XBee

Table des matières

"XBee" est une famille de composants sans-fil prêts à l'emploi développés qui implémentent différents protocoles, dont 802.15.4 et sa version de plus haut-niveau ZigBee, ainsi que des protocoles de réseau ad-hoc ("mesh") spécifique.

1. Présentation du XBee

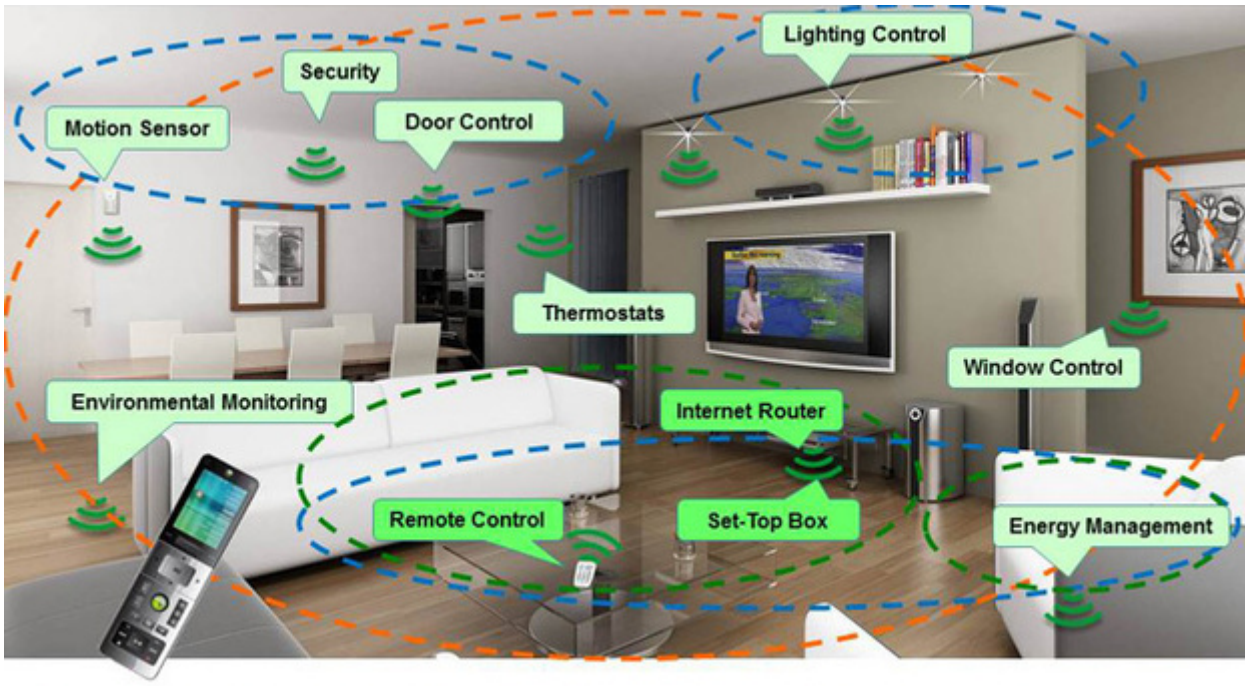
Les produits XBee sont des modules de communication sans fil certifiés par la communauté industrielle ZigBee Alliance. La certification Zigbee se base sur le standard IEEE 802.15.4 qui définit les fonctionnalités et spécifications des réseaux sans fil à dimension personnelle (Wireless Personal Area Networks : WPANs).

Les principales caractéristiques du XBee :

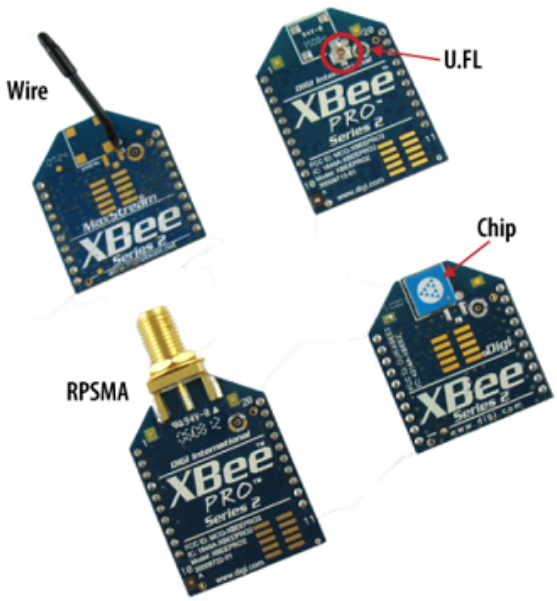
- fréquence porteuse : 2.4Ghz
- portées variées : assez faible pour les XBee 1 et 2 (10 - 100m), grande pour le XBee Pro (1000m)
- faible débit : 250kbps
- faible consommation : 3.3V @ 50mA (inférieure à 10 µA en mode "sleep").
- entrées/sorties : 6 10-bit ADC input pins, 8 digital IO pins
- sécurité : communication fiable avec une clé de chiffrement de 128-bits
- faible coût : ~ 25€
- simplicité d'utilisation : communication via le port série
- ensemble de commandes AT et API
- flexibilité du réseau : sa capacité à faire face à un nœud hors service ou à intégrer de nouveaux nœuds rapidement
- grand nombre de nœuds dans le réseau : 65000
- topologies de réseaux variées : maillé, point à point, point à multipoint

1.1. Applications

Le ZigBee a été conçu pour réaliser l'Internet des objets, un ensemble d'objets communicants voir "autonomes", une extension d'Internet aux objets physiques. La domotique est l'exemple le plus parlant.



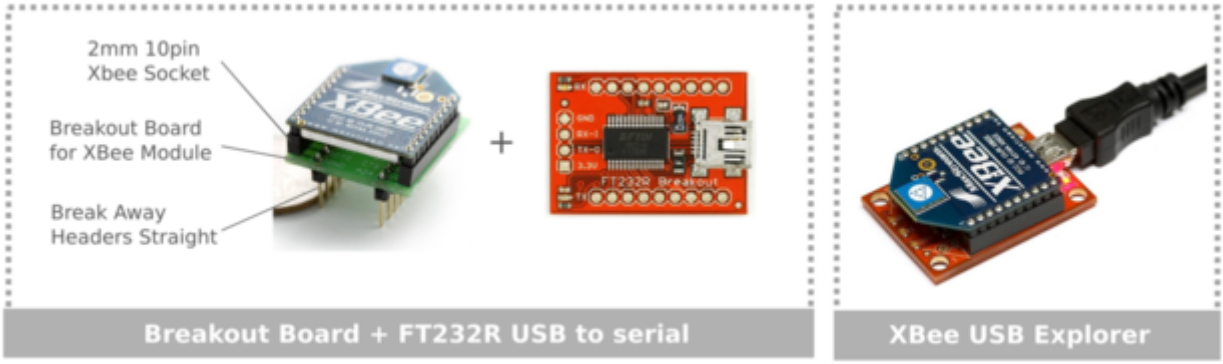
1.2. Antennes



- wire : simple, radiations omnidirectionnelles ;
- chip : puce plate en céramique, petite, transportable (pas de risques de casser l'antenne), radiations cardioïdes (le signal est atténué dans certaines directions) ;
- U.FL : une antenne externe n'est pas toujours nécessaire;
- RPSMA : plus gros que le connecteur U.FL, permet de placer son antenne à l'extérieur d'un boîtier.

1.3. Communication avec l'ordinateur

Pour établir une communication avec l'ordinateur, il y a deux options : l'assemblage de différents éléments ou le XBee USB Explorer.



La communication en direct sans passer par une Arduino permet de configurer rapidement le XBee.

Les paramètres importants sont :

- PAN ID (Personal Area Network) : Identifiant du réseau personnel. Cet identifiant doit être le même pour les modules XBee qui doivent appartenir au même réseau.
- SH (Serial Number High) : Bits de poids fort (32 bits) du numéro de série du module XBee.
- SL (Serial Number Low) : Bits de poids faible (32 bits) du numéro de série du module XBee
- DH (Destination Address High) : Bits de poids fort du numéro de série du module XBee avec lequel vous désirez "converser". Mettre 0 pour répondre au coordinateur du réseau.
- DL (Destination Address Low) : Bits de poids faible du numéro de série du module XBee avec lequel vous désirez "converser". Mettre 0 pour répondre au coordinateur du réseau.
- BD (Baud Rate) : Vitesse de transmission en bit/s.
- RO (Packetisation Timeout) : Nombre de caractères tamponnés dans le XBee avant de lancer une transmission.

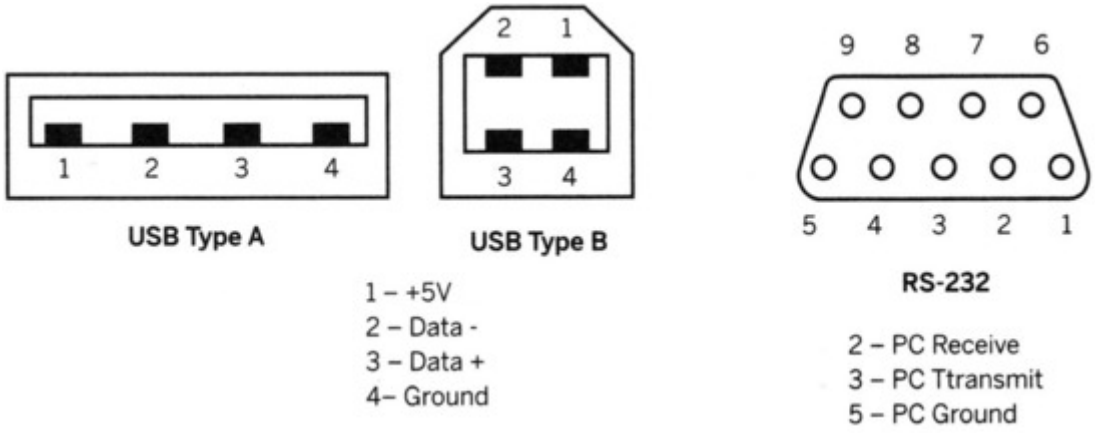
2. Notions de réseaux

2.1. Communication série

Pour transmettre des données, il faut :

- coder les données (émetteur) pour qu'il y ait le moins de pertes possibles ;
- les acheminer via un support physique ;
- les décoder (récepteur) suivant les mêmes règles.

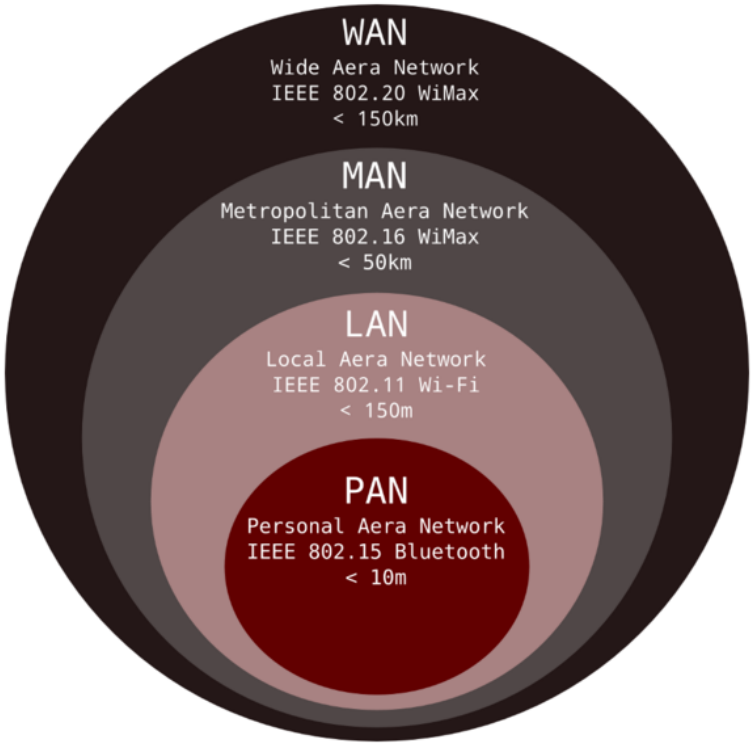
Au niveau physique, il s'agit surtout de l'envoi en série d'états électriques binaires (0 ou +5V par exemple). Le signal numérique est converti en signal analogique par des modems et transporté sur des supports filaires à base de cuivre ou de fibre optique, ou bien à travers le milieu aérien pour les transmissions non filaires. La transmission numérique des données est un ensemble de techniques fascinantes, qui consiste à trouver la meilleure solution pour transmettre les niveaux électriques représentant les bits.



2.2. Réseaux sans fils

Le standard IEEE[1] 802.15.4 décrit les règles et fonctionnalités sur lequel se base le ZigBee mais pas uniquement. Il fait partie d'un ensemble plus vaste, dont la racine est le groupe de travail 802.15 et encore plus en amont le groupe 802 qui spécifie les standards des réseaux personnels sans fil (WPAN).

Quand on aborde les réseaux sans fil, on est confronté au paramètre de portée, c'est-à-dire jusqu'à quelle distance l'information peut-elle être transportée en bonne état. Des catégories de réseau ont ainsi été créées pour différencier les zones géographiques : PAN, LAN, MAN, WAN. Cela ne concerne pas uniquement les réseaux sans fils puisqu'un réseau Ethernet, très commun dans les entreprises ou les associations, peut être un PAN ou un LAN.



Pour la transmission de données dans le milieu aérien, plusieurs options sont possibles. On utilise souvent des ondes électromagnétiques dans le domaine radio utilisant des fréquences porteuses

1 'Institute of Electrical and Electronics Engineers

réservées selon les pays.

FM 433 / 868 MHz
Toute la gamme
Radiometrix

AM 433 / 868 MHz
Modules
Telecontrolli

ZigBee®
Jennic
Firmtech

Bluetooth®
Free2move
Firmtech

Modules WLAN
Version boîtiers
ou modules OEM

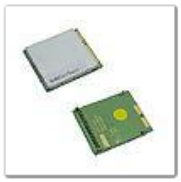
Modems Radio
Longue portée
868 MHz

Modules 2,4 Ghz
Transceivers
et Modems

FM 169 MHz
Toute la gamme
Radiometrix

Modules
GSM/GPRS
Modules Telit
Modules Teltonika

Modules divers
Circuits codeurs
et décodeurs



Transmission
Vidéo
Bande 2,4 GHz
Bande 5,8 GHz

Antennes
169 / 433 / 868 MHz
2,4 Ghz / GSM ...

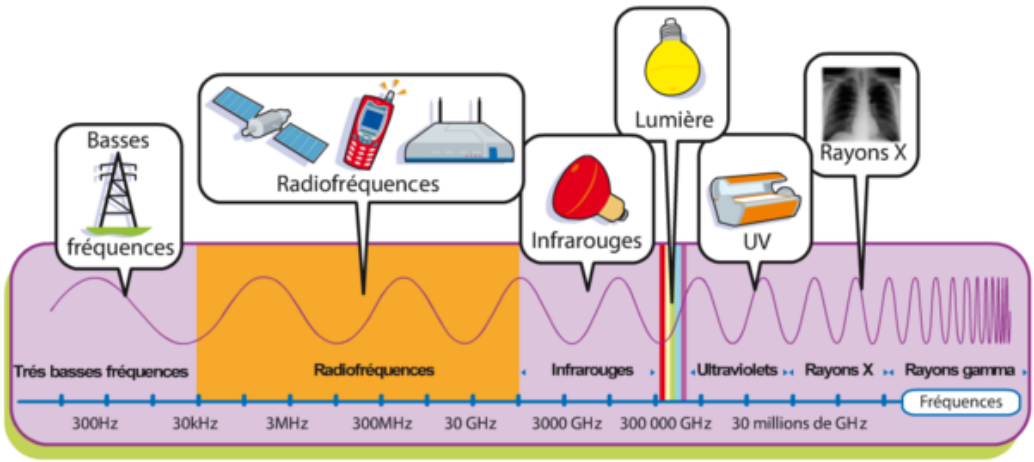
Hyperfréquence
Têtes HF
9,9 / 10,587 MHz

RFID
Lecteurs / Tags
Antennes

GPS
Récepteurs et
modules OEM

Téléecommandes
1 à 8 canaux
10 à 300 mètres

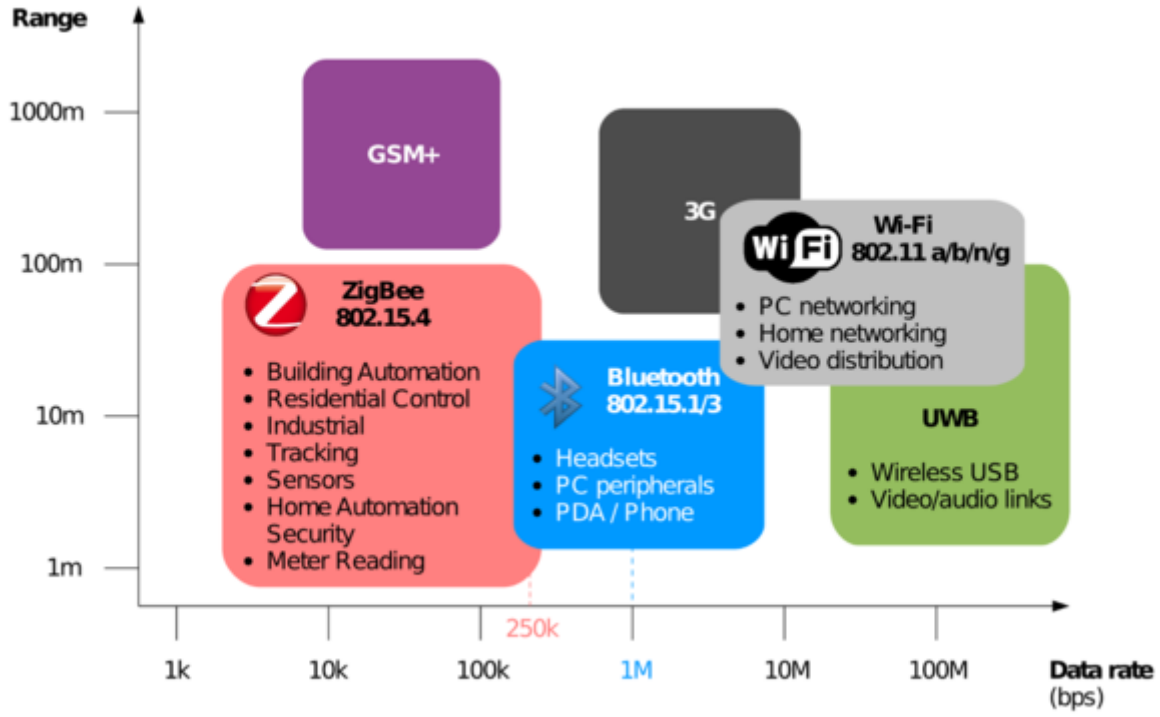
Ne sont répertoriés ici que les systèmes utilisant les radio-fréquences. Il existe aussi des transmissions par infra-rouges, qui sont directionnelles alors que les ondes radio sont omnidirectionnelles. Cela limite beaucoup leur utilisation. Les infra-rouges sont aussi des ondes électromagnétiques mais leur fréquence est beaucoup plus élevée. Elles n'utilisent donc pas d'antennes mais des émetteurs et récepteurs infra-rouges sous la forme de LEDs le plus souvent.



NB : les montages avec des dispositifs 433Mhz sont très économiques (~8€), et peuvent suffire dans

certains cas. La différence de taille avec une transmission Bluetooth, Wi-Fi ou ZigBee c'est que les données sont envoyées sans contrôles, c'est-à-dire que l'on n'est pas sûr qu'elles soient arrivées correctement du fait des interférences, des obstacles et de tout ce qui peut gêner les ondes. Si l'application n'est pas vitale, si quelques erreurs de temps en temps sont acceptables par le système alors cette solution peut être pertinente. En revanche, si les données sont critiques, reliées par exemple à un robot géant dans un lieu public ou à des appareils médicaux, cela n'est pas envisageable. On préférera dans ce cas des transmissions contrôlées et sécurisées par un protocole comme le Bluetooth, le Wi-Fi ou bien le ZigBee. Pour le 433Mhz, deux autres solutions sont tout de même possibles pour contourner le problème : vérifier les erreurs par programme ou le APC220 qui semble pouvoir fournir les vérifications demandées.

Le schéma ci-dessous permet de comparer le ZigBee, le Bluetooth et le Wi-Fi en termes de portée et de débits.

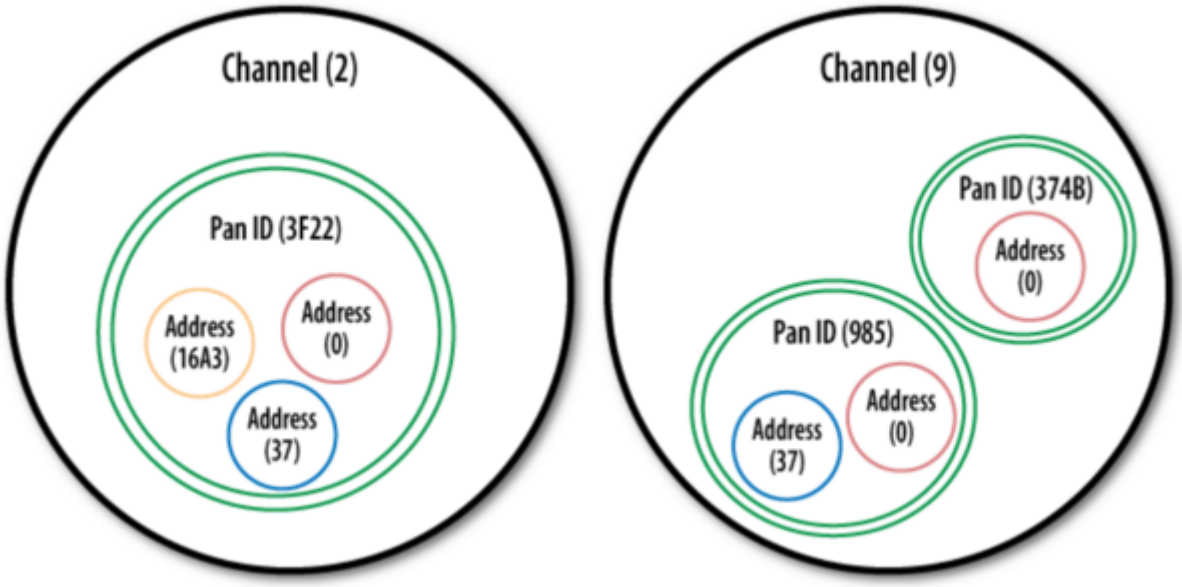


Cette vidéo présente les caractéristiques principales dans le choix des technologies sans fil.

3. Configuration

3.1. Adressage

Pour tout XBee, il faut impérativement définir l'adresse du réseau ATID, son adresse personnelle ATMY et si besoin, l'adresse de destination des paquets ATDL.



Le module dispose des registres suivant :

- "MY" pour donner l'adresse source sur 16 bits.
- "SH" et "SL" pour donner respectivement les 32 bits MSB et 32 bits LSB de l'adresse source sur 64 bits. Cette adresse est un n° de série unique donné en usine par le constructeur et se trouve dans les registres "SH" et "SL".
- "DH" et "DL" qui donnent respectivement les 32 bits MSB et 32 bits LSB de l'adresse du destinataire.

Il y a 2 types d'adressage possible. Par adresse courte sur 16 bits et par adresse longue sur 64 bits.

ADRESSE COURTE :

Il faut mettre la valeur de l'adresse sur 16 bits, inférieure à 0xFFFE dans le registre "MY" et l'adresse sur 16 bits dans "DL" avec les 32 bits de "DH" à "0".

Par défaut les modules sont programmés avec MY=00, donc en adresse courte et DH=00 et DL=00.

Exemple avec 2 modules :

Un module sera à l'adresse courte : 0001 et l'autre aura l'adresse : 0002.

	MODULE 1	**MODULE 2**
MY (16 bits)	00 01	00 02
DH (32 bits)	00 00 00 00	00 00 00 00
DL (32 bits)	00 00 00 02	00 00 00 01

ADRESSE LONGUE :

il faut mettre 0xFFFF ou 0xFFFE dans MY pour désactiver l'adressage court. L'adresse longue utilisée est la valeur des 64 bits du n° de série usine contenus dans les registres SH et SL. L'adresse de destination est alors les 64 bits contenus dans DH et DL.

MODE UNICAST :

Dans ce mode de fonctionnement, le module récepteur, envoi un "ACK" à celui qui a émis le paquet

de data. Si l'émetteur ne reçoit pas ce "ACK ", il renvoie jusqu'à 3 fois le paquet de data.

MODE BROADCAST :

Dans ce cas il n'y a pas de "ACK", envoyé par le récepteur, ni de répétition d'envoi par l'émetteur.

Tous les modules reçoivent et acceptent le paquet de data.

Pour envoyer des data sans tenir compte de l'adresse destinataire sur 16 ou 64 bits, il faut positionner l'adresse destinataire : DH =0x 00 00 00 00 et DL = 0x 00 00 FF FF.

Quand on programme le module, les paramètres sont entrés en hexadécimal. Les zéros non significatifs peuvent être omis.

3.2. Commandes de configuration

Pour modifier ou lire les paramètres du module, on va dialoguer par des commandes "AT" à 9600 Baud.

Il faut tout d'abord passer dans le mode "commande" en envoyant 3 fois le caractère "+" soit 0x2B en héxa en moins de 1 seconde. On doit respecter un temps de garde (de 1 seconde) avant et après l'envoi de ces 3 caractères. Le module répond par "OK" + "CR" (Carriage Return, soit 0x0D).

Le caractère "+" et le temps de garde sont modifiables par une commandes AT.

3.2.1. Commandes AT

Dans les télécommunications, l'ensemble de commandes Hayes est un langage de commandes spécifiques développé pour le modem Hayes en 1981. Les commandes sont une série de mots courts qui permettent de contrôler le modem avec un langage simple : composer un numéro de téléphone, connaître l'état de la ligne, régler le volume sonore, etc. Ce jeu de commandes s'est ensuite retrouvé dans tous les modems produits.

Elle est constituée des 2 caractères ASCII : "A" et " T" suivis de 2 caractères spécifiques à la commande, puis suit ou pas le caractère "Espace" et enfin suit un paramètre optionnel. On termine la commande par un "CR". Le module répond par "OK" suivi d'un "CR". Pour lire un paramètre, il suffira de laisser le champ paramètre en blanc. C'est le module qui renvoi alors la valeur de son paramètre.

"AT" + "ASCII commande" + "Espace" (option) + Paramètre (option) + "CR"

Si aucune commande AT n'est parvenue au module après son passage en mode commande pendant un temps de TIME OUT de 10 secondes (paramétrable par commande AT), le module retourne en mode IDLE.

Pour quitter le mode commande avant les 10 secondes du Time OUT, il faut envoyer la commande AT suivante : ATCN et le module répond alors par "OK"

Exemple :

ATDL 1F Cette commande fixe la valeur du registre DL à 0x1F. Le module répond par

	"OK".
ATDL	Le module renvoi 0x1F valeur dans DL.

On peut envoyer plusieurs commandes à la suite.

Exemple :

ATDL 1F,WR,CN	Cette commande fixe la valeur du registre DL à 0x1F. puis sauve les paramètres dans la mémoire EE PROM et fait sortir le module du mode AT. Le module répond par "OK","OK","OK".

Remarques :

- A la mise sous tension du Xbee, il faut que RTS=1 , sinon il n'est pas disponible pendant environ 10 secondes.
- Pour flasher le module avec un nouveau Firmware, il faut que DTR = 0 ou bien le câbler sur la RS232, afin que le logiciel X-CTU de MaxStream le gère lui même pour le flash.

  La broche DTR peut rester en l'air dans les autres cas d'utilisation (terminal, commande AT).
- Attention de ne pas avoir d'autres modules Xbee sous tension pendant le Flash, car ils risqueraient de répondre et de perturber la programmation du module.

3.2.2. Principales commandes AT

ATCN :	Pour quitter le mode commande.
ATCT + paramètre (0xFFFF):	Modifie ou lit le Time Out qui fait repasser le module en mode IDLE si aucune commande AT ne parvient. Le paramètre est le nbre de 100 ms. Par défaut il y a 0x64 soit 100ms x 100 = 10 sec.
ATGT + paramètre (0xFFFF):	Modifie ou lit le temps de garde. Le paramètre est le nbre de 1 ms. Par défaut il y a 0x3E8 soit 1ms x 1000 = 1 sec.
ATCC + paramètre (0xFF):	Modifie ou lit le caractère ASCII utilisé pour passer en mode commande. Par défaut on a 0x2B soit"+".
ATWR :	Sauve les paramètres dans la mémoire non volatile. Il faut impérativement attendre la réponse "OK" du module avant de lui envoyer une nouvelle commande.
ATCH + paramètre (0x0C à 0x17) :	Modifie ou lit le canal utilisé dans la bande 2,4 GHz. Par défaut il y a 0x0C.
ATDH + paramètre (0xFFFFFFFF) :	Modifie ou lit les 32 bits MSB de l'adressage destinataire. Par défaut il y a 0x00000000.
ATDL + paramètre (0xFFFFFFFF) :	Modifie ou lit les 32 bits LSB de l'adressage destinataire. Par défaut il y a 0x00000000.
ATMY + paramètre (0xFFFF) :	Modifie ou lit les 16 bits de l'adressage source. Par défaut il y a 0x0000.
ATSH :	Lit les 32 bits MSB du n° de série du module.
ATSL :	Lit les 32 bits LSB du n° de série du module.
ATNI + paramètre (20 octets	Sauve une chaîne de 20 caractères max pour l'identification du

ASCII) : réseau : NI. Le caractère "espace" met fin à la commande.

ATND : Cherche et donne les modules trouvés. Pour chacun o n obtient: MY + SH + SL + DB + NI. La commande se termine au bout de 2,5 seconde s et le module renvoie un "CR".

On peut faire suivre la commande d'un paramètre constitué des 20 caractères du NI d'un module. Dans ce cas on obtient en répons e uniquement les paramètres de ce module.

ATPL + paramètre (0 à 4) : Modifie ou lit la puissance de sortie du module. Par défaut il y a 4 soit la puissance max de 60 mW.

0	10 dBm soit 10 mW
1	12 dBm soit 16 mW
2	14 dBm soit 25 mW
3	16 dBm soit 40 mW
4	18 dBm soit 60 mW

ATBD + paramètre (0 à 7) : Modifie ou lit la vitesse en Baud de la liaison RS232. Par défaut on a 3 soit 9600 bauds.

0	1200 Bauds
1	2400 Bauds
2	4800 Bauds
3	9600 Bauds
4	19200 Bauds
5	38400 Bauds
6	57600 Bauds
7	115200 Bauds

ATID + paramètre (0xFFFF) : Modifie ou lit l'adresse du Pan ID. Il faut que cette valeur soit la même pour que les modules puissent communiquer entre eux.

ATRE Restaure les paramètres par défaut du module. Cette commande ne réinitialise pas le champ ID

ATNT + paramètre (0xFC) : Défini ou lit le temps qu’acceptera le module pour découvrir d’autre nœud du réseau lorsque ND est activé.

Temps = paramètre x 100 ms