



Un protocole pour les gouverner tous ?

Protocole THREAD

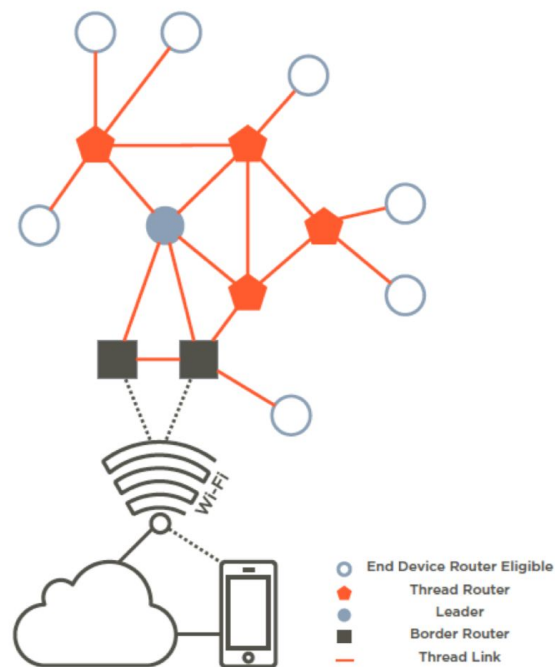
Proposition d'un standard de communication open-source pour l'IoT

Device to Device, sans-fil, fiable et à faible consommation

Repose sur la technologie 6LoWPAN (utilise l'IPv6) elle-même basée sur le protocole 802.15.4-2006

Spécialement conçu pour la maison connectée, de quelques appareils à plus de 250 sur un seul réseau (PAN)

Communique avec Internet sans médiateur

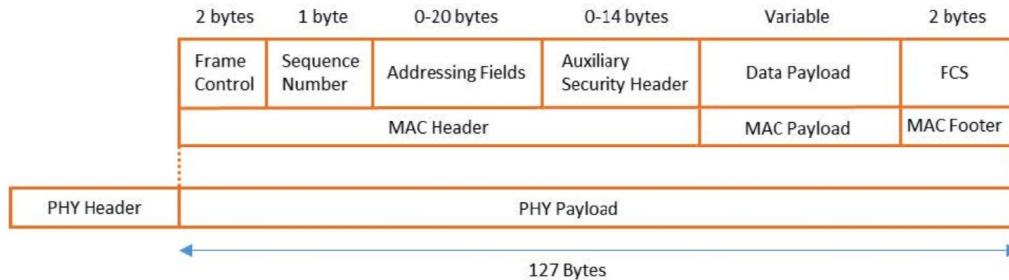


Couche PHY

Basé sur IEEE* 802.15.4

Contient l'émetteur/récepteur radio (RF)

Communique à 250 kbps sur une la bande 2.4 GHz



⚡ H R E A D

Standard

Application Layer

UDP + DTLS

RFC 768, RFC 6347, RFC 4279,
RFC 4492v RFC 3315, 5007

Distance Vector Routing

RFC 1058, RFC 2080

6LowPAN (IPv6)

RFC 4944, RFC 4862, RFC
6775

IEEE 802.15.4 MAC
(including MAC security)

IEEE 802.15.4 (2006)

IEEE 802.15.4 PHY

IEEE 802.15.4 (2006)

*IEEE : Institute of Electrical and Electronics Engineers

Initiation de la communication

Lorsqu'un nouvel appareil Thread est mis en marche il réalise un scan à la recherche de réseau existant.

Si aucun n'est trouvé il en crée un.

Si un réseau existe déjà, un routeur lui envoie un signal contenant le PAN ID, le XPAN ID et le nom du réseau.

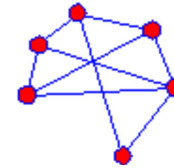
Un appareil peut être soit:

- Leader
- Router
- REED
- End device

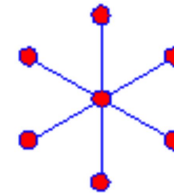
Topologie d'un réseau reposant sur Thread

Thread permet des réseaux en étoile ou maillé.

Maillé : Chaque noeud envoie et reçoit. Cela permet une grande tolérance aux pannes.



Etoilé : Tous les équipements passent par le noeud central pour communiquer. Permet un ajout facile de nouveaux équipements, mais si le concentrateur tombe en panne, aucun équipement ne peut communiquer.



Débit, consommation et portée de Thread

Une portée suffisante pour couvrir une maison (environ 40 mètres).

Un périphérique peut fonctionner pendant plusieurs années avec deux piles AA, grâce à une mise en veille intelligente.

Sécurisation du réseau

Si le Leader tombe en panne, un nouveau Leader est désigné parmi les routeurs du réseau.

Si un device redémarre, il doit avoir stocker en mémoire certaines informations (PAN ID, informations d'adressage) pour se reconnecter automatiquement au réseau.

Un réseau Thread est connecté à Internet, il doit donc être sécurisé. Pour cela une clé de chiffrement des adresses MAC des devices du réseau est générée afin d'éviter les attaques depuis l'extérieur du réseau.

MAC sécurité + principe de commissioning / authorizations / AES encryption

Démonstration



Merci de nous avoir écouté.

Des questions ?

