CentraleSupélec

Les Réseaux Zigbee

Thibault LENGAGNE, Sofian MEDBOUHI et Stanislas FECHNER

Centrale Supélec - Campus de Rennes

4 février 2016

Plan

Stratégie

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...

Fonctions principales

Zigbee doit permettre de construire un réseau avec des équipements

- de faible consommation (10mA reception, 19mA emission, 3uA hibernation)
- de faible débit/portée (100m)
- de faible puissance (de calcul)

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

Zigbee, IEEE 802.15.4

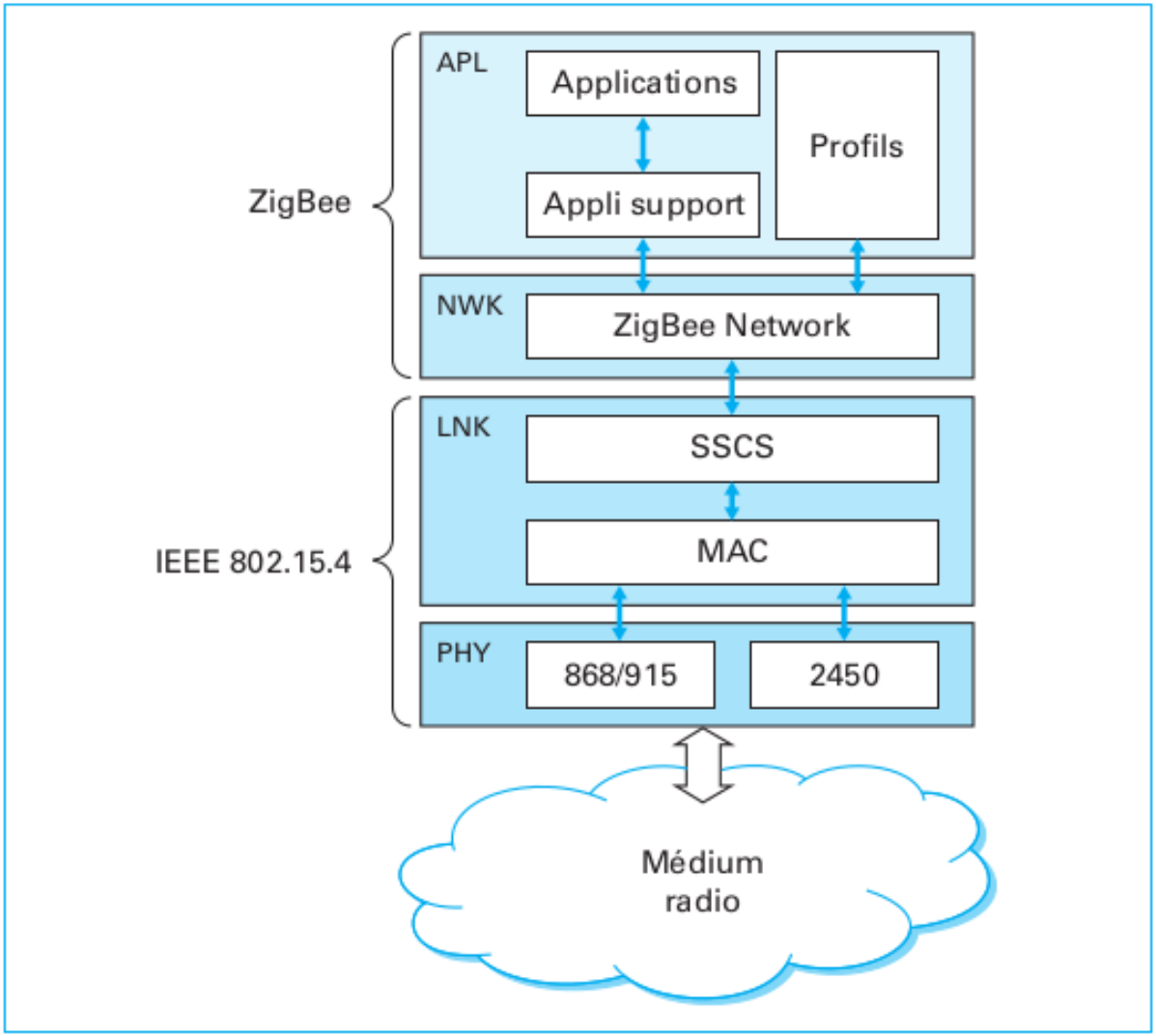
Zigbee IEEE 802.15.4

- 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..

Plan

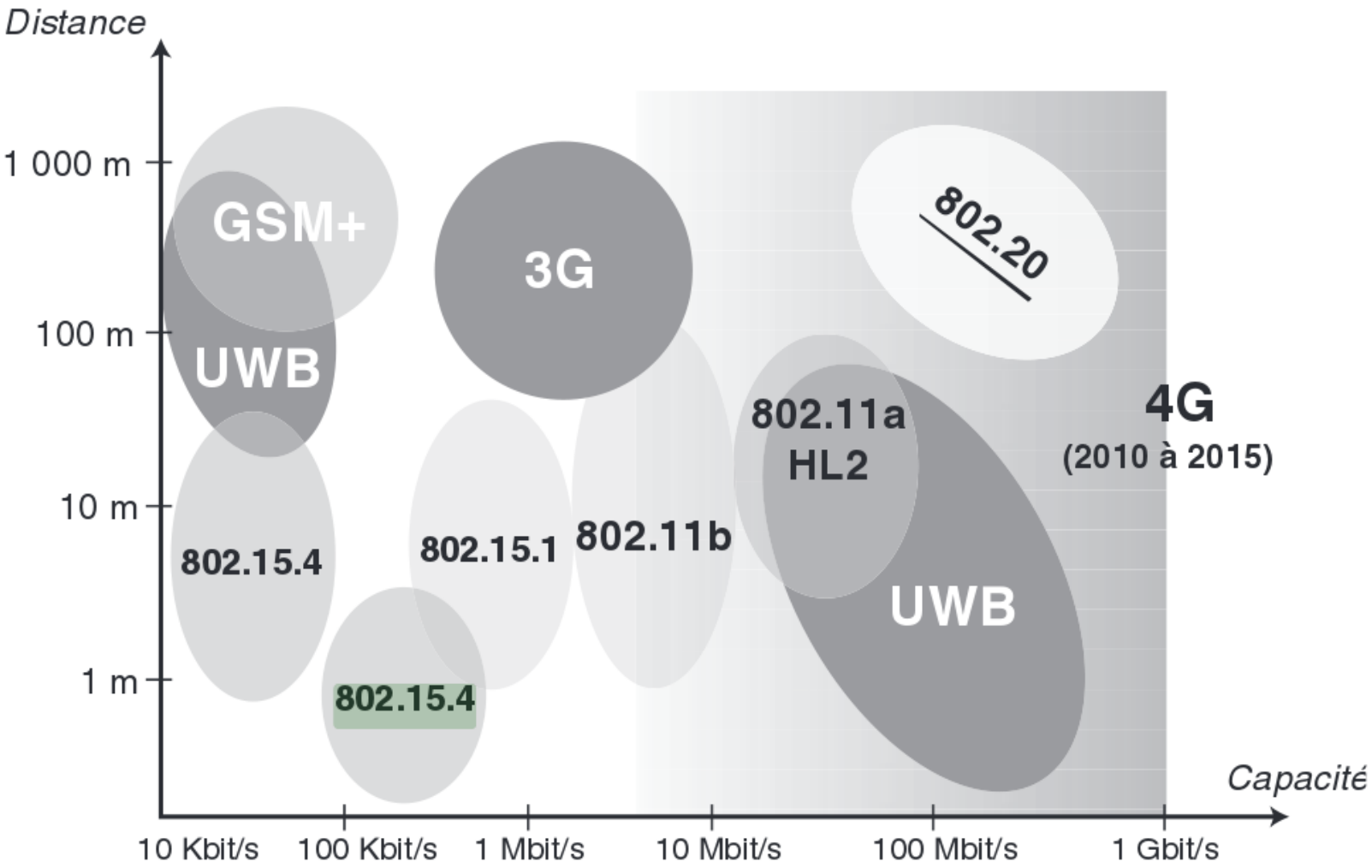
Zigbee et la norme 802.15.4

Le protocole Zigbee utilise ce protocole comme cadre de fonctionnement :



Comparatif

Schema comparatif des différents protocole sans fil



La couche physique

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

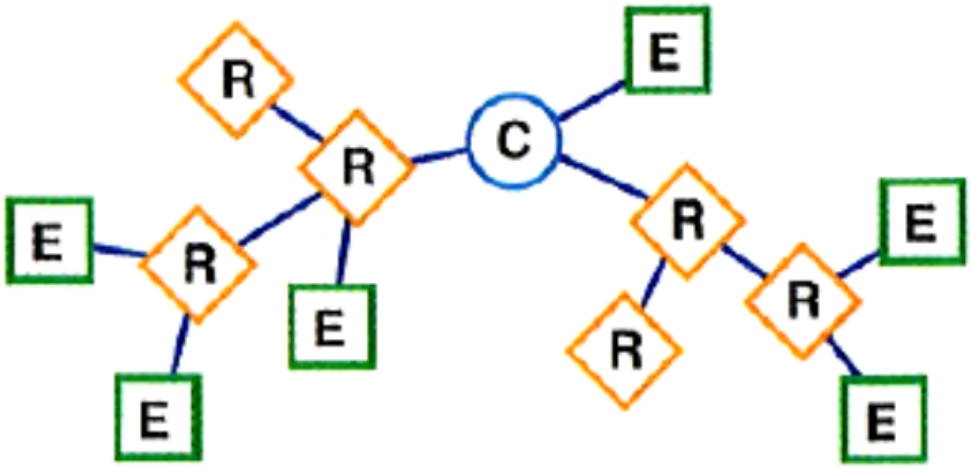
Débit

	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

La couche d'accès au medium (MAC)

Rôle des éléments du réseau

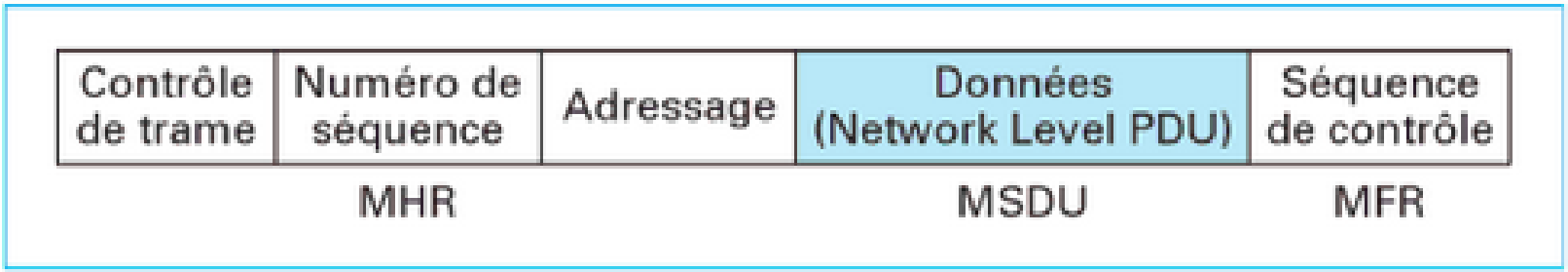
- Le coordinateur (ZC) est le noeud principal, il est unique
- Les FFD ou routeurs gèrent le routage et les terminaux
- Les RFD ou terminaux sont de simple capteurs aux extremités du réseau



La couche d'accès au medium (MAC)

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

La couche d'accès au medium (MAC)

Le mode non-Coordonnée

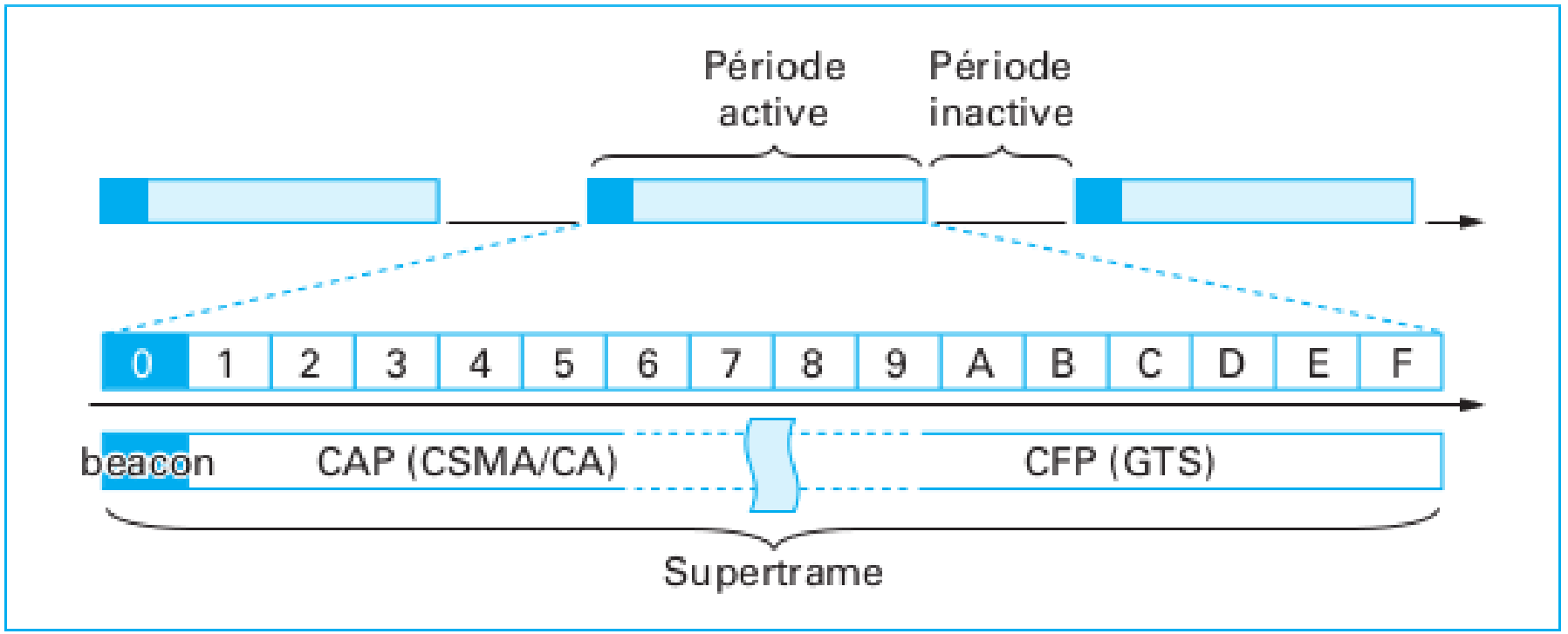
- Pas d'emission de *beacon*
- Fonctionnement CSMA/CA pour gérer les collisions
- Le coordinateur est éveillé en permanence

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
- Tous les dispositifs se réveillent quelques instants avatn l'emission du *beacon*


Période active
Période inactive
0
1
2
3
4
5
6
7
8
9
A
B
C
D
E
F
beacon
CAP (CSMA/CA)
CFP (GTS)
Supertrame

La sous-couche de convergence (LLC)

A la sous-couche MAC est ajouté une sous-couche de convergence LLC

- Vérification de l'intégrité des données reçues (CRC)
- 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)

Plan

Noeuds du réseau

Un réseau Zigbee contient trois types de noeuds

- **ZigBee Coordinator** : unique dans le réseau, la création du réseau s'articule autour de lui. Lorsque le réseau est crée, il se comporte comme un noeud routeur
- **ZigBee Router** : participe au routage, mais peut également envoyer et recevoir des messages
- **ZigBee End Device** : noeud le plus simple du réseau. Il n'est qu'un élément final et ne participe pas au routage des messages

Formation du réseau

La création du réseau démarre en installant le premier noeud, qui joue le rôle de coordinateur

- Le réseau est identifié par un canal et un identifiant de réseau. Cela permet à plusieurs réseau d'utiliser le même canal
- Un noeud recherche un réseau en scannant les canal autour de lui
- Lorsqu'il souhaite intégrer le réseau, il envoie une demande de connexion au noeud routeur le plus proche de lui

Topologie du réseau

Plusieurs type de topologies sont envisageable

- **Topologie en arbre** : les noeuds qui le peuvent se connectent au coordinateur, et les noeud trop éloignés se connectent au routeur le plus proche
- **Topologie maillée** : tous les noeuds routeurs à porté les uns des autres peuvent communiquer entre eux. Les noeuds terminaux ne sont connectés qu'à un routeur

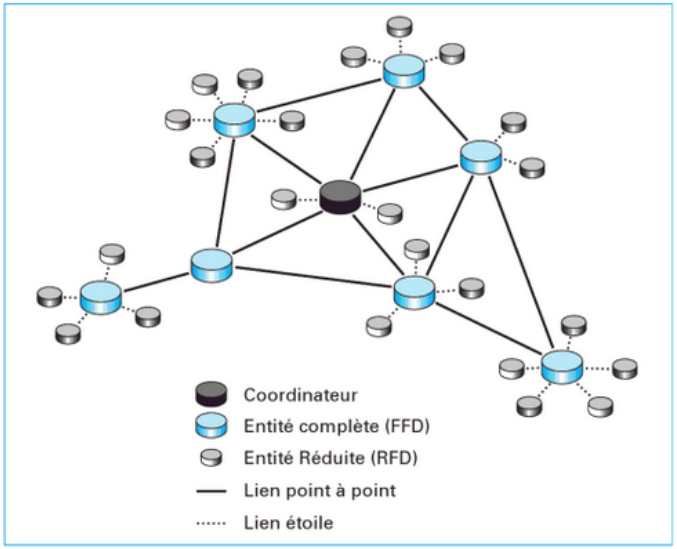


Figure 7 – Exemple de topologie maillée

Adressage

ZigBee autorise deux type d'adressages différents

- **Adressage libre** : l'addressage est determiné par le profil applicatif
- **Adressage en arbre** : Zigbee propose un algorithme de distribution d'adresses automatique. Cet algorithme suit l'arborescence du réseau autour du coordinateur
  - Décentralisé, ce qui minimise les échange au sein du réseau pour attribuer une nouvelle adresse
  - Unicité des adresses
  - Facilite le routage des messages

Routage

Selon le type d'addressage utilisé, deux protocoles de routage peuvent être utilisés

- **Routage à la demande** : le noeud vérifie sa table de routage. Soit il trouve une entrée correspondante à sa destination et transmet le message, sinon il diffuse une requète de demande de route. Cette requète de route atteint le noeud destinataire, qui répond en renvoyant un message qui emprunte la route inverse. Ce message atteint le noeud emetteur, qui peut alors envoyer son message en suivant cette route
- **Routage hiérarchique** : valable uniquement pour l'adressage en arbre. Ce type d'adressage étant deterministe, il est possible de determiner à quel voisin transmettre le message pour atteindre le noeud final

Couche Applicative

ZigBee propose plusieurs profils adaptés à différents usages

- **Gestion de bâtiments** : contrôle des accès, de l'éclairage, du chauffage
- **Périphérique électronique** : clavier ou souris sans fil, télécommande
- **Médical** : suivi des patients, monitioring des activités du corps humain pendant un effort physique

Chacun de ces profils est en fait un protocole qui determine la nature des messages a transmettre afin de faire fonctionner le réseau

La sécurité chez Zigbee ?

Implémente une variation de AES-CCMP

- Clé de 128 bits
- MIC de longueur variable
- 3 variations : ’link key" "network key", "master key" (pro)
- diffusion des clés : OTA/flashage

Chiffrement symétrique basé sur un chiffrement conforme au RGS

La sécurité chez Zigbee ?

Cependant deux failles majeures

- la clé est diffusée en plaintext
- limitations importantes : révocation, durée de vie

Ce qui nous amène à des attaques fonctionnelles concrètes

- Sniffer la clé
- Attaques de type replay
- Aide des constructeurs : clé dans le firmware, encore plus mauvaises implémentations, etc..

Un framework comparable (dans l'idée) à aircrack existe déjà : killerbee

Plan

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

Conclusion

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
- Des problèmes liés à la sécurité
  - Le réseau contient des noeuds à communication chiffrés, d'autres non, attaque MitM
  - Attaques restreintes (faible puissance de calcul)
  - Mais à venir !