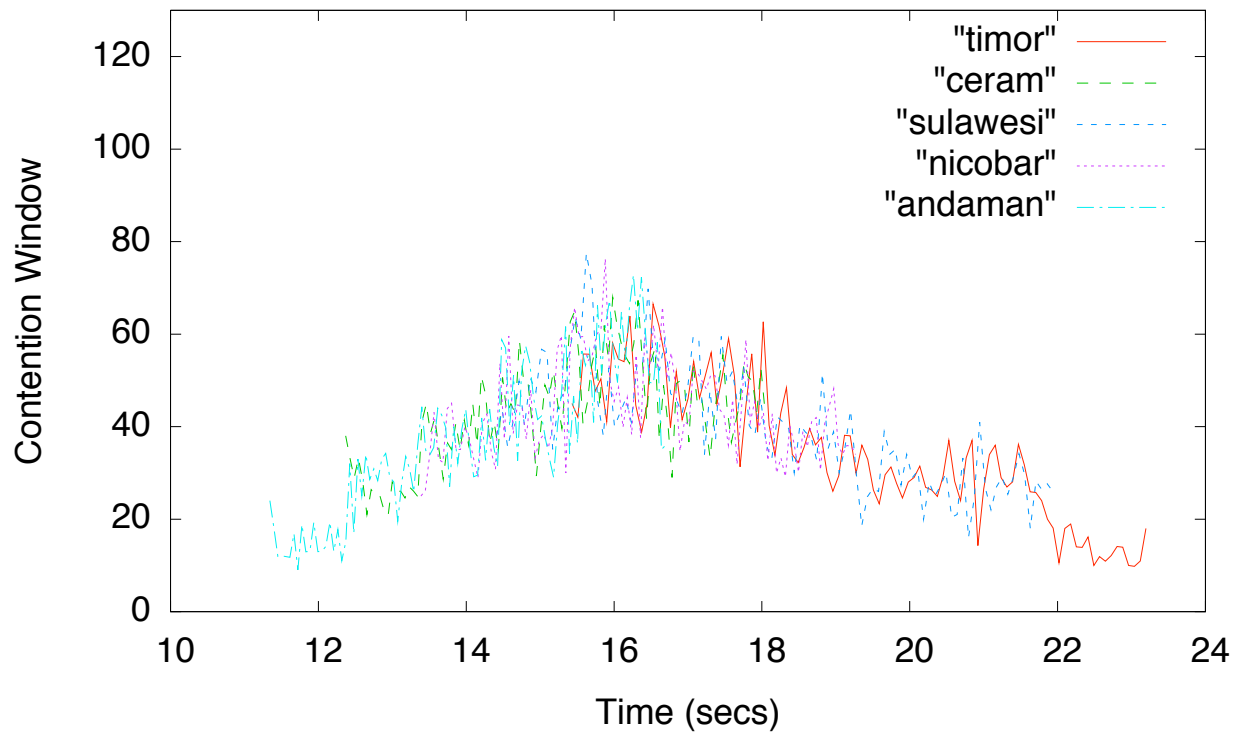
- Pas d'outil disponible
- Nécessité de construire des outils par des moyens détournés



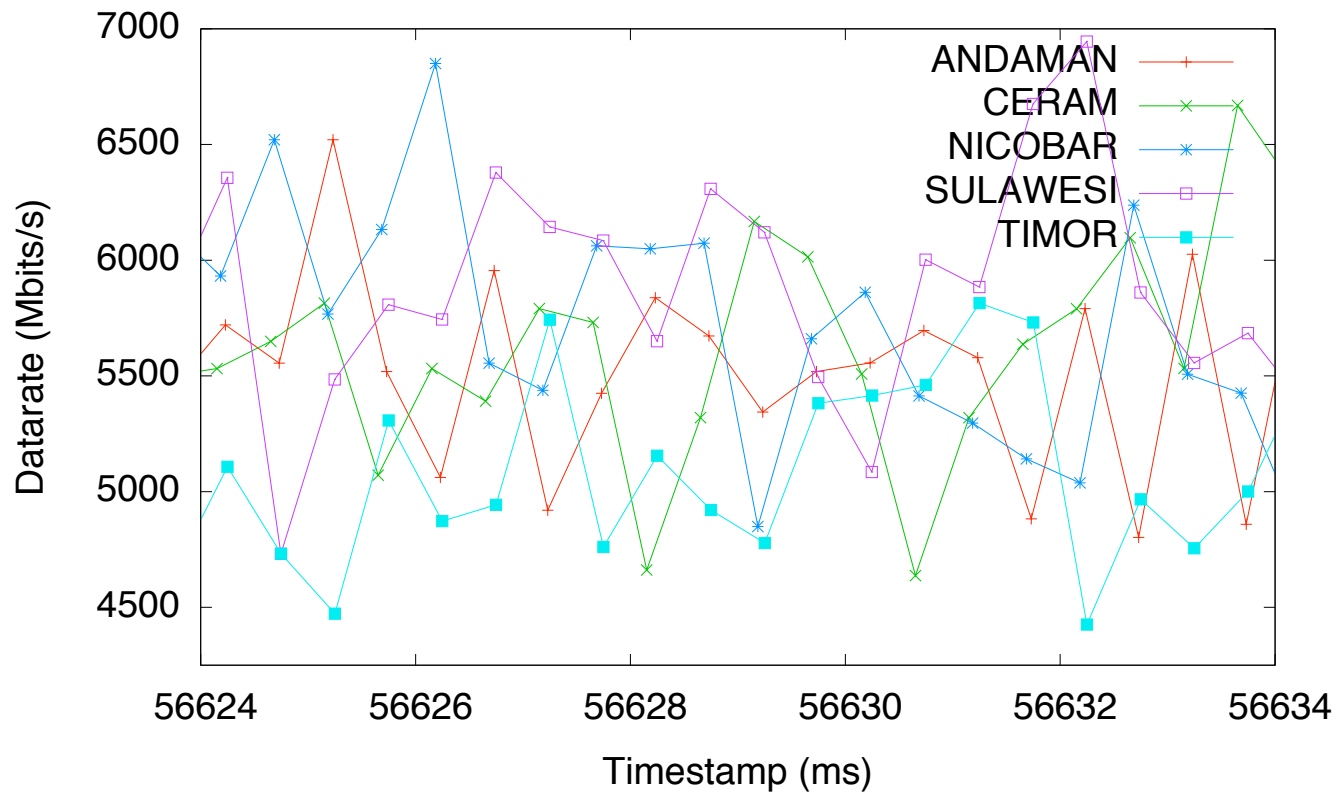
Performances : évolution de la contention (DCF)



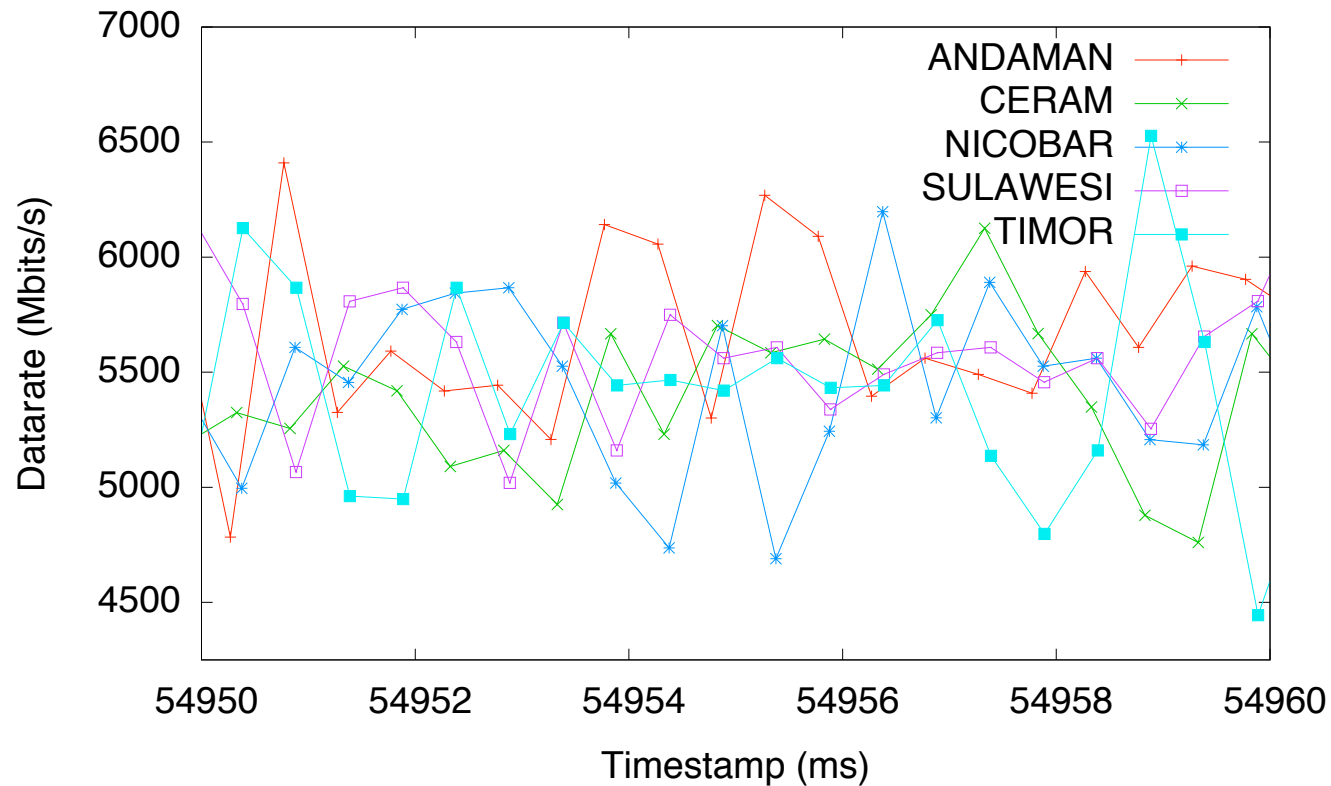
Performances : évolution de la contention (Idle Sense)



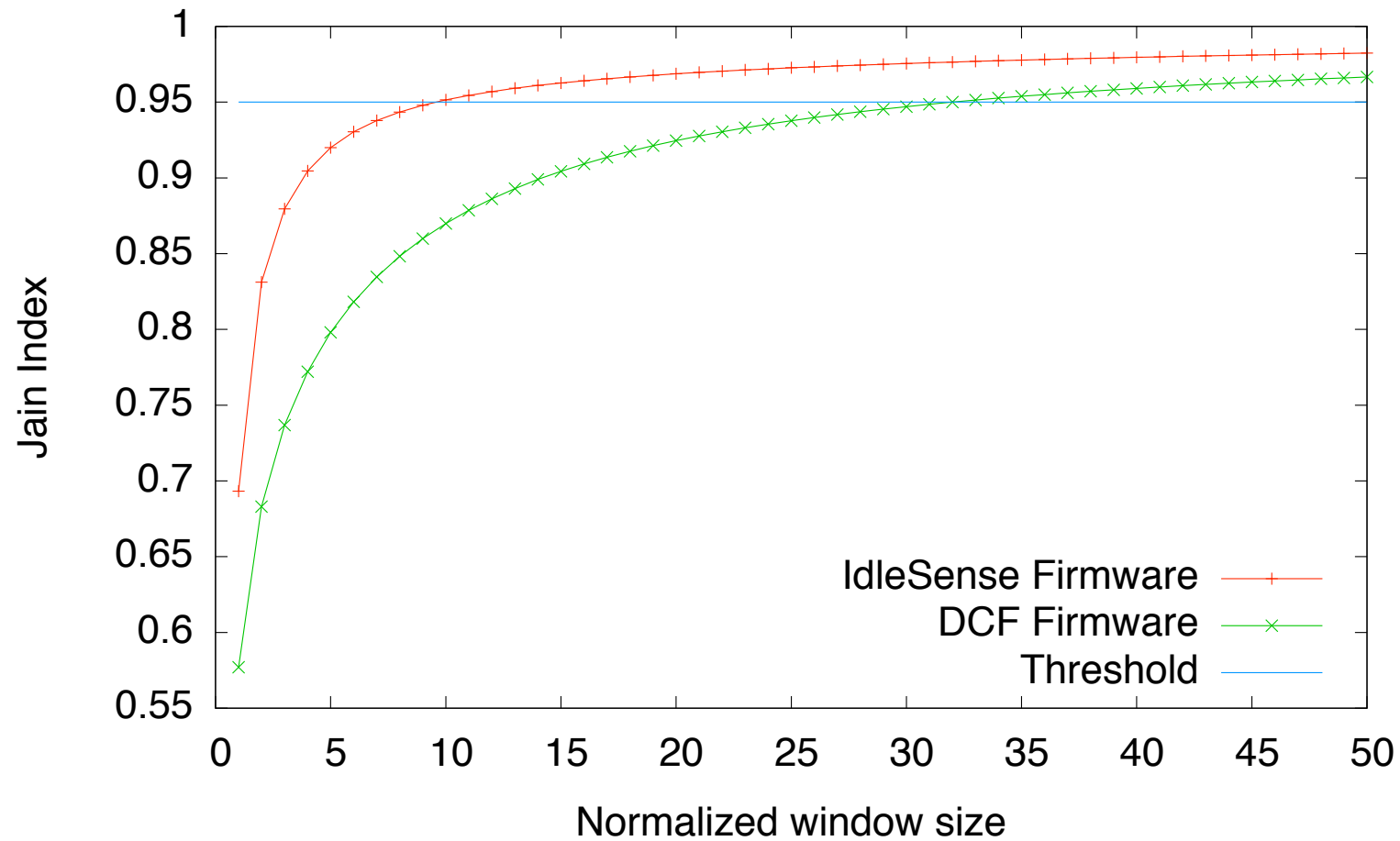
Performances : évolution du débit (DCF)



Performances : évolution du débit (Idle Sense)



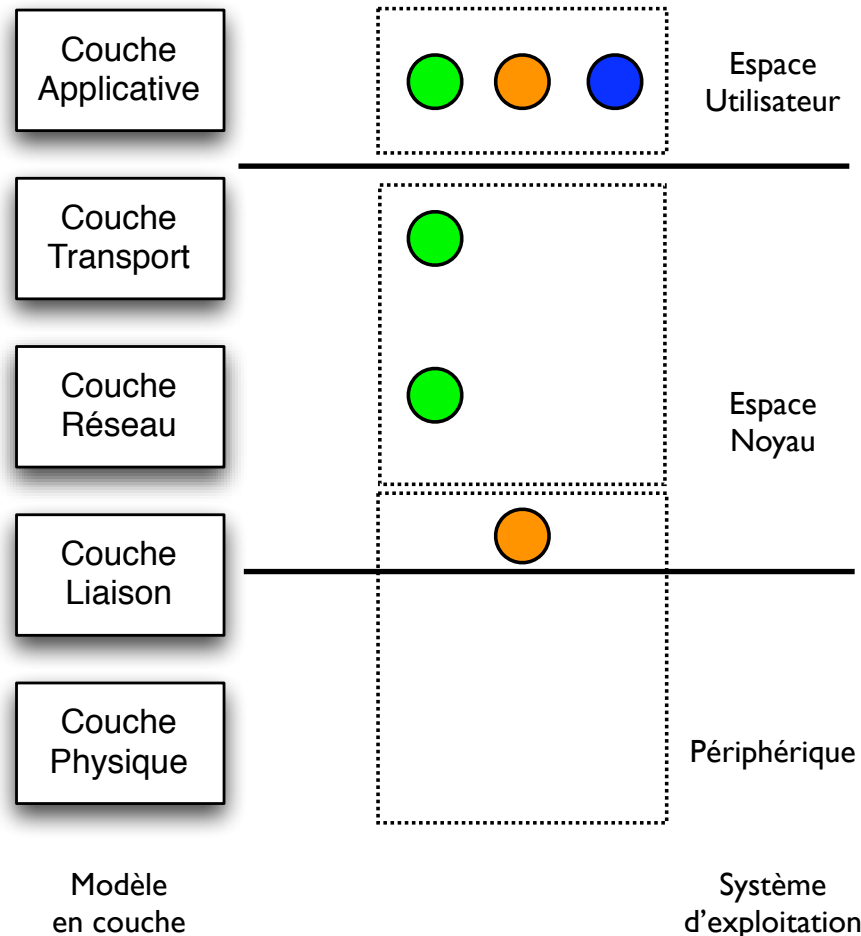
Vérification pratique de l'équité






Bilan

- L'implémentation d'Idle Sense est possible sur une plate-forme programmable temps réel
- Prélude à l'utilisation des Software Defined Radio
 - Granularité encore plus fine
 - Souplesse pour la configuration

2ème contribution : Réalisation d'un outil de manipulation de paquet

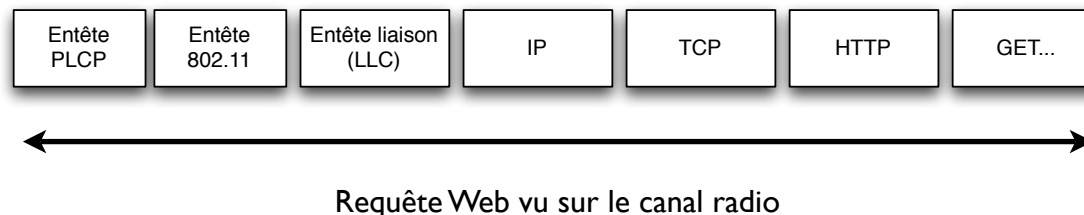


- Les frameworks existants s'appuient exclusivement sur le modèle en couche

- Click 
- XIAN 
- PRAWN 

Travaux connexes

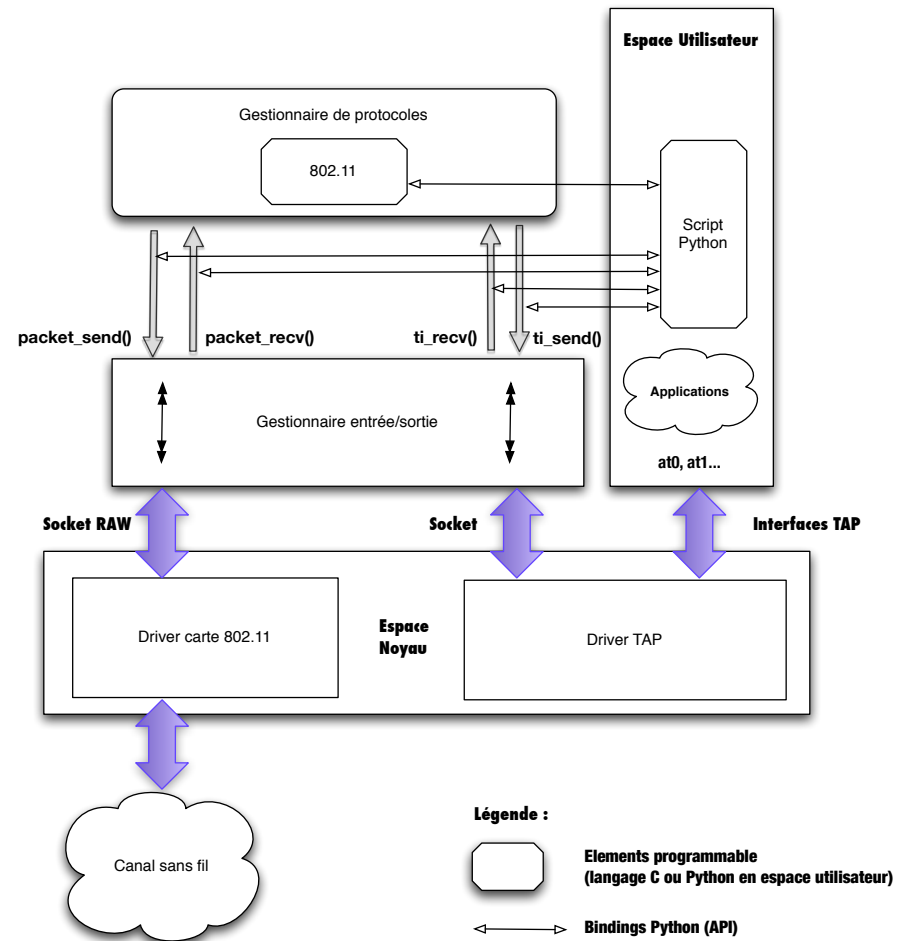
- Sécurité en réseau : contourner le système
- Injection de trafic arbitraire
- Principe : un paquet offre une vision globale et inter-couches



PACMAP : PACket MAniPulation tool

- Outil visant à assurer le rôle d'hyperviseur au sens réseau
- Envoi/réception des paquets et génération d'évènements
- ◆ Ensemble minimum des fonctions d'interactions

PACMAP sous linux



Interfaces programmables

- en Python ou en C
- Événements implémentés
 - ◆ Envoi / réception sur le canal radio ou dans le système d'exploitation
 - ◆ Évènements 802.11 : authentification, association etc...

Possibilités

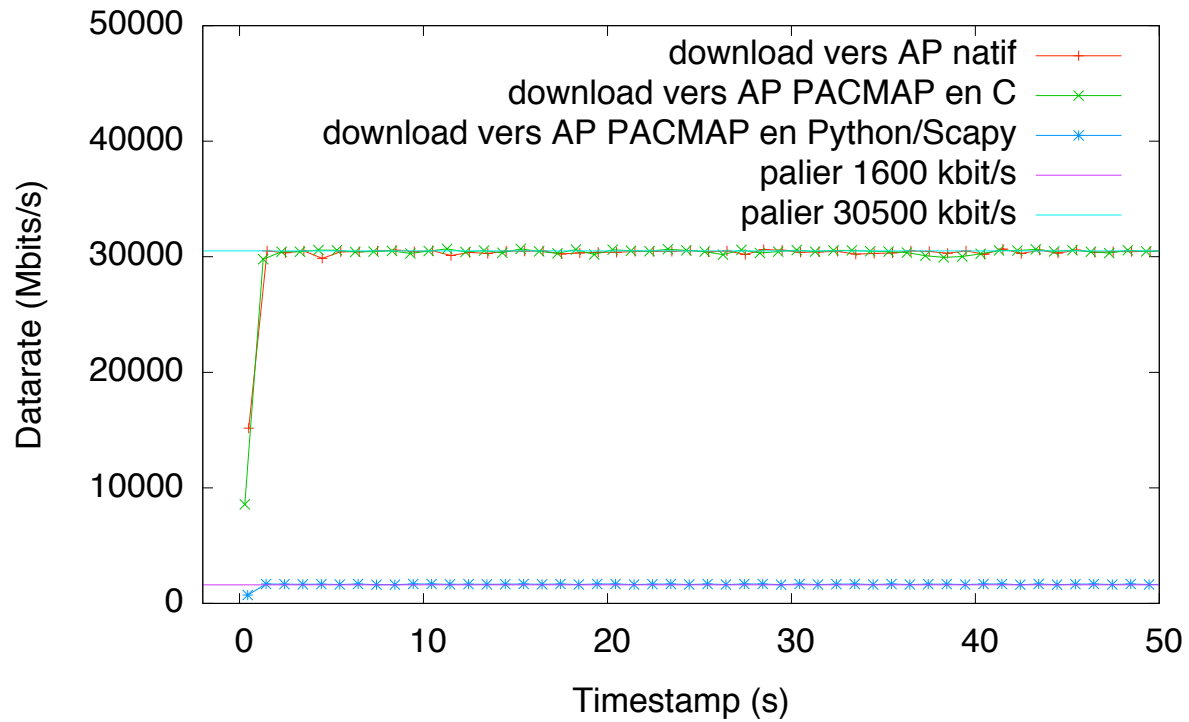
- Interfaçage possible avec des bibliothèques externes, comme Scapy

```
def proto80211_auth(packet, length):  
    dot11_frame = Packet(packet)  
    dot11_frame.decode_payload_as(Dot11)  
    dot11_answer = dot11_frame  
    addr1= dot11_frame.getlayer(Dot11).addr2  
    dot11_answer.getlayer(Dot11).addr1= addr1  
    dot11_answer.getlayer(Dot11).addr2= bssid  
    dot11_answer.getlayer(Dot11Auth).seqnum=0x02  
    pacmap.sendpacket(str(dot11_answer),len(str(dot11_answer)),1)  
    return 1
```

Performances de l'implémentation

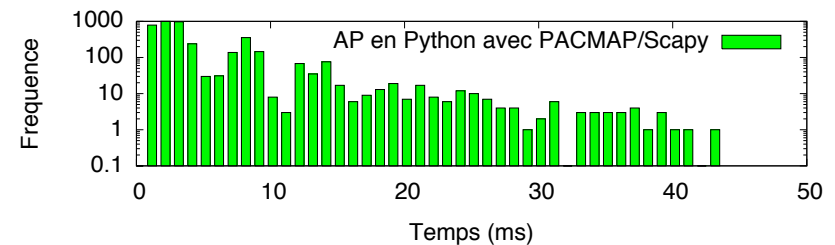
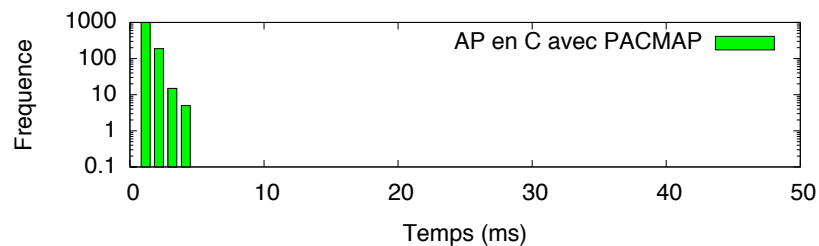
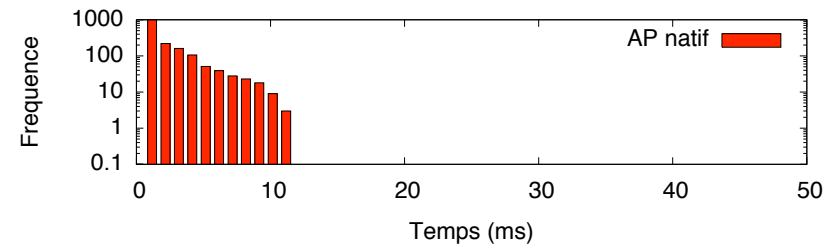
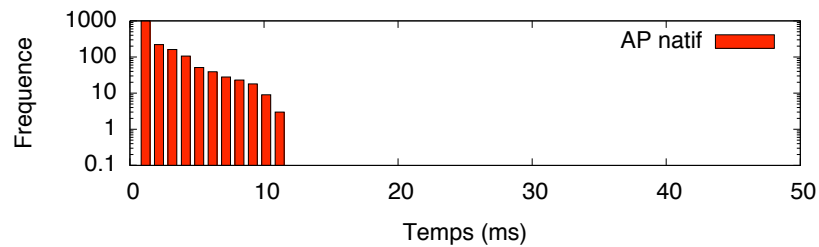
- Python : langage scripté, charge importante pour le système hôte
- Langage natif plus adapté aux manipulations exigeant des performances (latence/débits)
- Vérifications sur l'implémentation d'une pile 802.11 simplifiée (pas de chiffrement)

Performance PACMAP débit



Performance PACMAP

latence



Implémentation en C

Implémentation en Python

Bilan

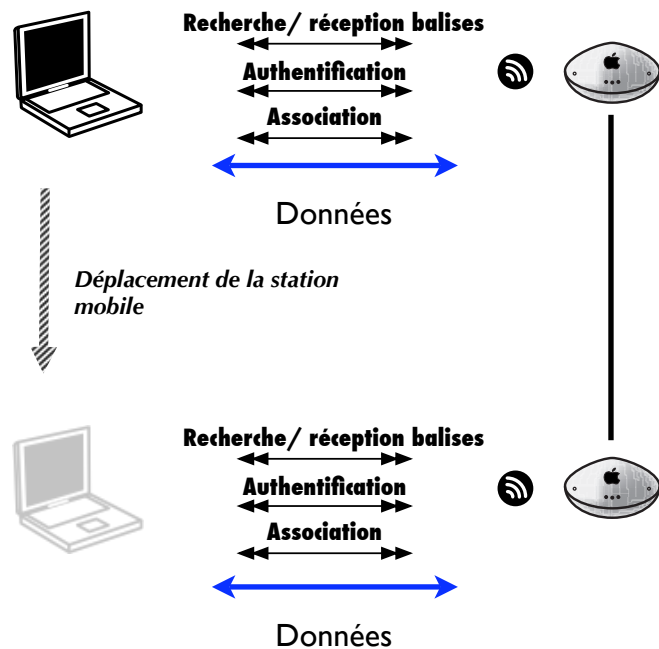
- Facilité de développement et de test
- Performances acceptables en script, indifférenciables en natif

3ème contribution :

application à la gestion de la mobilité

- Le déplacement des terminaux mobiles est mal géré au sein d'un même réseau sans fil constitué de points d'accès interconnectés
- La connectivité semble s'interrompre lors du passage d'un point d'accès à un autre

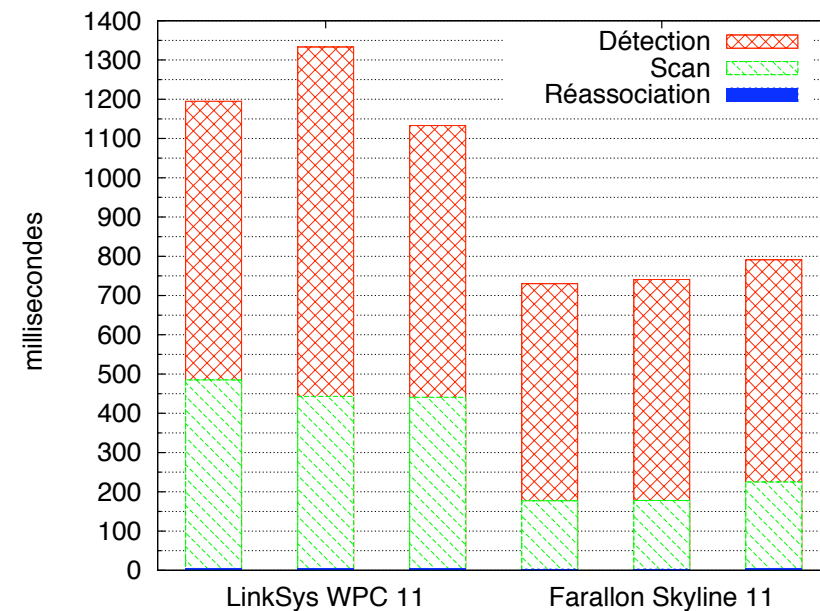
Origine du problème



- Approche classique
- Mobilité contrôlée par le terminal
- Délai de handover long

Observations

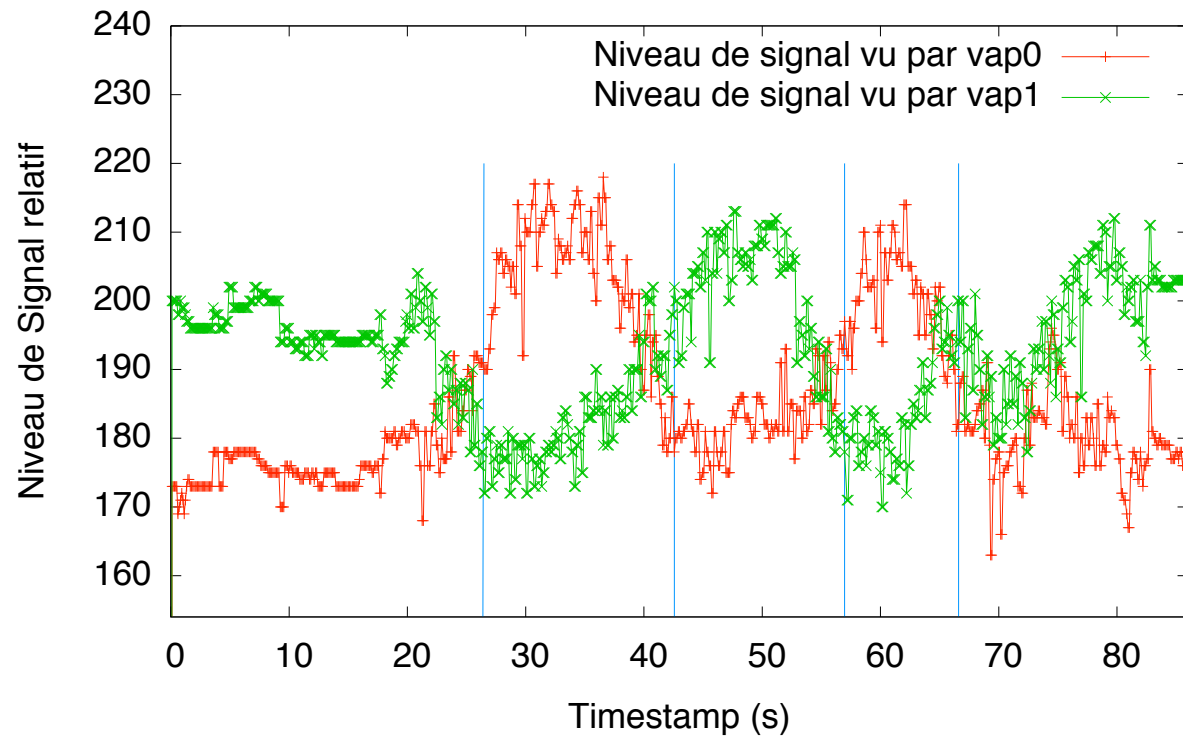
- Thèse de Sorin Paun (2003)
- Délais observés (600 ms) incompatibles avec la VoIP (200 ms pour maintenir l'intelligibilité)



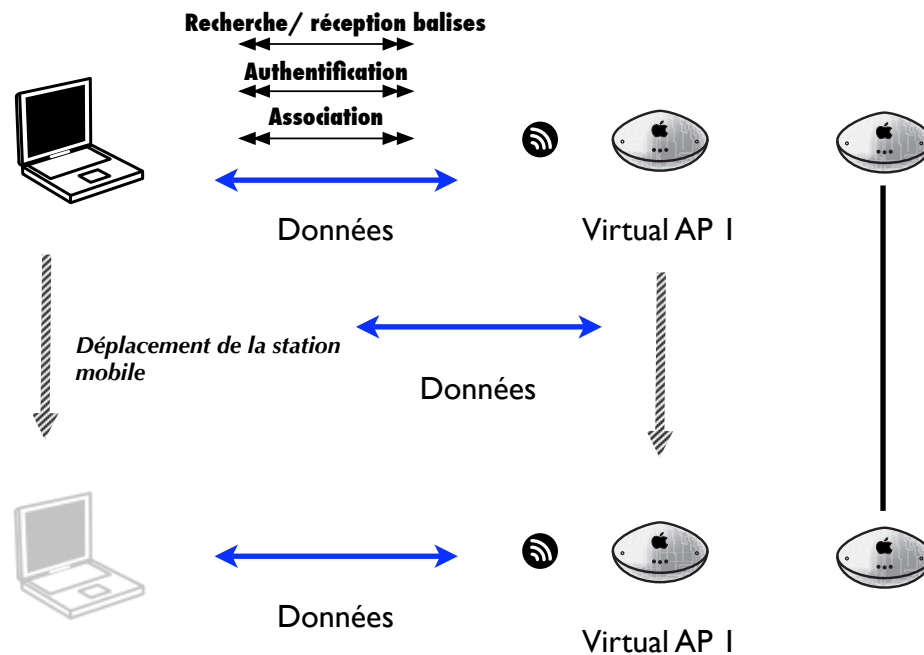
Observations

- Minimiser les phases de détection/scan
 - Le client doit donc toujours croire que sa connectivité est maintenue
 - or, celle-ci est assurée par la réception continue des balises
- En fabriquant des balises, on maintient la connexion

Suivi du client



Virtual AP



- Solution issue de notre proposition de virtualisation
- Première étude sur un cas concret n'incluant pas toutes les subtilités des réseaux réels

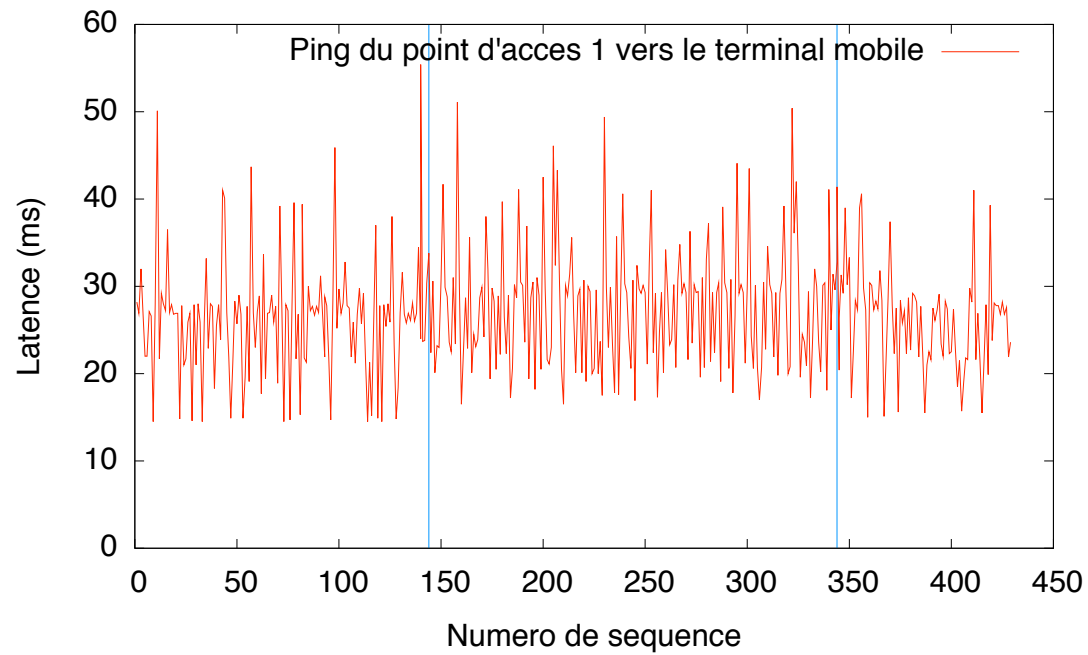
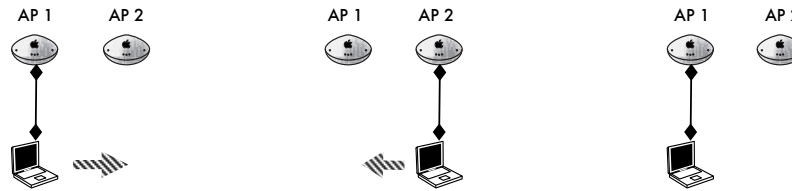
Remarques

- Limitations
 - Un seul canal géré mais ajout d'une information dans les balises possible
 - Pas de contexte de sécurité mais à priori faisable (s'inspirer de Radius)

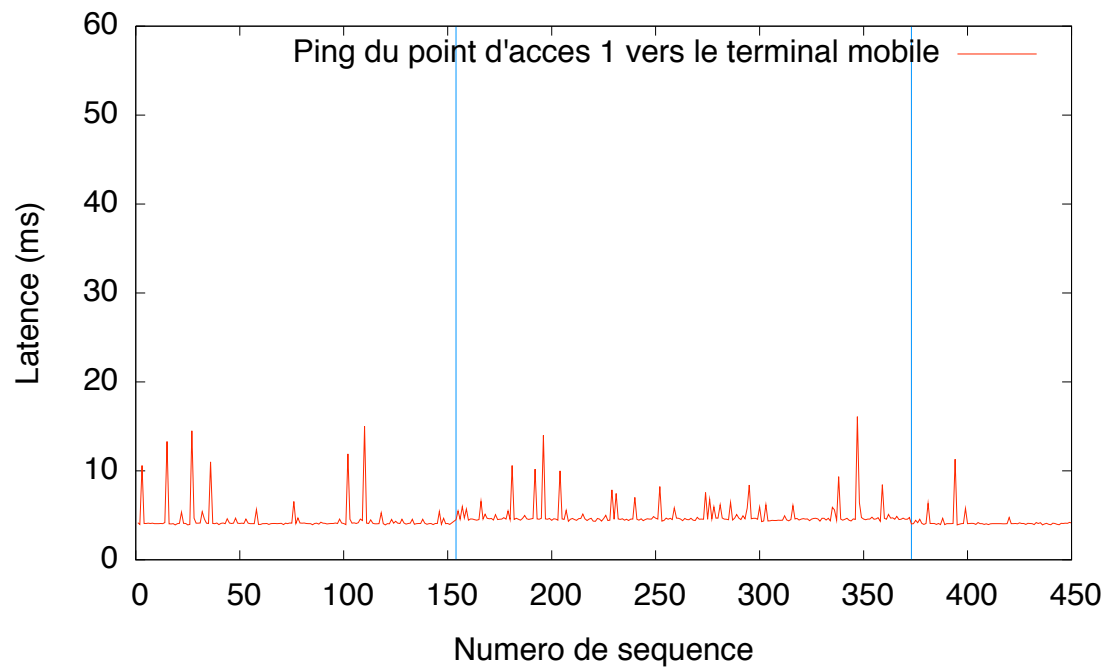
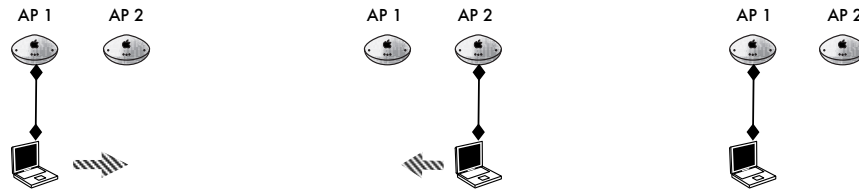
Prototypage

- En Python puis en C
 - 250 lignes en python, 1000 lignes en C
- L'évaluation des performances consiste à étudier l'évolution de la latence d'un ping émis toutes les 200 ms

Latence (Python)



Latence (natif)



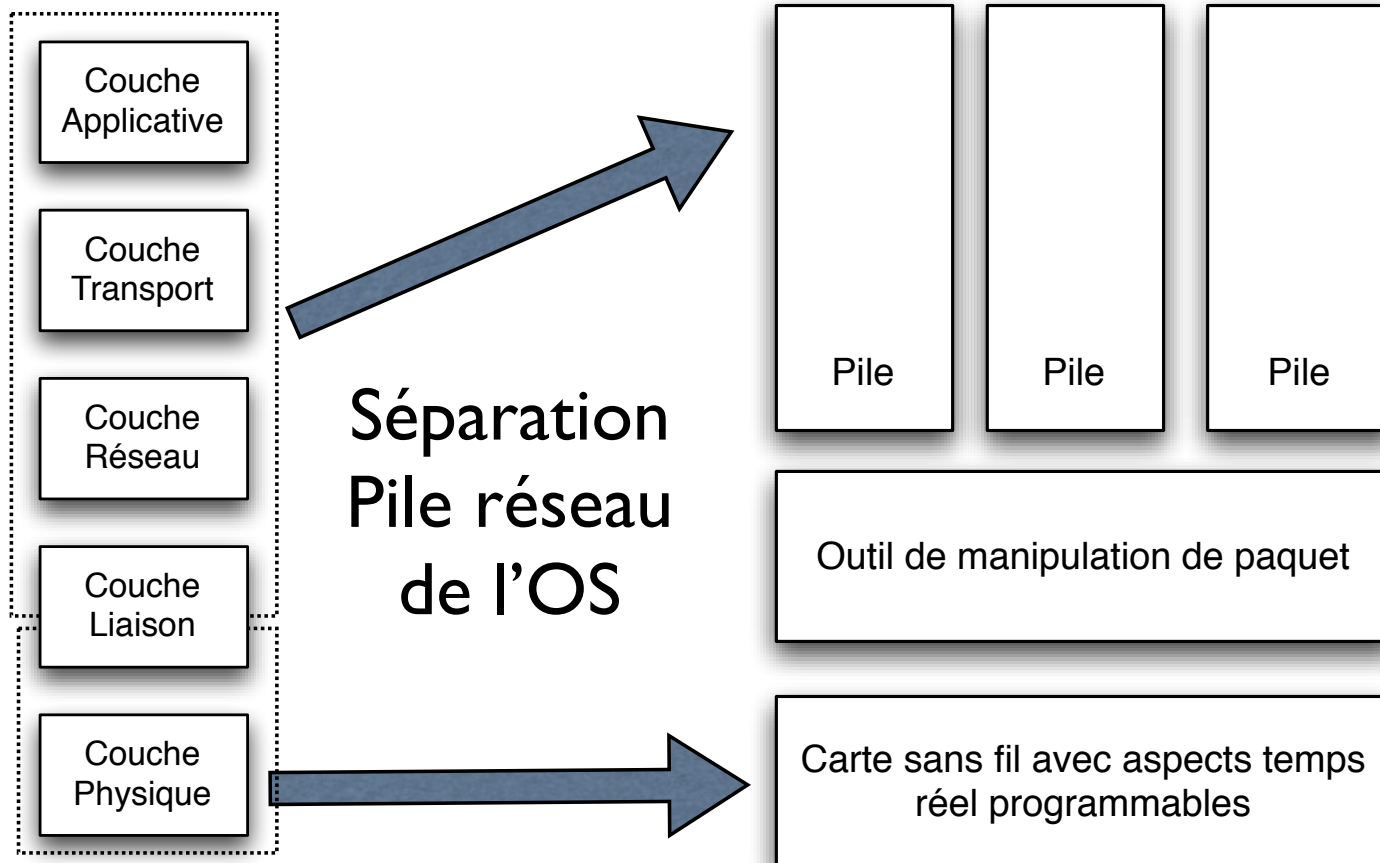
Conclusions Virtual AP

- Un VAP par terminal, chaque mobile se promène avec son AP
 - ◆ Le mobile est fixe par rapport au réseau
- Permet également d'associer un contexte dans l'AP virtuel pour chaque terminal
 - ◆ Extension à des services spécifiques par client

Conclusions Virtual AP

- Perspectives
 - Balisage des canaux supplémentaires doit permettre un changement de canal au niveau de la station
 - Implémentation possible au-dessus de PACMAP

Conclusions



Conclusions

- Le modèle architectural proposé a permis
 - d'isoler les éléments critiques au sein d'une partie temps réelle à l'échelle des symboles radio
 - de gérer des instances multiples de différentes piles réseaux et d'ouvrir la porte à de nouveaux concepts (Virtual AP par exemple)

Perspectives

- Arrivée de la radio logicielle
 - va permettre de s'affranchir des contraintes des plate-formes embarquées
 - va permettre d'obtenir une virtualisation complète du matériel
 - s'intègre parfaitement dans notre modèle

Merci !

- Questions ?