

Performances des mécanismes de sécurité du framework 6TiSCH

Défense de mémoire

Rémy DECOCQ

Faculté des Sciences
Université de Mons



26/06/20

Outline

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* :

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

Caractéristiques des *Wireless Sensors Networks* :

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

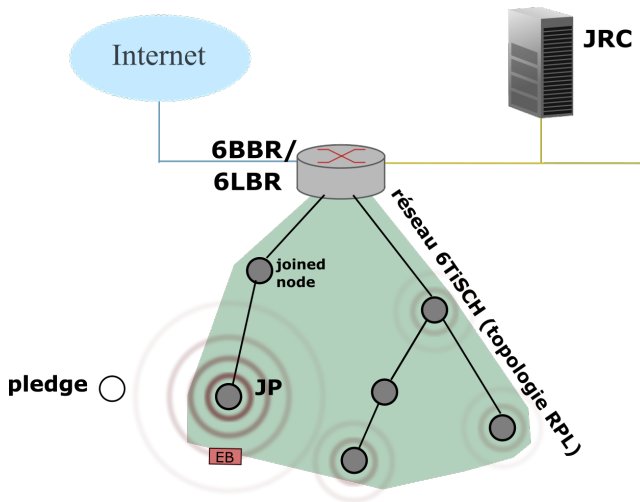


FIGURE 1 – Architecture type d'un WSN où 6TiSCH est déployable

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

Outline

- 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

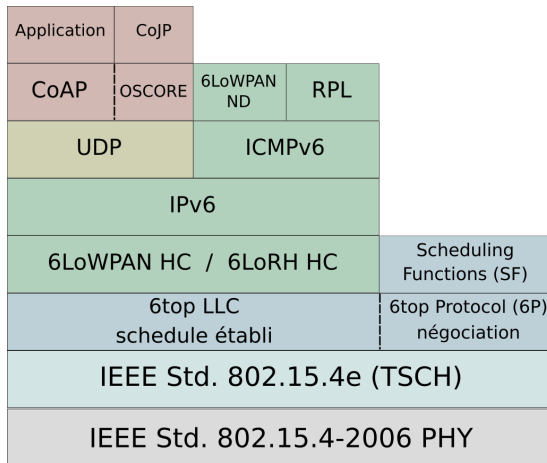


FIGURE 2 – Pile réseau 6TiSCH

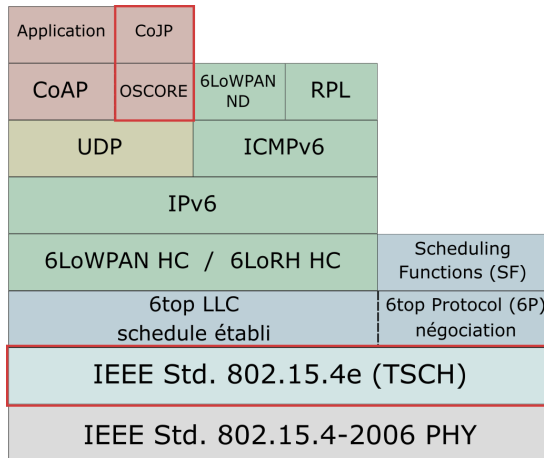


FIGURE 3 – Pile réseau 6TiSCH



Principes fondamentaux de TSCH

Combinaison de :

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

Une communication entre noeuds 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 noeuds communiquant possèdent et partagent cette information
→ communications déterministes sur base d'un *schedule*

channelOffset ↓	0	A	A	
	1		D	A/D
	2	C		
	3	D		
		0	1	2
		slotOffset →		

FIGURE 4 – Matrice des communications

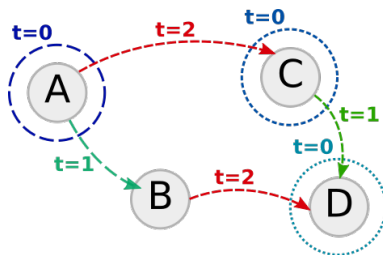


FIGURE 5 – Noeuds communiquant

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

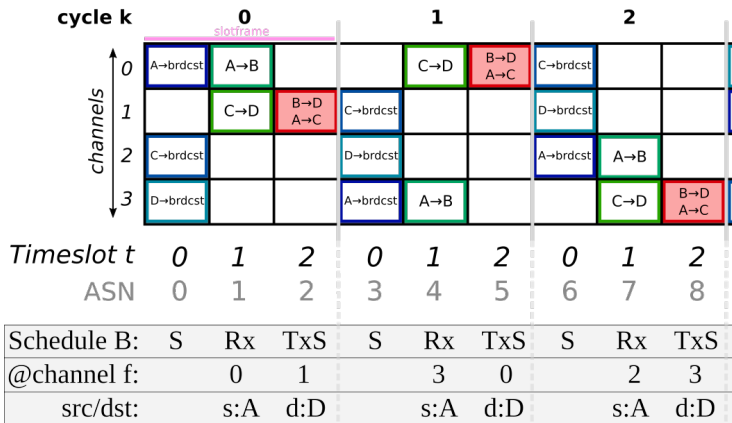


FIGURE 6 – Effet de sauts de fréquence d'un cycle à l'autre de slotframe

La joining phase

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

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

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

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

→ joining phase pour se synchroniser + obtenir les clés

Le pledge possède un contexte de sécurité pré-établi (PSK) partagé avec le JRC.

→ échanges pledge ↔ JRC (*Join Exchange CoJP*) protégés au niveau applicatif par un contexte partagé (*OSCORE*)

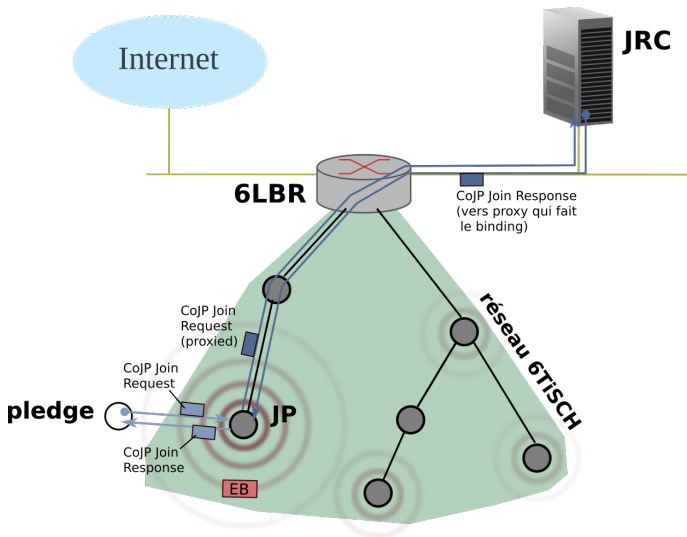


FIGURE 7 – Join Exchange CoJP opéré lors de la joining phase d'un pledge

Outline

- 1 Introduction
 - Les réseaux IloT (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 noeud annonce certains de ses voisins, proposés aux pledges qui évitent une écoute active naïve (**processus itératif d'écoute** de proposition en proposition).

Détermination du "meilleur voisin" basée sur \neq critères

Maintien d'une *NPtable* par pledge et noeuds émettant EBs

<u>noeud 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 8 – Exemple de NPtable et statuts d'écoute possibles (None/0/RSSI)

CYCLE t

NPtable			
neighbors	JM	scheduleNP	EB 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
```

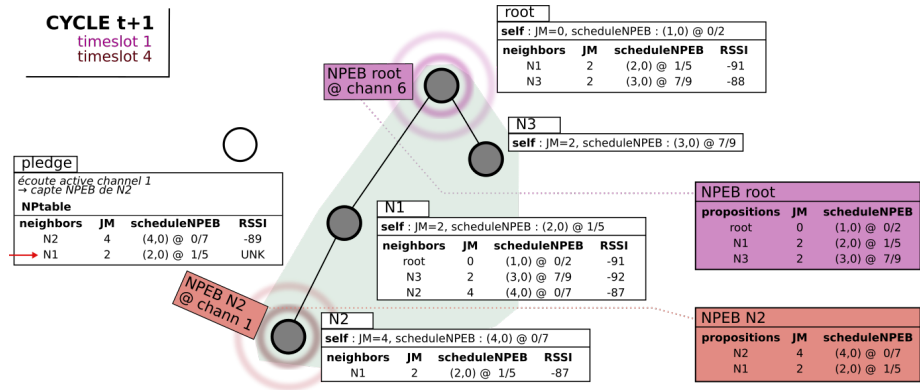
neighbors	JM	scheduleNPEB	RSSI
root	0	(1,0) @ 1/2	-91
N3	2	(3,0) @ 8/9	-92
N2	4	(4,0) @ 1/7	-87

N2

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

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

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



Impact de sécurité sur la joining phase

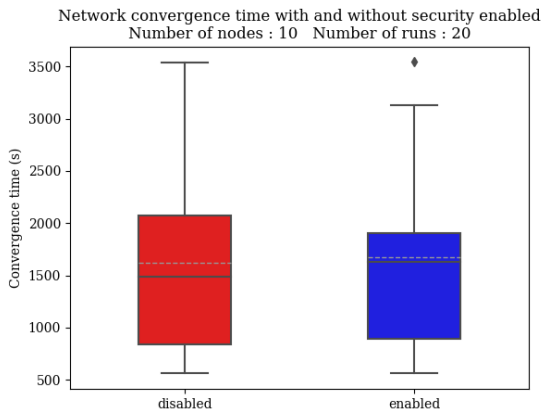


FIGURE 13 – Temps de convergence avec/sans sécurité (Join Exchange CoJP)

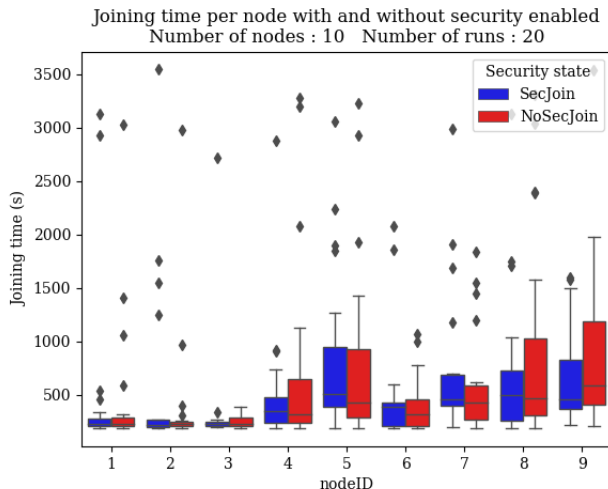


FIGURE 14 – Temps de join pour chaque noeud individuellement

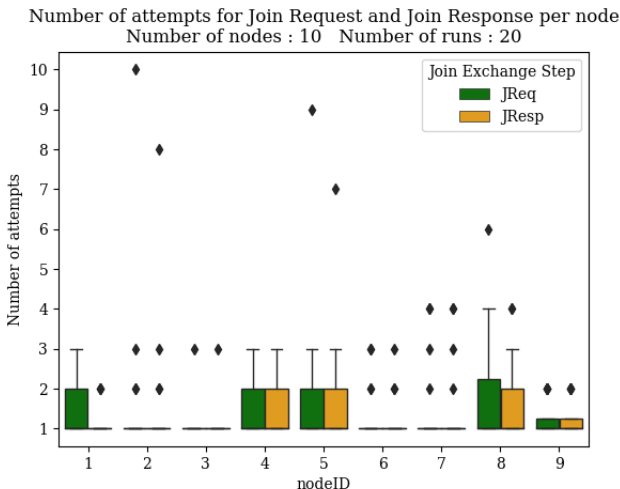


FIGURE 15 – Tentatives nécessaires pour chaque partie du Join Exchange CoJP

Performances de la méthode NPEB

Intuitivement, la méthode NPEB a pour objectif de

- 1 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 : réseau de 30 noeuds, 10 runs et résultats agrégés

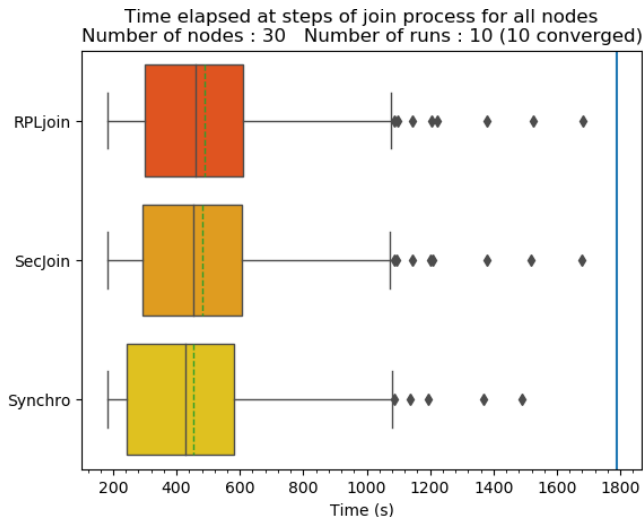


FIGURE 16 – [EBs] Temps requis pour \neq étapes tous noeuds et runs confondus

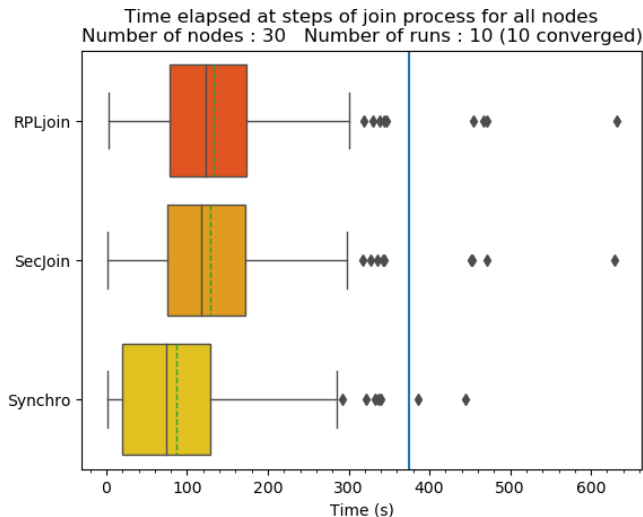


FIGURE 17 – [NPEBs] Temps requis pour \neq étapes tous noeuds et runs confondus

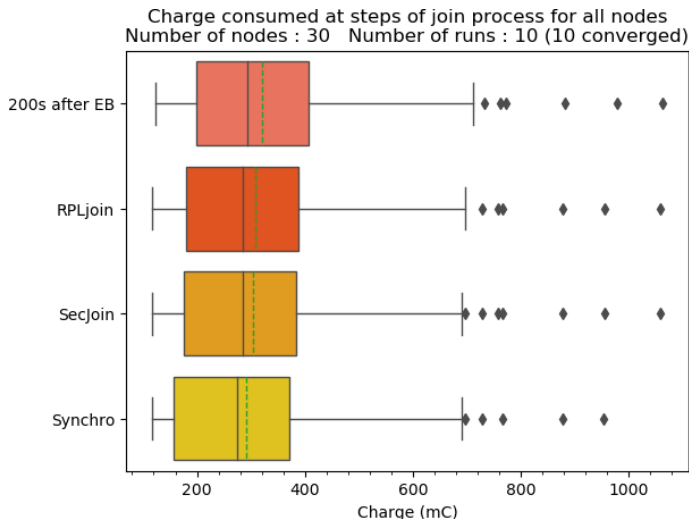


FIGURE 18 – [EBs] Charges consommées aux \neq étapes tous noeuds et runs confondus

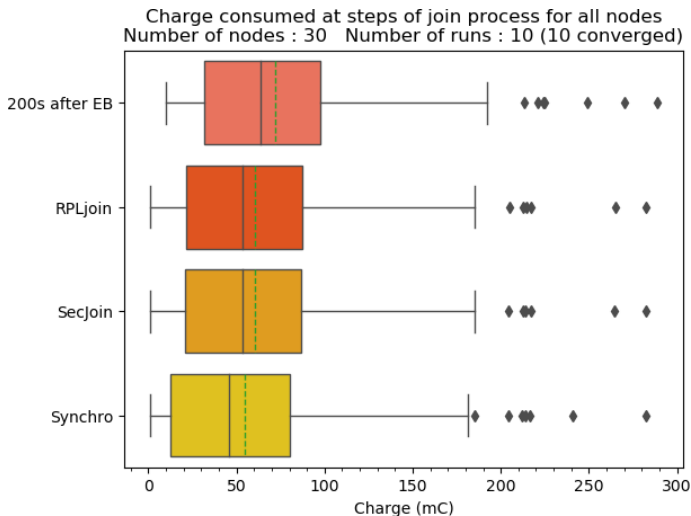


FIGURE 19 – [NPEBs] Charges consommées aux \neq étapes tous noeuds et runs confondus



Performances des mécanismes de sécurité du framework 6TiSCH

Q&A
