Protocole Zigbee

Table des matières

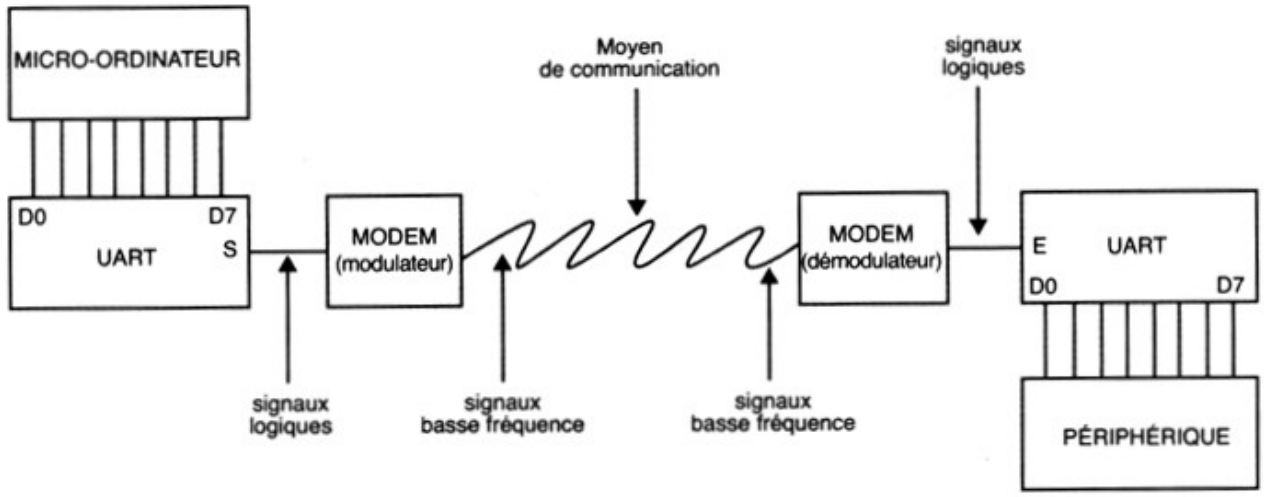
Lorsque l'on souhaite pouvoir communiquer en temps réel avec une application alors qu'aucune liaison filaire ne peut être établie, on peut faire appel à une liaison radio. Pour cela, il existe au moins deux approches distinctes, celle consistant à recourir à un réseau sans fil (WiFi) et celle constituant à utiliser une liaison radio plus spécifique (au moyen par exemple de module Xbee).

Pour transmettre des données numériques sur une grande distance, que ce soit au moyen d'une liaison filaire ou sans fil, on a pas trouvé mieux aujourd'hui que le modem. Les modems actuels sont plus performants que les anciens modems (1998 : standard V90 avec une vitesse ne dépassant pas les 56 kbit/s en aval et 33,6 kbit/s en amont) grâce notamment à des techniques plus élaborées comme le QPSK (Quadrature Phase Shift Keying) par exemple.

1. Les modems

Un modem qui est l'acronyme de modulateur-démodulateur a pour fonction première de transformer les signaux numériques en signaux analogiques.

Comme schématisé sur la figure page suivante, le modem s'intercale au sein d'une liaison numérique série lorsque celle-ci doit parcourir de grandes distances ou utiliser un support de transmission autre qu'un simple fil.



Le modem s'intercale au sein d'une liaison série

Si les signaux numériques ne peuvent voyager sur de longues distances sans subir des déformations qui les rendent inutilisables, il n'en est pas de même des signaux analogiques qui peuvent tout à la fois voyager loin mais aussi voyager sur de très nombreux supports physiques : fils bien sûr mais aussi liaison radio, faisceaux infrarouges, fibres optiques, etc.

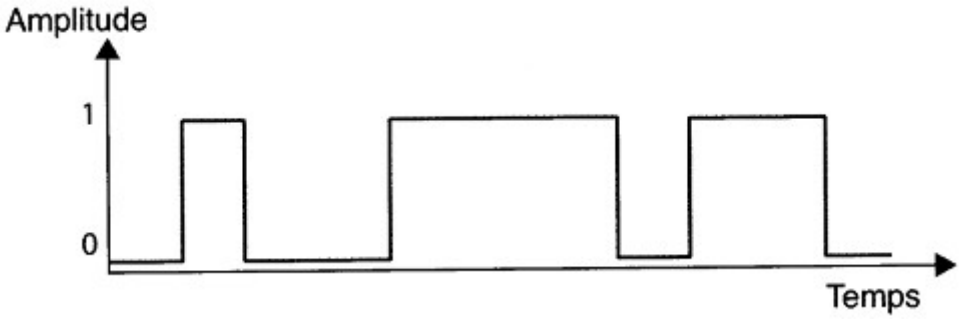
2. Principe de la modulation ASK

Le modem le plus simple, que l'on rencontre encore aujourd'hui dans nombre de modules de liaison radio aux fréquences autorisées de 433 MHz et 868 MHz, utilisé par exemple pour télécommander des alarmes, des portails ou des portes de garage électrique ou bien encore des volets roulants, est le modem ASK[1]. C'est-à-dire modulation par variation d'amplitude.

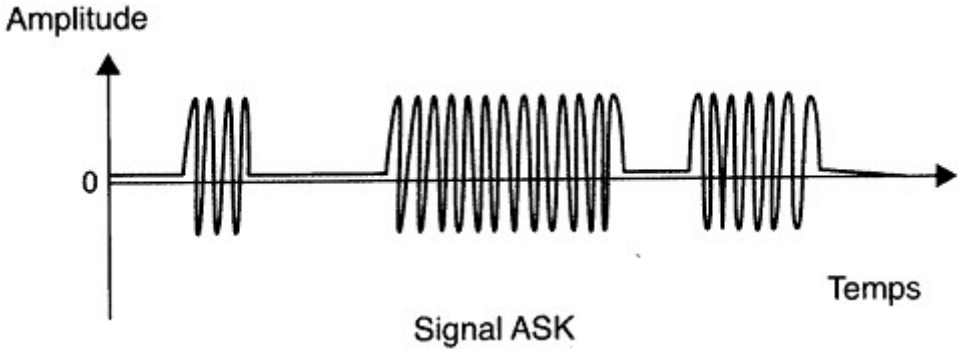
Comme le montre la figure ci-dessous, son principe est fort simple puisqu'il consiste à représenter un niveau zéro logique par une absence de signal et un niveau un logique par un signal sinusoïdal à une fréquence qui dépend de la vocation du modem.

Généralement, ce signal est à fréquence relativement basse, de quelques kHz à quelques dizaines de kHz afin de pouvoir voyager sur de nombreux supports.

1 Amplitude Shift Keying



Données à transmettre



Principe de la modulation ASK

Le modem ASK présente cependant quelques inconvénients liés au bruit. Le bruit peut se superposer au signal transmis et peut donc perturber la réception des niveaux zéros logiques, risquant alors d'être confondus avec des niveaux un si ce dernier atteint une amplitude trop importante.

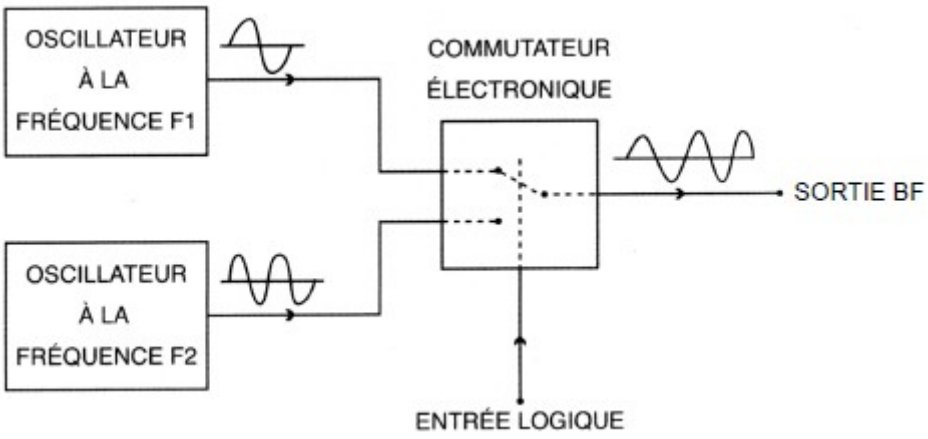
3. Principe de la modulation FSK

Pour des transmissions plus fiables, on préfère généralement le modem FSK[2] qui signifie modulation par variation de fréquence.

Comme le montre la figure ci-dessous, un tel modem traduit un zéro logique par un signal à une fréquence F1 et un un logique par un signal à une fréquence F2.

Il est alors beaucoup plus difficile de perturber le signal émis par un tel modem avec des bruits car, contrairement au modem ASK, il n'existe plus de phases de silences pendant la transmission qui se fait à niveau constant.

2 Frequency Shift Keying



Principe de la modulation FSK

Ces modems se rencontrent aujourd'hui sur des modules similaires à ceux évoqués précédemment pour la modulation ASK, mais lorsque l'on souhaite une télécommande d'une grande fiabilité, ils sont vendus généralement à un prix un peu plus élevé même si, techniquement parlant, cela ne se justifie pas vraiment…

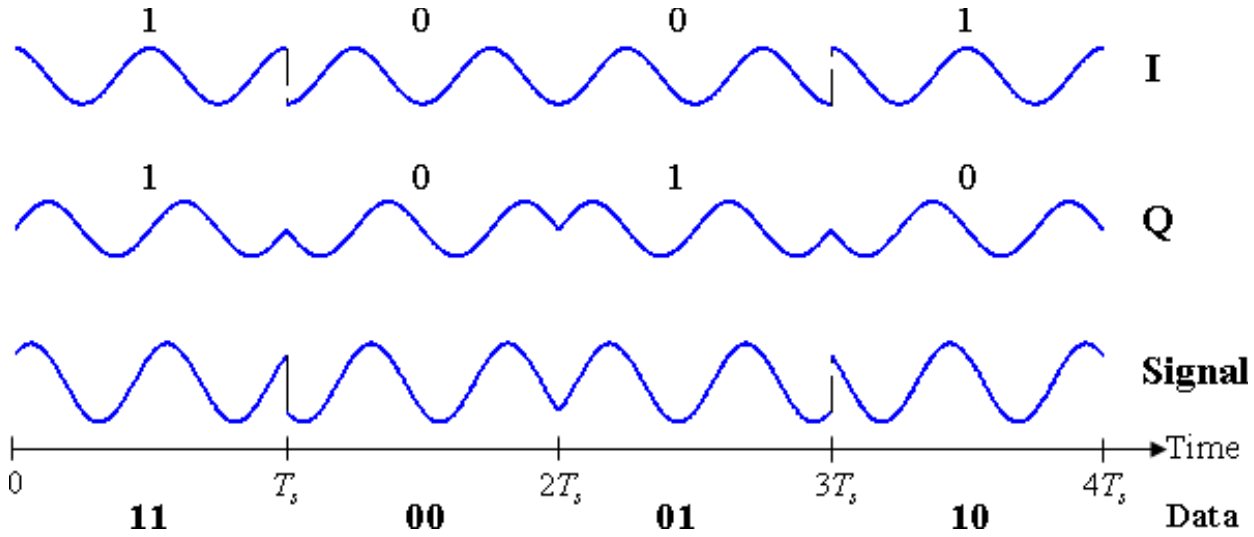
Pour efficaces qu'elles soient, ces deux techniques présentent cependant l'inconvénient d'être limitées en termes de vitesse maximum de transmission des données ce qui est assez facile à comprendre.

Considérons par exemple le modèle FSK. Si l'on souhaite que le démodulateur, c'est-à-dire la partie du modem qui traduit les signaux analogiques en signaux logiques, puisse fonctionner correctement, il faut qu'il puisse mesurer la fréquence de chacun des deux signaux transmis, pour chaque niveau logique, zéro ou un et donc qu'il puisse disposer d'au moins une période complète du signal analogique. La durée d'un bit ne peut donc en aucun cas être inférieure à la durée d'une période du signal modulant. En pratique, pour assurer un fonctionnement correct, on préfère prendre un facteur deux et disposer ainsi de deux périodes du signal analogique par bit du signal numérique. Ainsi, un signal basse fréquence de 1 200 Hz par exemple, ne peut pas véhiculer d'information numérique plus rapide que 600 bits par seconde environ.

Pour aller vite, il faut donc nécessairement augmenter la fréquence des signaux analogiques transmis ce qui pose rapidement un problème car, plus leur fréquence est élevée, plus leur transmission est difficile pour diverses raisons telles que, par exemple, l'influence des capacités parasites en liaison filaire ou l'augmentation de la fréquence porteuse nécessaire en liaison radio.

4. Principe de la modulation QPSK

D'autres systèmes ont donc été imaginés, dont la modulation de type QPSK[3] utilisée sur les modules Xbee. Cette modulation fonctionne par rotation de phase d'un quart de période des signaux transmis, selon le principe ci-dessous.



Principe de la modulation QPSK

On constate sur la figure, que ce type de modulation ne code plus un mais deux bits simultanément et permet donc, en théorie, de doubler le débit permis pour une modulation FSK classique, au prix il est vrai de modulateur et de démodulateur plus délicats à réaliser ; mais des circuits intégrés spécialisés existent aujourd'hui pour ce faire.

5. Les modules Xbee

Proposés depuis quelques années par la société Digi International, les modules Xbee sont des modems radio très élaborés, fonctionnant dans ce que l'on appelle aujourd'hui la bande ISM[4], c'est-à-dire sur une fréquence de 2,4 Ghz.

Les modules Xbee vont au-delà du simple modem puisqu'ils permettent de constituer de véritables réseaux sans fil et supportent de ce fait la notion d'adressage.

Une norme concerne d'ailleurs le protocole utilisé sous la référence IEEE 802.15.4.

3 Quarter Period Shift Keying
4 Industrie Science et Médical

Quelques modules Xbee

Ces modules peuvent être utilisés avec un ordinateur ou une carte micro-contrôlée mais ils peuvent aussi fonctionner seuls. Ils disposent de six entrées analogiques et de huit entrées numériques dont ils peuvent transmettre l'état tout seul si on les a préalablement configurés correctement.

Ils existent deux gammes de modules, la gamme Xbee « normale » et la gamme Xbee « pro ».

Les modules peuvent fonctionner dans deux modes principaux distincts :

- le mode transparent qui permet le remplacement immédiat de n'importe quelle liaison série asynchrone filaire par une liaison radio sans aucune manipulation particulière au niveau des modules Xbee, ce mode peut supporter ou non, au gré de l'utilisateur, la programmation d'un certain nombre de fonctions du modem au moyen de commande dites commandes AT.
- le mode API[5] qui permet d'accéder aux possibilités plus fines de mise en réseau des modules mais ne se justifie vraiment que lorsque l'on veut gérer tout un groupe de modules avec des possibilités de diffusion multiple, d'adressage, etc.

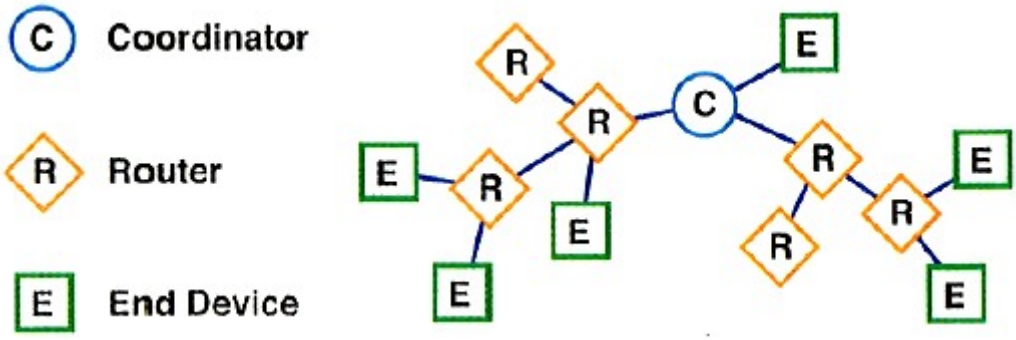
Quel que soit le mode utilisé, les modules Xbee sont capables de transmettre les données jusqu'à une vitesse maximum de 250 kbits/s et la transmission peut être sécurisée si on le souhaite au moyen d'un algorithme de cryptage de type AES[6] avec une clé sur 128 bits.

Les modules Xbee (série 1) ont une puissance haute fréquence de 1 mW, ce qui leur confère une portée moyenne de 30 m en intérieur et de 100 m en extérieur, tandis que les modules Xbee pro voient cette puissance portée à 60 mW (100 m pour l'intérieur et jusqu'à 1 500 m pour l'extérieur). Ces modules s'alimentent sous une tension pouvant varier de 2,8 à 3,4 V.

5.1. Le réseau Zigbee

D'après l'exemple de la figure ci-dessous, il existe trois types de périphériques dans le réseau ZigBee : le coordinateur, le routeur et les « End-Devices ».

5 Application Program Interface
6 Advanced Encryption Standard



5.2. Fonction « sleep »

Seuls les « End Devices » peuvent se mettre en sommeil dans le réseau ZigBee.

5.3. Adressage

L'adressage se fait sur deux couches.

MAC sur 64 bits et adresse « réseau » sur 16 bits.

5.4. Sécurité

Le cryptage utilisé est AES. Le réseau peut également être verrouillé pour empêcher d'autres périphériques de s'y connecter.

5.5. Communications série

Le module Xbee dispose d'un port série asynchrone. À l'aide de ce port, le module peut communiquer avec n'importe quel système disposant d'un UART compatible avec ses niveaux de tension (3,3 V).

Si vous souhaitez connecter un module Xbee à un ordinateur, un convertisseur de signaux RS232 ou USB doit être utilisé.

Les données entrant dans le module Xbee doivent prendre la forme d'un signal série asynchrone (le signal, au repos est au niveau haut lorsqu'aucune donnée n'est transmise).

Chaque octet de donnée est formée par un bit de départ, huit bits de données (LSB[7] en premier) et un bit de stop. L'UART assurera toutes les tâches comme le timing et le contrôle de la parité. Par défaut le module Xbee fonctionne en mode transparent.

5.6. Adressage des modules

Il est souvent nécessaire de configurer les modules Xbee. Pour cela, il convient de passer en mode « commande », de leur envoyer des ordres de configuration, puis de procéder à l'écriture de cette suite de paramètres dans leur mémoire.

Il existe deux moyens pour effectuer cette opération : soit utiliser un logiciel émulateur de terminal tel l'hyperterminal de Windows, soit utiliser le logiciel dédié appelé X-CTU.

Ce dernier est fourni gratuitement par le fabricant des modules, il permet de lire et de configurer tous les modèles de Xbee.

7 Less Significant Bit

Chacun des paquets de données envoyés par RF[8] contient une adresse source et une adresse de destination dans son en-tête. Le module Xbee se conforme à la spécification 802.15.4 et supporte aussi bien l'adressage court sur 16 bits que l'adressage long sur 64 bits.

Une adresse unique est assignée à chaque module lors de la fabrication et peut être lue aux moyens des commandes SL (Serial number Low) et SH (Serial number High).

Un module utilisera son adresse unique sur 64 bits si la valeur de son adresse source sur 16 bits est configurée à 0xFFFF ou 0xFFFE.

Pour envoyer un paquet de données à un module, en utilisant son adresse sur 64 bits, il suffit de configurer l'adresse de destination du module émetteur (DL + DH, adresse basse + adresse haute) avec l'adresse source du module récepteur (SL + SH). Pour envoyer un paquet de données à un module en utilisant cette fois un adressage court sur 16 bits, il convient de paramétrer l'adresse de destination (DL, adresse basse) du module émetteur avec la valeur du paramètre MY (sur X-CTU) du destinataire et de configurer l'adresse haute (DH) à 0.

Le mode unicast est le mode dans lequel le module Xbee opère par défaut. C'est le seul mode ou plusieurs tentatives d'envois peuvent avoir lieu. Lors de la réception d'un paquet de données, le module récepteur envoie un accusé de réception (Acknowledge) au module émetteur. Si le module émetteur ne reçoit pas cet accusé, il réitère cet envoie jusqu'à trois fois, ou jusqu'à ce qu'il reçoive l'accusé de réception.

Adresse courte sur 16 bits

Dans le mode unicast, les modules peuvent être configurés avec une adresse courte sur 16 bits ou MY sera inférieur à 0xFFFE.

En configurant le paramètre DH à 0, l'adressage se fera sur 16 bits.

Pour deux modules communicant, l'adresse de destination du module émetteur devra être égale au paramètre MY du module récepteur.

Adresse longue sur 64 bits

Lorsqu'un périphérique de fin « End device » est associé à un périphérique coordinateur, son paramètre MY est configuré à 0xFFFE afin de passer en adressage sur 64 bits.

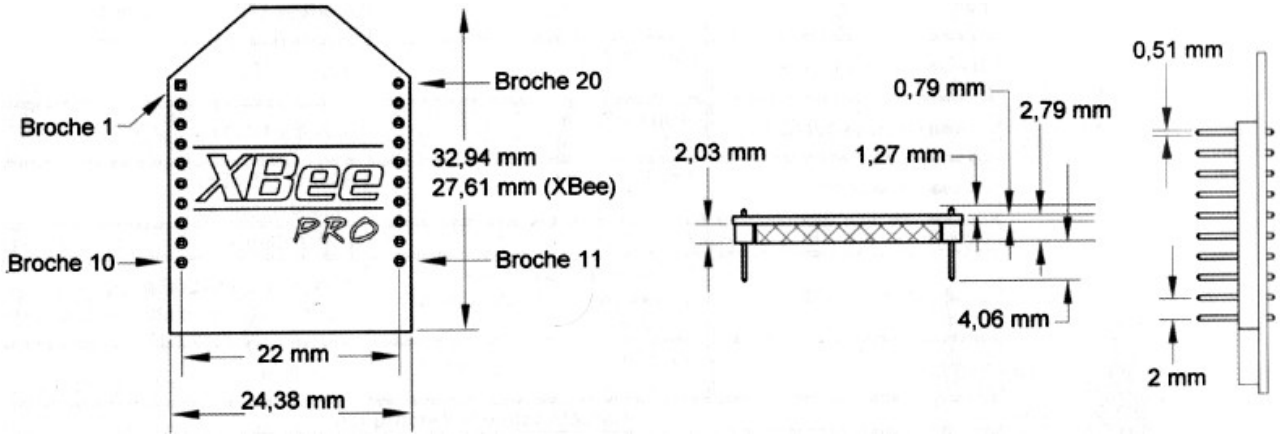
L'adresse sur 64 bits du module est stockée comme paramètre SL et SH. Afin d'envoyer un paquet de données à un module choisi, l'adresse de destination (DL + DH) d'un des modules doit correspondre à l'adresse source de l'autre (SL + SH).

Le mode broadcast est le mode dans lequel chaque module Xbee accepte le paquet de données reçu qui contient une adresse de broadcast. Configurer dans ce mode, les modules récepteurs n'envoient pas d'accusé réception et les modules émetteurs ne procèdent pas à une répétition des envois.

Pour envoyer un paquet de données à tous les modules, indépendamment d'un adressage 16 bits ou 64 bits, les adresses de destination de tous les modules devront être configurées de la manière suivante : DL = 0x0000FFFF et DH = 0x00000000.

8 Radio Frequency

5.7. Dimensions et brochage du Xbee



Broche	Nom	Direction	Fonction(s) de la broche
1	VCC	-	Entrée alimentation
2	DOUT	Sortie	Sortie données UART
3	DIN / CONFIG/	Entrée	Entrée données UART
4	CD / DOUT_EN / DO8	Sortie	Carrier detect / TX enable / sortie numérique 8
5	RESET/	Entrée	Reset du module (impulsion minimum de 200ns)
6	PWM0 / RSSI	Sortie	Sortie PWM0 / indicateur réception du signal RF
7	PWM1	Sortie	Sortie PWM1
8	(réservé)	-	Ne pas connecter
9	DTR / SLEEP-RQ / DI8	Entrée	Ligne de contrôle du mode Sleep / Entrée numérique 8
10	GND	-	Masse du module
11	AD4 / DIO4	Entrée/sortie	Entrée analogique 4 / entrée/sortie numérique 4
12	DIO7 / CTS/	Entrée/sortie	Contrôle du flux CTS/ / entrée/sortie numérique 7
13	ON / SLEEP	Sortie	Indicateur de statut du module
14	VREF	Entrée	Tension de référence pour les entrées analogiques
15	AD5 / DIO5 / Associate	Entrée/sortie	Entrée analogique 5 / entrée/sortie numérique 5 / indicateur d'association avec un autre module
16	AD6 / DIO6 / RTS/	Entrée/sortie	Entrée analogique 6 / entrée/sortie numérique 6 / Contrôle du flux RTS/
17	AD3 / DIO3	Entrée/sortie	Entrée analogique 3 / entrée/sortie numérique 3
18	AD2/ DIO2	Entrée/sortie	Entrée analogique 2 / entrée/sortie numérique 2
19	AD1 / DIO1	Entrée/sortie	Entrée analogique 1 / entrée/sortie numérique 1
20	AD0 / DIO0	Entrée/sortie	Entrée analogique 0 / entrée/sortie numérique 0

5.8. Caractéristiques du Xbee

Fonctions	**Module XBee série 1** Module XBee série 2	**Module XBee-Pro série 1**
Transmissions en intérieur	Jusqu'à 30 m Jusqu'à 40 m (série 2)	Jusqu'à 100 m
Transmission en extérieur	Jusqu'à 100 m Jusqu'à 120 m (série 2)	Jusqu'à 1500 m
Puissance de sortie	1 mW (0 dBm) 2 mW (+3dBm) (série 2)	60 mW (18 dBm) Ajustable par soft
Débit des données RF	250.000 bps	250.000 bps
Débit des données UART	1200 bps à 115.200 bps (autres débits non standards possibles)	1200 bps à 115.200 bps (autres débits non standards possibles)
Sensibilité	-92 dBm -98 dBm (série 2)	-100 dBm
Caractéristiques électriques		
Tension d'alimentation	**2,8 V à 3,4 V**	**2,8 V à 3,4 V**
Courant en émission	45 mA à 3,3 V 40 mA à 3,3 V (série 2)	10 dBm : 137 mA à 3,3 V 12 dBm : 155 mA à 3,3 V 14 dBm : 170 mA à 3,3 V 16 dBm : 188 mA à 3,3 V 18 dBm : 215 mA à 3,3 V
Courant en attente ou en réception	50 mA à 3,3 V 40 mA à 3,3 V (série 2)	55 mA à 3,3 V
Courant en mode «SLEEP»	< 10 µA 1 µA (série 2)	< 10 µA