

Les Réseaux Zigbee

Thibault LENGAGNE, Sofian MEDBOUHI et Staninslas FECHNER

Centrale Supélec - Campus de Rennes

30 janvier 2016

- 1 Introduction
- 2 La norme IEEE 802.15.4
- 3 Les couches 4 à 7
- 4 Conclusion

Zigbee IEEE 802.15.4

- IEEE 802.15.4 définit les couches basses (physique et mac)
- Zigbee définit les couches réseau et applicative
- Cependant Zigbee fonctionne toujours sur 802.15.4, on confond souvent les deux..

Zigbee doit permettre de construire un réseau avec des équipements

- de faible consommation
- de faible débit/portée
- de faible puissance (de calcul)

Ce qui n'empêche pas le protocole d'implémenter AES128 notamment pour la payload

Zigbee est porté par la *Zigbee Alliance*

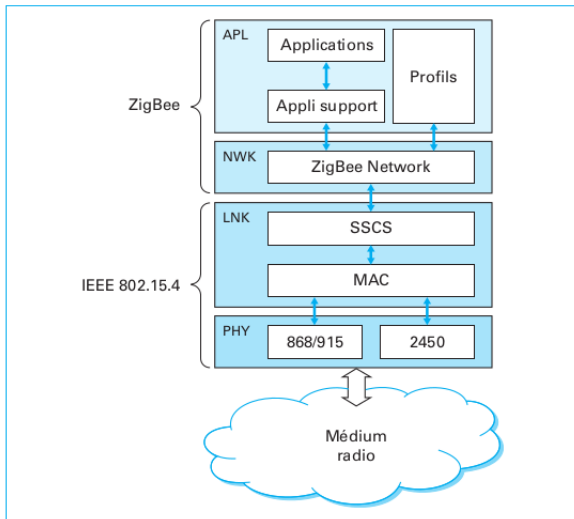
- créée en 2003
- à l'époque sans concurrent important
- désormais en compétition avec WeMo, Brillo et Thread (nous y reviendrons)

Les enjeux sont importants pour l'IoT. Applications à la domotique, contrôle industriel, smart cities...

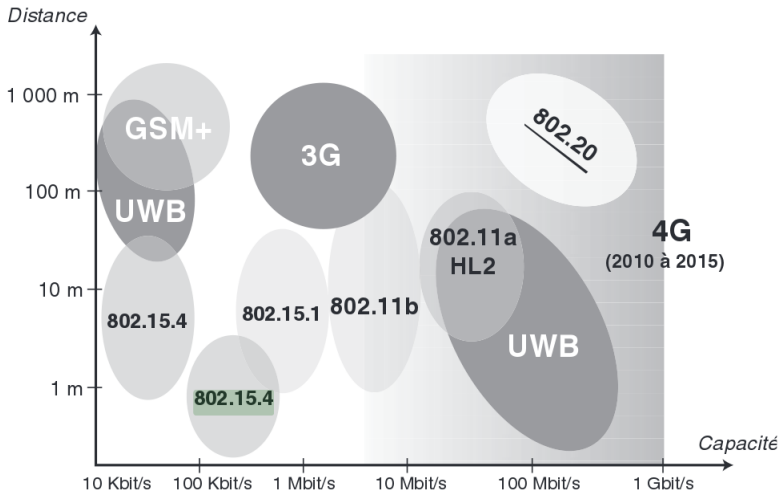
- 1 Introduction
- 2 La norme IEEE 802.15.4
- 3 Les couches 4 à 7
- 4 Conclusion

Zigbee et la norme 802.15.4

Le protocole Zigbee utilise ce protocole comme cadre de fonctionnement :



Schema comparatif des différents protocole sans fil



Contient l'émetteur/récepteur radio, avec un mécanisme de contrôle de qualité du signal et CCA

Débit

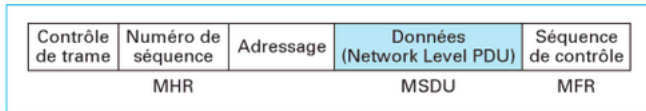
	Bande	Couverture	Débit données	Numéro de canal
2,4 GHz	ISM	Mondiale	250 Kbit/s	16
868 MHz		Europe	20 Kbit/s	1
915 MHz	ISM	Amerique	40 Kbit/s	10

Rôle des éléments du réseau

- Le coordinateur (ZC) est le noeud principal, il est unique
- Les FFD ou routeurs gèrent le routage et les terminaux
- Les RFD ou terminaux sont de simple capteurs aux extrémités du réseau

Format de trame

- En-tête (contrôle de trame, numéro de séquence, adressage)
- Données
- Pied (CRC)



Il existe deux modes de fonctionnement

- Le mode non-coordonnée
- Le mode coordonnée, ou balisé

Le mode non-Coordonnée

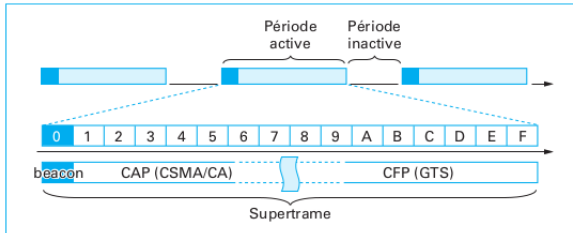
- Pas d'émission de *beacon*
- Fonctionnement CSMA/CA pour gérer les collisions
- Le coordinateur est éveillé en permanence

La sous-couche d'accès au medium (MAC)

Le mode Coordonnée

Le coordinateur diffuse périodiquement des *beacon*. Tous les dispositifs sont informés de :

- La durée de la *superframe* et quand ils peuvent transmettre des données en CSMA/CA
- A partir de quel moment le coordinateur rentre en hibernation et pour quelle durée



La sous-couche de convergence (LLC)

- Vérification de l'intégrité des données reçues
- Contrôle de flux, afin d'éviter la saturation
- La convergence d'adressage (correspondance couche 2 et 3 du modèle OSI, gestion du broadcast et en multicast)

- 1 Introduction
- 2 La norme IEEE 802.15.4
- 3 Les couches 4 à 7**
- 4 Conclusion



Exemple :



- Zigbee propose un algorithme de distribution d'adresses atomatique et décentralisé

-

Exemple :

-

-

- 1 Introduction
- 2 La norme IEEE 802.15.4
- 3 Les couches 4 à 7
- 4 Conclusion**

Zigbee est toujours le protocole de référence :

- Porté par un consortium à la différence de Thread/Brillo (Google) Homekit (Apple) WeMo (Belkin), composé de Phillips/TexasInstrument/Schneider/NXP...
- Connu depuis longtemps d'où 75% des parts de marché
- Possibilité pour les constructeurs de modifier les "profils Zigbee" i.e enrichir la couche applicative
- protocole en évolution constante : Zigbee 3.0 en développement

Cependant quelques écueils qui pourraient se révéler graves

- Non compatible avec IP à la différence de 6LowPAN (sur lequel est basé Thread), ces protocoles devraient représenter 35% des ventes en 2019 (2% ajdh)
- une force est une faiblesse : pas d'entité unique qui porte le standard
- de même les profils différents sont mal utilisés : amènent à des incompatibilités
- problèmes liés à la sécurité
 - Le réseau contient des noeuds à communication chiffrés, d'autres non, attque MiM
 - Attaques restreintes (faible puissance de calcul)
 - mais à venir !