Performances des mécanismes de sécurité du framework 6TiSCH

Défense de mémoire

Rémy Decocq

Faculté des Sciences
Université de Mons

UMONS
Université de Mons

Faculté
des Sciences

26/06/20

Outline

Contexte

Équipements de l'*Industrial IoT* (nœud) :

- Limités en ressources : mémoire, CPU, stockage, radio
- Limités en capacité énergétique (batteries)

Caractéristiques des *Wireless Sensors Networks* :

- *Multipath fading* et interférences
- Forte densité de nœuds déployés de façon imprécise
- Transmissions *multi-hops*
- Changements dans la topologie (mobilité)
- Phénomène de *clock drifting* entre horloges

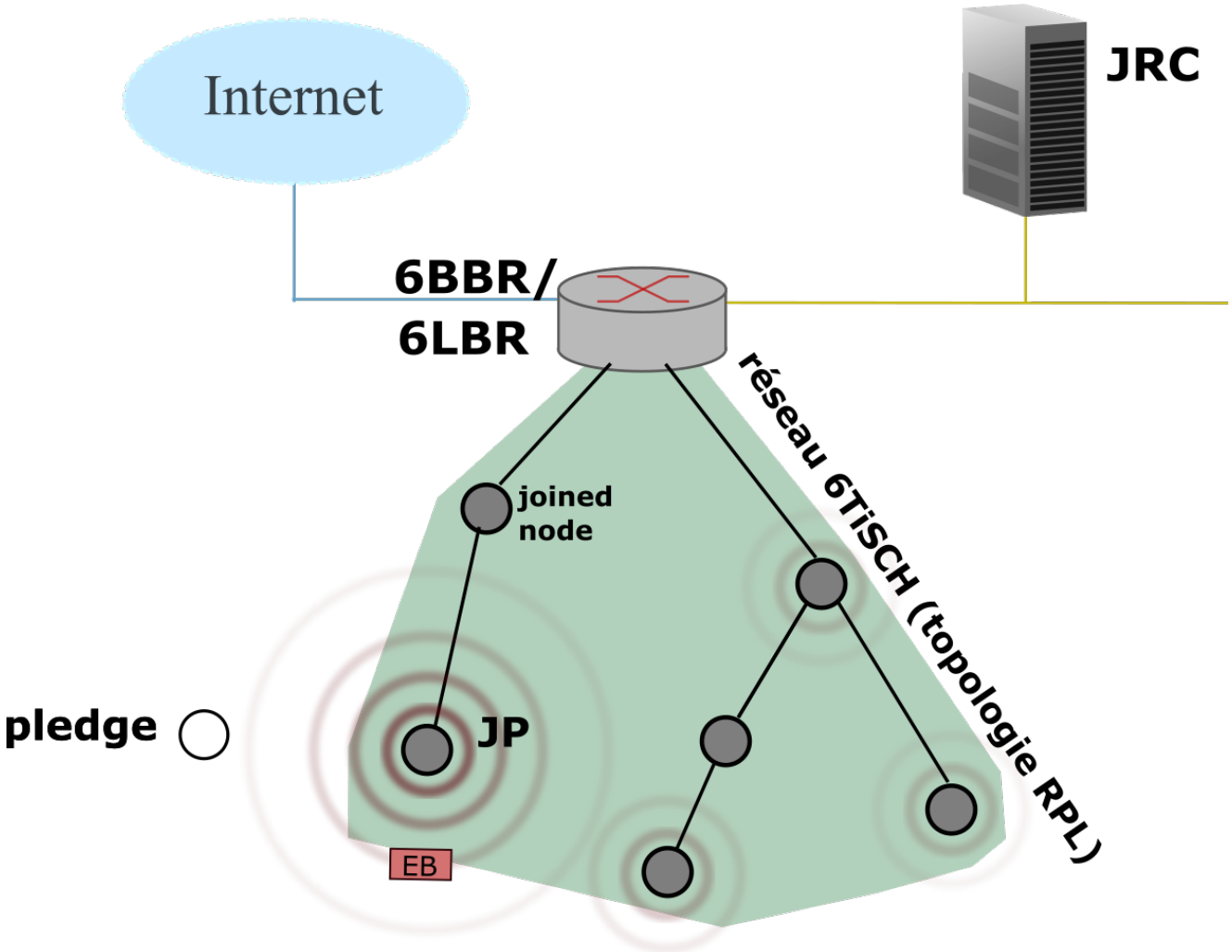

FIGURE 1 – Acteurs d'une architecture type d'un WSN où 6TiSCH est déployable

6TiSCH

Groupe de travail IETF *IPv6 over the TSCH mode of IEEE802.15.4e*

Standardisation de la pile 6TiSCH complète pour :

- Communications IPv6 $\rightarrow$ interopérabilité avec Internet
- Intégration du mode TSCH décrit par l'amendement IEEE802.15.4e
- Encadrer sécurité du réseau et joining phase

Outline

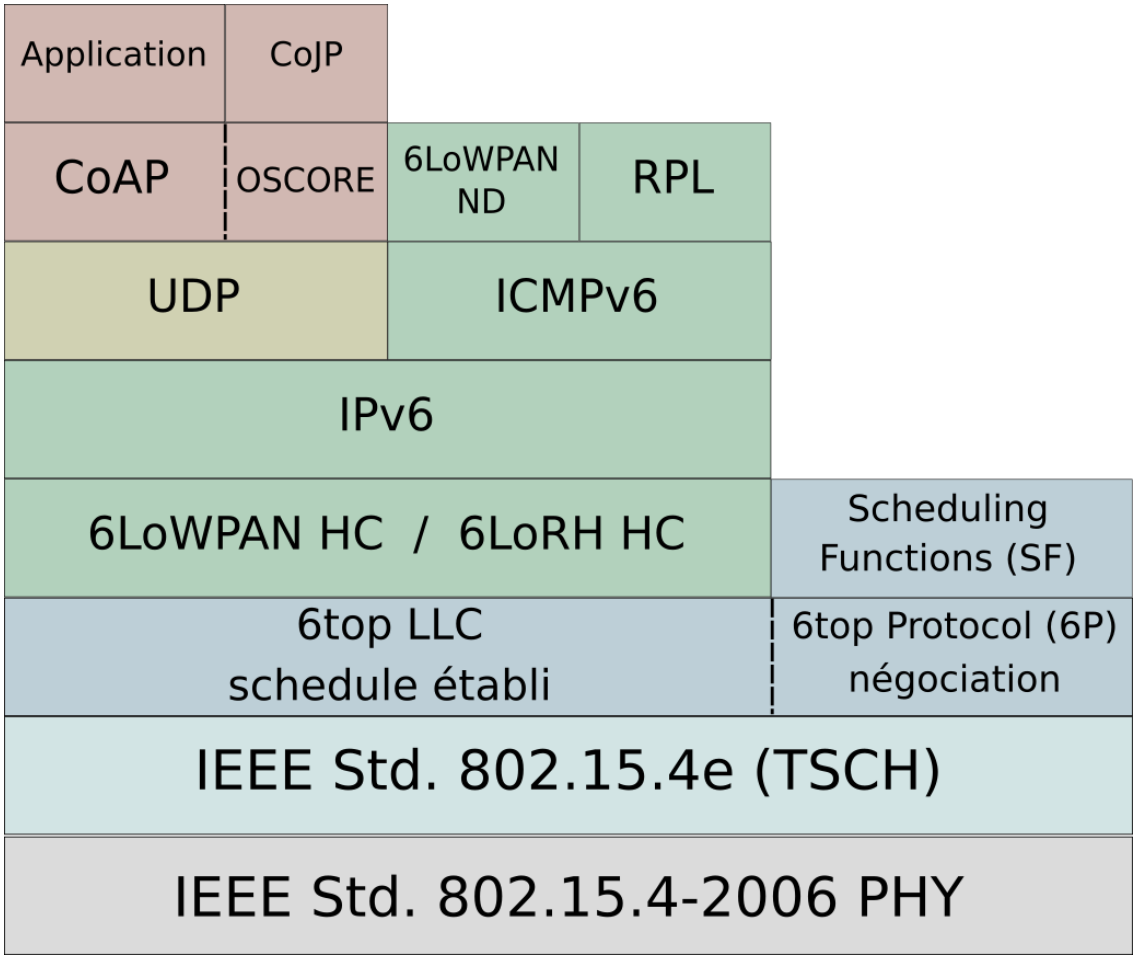

FIGURE 2 – Pile réseau 6TiSCH

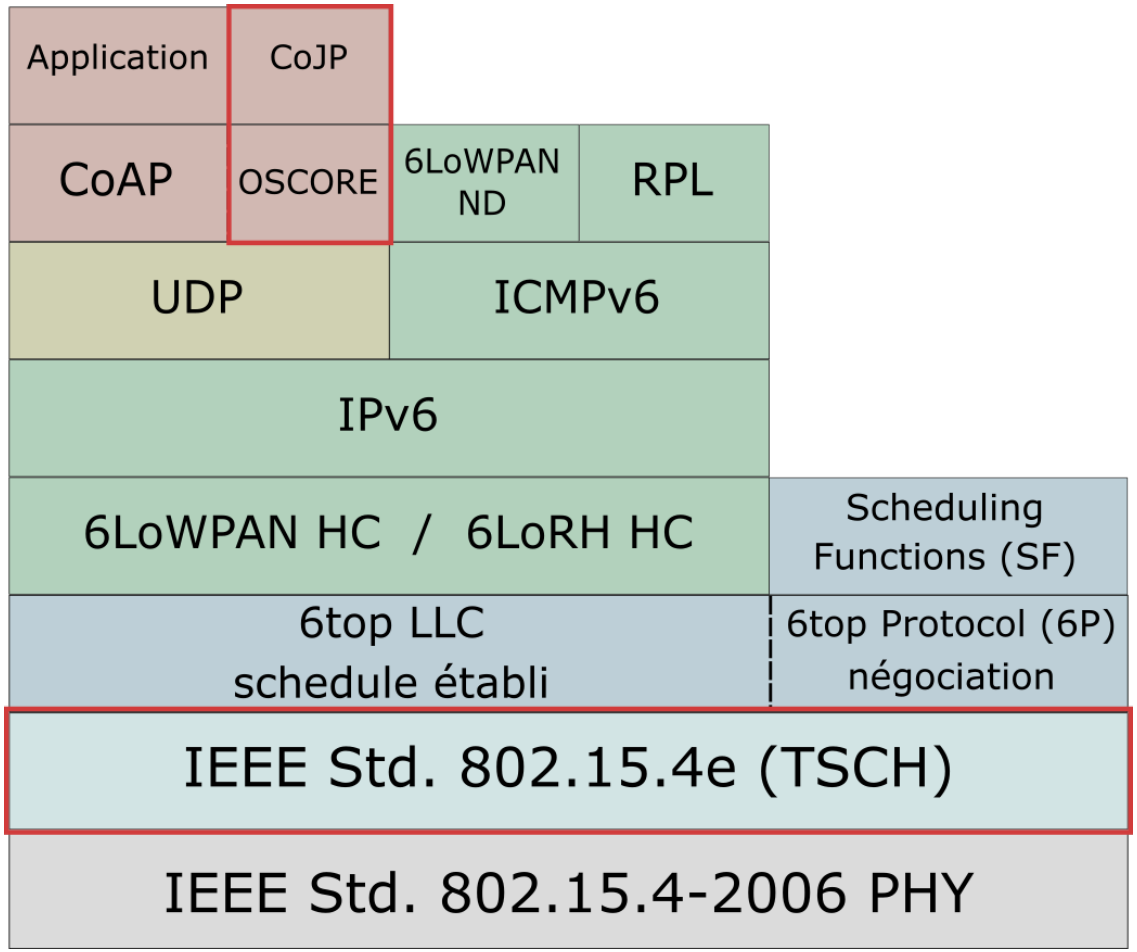

FIGURE 3 – Pile réseau 6TiSCH

Principes fondamentaux de TSCH

TSCH (*Time Slotted Channel Hopping*)
Combinaison de :

1. TDMA → multiplexage en temps (*timeslot*)
2. FDMA → multiplexage en fréquences (*channelOffset*)

Une communication entre nœuds voisins est caractérisée par un couple (*timeslot*, *channelOffset*) où

1. *timeslot* donne le moment de la communication
2. *channelOffset* donne la fréquence à laquelle elle a lieu

Les nœuds communiquant possèdent et partagent cette information
→ communications déterministes sur base d'un *schedule*

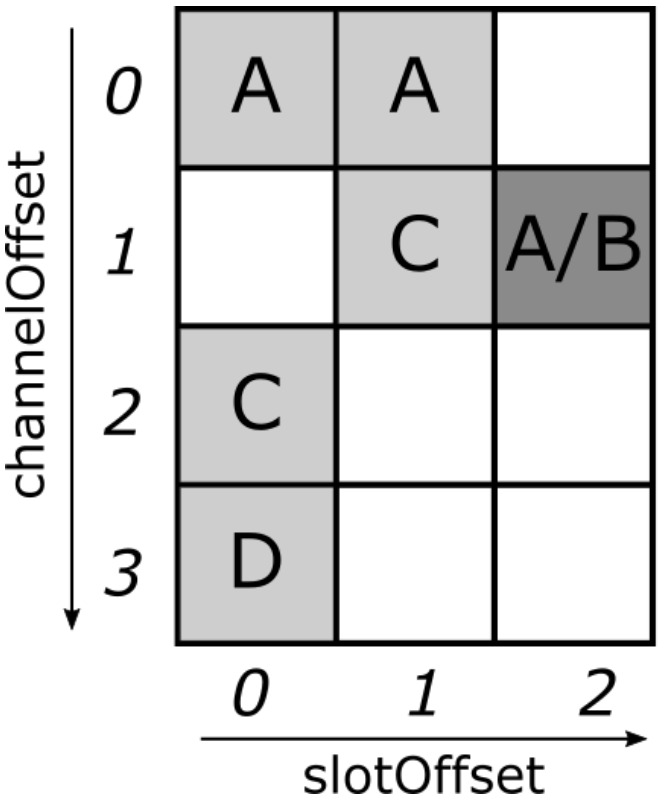

FIGURE 4 – Matrice des communications

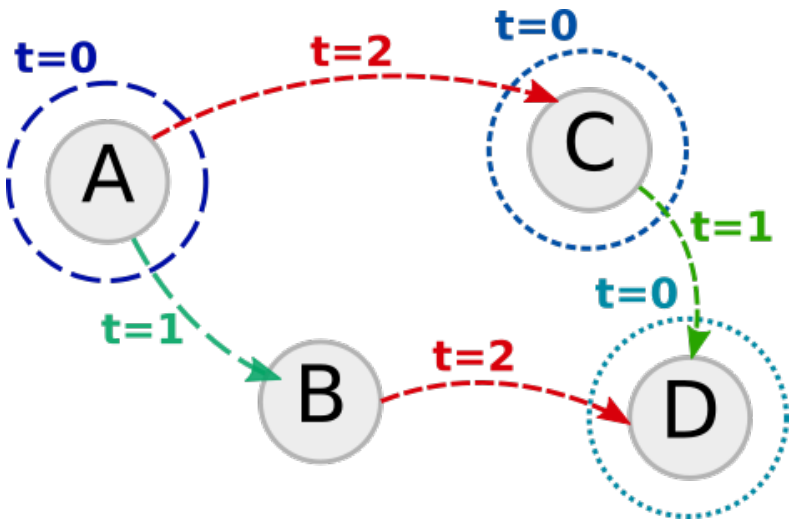

FIGURE 5 – Nœuds communiquant

$$f_{eff} = HoppSeq[f \mod n_{ch}] \quad \text{où } f = ASN + channelOffset$$

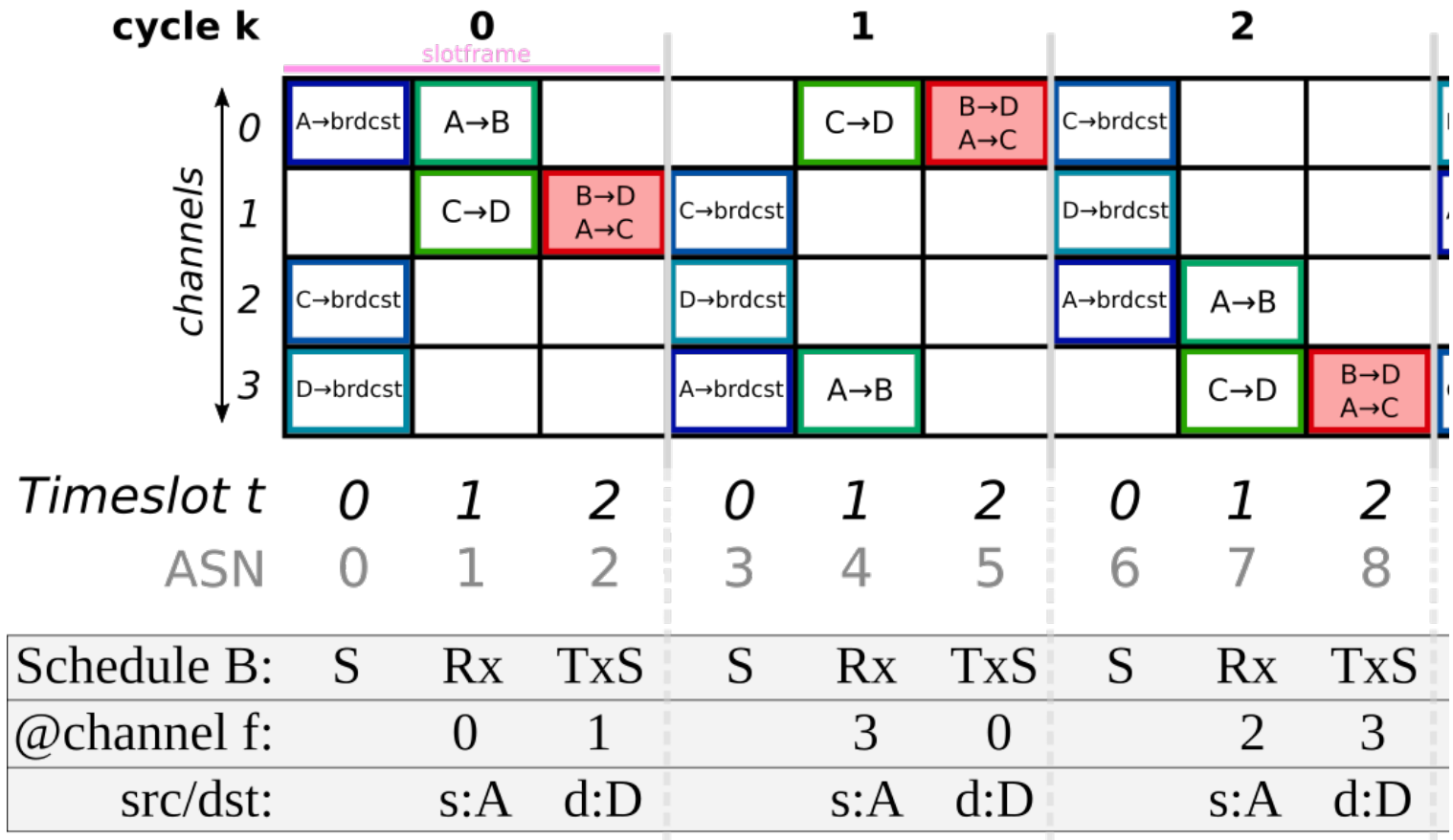

FIGURE 6 – Effet de sauts de fréquence d'un cycle à l'autre de slotframe

La joining phase

Réseau 6TiSCH de nœuds déjà raccordés protégé au niveau L2 par les mécanismes de protection IEEE802.15.4 et **clés** distribuées par l'autorité du réseau (*JRC*).

Un nœud qui veut rejoindre (*pledge)* n'a pas ces clés.

Un nœud déjà raccordé fait office de *Join Proxy* intermédiaire entre le pledge et l'autorité du réseau.

$\rightarrow$ émission de frame spéciales (EBs) par les nœuds déjà raccordés
$\rightarrow$ le pledge initie la joining phase pour se synchroniser + obtenir les clés

Le pledge possède un contexte de sécurité pré-établi (PSK) partagé avec le JRC.
$\rightarrow$ échanges pledge $\leftrightarrow$ JRC (*Join Exchange CoJP*) protégés au niveau applicatif par un contexte partagé (*OSCORE*)

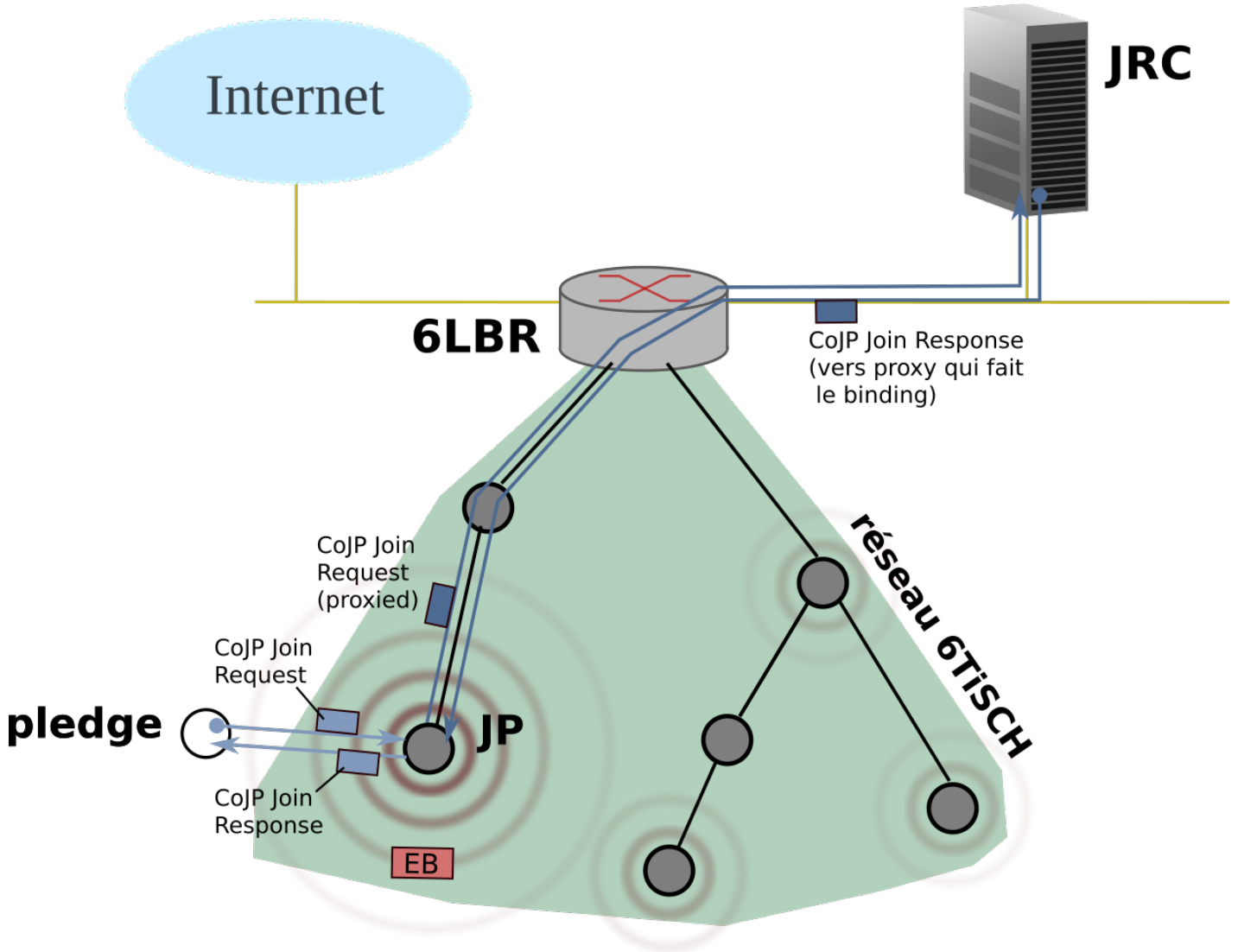

FIGURE 7 – Join Exchange CoJP opéré lors de la joining phase d'un pledge

Outline

Principes de la méthode NPEB

NPEB : *Neighbors propositions EB*, augmentation des EBs standards

Principe : un nœud annonce certains de ses voisins, proposés aux pledges qui évitent une écoute active naïve (**processus itératif d'écoute** de proposition en proposition, passe en sommeil entre).

Détermination du "meilleur voisin" basée sur $\neq$ critères

Maintien d'une *NPtable* par pledge et nœuds émettant NPEBs

nœud voisin	Join Metric	Cell émission NPEB	Cycle courant	# de cycles	RSSI
80-97-DF-48-00-01	0	(1, 0)	0	2	None
57-5F-CC-B1-00-02	14	(1, 2)	5	5	0
18-14-DA-48-00-03	7	(2, 11)	3	7	-83 (dBm)

FIGURE 8 – Exemple de NPtable et statuts d'écoute possibles (None/0/*RSSI*)

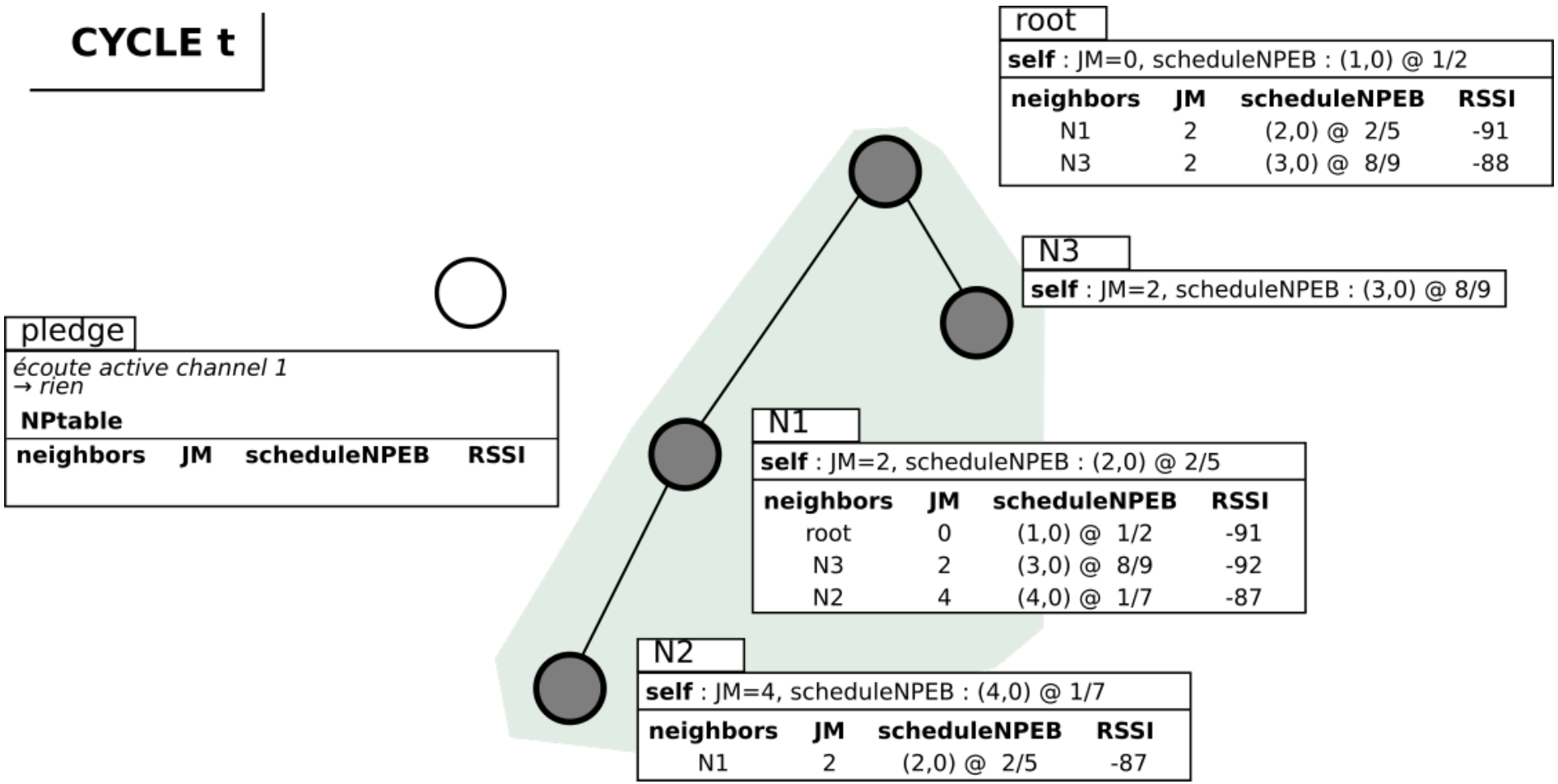

FIGURE 9 – [Cycle t] État initial du réseau où les NPtables des nœuds sont déjà alimentées

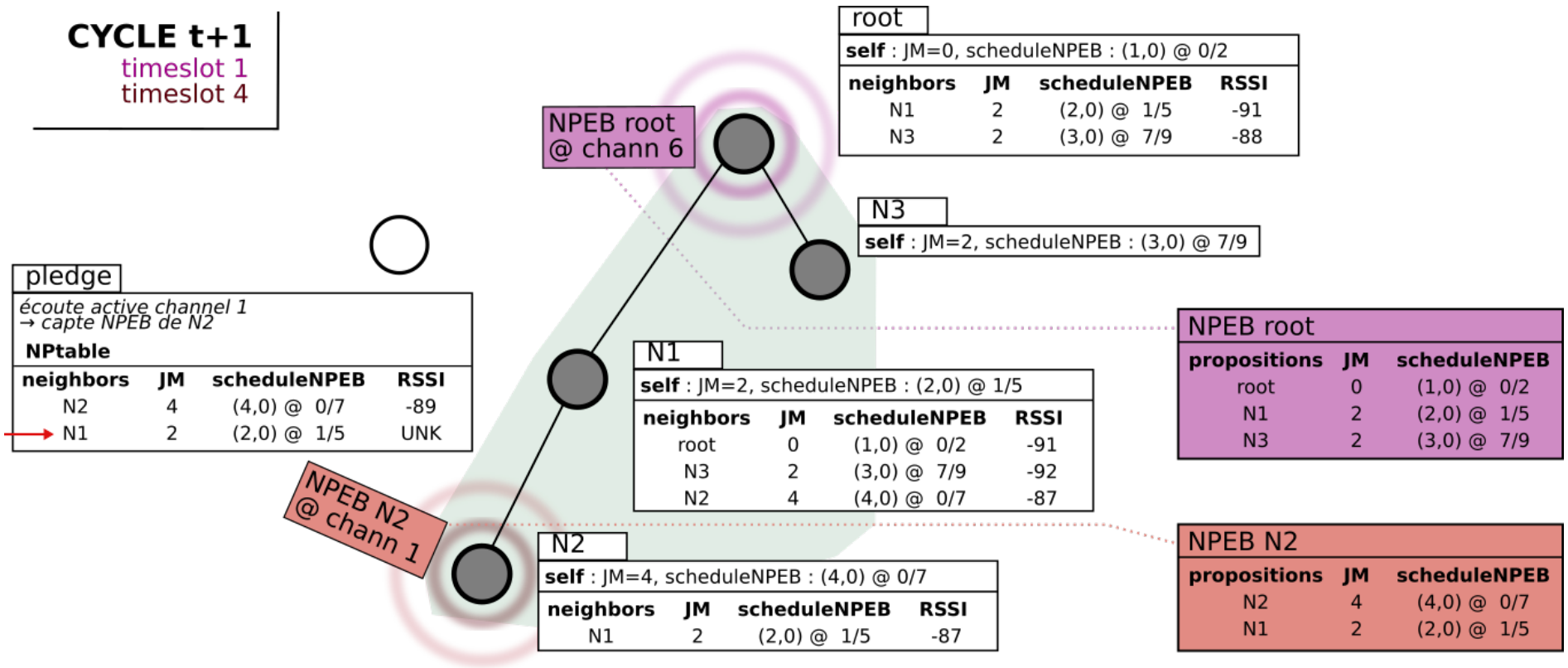

FIGURE 10 – [Cycle t+1] Une itération de slotframe écoulée, deux NPEBs programmés pour ce nouveau cycle

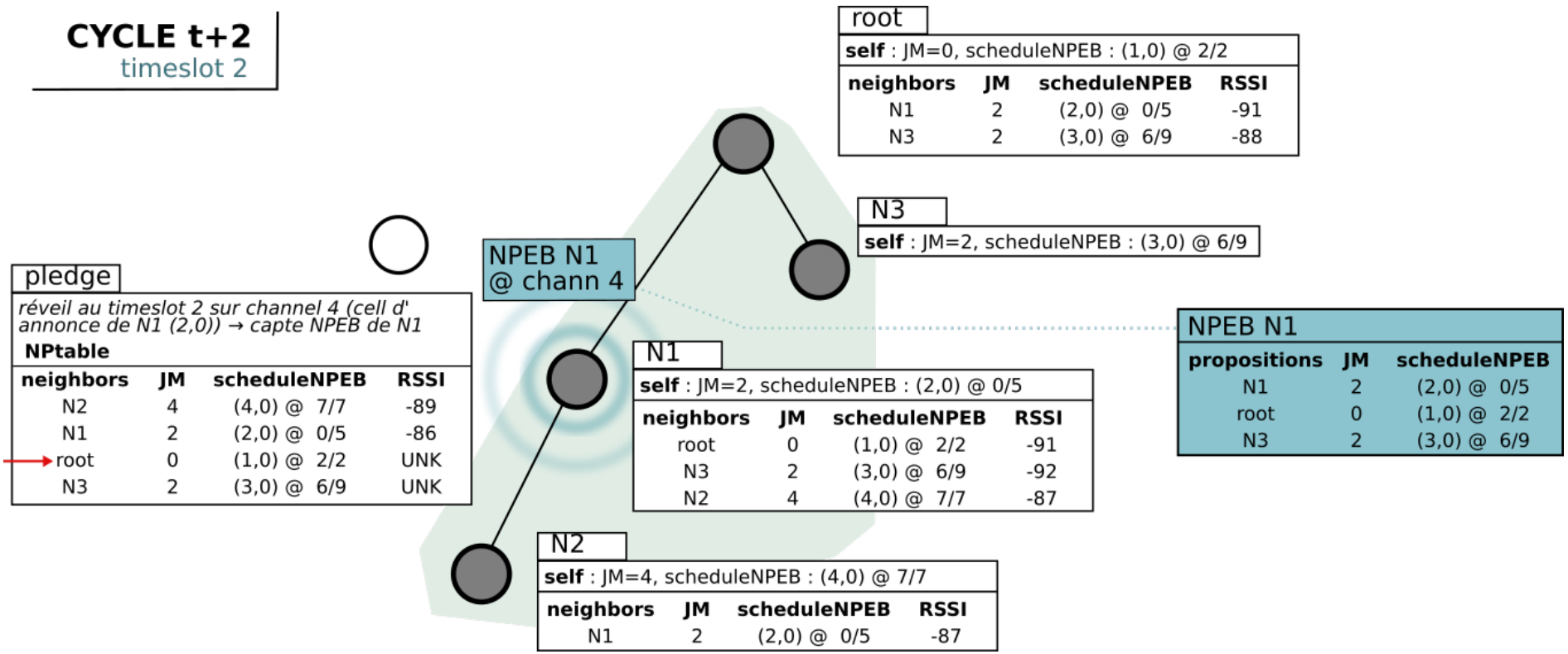

FIGURE 11 – [Cycle t+2] sommeil du pledge jusqu'à la cell d'annonce indiquée par N1

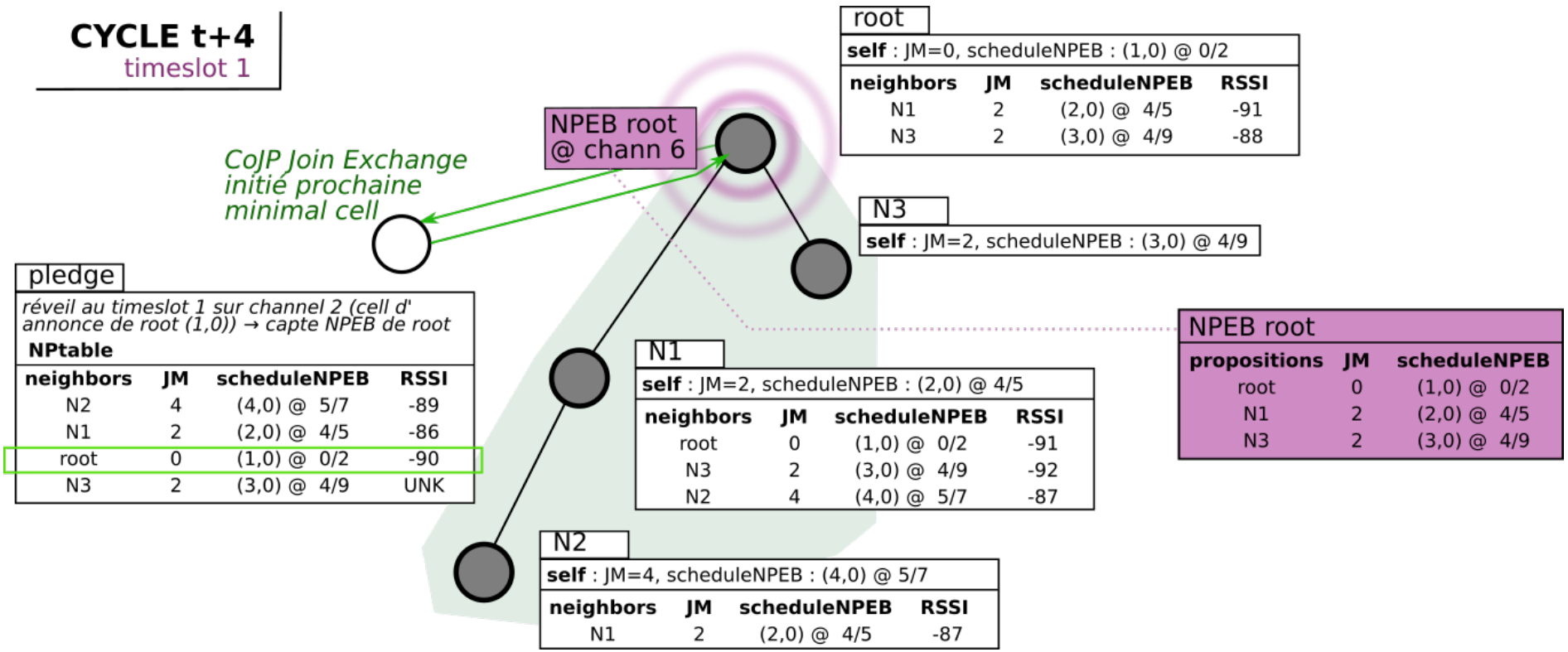

FIGURE 12 – [Cycle t+4] sommeil du pledge jusqu'à la cell d'annonce indiquée par root et lancement de la suite du processus de join avec celui-ci

Impact de sécurité sur la joining phase

Expérimentations dans le simulateur 6TiSCH :

- disposition des nœuds aléatoires
- $\forall$ nœud, min. 3 voisins avec PDR $> 50\%$
- configuration de la pile 6TiSCH conforme aux standards
- même seed pour runs parallèles

Expérimentations : avec/sans joining phase sécurisée (i.e. Join Exchange CoJP), réseau de 10 nœuds, 20 runs

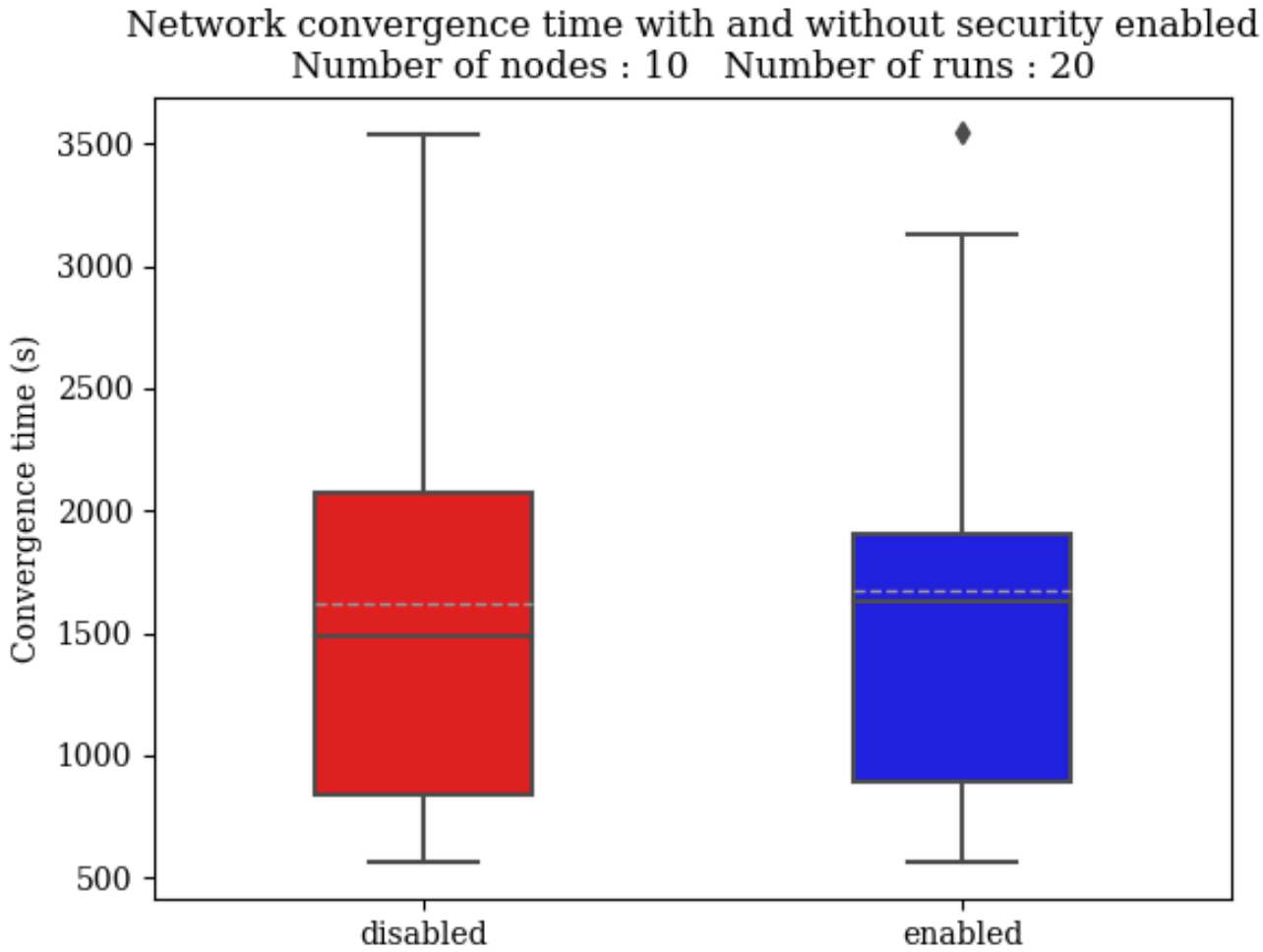

FIGURE 13 – Temps de convergence avec/sans sécurité (Join Exchange CoJP)

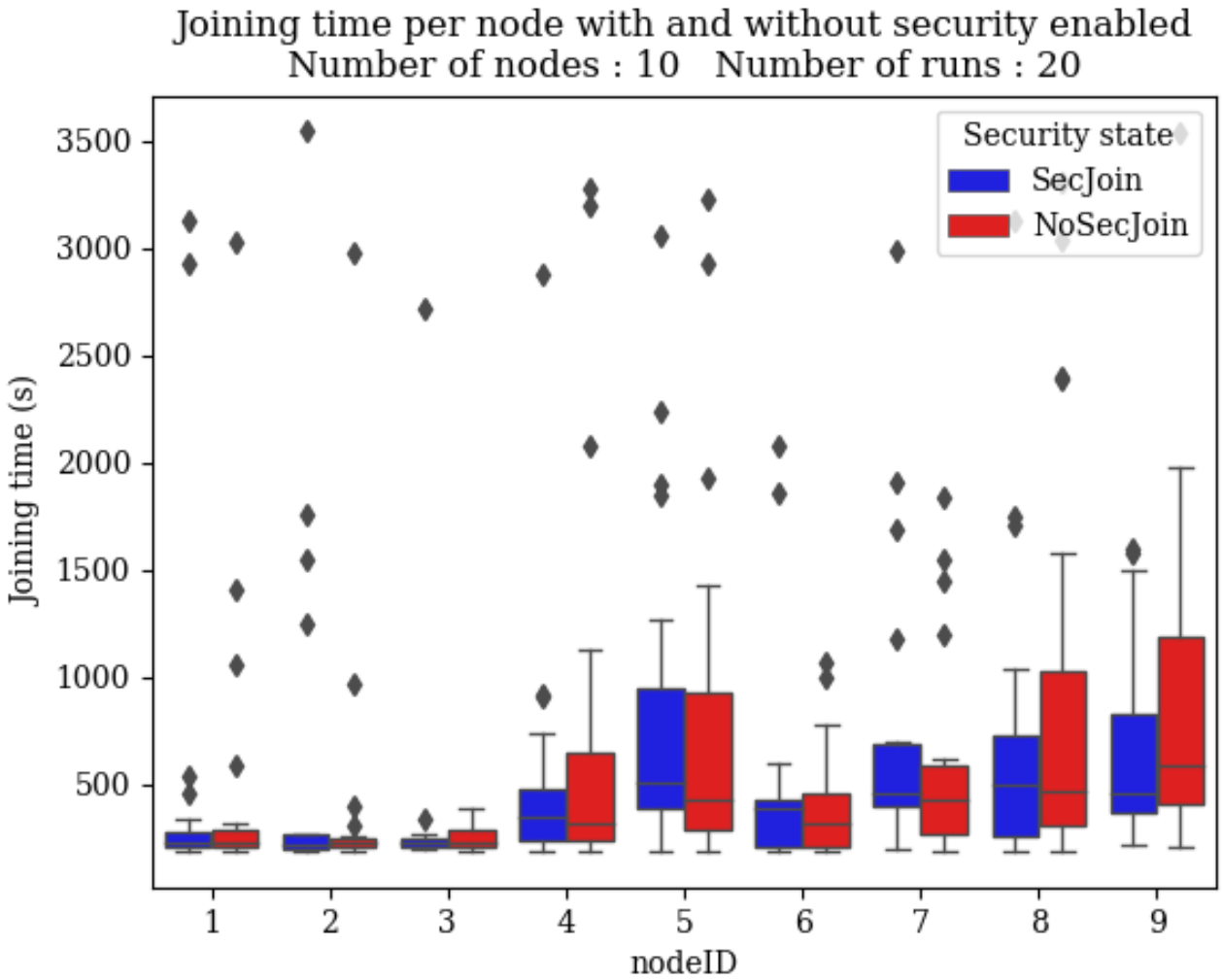

FIGURE 14 – Temps de join pour chaque nœud individuellement

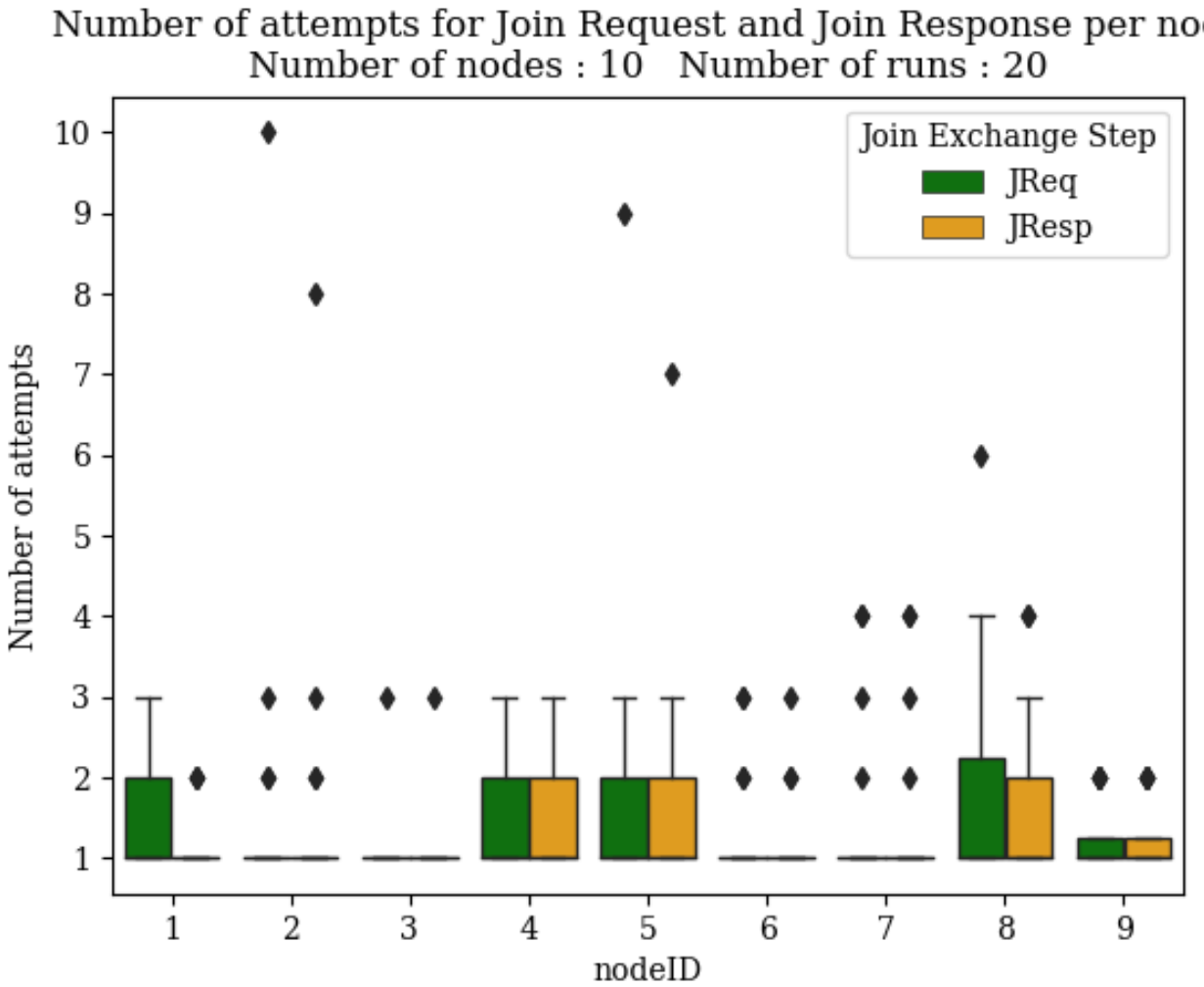

FIGURE 15 – Tentatives nécessaires pour chaque partie du Join Exchange CoJP

Performances de la méthode NPEB

Intuitivement, la méthode NPEB a pour objectif de

1. accélerer et optimiser en terme d'énergie (du point de vue du pledge) le processus de join
2. permettre au pledge de sélectionner le meilleur voisin possible avec lequel initier le processus de join

1. → division de l'analyse en fonction des étapes du processus de join, comparaison avec/sans NPEB
2. → aucune amélioration significative, non présenté ici

Expérimentations : avec/sans méthode NPEB implémentée dans le simulateur, réseau de 30 nœuds, 10 runs et résultats agrégés

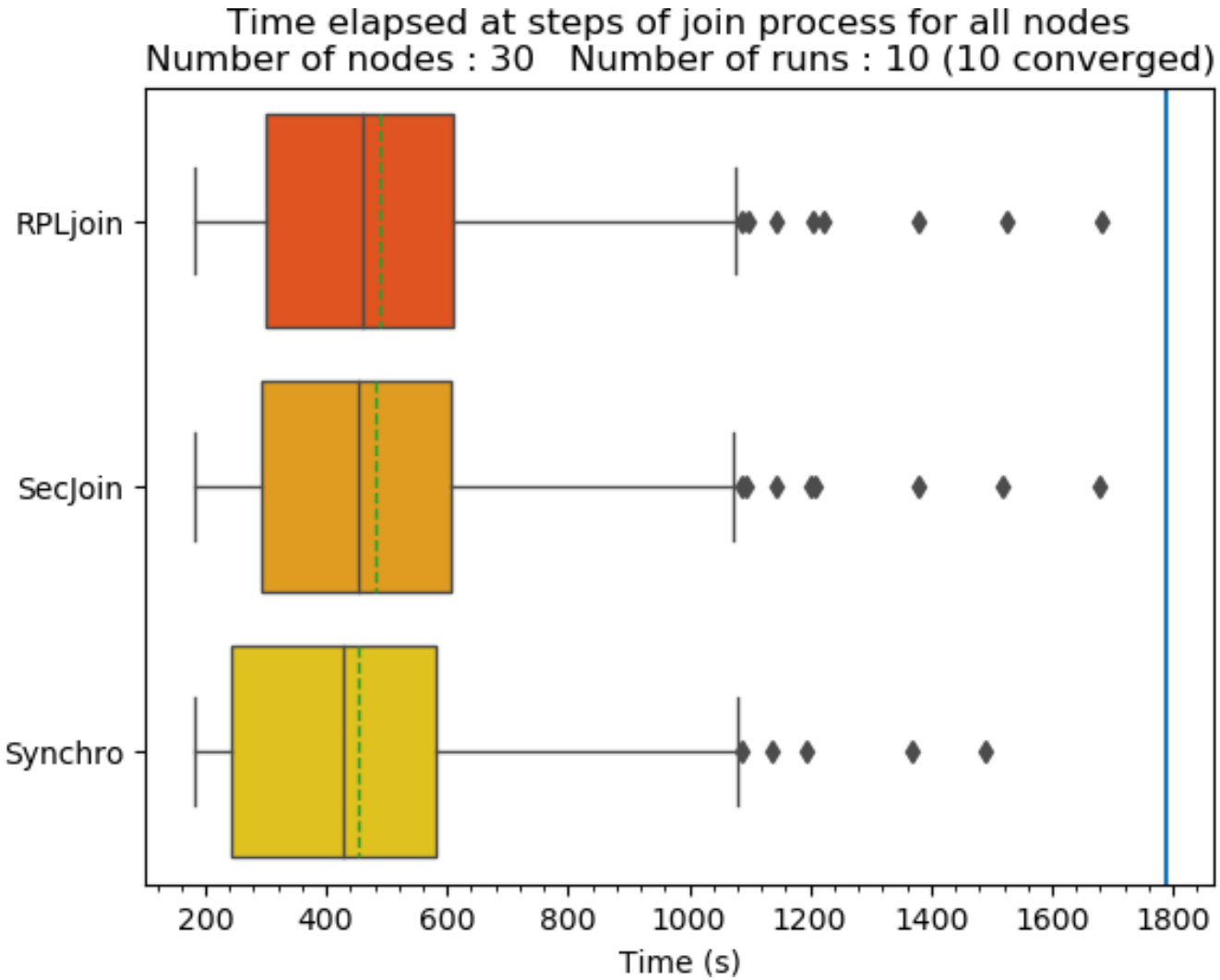

FIGURE 16 – [EBs] Temps requis pour ≠ étapes tous nœuds et runs confondus

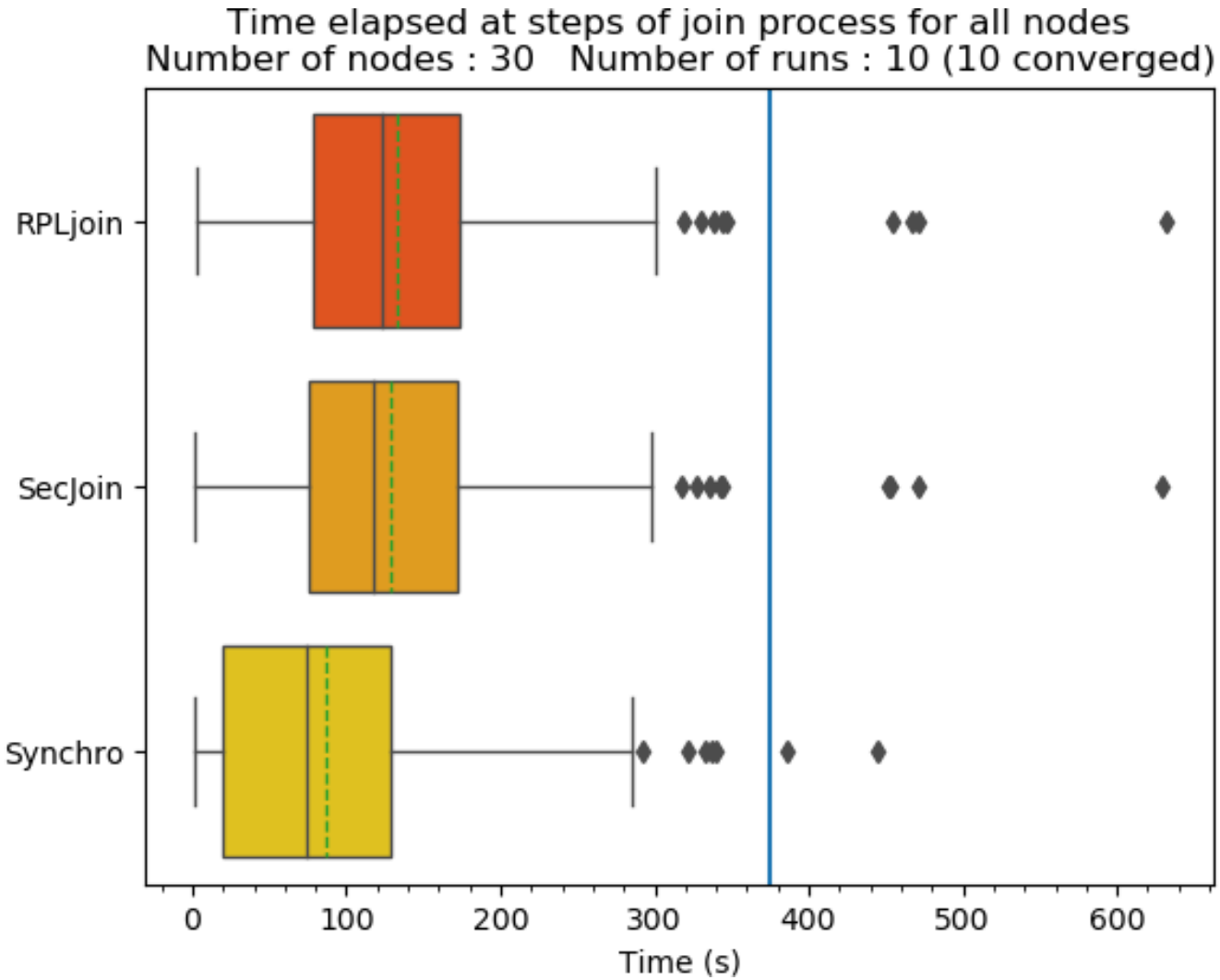

FIGURE 17 – [NPEBs] Temps requis pour ≠ étapes tous nœuds et runs confondus

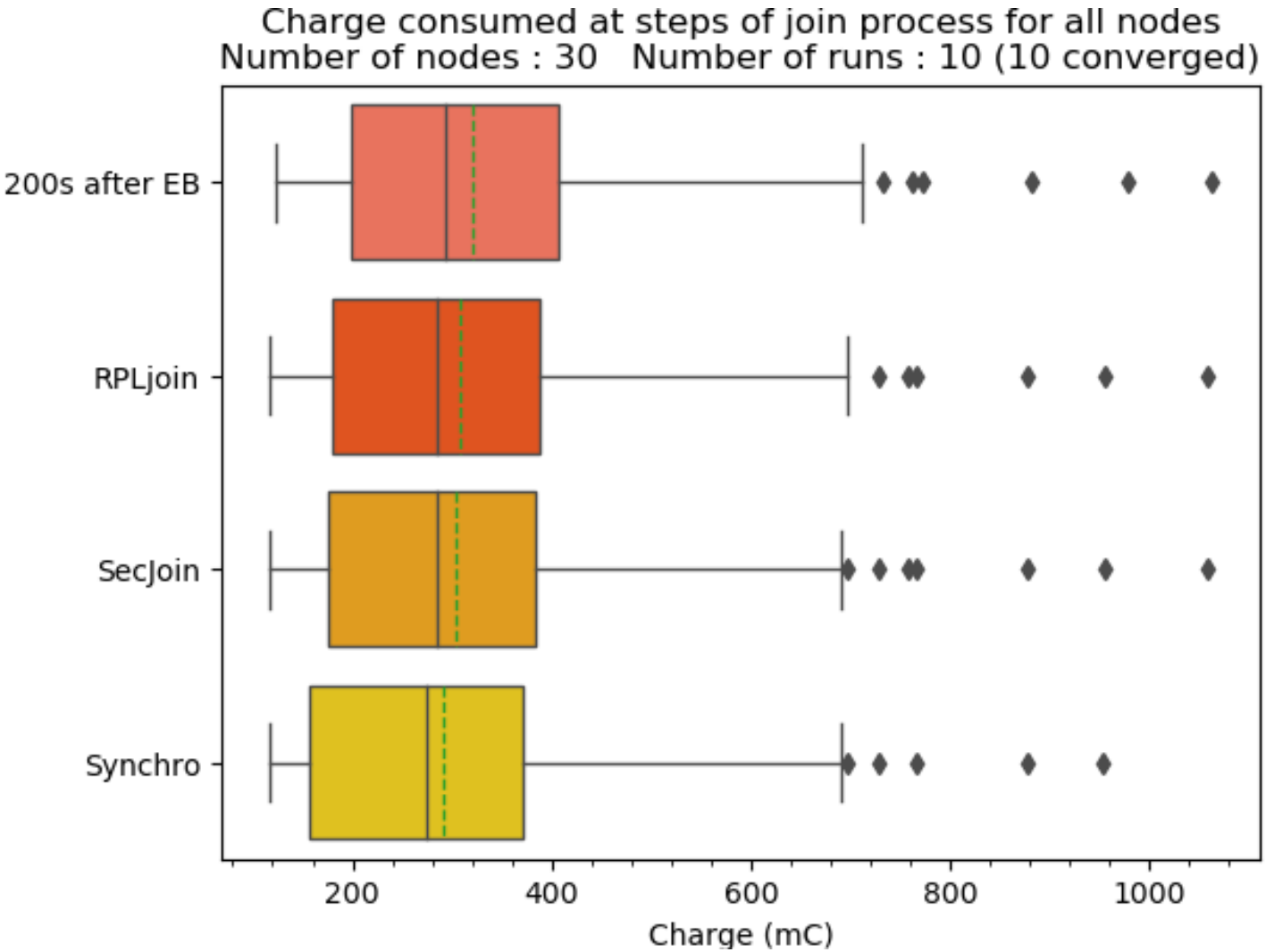

FIGURE 18 – [EBs] Charge consommée aux ≠ étapes tous nœuds et runs confondus

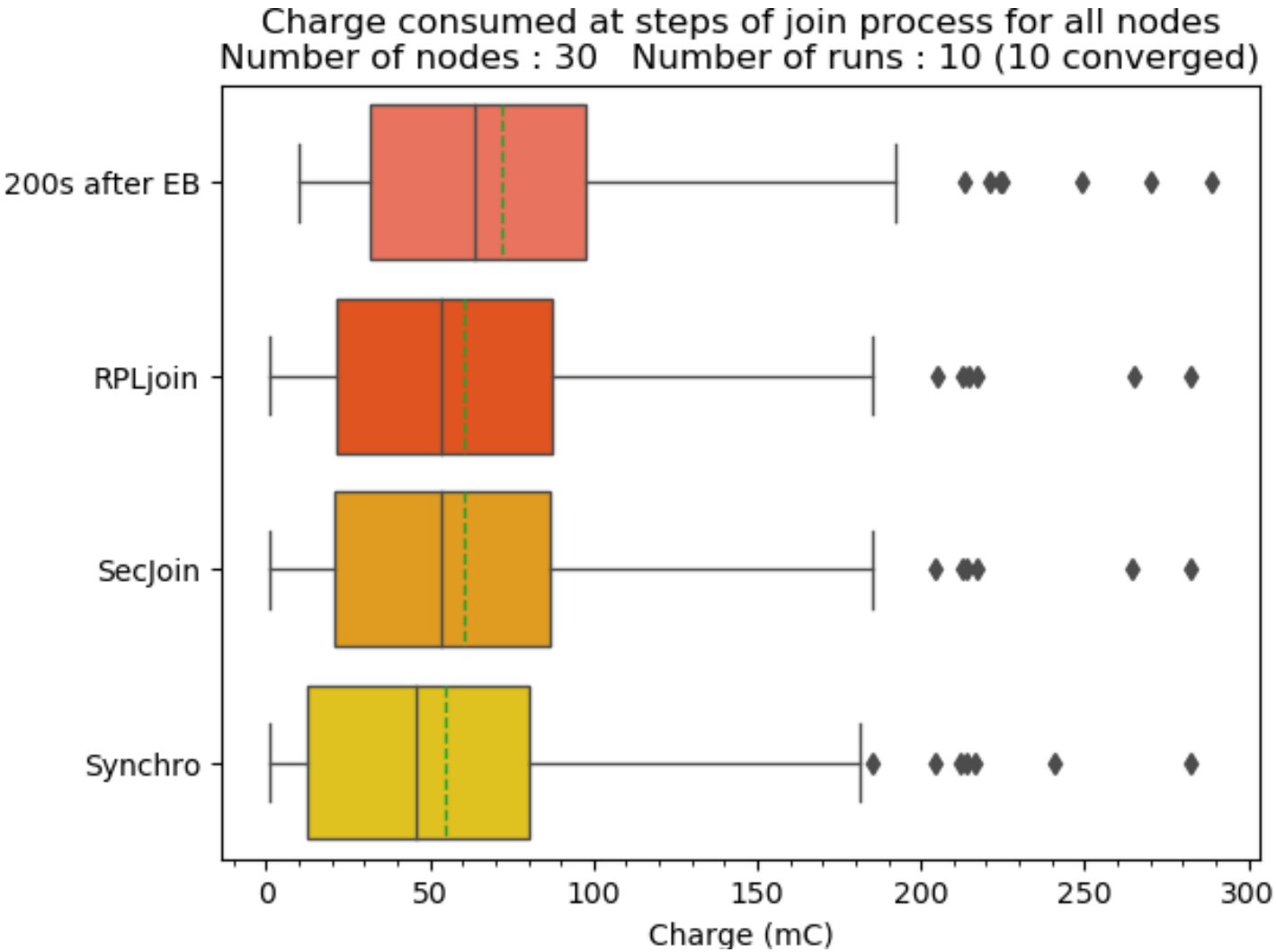

FIGURE 19 – [NPEBs] Charge consommée aux ≠ étapes tous nœuds et runs confondus

Conclusion

- État de l'art
  - Revue de la pile dans son entièreté, conforme aux standards dans leur état actuel (standardisation toujours en cours)
  - Détail de la sécurité de la joining phase fait dans aucun papier publié à ce jour excepté les standards qui la décrivent eux-mêmes

- Expérimentations sur la joining phase
  - Première quantification de l'impact de la sécurité sur la Joining Phase
  - Élaboration de la méthode NPEB pour gagner en performances, un objectif non atteint significativement (sélection meilleur voisin)
    $\rightarrow$ améliorations possibles par paramètres et processus décisionnels

Performances des mécanismes de sécurité du framework 6TiSCH

Q&A