

# Performances des mécanismes de sécurité du framework 6TiSCH

Défense de mémoire

Rémy DECOCQ

Faculté des Sciences  
Université de Mons



26/06/20

# Sommaire

## 1 Introduction

- Les réseaux IIoT (WSNs)
- 6TiSCH

## 2 État de l'art de la pile 6TiSCH

- Principes fondamentaux de TSCH
- La joining phase

## 3 Méthode NPEB et expérimentations

- Principes de la méthode NPEB
- Évaluation de l'impact de sécurité sur la joining phase
- Évaluation des performances de la méthode NPEB

## 4 Conclusion



# Contexte

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

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

Caractéristiques des *Wireless Sensors Networks* :

- Topologie en arborescence, noeud racine "sink"
- Transmissions radios multi-sauts
- ...

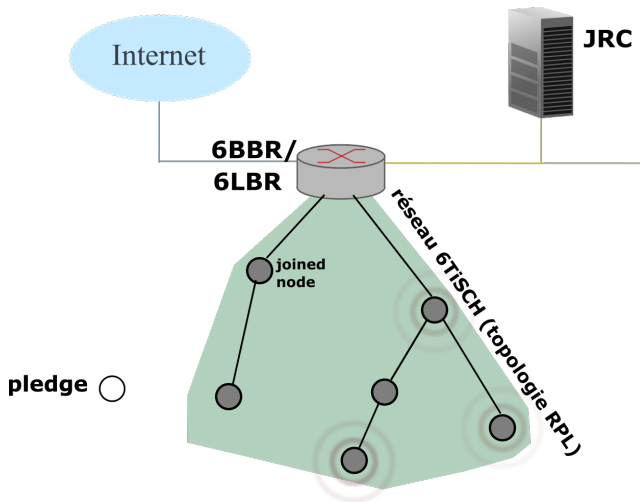


FIGURE 1 – Acteurs d'une architecture type d'un WSN où 6TiSCH est déployable

# 6TiSCH

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

Standardisation de la pile 6TiSCH complète pour :

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

# Sommaire

- 1 Introduction
  - Les réseaux IIoT (WSNs)
  - 6TiSCH
- 2 État de l'art de la pile 6TiSCH
  - Principes fondamentaux de TSCH
  - La joining phase
- 3 Méthode NPEB et expérimentations
  - Principes de la méthode NPEB
  - Évaluation de l'impact de sécurité sur la joining phase
  - Évaluation des performances de la méthode NPEB
- 4 Conclusion

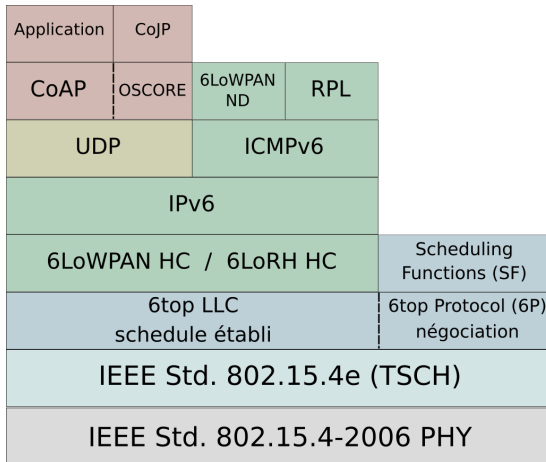


FIGURE 2 – Pile réseau 6TiSCH

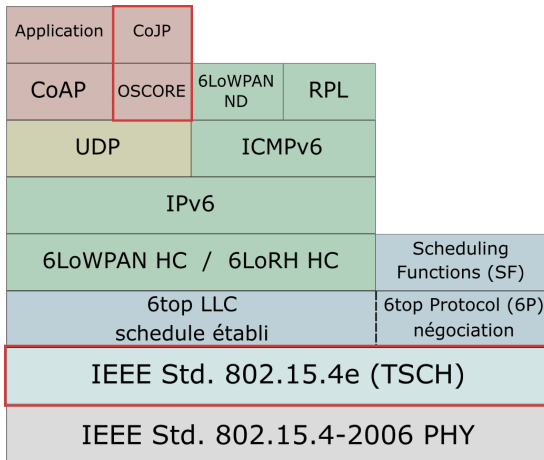


FIGURE 3 – Pile réseau 6TiSCH



# 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*

channelOffset

0	A	A	
1		C	A/B
2	C		
3	D		

slotOffset

FIGURE 4 – Matrice des communications

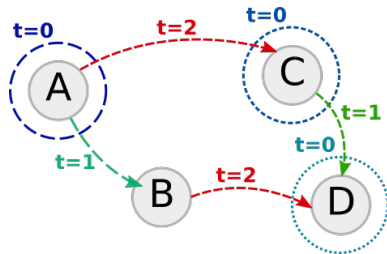


FIGURE 5 – Nœuds communiquant

## La joining phase

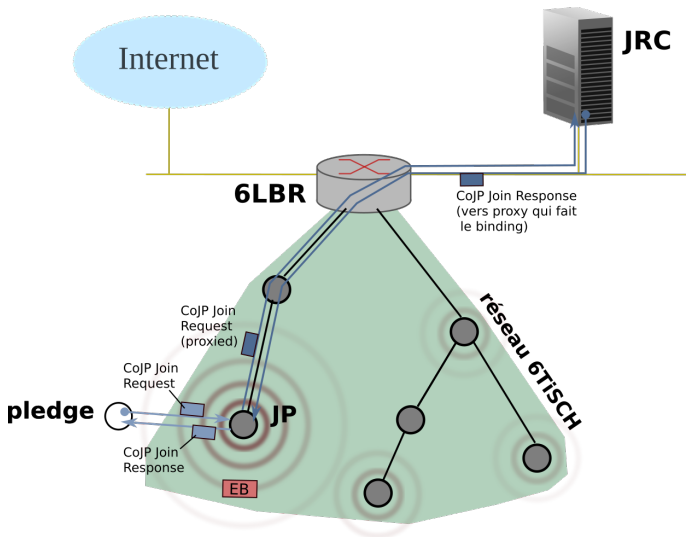
Réseau 6TiSCH de nœuds déjà raccordés protégé au niveau L2 par les mécanismes de protection IEEE802.15.4 et **clés** distribuées par l'autorité du réseau (**JRC**).

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.

→ émission de frame spéciales (**EBs**) par les nœuds déjà raccordés

→ le pledge initie la joining phase pour se synchroniser + obtenir les clés



**FIGURE 6** – Join Exchange CoJP opéré lors de la joining phase d'un pledge

# Sommaire

## 1 Introduction

- Les réseaux IIoT (WSNs)
- 6TiSCH

## 2 État de l'art de la pile 6TiSCH

- Principes fondamentaux de TSCH
- La joining phase

## 3 Méthode NPEB et expérimentations

- Principes de la méthode NPEB
- Évaluation de l'impact de sécurité sur la joining phase
- Évaluation des performances de la méthode NPEB

## 4 Conclusion

# 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

<u>nœud voisin</u>	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 7 – Exemple de NPtable et statuts d'écoute possibles (None/0/RSSI)

**CYCLE t****pledge**

écoute active channel 1  
→ rien

**NPtable**

neighbors	JM	scheduleNPEB	RSSI

**root**

**self** : JM=0, scheduleNPEB : (1,0) @ 1/2

neighbors	JM	scheduleNPEB	RSSI
N1	2	(2,0) @ 2/5	-91
N3	2	(3,0) @ 8/9	-88

**N3**

**self** : JM=2, scheduleNPEB : (3,0) @ 8/9

**N1**

**self** : JM=2, scheduleNPEB : (2,0) @ 2/5

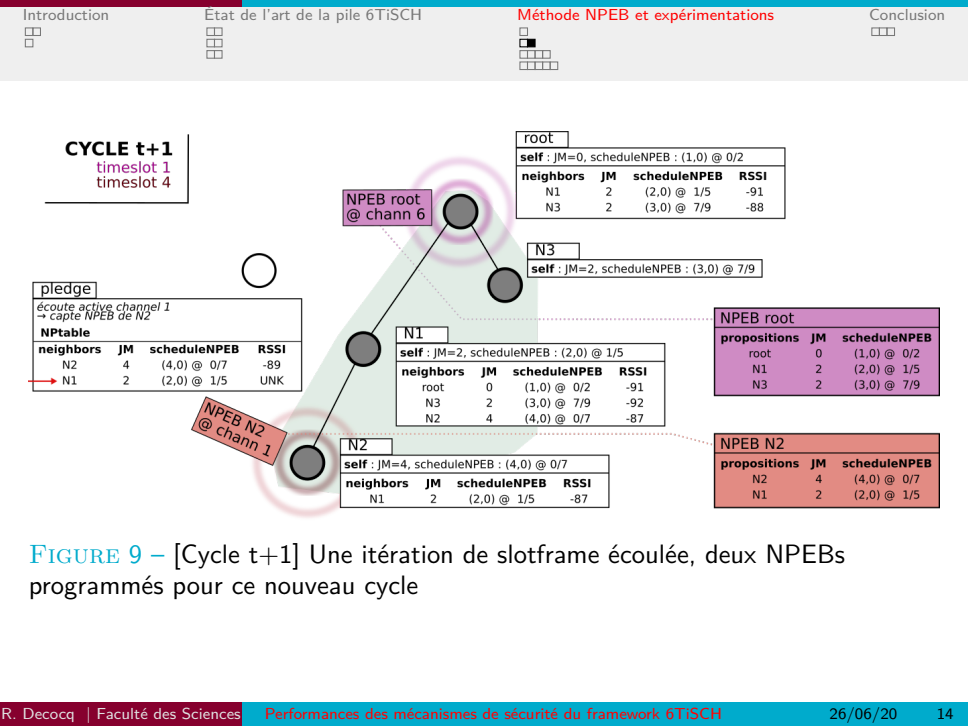
neighbors	JM	scheduleNPEB	RSSI
root	0	(1,0) @ 1/2	-91
N3	2	(3,0) @ 8/9	-92
N2	4	(4,0) @ 1/7	-87

**N2**

**self** : JM=4, scheduleNPEB : (4,0) @ 1/7

neighbors	JM	scheduleNPEB	RSSI
N1	2	(2,0) @ 2/5	-87

**FIGURE 8 – [Cycle t]** État initial du réseau où les NPtables des nœuds sont déjà alimentées





## timeslot 2

réveil au timeslot 2 sur channel 4 (cell d'annonce de N1 (2,0)) → capte NPEB de N1

**NPtable**

neighbors	JM	scheduleNPEB	RSSI
N2	4	(4,0) @ 7/7	-89
N1	2	(2,0) @ 0/5	-86
→ root	0	(1,0) @ 2/2	UNK
N3	2	(3,0) @ 6/9	UNK

NPEB N1  
@ chann 4

N1

```
self : JM=2, scheduleNPEB : (2,0) @ 0/5
```

neighbors	JM	scheduleNPEB	RSSI
root	0	(1,0) @ 2/2	-91
N3	2	(3,0) @ 6/9	-92
N2	4	(4,0) @ 7/7	-87

N2

```
self : |M=4, scheduleNPEB : (4,0) @ 7/7
```

neighbors	JM	scheduleNPEB	RSSI
N1	2	(2.0) @ 0/5	-87

root

```
self : JM=0, scheduleNPEB : (1,0) @ 2/2
```

neighbors	JM	scheduleNPEB	RSSI
N1	2	(2,0) @ 0/5	-91
N3	2	(3,0) @ 6/9	-88

N3

```
self : IM=2, scheduleNPEB : (3.0) @ 6/9
```

NPEB N1

propositions	JM	scheduleNPEB
N1	2	(2,0) @ 0/5
root	0	(1,0) @ 2/2
N3	2	(3,0) @ 6/9

**FIGURE 10** – [Cycle  $t+2$ ] sommeil du pledge jusqu'à la cell d'annonce indiquée par N1



# 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

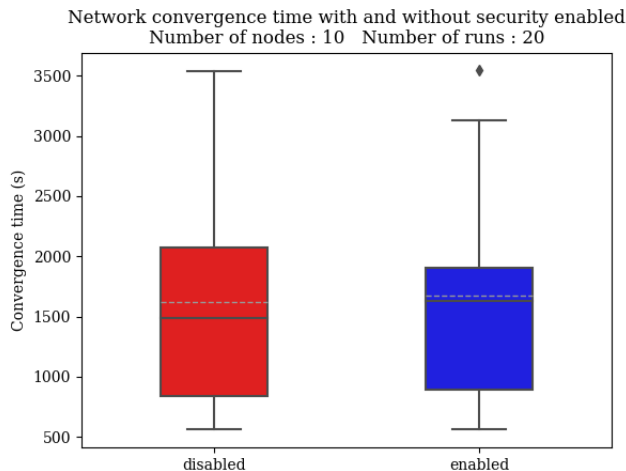


FIGURE 12 – Temps de convergence avec/sans sécurité (Join Exchange CoJP)

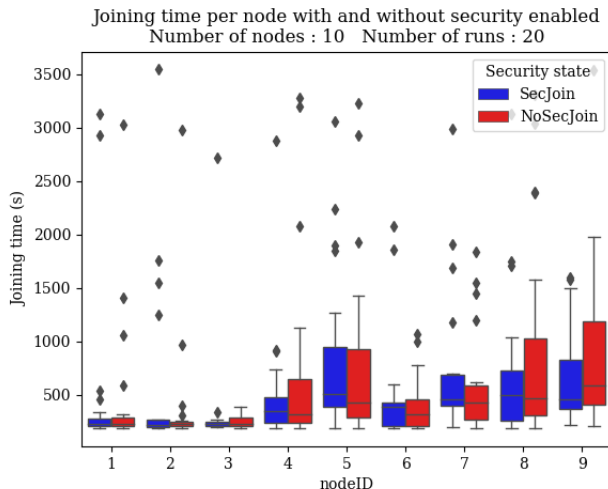


FIGURE 13 – Temps de join pour chaque nœud individuellement

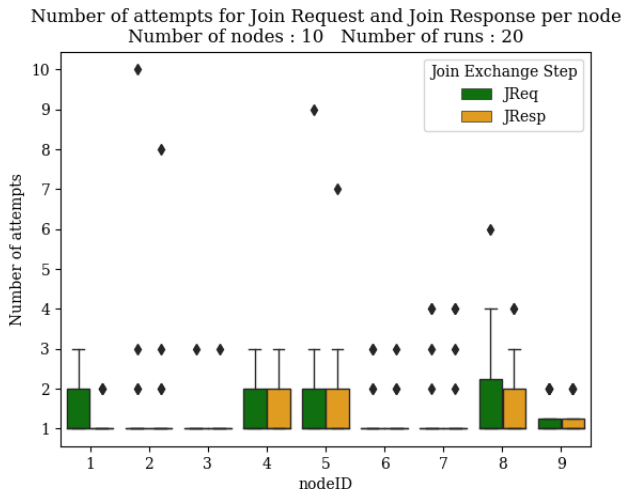


FIGURE 14 – Tentatives nécessaires pour chaque partie du Join Exchange CoJP

# Performances de la méthode NPEB

Intuitivement, la méthode NPEB a pour objectif de

- 1 accélérer 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

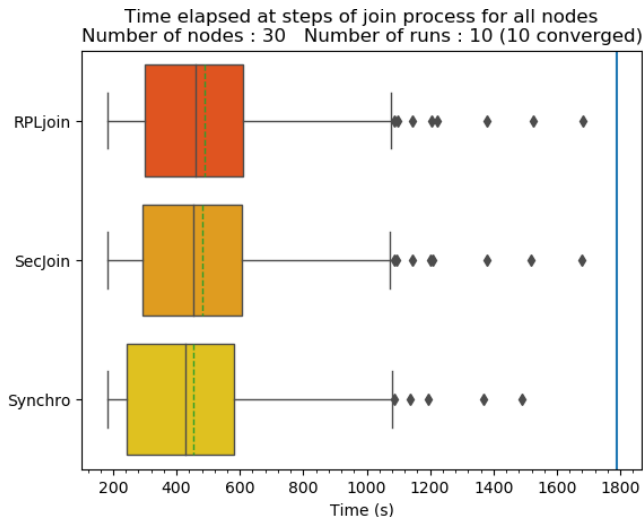


FIGURE 15 – [EBs] Temps requis pour  $\neq$  étapes tous nœuds et runs confondus



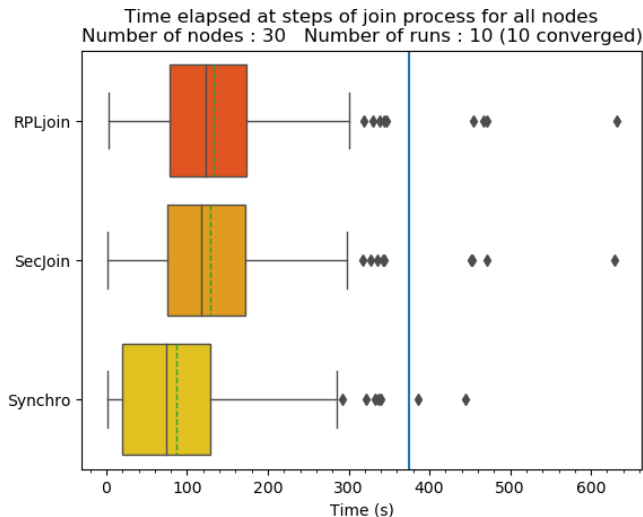


FIGURE 16 – [NPEBs] Temps requis pour  $\neq$  étapes tous nœuds et runs confondus

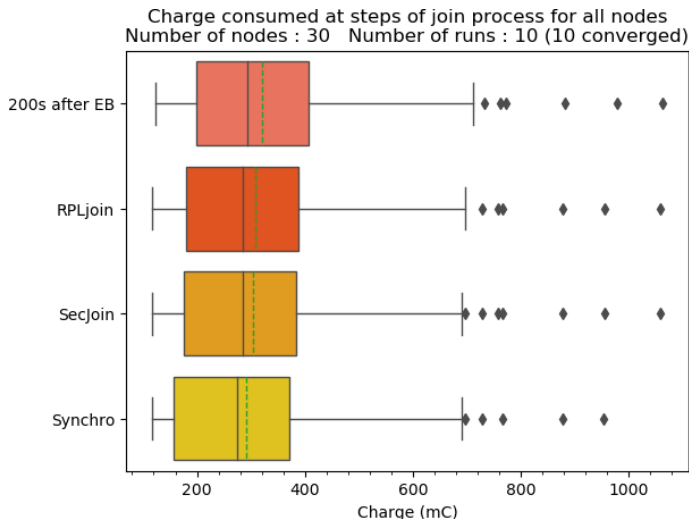


FIGURE 17 – [EBs] Charge consommée aux  $\neq$  étapes tous nœuds et runs confondus

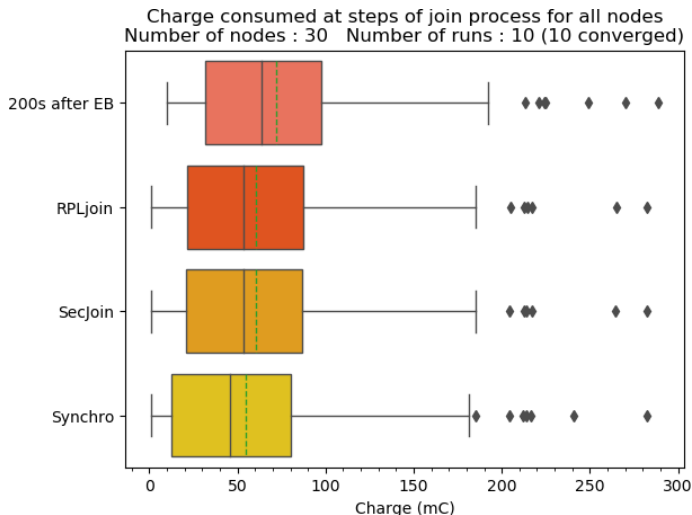


FIGURE 18 – [NPEBs] Charge consommée aux  $\neq$  étapes tous nœuds et runs confondus



# 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)
    - améliorations possibles par paramètres et processus décisionnels



# Performances des mécanismes de sécurité du framework 6TiSCH

## Q&A

---



# Appendix

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

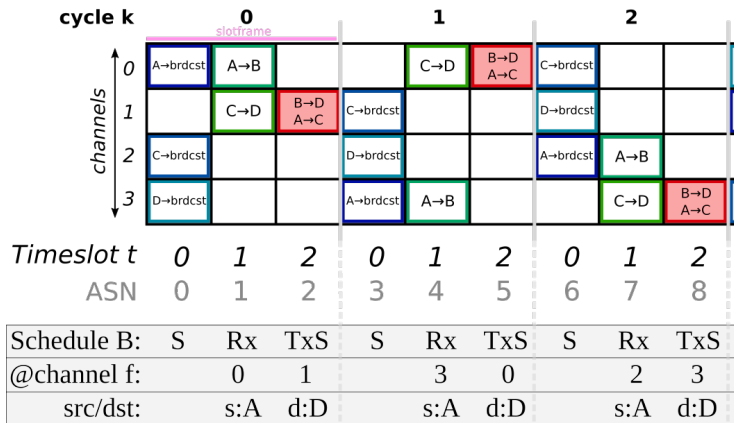


FIGURE 19 – Effet de sauts de fréquence d'un cycle à l'autre de slotframe