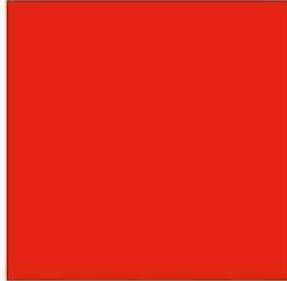
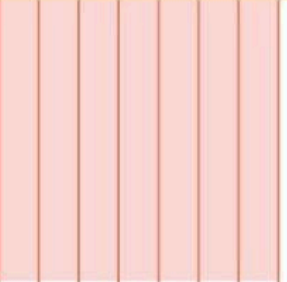
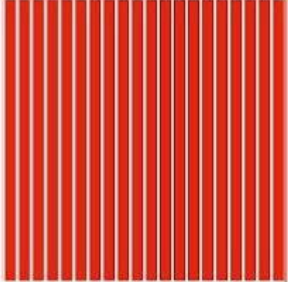
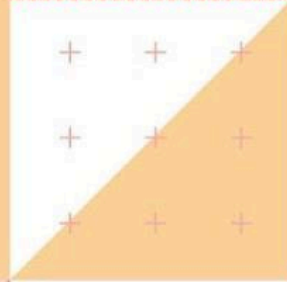
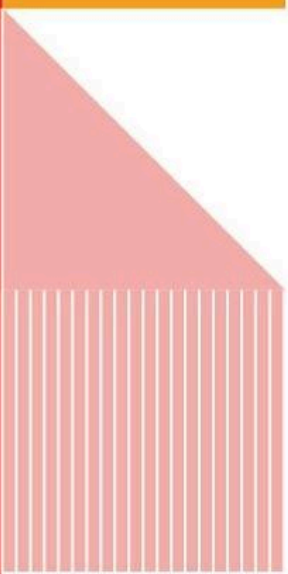
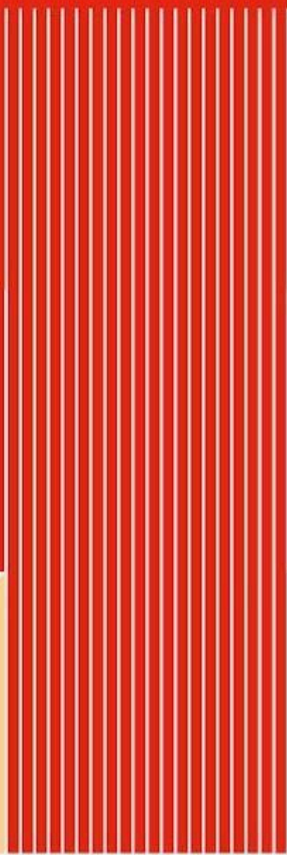
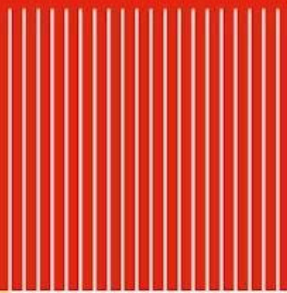


# Le Bluetooth Low Energy (BLE)

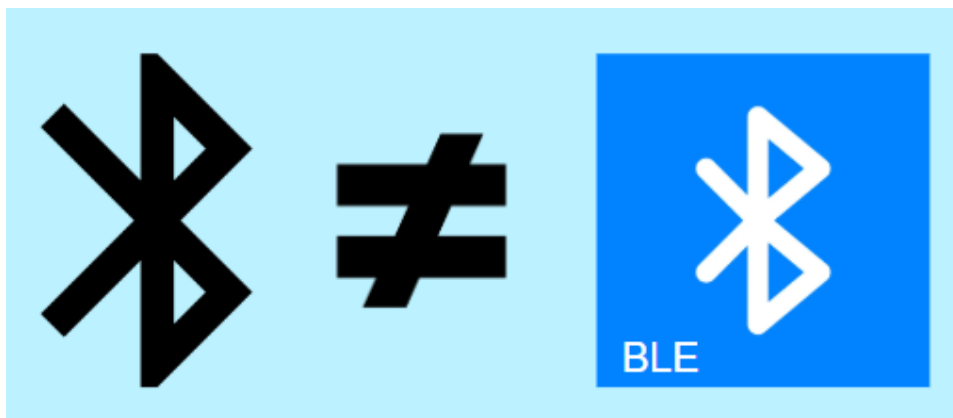
Henriet Baptiste  
Jaulhiac Paul  
Vasseur Cyril  
Jobard Yann



<b>1/ Présentation générale</b>	<b>2</b>
<b>2/ La couche physique</b>	<b>3</b>
Bandes de Fréquence et Organisation des Canaux :	3
Assignation des Canaux et Communication	3
Adaptive Frequency Hopping	3
Modulation, Débit de Données et Efficacité de Transmission	4
Coexistence avec les Réseaux 802.11 (Wi-Fi®)	4
Absence de Synchronisation d'Horloge Continue	5
<b>3/ La couche MAC</b>	<b>6</b>
Fonctionnalités de la Couche MAC	6
Phase de négociation - Handshaking	7
Paquet BLE	8
<b>4/ BLE et consommation énergétique</b>	<b>9</b>
Mode de Fonctionnement en Rafale	9
Diffusion Périodique et Flexibilité des Intervalles de Connexion	9
Consommation Différenciée Selon le Rôle du Dispositif	10
Puissance d'Émission et Contrôle de la Latence	11
Protocoles de Couche Basse Optimisés	11
Une Optimisation du Système qui permet l'Efficacité Énergétique	11
<b>5/ Sécurité</b>	<b>12</b>
Mode de sécurité 1	12
Mode de sécurité 2	13
<b>Conclusion</b>	<b>15</b>
<b>Sitographie</b>	<b>15</b>

# 1/ Présentation générale

Le Bluetooth Low Energy (BLE) est une technologie de communication sans fil spécifiquement conçue pour répondre aux besoins des objets connectés (IoT). Optimisé pour des échanges de données légers et peu fréquents, le BLE favorise l'intégration d'appareils dans des domaines variés, tels que la santé connectée, la domotique ou les dispositifs portables. Contrairement au Bluetooth classique, qui privilégie des connexions stables et à haut débit pour des usages comme le streaming audio, le BLE mise sur des **connexions légères, spontanées** et une **faible consommation énergétique**. Cette approche, bien que sacrifiant les débits élevés et une partie de la portée, le rend idéal pour les dispositifs fonctionnant sur batterie et les communications intermittentes, consolidant ainsi son rôle clé dans l'essor de l'IoT.



Une des forces du BLE réside dans sa capacité à gérer simultanément **plusieurs connexions**. Cette flexibilité permet à un appareil de jouer des rôles variés, que ce soit comme maître ou esclave, et de basculer entre ces rôles selon les besoins. De plus, la rapidité avec laquelle des connexions peuvent être établies et rompues facilite une interaction spontanée entre les dispositifs, rendant la technologie idéale pour des environnements dynamiques et interconnectés.

La technologie se distingue également par sa **faible consommation énergétique**, un critère essentiel pour des dispositifs fonctionnant sur batterie, souvent pendant plusieurs années. Cette efficacité repose sur l'idée d'activer la radio uniquement lorsque cela est nécessaire, conformément à la philosophie du BLE : "Turn radio on as seldom as possible", *Michael K. K. Lee*. Cette approche réduit non seulement les besoins en énergie mais minimise aussi les coûts de production, renforçant son accessibilité pour des **applications IoT en masse**.

Dans ce rapport, nous examinerons en détail les aspects techniques et opérationnels qui font du BLE une technologie incontournable. Nous commencerons par analyser ses couches **physiques** et **MAC**, avant de nous intéresser à ses optimisations en termes de **consommation énergétique** et enfin à ses mécanismes de **sécurité**, qui garantissent des communications fiables et sécurisées dans un environnement connecté.

## 2/ La couche physique

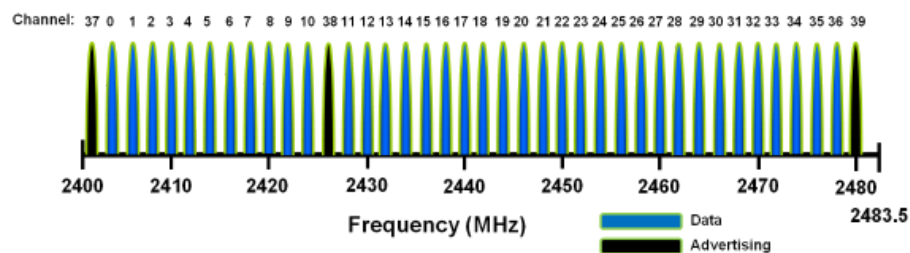
### Bandes de Fréquence et Organisation des Canaux :

Le **Bluetooth Low Energy (BLE)** utilise la bande ISM de 2,4 GHz, commune aux applications industrielles, scientifiques et médicales, pour permettre la communication entre appareils. Cette bande est divisée en **40 canaux de 2 MHz** chacun, de 2,400 GHz à 2,4835 GHz, débutant à 2,402 GHz. Cette organisation en canaux permet de gérer simultanément plusieurs types de transmissions.

### Assignation des Canaux et Communication

Les 40 canaux BLE se répartissent en deux catégories :

- **Canaux de publicité** : Les canaux 37, 38 et 39 sont dédiés à la publicité. Ils servent principalement à la découverte de dispositifs, à l'établissement de connexions et aux transmissions de diffusion.
- **Canaux de données** : Les 37 autres canaux (0-36) sont utilisés pour les communications bidirectionnelles entre dispositifs connectés, exploitant un système de saut de fréquence adaptatif (Adaptive Frequency Hopping) pour gérer les événements de connexion et réduire les interférences.

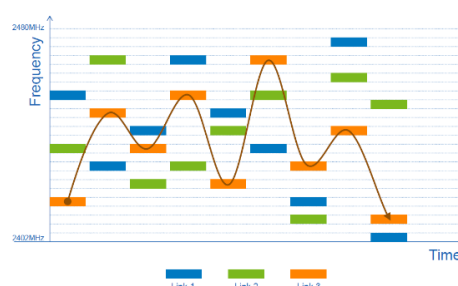


### Adaptive Frequency Hopping

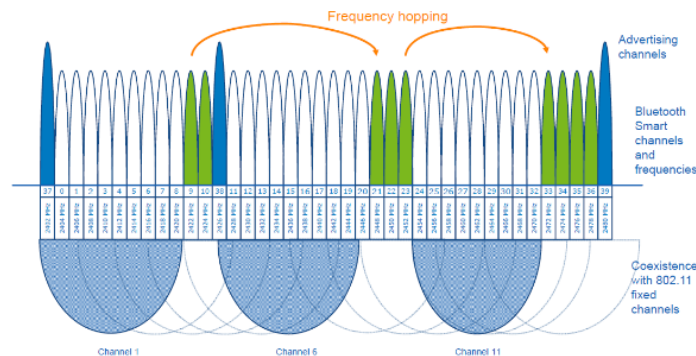
Lorsqu'un dispositif BLE est en communication active sur les canaux de données, il utilise un **algorithme de saut de fréquence** pour parcourir les 37 canaux de données disponibles. Ce mécanisme suit la formule :

$$fn+1 = (fn + hop) \bmod 37$$

où  $fn+1$  est le canal de fréquence pour le prochain événement de connexion, et **hop** est un incrément défini lors de l'établissement de la connexion, avec une valeur comprise entre 5 et 16. Cet incrément est ajouté au canal actuel pour déterminer le canal suivant, modulo 37.



Ce saut de fréquence garantit que les dispositifs BLE évitent les canaux encombrés ou sujets aux interférences, comme ceux utilisés par le Wi-Fi. Par exemple, si un dispositif BLE se trouve dans une zone où les réseaux Wi-Fi occupent les canaux 1, 6 et 11, il peut marquer les canaux 0-8, 11-20 et 24-32 comme « mauvais » et les éviter. À chaque cycle de communication, le BLE remappe automatiquement les canaux identifiés comme problématiques vers des canaux « bons » pour maintenir une connexion stable.



### Modulation, Débit de Données et Efficacité de Transmission

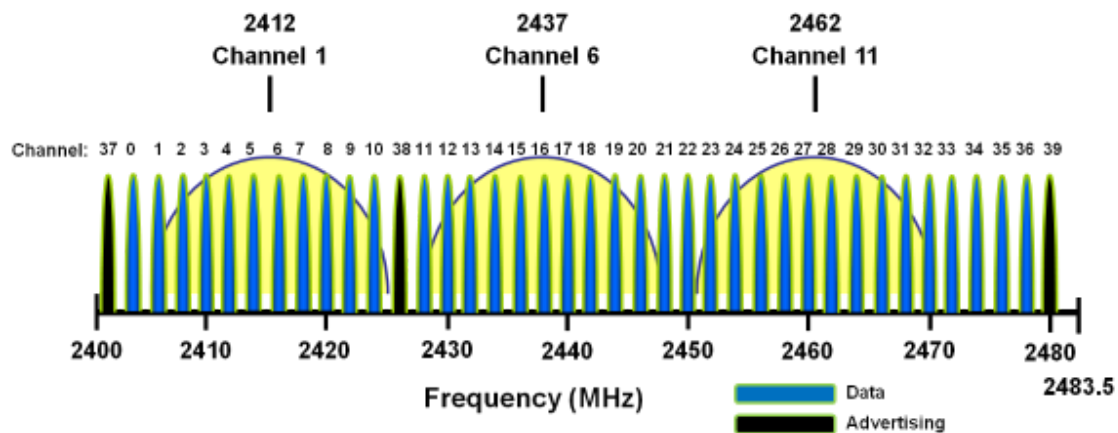
Lors de la transmission, la radio BLE utilise une modulation en **Gaussian Frequency-Shift Keying (GFSK)**. Cette modulation implique que les données sont préalablement filtrées avec un filtre gaussien avant d'être appliquées à la fréquence porteuse, ce qui adoucit les transitions de fréquence et minimise les interférences avec d'autres technologies dans la même bande. En pratique un 0 aura une valeur de fréquence plus faible que la fréquence centrale tandis que le 1 logique aura une fréquence plus élevée.

Le débit de données théorique est de **1 Mbps** (un bit par symbole). Cependant, le **débit réel** est réduit par les charges protocolaires qui limitent le débit effectif en dessous de 1 Mbps, ce qui convient néanmoins pour des transmissions rapides de petits paquets de données, typiques des réseaux WSN. En pratique le débit tourne plus autour de 0,2/ 0,3 Mbps dû aux limitations imposées par le low energy et à l'aspect ponctuel des échanges.

### Coexistence avec les Réseaux 802.11 (Wi-Fi®)

Pour minimiser les interférences avec les réseaux Wi-Fi, les canaux de publicité ont été spécifiquement positionnés pour éviter le chevauchement avec les canaux Wi-Fi les plus courants. Cette configuration facilite la coexistence des deux technologies dans les environnements IoT et assure la continuité de service, même dans des zones denses en signaux radio.

## 2.4 GHz PHY Channel Assignment Bluetooth® Low Energy vs. IEEE 802.11 (United States)



### Absence de Synchronisation d'Horloge Continue

Contrairement à d'autres protocoles de réseaux de capteurs, le BLE n'intègre pas de mécanisme de synchronisation d'horloge interne à la couche MAC. Les transmissions BLE sont basées sur des événements ponctuels, sans nécessiter une synchronisation d'horloge continue entre les nœuds. Cela est adapté pour des dispositifs fonctionnant en mode basse consommation, car ils n'ont besoin d'être actifs que pour des périodes courtes lors des événements de connexion. Ce fonctionnement permet de minimiser l'énergie consommée, ce qui est essentiel dans des applications IoT à faible consommation d'énergie.

### 3/ La couche MAC

La couche MAC, également appelée Link Layer, est l'interface directe avec la couche physique. Elle est majoritairement implémentée en matériel, car elle doit respecter les contraintes de temps réel spécifiées par le Bluetooth Low Energy (BLE). Une partie complémentaire est gérée par **SoftDevice**, un logiciel embarqué.

#### Fonctionnalités de la Couche MAC

- **Gestion de l'accès aux canaux**

La couche MAC encapsule les données des couches supérieures en paquets BLE, qui sont transmis bit par bit à la couche physique. Ces paquets incluent un CRC (Cyclic Redundancy Check) pour vérifier leur intégrité, réduisant ainsi les risques d'erreurs pendant la transmission.

- **Découverte de voisins**

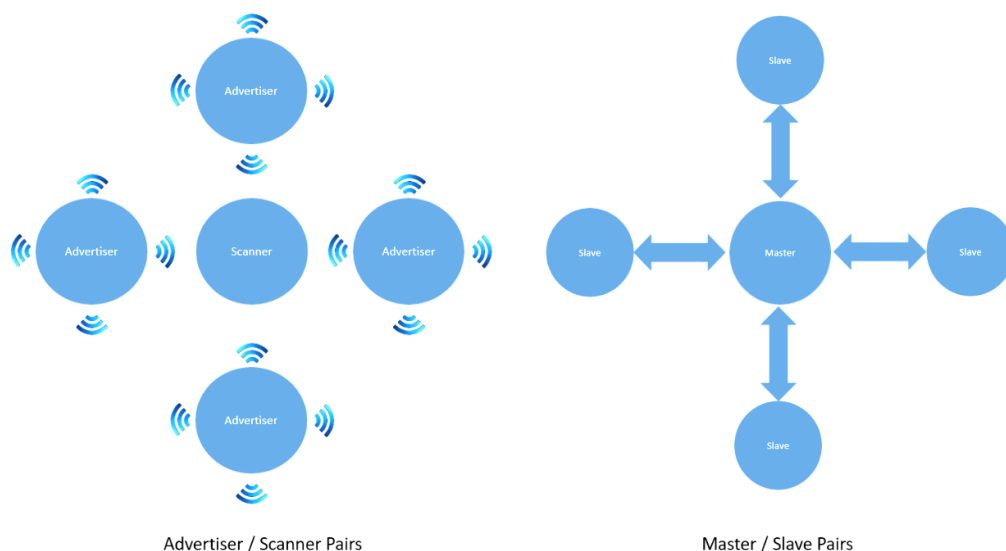
Les appareils BLE utilisent des rôles spécifiques pour se découvrir : l'**Advertiser** envoie des paquets de publicité pour signaler sa présence, tandis que le **Scanner** recherche ces paquets pour détecter les appareils voisins.

- **Établissement des connexions**

Une fois un voisin détecté, le **Master** initie la connexion et prend en charge sa gestion. L'appareil connecté devient alors le **Slave**, suivant la synchronisation définie par le **Master**. Les adresses BLE permettent d'identifier et de différencier les appareils connectés.

- **Ordonnancement des communications**

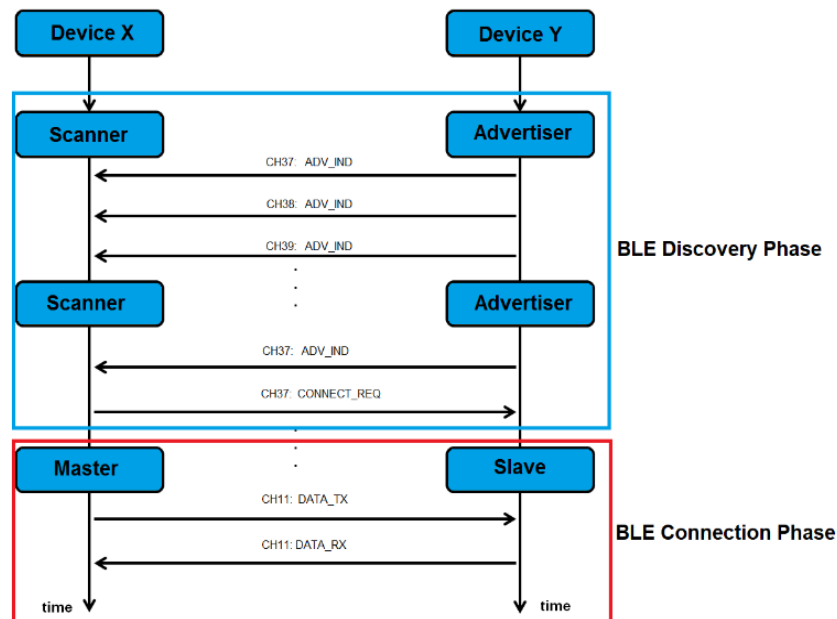
La couche MAC gère l'ordonnancement des échanges et peut sécuriser les données échangées à l'aide de l'algorithme de chiffrement AES-CCM 128 bits, garantissant la confidentialité et l'intégrité des communications.



*Schéma illustrant le changement de rôle issu de <https://embeddedcentric.com/>*

Le schéma ci-dessus illustre le changement de rôle qui s'opère à cheval entre les phases de découverte des voisins et établissement de connexions. Lorsqu'un appareil **Scanner** détecte un **Advertiser** voisin, il s'ensuit une négociation (handshaking), durant laquelle le **Scanner** devient **Master**, et l'**Advertiser** devient **Slave**. Ce mécanisme assure une communication efficace et synchronisée entre les appareils BLE.

#### Phase de négociation - Handshaking



*Schéma illustrant le handshaking issu de <https://embeddedcentric.com/>*

#### **Phase de découverte :**

La phase de découverte permet aux appareils BLE de se détecter mutuellement grâce à des paquets publicitaires envoyés par l'Advertiser sur trois canaux (37, 38, 39) à des intervalles configurables. Ces intervalles, ajustables selon les besoins de consommation énergétique, varient généralement de 20 ms (consommation élevée) à 10,24 secondes (consommation faible). Le Scanner, de son côté, recherche ces paquets lors de fenêtres de scan actives définies au sein d'intervalles plus longs. Ces paramètres, tels que le Scan Interval et le Scan Window, sont configurables et influencent la probabilité de détection et la consommation énergétique. Un équilibre entre ces durées garantit une efficacité énergétique tout en maximisant les chances de détection.

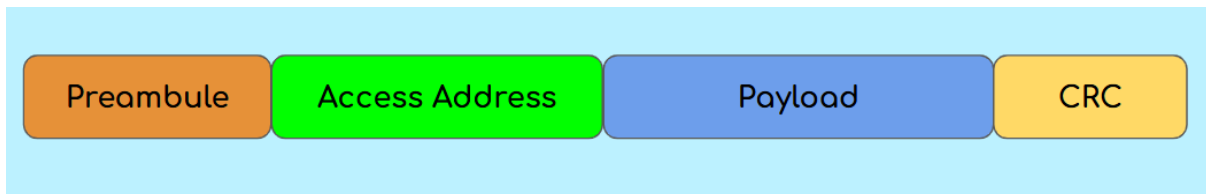
#### **Phase de connexion :**

Lorsqu'un Scanner détecte un Advertiser, il initie la connexion et devient le Master, tandis que l'Advertiser devient le Slave. Plusieurs paramètres de connexion sont négociés : l'intervalle de connexion (de 7,5 ms à 4 s), qui régit la fréquence des échanges de données, et la latence du Slave, qui lui permet de sauter certains événements pour économiser de l'énergie. D'autres paramètres, comme le délai de supervision (100 ms à 32 s) et la longueur des paquets, influencent la qualité et la durée de la connexion. Le Master détient toujours le contrôle final sur ces réglages, assurant une communication efficace entre les deux appareils.



## Paquet BLE

Les paquets du BLE sont composés de 4 éléments. Ils sont regroupés en deux catégories principales : **advertising** (pour la découverte et la connexion initiale) et **données** (pour la communication après la connexion). Ces éléments essentiels assurent un fonctionnement efficace et fiable de la couche MAC.



- **Préambule :**

Sert à synchroniser les fenêtres de transmission et réception entre les appareils connectés en alignant leurs PLL (Phase-Locked Loop). Ce mécanisme garantit une communication fluide en verrouillant les horloges. Taille : 1 octet.

- **Adresse d'accès :**

Identifie une connexion BLE de manière unique. Pendant la phase d'advertising, elle est fixe à 0x8E89BED6, mais pour une connexion active, elle est générée aléatoirement. Cela réduit les risques de collision entre deux connexions opérant sur les mêmes canaux (probabilité de collision :  $1/2^{32}$ ). Taille : 4 octets.

- **Charge utile (payload) :**

Contient les données transmises, dont la taille dépend du type de paquet et de la version BLE :

**Paquets d'advertising :**

- BLE 4.0 : jusqu'à 31 octets, avec une extension possible de 31 octets pour les réponses au scan.
- BLE 5.0 et versions ultérieures : jusqu'à 255 octets, grâce à l'extension d'advertising.

**Paquets de données :**

- BLE 4.0 : charge utile de 27 octets (dont 20 octets pour les données utilisateur).
- BLE 4.2 et versions ultérieures : charge utile de 251 octets (dont 244 octets pour les données utilisateur).

- **CRC (Cyclic Redundancy Check) :**

Garantit l'intégrité des données en vérifiant les erreurs lors de la transmission sans fil. En cas de corruption de données, le CRC permet au récepteur de détecter les paquets erronés. Taille : 3 octets.

## 4/ BLE et consommation énergétique

Le Bluetooth Low Energy (BLE) est une technologie sans fil spécifiquement conçue pour minimiser la consommation d'énergie, un objectif qui le distingue nettement de la version classique du Bluetooth. Ce type de Bluetooth est idéal pour les dispositifs comme les capteurs de l'Internet des objets (IoT), les montres connectées, les appareils de santé, et d'autres dispositifs qui doivent rester opérationnels sur le long terme sans recharge fréquente. Dans cette partie du rapport, nous allons donc nous intéresser aux mécanismes et spécificités du BLE qui contribuent à réduire sa consommation d'énergie.

### Mode de Fonctionnement en Rafale

Le Bluetooth Low Energy utilise un mode de fonctionnement en rafale. Contrairement aux technologies nécessitant une connexion constante, BLE repose sur un modèle de communication intermittente. Les dispositifs BLE passent la majeure partie de leur temps en mode veille pour économiser l'énergie et ne se "réveillent" que pour transmettre ou recevoir des données, avant de retourner en veille une fois l'échange terminé.

Cette approche minimise le temps pendant lequel l'émetteur/récepteur est actif, limitant ainsi la consommation de la batterie. En réduisant la durée et la fréquence d'activation, le BLE permet à des dispositifs tels que des capteurs de mouvement, des montres de fitness, ou des systèmes connectés employés dans le secteur médical, comme les thermomètres connectés, les tensiomètres portables, ou les dispositifs de surveillance de la glycémie, de fonctionner pendant des mois voire des années avec une seule pile bouton.

### Diffusion Périodique et Flexibilité des Intervalles de Connexion

Le BLE utilise un processus de diffusion périodique pour signaler la présence d'un dispositif sans établir de connexion active. Cette diffusion consiste à envoyer de petits paquets d'information de manière régulière, et les dispositifs peuvent ajuster la fréquence des diffusions selon leurs besoins : certaines applications peuvent nécessiter des transmissions toutes les secondes, tandis que d'autres peuvent émettre une diffusion toutes les 10 secondes ou plus, réduisant ainsi la consommation énergétique.

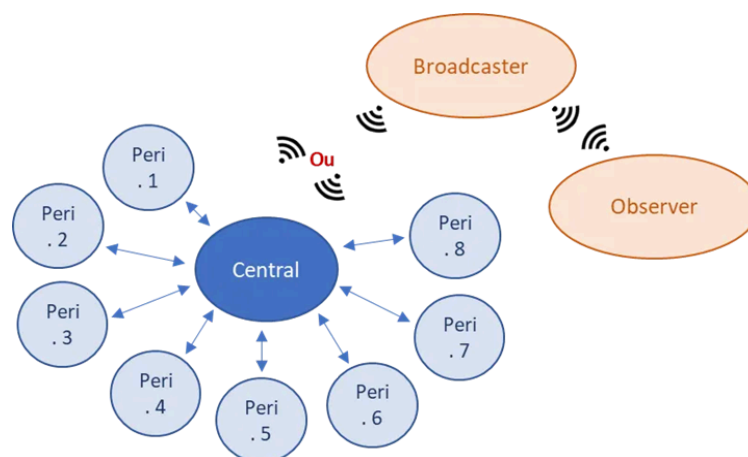
Lorsqu'une connexion est établie entre deux dispositifs BLE, il est possible d'optimiser les intervalles de connexion pour minimiser la consommation d'énergie. Les dispositifs se connectent, transfèrent rapidement les données requises, puis se déconnectent, minimisant le temps passé en mode actif. De plus, BLE permet une grande flexibilité des intervalles d'activation, que l'appareil soit connecté ou non, concernant à la fois la diffusion, le balayage, et la transmission de données. Par exemple, un capteur BLE dans une maison intelligente pourrait être configuré pour se réveiller toutes les heures pour mesurer la température ambiante, ou un dispositif de surveillance de la santé pourrait balayer les données périodiquement pour réagir à un événement particulier. Cette flexibilité permet de contrôler plus précisément la durée de vie de la batterie et d'adapter la consommation d'énergie aux besoins de l'application.

## Consommation Différenciée Selon le Rôle du Dispositif

Le Bluetooth Low Energy définit différents types de connexions et rôles pour les dispositifs, chacun ayant un impact sur la consommation d'énergie. Un objet connecté en BLE peut avoir jusqu'à quatre fonctions différentes : **Broadcaster**, **Observer**, **Central** et **Périphérique**.

- **Broadcaster** : Le Broadcaster agit comme un serveur qui transmet régulièrement des données à un appareil sans accepter de connexion entrante. Ce rôle est idéal pour des dispositifs qui n'ont besoin que de diffuser des informations sans s'engager dans des échanges bidirectionnels, minimisant ainsi la consommation d'énergie.
- **Observer** : L'Observer est un dispositif qui écoute et interprète les données envoyées par un Broadcaster. Dans ce mode, l'Observer ne peut pas envoyer de données ni établir de connexions vers le serveur. Cette approche est utilisée pour des applications où il est nécessaire de recevoir des informations de manière passive, sans émettre de connexions, ce qui réduit également la consommation.
- **Central** : Le rôle Central est souvent attribué à des dispositifs tels que des smartphones ou des tablettes. Un Central peut interagir de deux manières : en mode diffusion (advertising) ou en mode connecté. Le Central est responsable de l'établissement de la connexion et de l'échange de données avec d'autres dispositifs. Il est souvent le dirigeant de la communication, ce qui lui confère une certaine flexibilité mais implique une consommation d'énergie plus élevée que celle des autres rôles.
- **Périphérique** : Le Périphérique accepte les connexions d'un Central et lui envoie des données de manière périodique. Ce rôle a pour objectif de packager les données de façon universelle via le protocole afin qu'elles soient comprises par les autres dispositifs. Les périphériques sont optimisés pour une faible consommation d'énergie, car ils envoient des données uniquement lorsqu'une demande est faite par le Central.

Ces différents rôles permettent au BLE de s'adapter à diverses applications tout en optimisant la consommation d'énergie. En fonction des exigences de chaque application, les rôles des dispositifs peuvent être ajustés afin de trouver un équilibre entre performance et autonomie.



Les différents rôles au sein d'un système BLE

## Puissance d'Émission et Contrôle de la Latence

Un autre facteur qui contribue à la faible consommation d'énergie de BLE est l'utilisation d'une puissance d'émission réduite. BLE est principalement conçu pour des communications à courte portée, avec une puissance d'émission limitée qui permet de maintenir une faible consommation d'énergie. De plus, la puissance peut être ajustée dynamiquement pour équilibrer la portée et l'économie d'énergie. Lorsque deux dispositifs sont à proximité, la puissance d'émission peut être réduite, économisant ainsi la batterie.

Le Bluetooth Low Energy offre également des options avancées pour le contrôle de la latence des communications. Les dispositifs peuvent choisir de retarder certaines communications pour réduire la consommation d'énergie. Par exemple, un dispositif pourrait accumuler des données et les transmettre moins fréquemment au lieu d'envoyer chaque événement immédiatement après qu'il se soit produit. Cette approche permet de maintenir les dispositifs en mode veille plus longtemps et d'éviter les cycles répétitifs de réveil et de transmission.

## Protocoles de Couche Basse Optimisés

Le BLE est conçu avec des protocoles de couche basse optimisés pour une faible consommation d'énergie. Les différentes couches du protocole sont simplifiées pour permettre des communications courtes et rapides, minimisant ainsi le temps pendant lequel la communication du dispositif est active. En outre, la gestion des états de veille est très précise. Contrairement au Bluetooth classique, qui maintient souvent des connexions ouvertes même lorsqu'il n'y a pas de données à transmettre, le BLE permet aux dispositifs de fermer la connexion et de passer en veille sans délai, économisant ainsi l'énergie.

## Une Optimisation du Système qui permet l'Efficacité Énergétique

Les mécanismes de faible consommation d'énergie de BLE en font une technologie particulièrement adaptée pour les dispositifs connectés fonctionnant sur batterie, surtout lorsqu'une autonomie longue est essentielle. En combinant des intervalles de connexion optimisés, des modes de diffusion réduits, une gestion adaptative des émissions et une grande flexibilité des intervalles d'activation, le BLE parvient à minimiser la consommation énergétique de manière significative, c'est-à-dire jusqu'à deux fois, voire dix fois, moins que le Bluetooth classique, selon les sources. Ces caractéristiques rendent les dispositifs BLE idéaux pour une large variété d'applications dans le monde de l'Internet des objets, des capteurs portables et de la santé connectée. Les capacités de BLE à économiser l'énergie assurent non seulement une longue durée de vie pour les dispositifs, mais également une réduction des besoins de maintenance et de remplacement de batteries, améliorant ainsi l'expérience globale des utilisateurs et la viabilité des solutions sans fil.

Ces avantages rendent le Bluetooth Low Energy pertinent non seulement pour les petites applications, mais également pour des infrastructures plus larges, où la minimisation des coûts de maintenance et la longévité des dispositifs sont des critères clés pour le succès technologique et économique.

## 5/ Sécurité

La technologie Bluetooth Low Energy implémente deux modes de sécurité, chacun avec plusieurs niveaux de sécurité.

Toute communication commence au mode de sécurité 1 niveau 1, puis change en fonction du mode et du niveau choisis dans le Generic Access Profile (GAP).

### Mode de sécurité 1

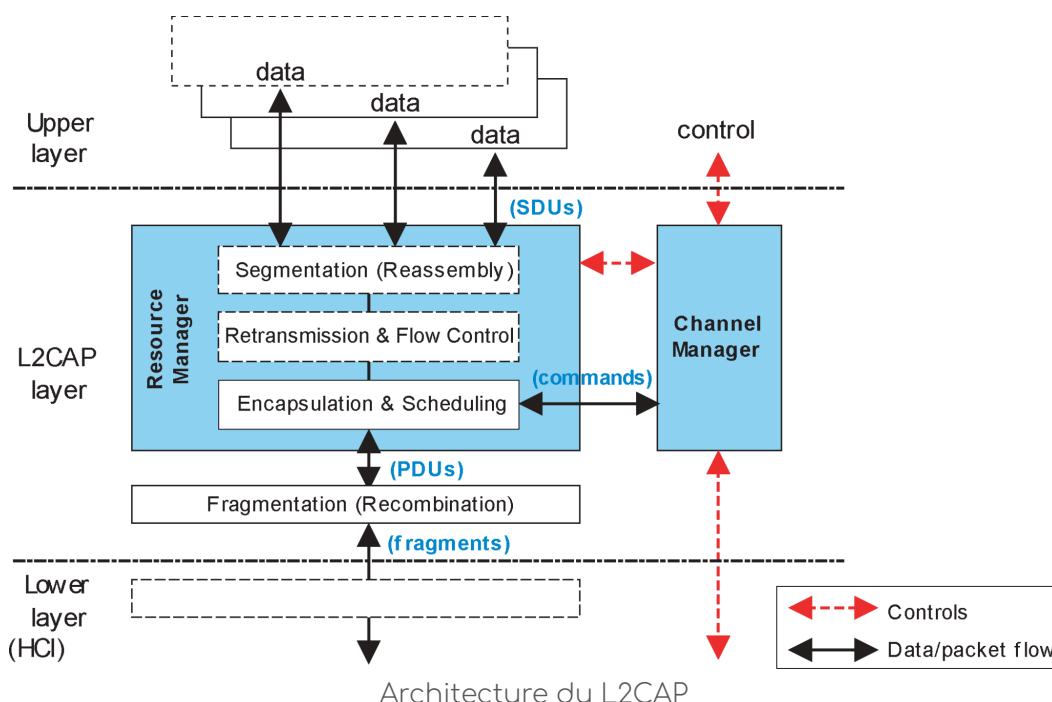
Ce mode de sécurité présente 4 niveaux différents. Les niveaux de ce mode sont hiérarchisés, c'est-à-dire que chaque niveau valide les attentes de sécurité de tous les niveaux inférieurs.

#### Niveau 1 :

Le niveau le moins sécurisé du mode 1. Il ne présente aucune sécurisation, soit pas d'authentification ou d'encodage. Les appareils utilisant ce niveau de sécurité se connectent sans appairage, et ne peuvent donc communiquer qu'entre eux.

#### Niveau 2 :

Le premier niveau implémentant des solutions de sécurisation. L'établissement de connexion entre les appareils n'est pas sécurisé à ce niveau, l'appairage se fait sans authentification, selon la méthode Just Works. Une fois la connexion établie, la connexion est sécurisée. Cette sécurisation est implémentée au niveau du protocole L2CAP



#### Niveau 3 :

L'appairage se fait avec authentification, selon les méthodes Passkey entry ou Out-of-Band. L'authentification Out-of-Band utilise des canaux séparés pour l'authentification et la communication. Pour l'authentification Passkey entry, l'un des deux appareils affiche une clé à 6 chiffre que l'utilisateur confirme puis entre sur l'autre appareil

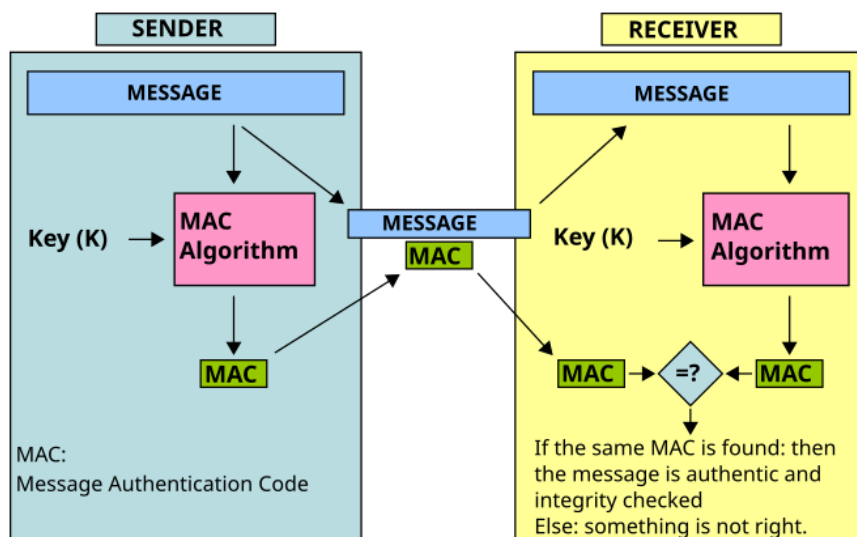
afin de réduire les chances d'usurpation, notamment Man in the middle. L'action de l'utilisateur est obligatoire dans les deux cas.

#### Niveau 4 :

Les appareils s'échangent une paire de clé publique/privée selon l'algorithme Diffie-Hellman afin de réaliser l'appairage, c'est la procédure LE Secure Connections qui remplace le Legacy Pairing hérité de Bluetooth. Une clé de liaison de 128 bits est générée. L'appairage peut se faire selon n'importe laquelle des 4 méthodes (Just Works, Passkey entry, OOB ou Numeric Comparison). Numeric Comparison affiche une clé à 6 chiffres sur les deux appareils, l'utilisateur confirme alors la connexion si les deux clés sont identiques. La communication est ensuite encodée par une clé de 8 à 128 bits.

#### Mode de sécurité 2

Le mode de sécurité 2 implémente la signature des données basée sur la connexion. Il présente 2 niveaux de sécurisation.



Signature des données basée sur la connexion

#### Niveau 1 :

Au niveau 1, l'appairage se fait sans interaction utilisateur ou authentification, selon la méthode Just Works, il n'y a donc aucune protection contre les Man-in-the-Middle et la connexion est généralement peu sécurisée. Les appareils doivent échanger une Connection Signature Resolving Key (CSRK) pour établir la signature des données.

#### Niveau 2 :

L'appairage se fait avec authentification et interaction utilisateur, selon les méthodes OOB, Passkey Entry ou Numeric Comparison, protégeant contre les Man-in-the-Middle. Les données sont encodées durant la communication.

## Conclusion

Pour conclure sur ce rapport, nous avons donc réalisé au cours de ce rapport que le Bluetooth Low Energy tire parti de la bande ISM de 2,4 GHz pour offrir une communication efficace et robuste grâce à une organisation précise des canaux et à l'utilisation de techniques telles que le saut de fréquence adaptatif. Cette stratégie permet de réduire les interférences, notamment dans des environnements partagés avec le Wi-Fi, et d'assurer une coexistence harmonieuse des technologies. De plus, le choix de la modulation GFSK et l'absence de synchronisation continue renforcent l'efficacité énergétique du BLE, en faisant une solution idéale pour les dispositifs IoT à faible consommation. Cette architecture démontre ainsi un équilibre entre performance, fiabilité et optimisation énergétique.

Nous avons ensuite pu nous concentrer sur la couche MAC du BLE qui joue un rôle central en assurant la communication efficace et sécurisée entre les appareils connectés. Elle gère l'accès aux canaux, la découverte des voisins, et l'établissement des connexions grâce à des mécanismes tels que le handshaking et le chiffrement AES-CCM 128 bits. Les paquets BLE, optimisés pour la simplicité et la fiabilité, permettent une transmission rapide et économe en énergie, tout en garantissant l'intégrité des données via le CRC. Ces fonctionnalités, associées à des paramètres configurables comme les intervalles de connexion et la gestion de la latence, font de la couche MAC une interface clé pour répondre aux exigences de faible consommation et de robustesse des communications dans l'écosystème IoT.

Comme évoqué précédemment, nous avons pu montrer que le BLE se distingue par sa capacité à minimiser la consommation d'énergie, répondant ainsi aux besoins des dispositifs IoT et des appareils fonctionnant sur batterie. Grâce à des mécanismes comme le mode de fonctionnement en rafale, la diffusion périodique, et la gestion adaptative des intervalles de connexion, le BLE permet d'optimiser la durée de vie des dispositifs tout en maintenant une efficacité énergétique remarquable. Les différents rôles des appareils BLE permettent une flexibilité d'utilisation adaptée à diverses applications, tandis que la puissance d'émission ajustable et les protocoles optimisés contribuent à réduire davantage la consommation. En intégrant ces caractéristiques, le BLE offre une solution viable et durable, particulièrement pertinente pour des environnements nécessitant autonomie et fiabilité sur le long terme.

Pour finaliser notre étude, nous nous sommes focalisés sur l'aspect sécurité du Bluetooth Low Energy, celui-ci propose une architecture de sécurité flexible, adaptée à divers besoins. Les modes de sécurité 1 et 2, avec leurs niveaux hiérarchisés, permettent une gradation de la sécurisation, allant de l'absence totale de protection à des mécanismes avancés tels que l'encodage et l'authentification renforcée. Ces niveaux garantissent une compatibilité entre appareils tout en offrant des options pour répondre aux exigences spécifiques en matière de confidentialité et de résistance aux attaques. Ainsi, le BLE s'affirme comme une technologie polyvalente et évolutive pour des communications sécurisées.

## Sitographie

- <https://developerhelp.microchip.com/xwiki/bin/view/applications/ble/introduction/bluetooth-architecture/bluetooth-controller-layer/physical/>
- <https://iotindustriel.com/glossaire-iiot/bluetooth-low-energy-ble-cest-quoi/#:~:text=BLE%20utilise%20la%20m%C3%AAme%20bande,canaux%20diff%C3%A9rents%20du%20Bluetooth%20s%20tandard.>
- <https://ieeexplore.ieee.org/document/9555832>
- <https://developerhelp.microchip.com/xwiki/bin/view/applications/ble/introduction/bluetooth-architecture/bluetooth-host-layer/gap/security/>
- [Guide to Bluetooth Security](#)
- [Bluetooth GAP documentation](#)
- <https://elainnovation.com/quest-ce-que-le-bluetooth-low-energy/>
- <https://www.digikey.fr/fr/articles/moving-forward-with-bluetooth-low-energy>
- [https://www.researchgate.net/publication/343343474\\_Wake-up\\_radio\\_enabled\\_BLE\\_wearables\\_empirical\\_and\\_analytical\\_evaluation\\_of\\_energy\\_efficiency](https://www.researchgate.net/publication/343343474_Wake-up_radio_enabled_BLE_wearables_empirical_and_analytical_evaluation_of_energy_efficiency)
- <https://www.mistywest.com/posts/low-power-optimizations-for-a-bluetooth-connected-wearable/>
- [https://en.wikipedia.org/wiki/Bluetooth\\_Low\\_Energy](https://en.wikipedia.org/wiki/Bluetooth_Low_Energy)
- <https://embeddedcentric.com/introduction-to-bluetooth-low-energy-bluetooth-5/>