L'INTERNET DES OBJETS

Olivier Hersent
David Boswarthick
Omar Elloumi

L'USINE NOUVELLE

L'INTERNET DES OBJETS

Les principaux protocoles M2M et leur évolution vers IP

avec BACnet, LonWorks, ModBus, KNX, Z-Wave, 6LoWPAN, ZigBee SE 2.0, ETSI M2M…

Traduit de l'anglais par **Hervé Soulard**

DUNOD

L'édition originale de cet ouvrage a été publiée par John Wiley & Sons sous le titre :

The Internet of Things ; Keys Applications and Protocols, 2nd edition

ISBN : 978-1-119-99435-0

Illustration de couverture : © 3 darcastudio
Montage de l'illustration de couverture : © Clément Pinçon

5 rue Laromiguière, 75005 Paris
www.dunod.com

ISBN 978-2-10-070552-8

Table des matières

B

Les protocoles M2M généralistes pour le bâtiment et le contrôle commande

C

Les protocoles M2M pour le comptage et la métrologie

D

La nouvelle génération : protocoles fondés sur IP

Avant-propos

L'innovation survient rarement là où on l'attend. De nombreux pays ont dépensé des sommes considérables pour améliorer la bande passante proposée aux internautes et aller vers le très haut débit, mais ont fini par découvrir qu'une personne ne regarde qu'un nombre limité de films en très haute définition à la fois. Sans oublier que le nombre d'êtres humains sur Terre est lui aussi limité.

Les prochaines années nous réservent d'autres surprises en raison de l'émergence de l'Internet des objets (IdO). Votre téléphone mobile et votre ordinateur sont déjà connectés à Internet, peut-être même le GPS de votre véhicule. Dans les années à venir, votre voiture, votre bureau, votre domicile et tous les appareils électroménagers qu'ils contiennent, y compris les compteurs d'électricité, de gaz et d'eau, l'éclairage public, le système d'arrosage automatique, les pèse-personne, les tensiomètres et même les murs seront connectés à l'IdO. Demain, les appareils électroménagers profiteront de nombreuses améliorations. Par exemple, le chauffage ne sera pas déclenché si la météo prévoit des températures clémentes mais sera déclenché plus tôt que prévu si le vent permet d'accéder à de l'énergie propre à ce moment, le jardin ne sera arrosé automatiquement que s'il ne pleut pas, une assistance routière sera apportée immédiatement en cas de besoin, etc. Ces améliorations faciliteront nos vies et permettront une utilisation plus efficace des ressources naturelles.

Pourquoi cette agitation se produit-elle maintenant ? Comme souvent, elle provient d'une combinaison de petites innovations qui, réunies, ont permis d'atteindre le seuil critique de déclenchement :

- Les technologies de **bus de terrain**, en utilisant des protocoles et normes parfois propriétaires (LON, KNX, DALI, CAN, ModBus, M-Bus, ZigBee, Z-Wave), ont exploré de nombreux domaines verticaux. Ceux-ci ont progressivement commencé à se chevaucher lorsque les cas d'utilisation se sont complexifiés, et des protocoles ont émergé pour faciliter l'interopérabilité (par exemple BACnet et oBix). Mais les déploiements de bus de terrain actuels continuent à exploiter des réseaux parallèles qui ne collaborent pas. La nécessité d'une technologie réseau commune qui pourrait travailler au-dessus de n'importe quelle couche physique, comme IP, est à présent une évidence.
- Malgré le besoin d'une technologie de mise en réseau indépendante des technologies de communication des bus de terrain, IP n'a pas été envisagé pour les

couches physiques à faible débit car la taille importante de ses en-têtes le rend inefficace dans les réseaux de bus de terrain généralement employés. Mais cela est bien fini : avec 6LoWPAN, non seulement la **technologie IP** a trouvé sa voie dans les réseaux à faible débit, mais, surprise, il s'agit de la version IPv6. Par ailleurs, sa mise en œuvre se fait avec un protocole de routage standard permettant de former un réseau IP maillé unique au-dessus de multiples couches physiques. Des technologies de bus de terrain de couche 2 différentes peuvent enfin collaborer et former des réseaux plus vastes.

- Les réseaux de bus de terrain locaux mettent aujourd'hui en place des **algorithmes** sophistiqués pour optimiser les systèmes CVC (chauffage, ventilation et climatisation) dans les bureaux et les habitations. Les exigences d'efficacité énergétique des nouveaux bâtiments ont créé un besoin d'algorithmes encore plus complexes, comme la régulation prédictive qui tient compte des prévisions météo ou le déplacement de charge qui optimise la part CO_2 de l'électricité. Dans de nombreux secteurs d'automatisation, les outils de pointe exigent que le bus de terrain local collabore avec des applications centralisées hébergées et des sources de données. La technologie qui permet cela a progressé par étapes : oBix a introduit le concept d'interface uniforme (REST) dans les réseaux de capteurs, ETSI M2M a ajouté la gestion de la sécurité, ainsi que des améliorations nécessaires pour les réseaux publics à grande échelle.
- Enfin, des **technologies radio** pervasives à faible débit, adaptées aux objets autonomes fonctionnant sur batterie et à très faible coût, sont apparues, permettant d'envisager un accès Internet partout, pour tout objet, dans les années qui viennent.

L'industrie manquait seulement d'un marché véritablement attrayant pour lancer les énormes efforts de recherche et de développement nécessaires à l'intégration de toutes ces technologies et à la mise en place d'un Internet des objets à toute épreuve.

Ce marché est venu du secteur de l'énergie :

- L'augmentation de la part des sources d'énergie renouvelables dans la production globale de l'électricité a augmenté le caractère aléatoire d'un système d'approvisionnement traditionnellement déterministe.
- En parallèle, l'introduction en masse des véhicules électriques et hybrides rechargeables rend la demande encore plus complexe. Ces véhicules sont des objets itinérants qui doivent être authentifiés auprès du réseau et qui nécessitent des protocoles de gestion de charge.

La règle actuelle des fournisseurs d'électricité, « la demande est imprévisible et notre expertise est d'adapter la production à la demande », est en passe de s'inverser, pour

devenir « la production est imprévisible et notre expertise est d'adapter la demande à la production ».

Avec un tel changement des règles du jeu, les atouts essentiels d'un fournisseur d'énergie seront non plus ses moyens de production mais son réseau de communication et son système d'information de nouvelle génération. Mais il lui reste encore à les construire intégralement, ce qui ouvre un énorme marché pour des technologies M2M robustes, adaptées à l'importance de l'enjeu et aux échelles considérées. La modification spectaculaire de la distribution de l'électricité préfigure une évolution plus générale de l'Internet vers l'Internet des objets, dans laquelle les applications réseau auront un impact plus important sur notre vie quotidienne, y compris sur les objets que nous manipulons et utilisons, dont un grand nombre deviendra connecté.

Cet ouvrage cible un public d'ingénieurs qui sont impliqués ou souhaitent s'impliquer dans une automatisation à grande échelle sur de nombreux sites, par exemple des projets de type *smart grid*, et qui doivent acquérir une vision globale de l'état de l'art des communications M2M.

Un grand nombre de ces projets impliqueront des interfaces avec des systèmes existants. Nous proposons une vue d'ensemble de nombreux bus de terrain et technologies d'automatisation largement déployés : BACnet, CAN, LON, M-Bus/wMBUS, ModBus, LON, KNX, ZigBee, Z-Wave, ainsi que les normes de comptage C.12 et DLMS/COSEM. Nous entrons également en détail dans deux couches physiques répandues, 802.15.4 et CPL, et nous présentons les technologies émergentes de communication à longue portée par radio à faible puissance d'émission : la technologie ultra-narrowband et la technologie à étalement de spectre LoRa™.

Cet ouvrage ne fera pas de vous un expert de toutes ces technologies mais vous permettra d'acquérir suffisamment d'informations pour comprendre précisément le fonctionnement, le domaine d'application et les possibilités de chacune. Les descriptions accélérées devraient vous permettre ensuite de découvrir plus facilement les détails par vous-même en naviguant dans les spécifications.

Le futur des protocoles de bus de terrain se trouve dans leur convergence au-dessus du protocole fédérateur de l'Internet IP. Nous décrivons 6LoWPAN et RPL, ainsi que le premier protocole d'automatisation conçu explicitement pour les réseaux 6LoWPAN : ZigBee SE 2.0. Nous faisons également une introduction à la norme ETSI M2M émergente. Elle représente l'élément manquant tant attendu par les fournisseurs de services qui souhaitent offrir une infrastructure M2M publique générale, partagée par toutes les applications.

Je voudrais remercier ici les nombreuses personnes qui ont aidé à documenter ou à rédiger cet ouvrage : Gilles Lefevre, inlassable relecteur et surtout rédacteur de spécifications, auquel je dois notamment le détail de toutes les spécifications

d'interfaces REST avec les bus terrain, Paul Bertrand, inventeur de la technologie de bus de terrain CPL WPC et concepteur du premier portage de 6LoWPAN sur CPL, pour avoir accepté d'écrire, vous l'aurez deviné, le chapitre sur les courants porteurs en ligne. Jean-Marc Ballot (Alcatel) pour les chapitres sur C.12 et DLMS, qui ont nécessité un important travail de documentation. Noe-Jean Caramelli, pour ses recherches sur les protocoles de sécurité adaptés au très bas débit. Philippe Magneron pour son support au sein de l'association KNX et avoir contribué à faire émerger l'interface REST présentée ici. Nicolas Sornin, Olivier Seller et François Sforza (Cicleo/Semtech) pour leur travail extraordinaire sur le bas débit radio, et notre travail commun sur l'optimisation d'une couche MAC pour ces réseaux. Nicolas Jordan pour son aide à décliner le concept de boutique d'application pour l'Internet des Objets, Jean-Baptiste Reich pour sa relecture des chapitres ETSI M2M et des tutoriaux vidéo… et toute l'équipe de mes collègues et complices de Netcentrex et aujourd'hui Actility, qui contribuent à accoucher à travers toutes les frustrations du monde réel nos rêves communs.

Malgré tous mes efforts, il est possible que cet ouvrage contienne encore quelques erreurs, mais elles auraient été beaucoup plus nombreuses sans l'aide des relecteurs experts : Cedric Chauvenet et Mathieu Pouillot pour 6LoWPAN/RPL et ZigBee, Bob Dolin, Jeff Lund, Larry Colton et Mark Ossel chez Echelon pour LON, Benoit Guennec et Baptiste Vial (Connected Object) pour Zwave notamment.

N'hésitez pas à m'indiquer les éventuelles erreurs résiduelles que vous pourriez découvrir afin que je puisse améliorer la prochaine édition (olivier.hersent@actility.com).

La collecte et la lecture de la documentation nécessaire à la rédaction de cet ouvrage m'ont permis de découvrir de nouveaux horizons et d'ouvrir de nouvelles perspectives. J'espère que vous apprécierez le lire autant que j'ai apprécié l'écrire.

Olivier Hersent

Tutoriels en ligne

En complément de cet ouvrage vous trouverez ci-dessous 10 tutoriels, **en anglais**, accessibles librement en ligne à l'aide de leur QR code. Que vous soyez développeur, ingénieur ou décideur ils vous aideront à découvrir l'univers M2M.

Video 1: What is ETSI M2M ?

In this video we will give you an introduction to ETSI M2M and why do people need it. It is targeted to audience who want a system level architecture. Most of these topics are further illustrated in details in the upcoming videos.

Video 2: Introducing Gateway-to-Cloud interface : mId

In this video we will install a new ETSI M2M gateway (the GSC function defined in ETSI TS 102 690 and TS 102 921), and then register it to an NSC in the cloud..

Video 3: Installing a new ETSI M2M gateway using open-source Cocoon & First interactions with ONG browser

This video covers the technical aspect of ETSI M2M on Cocoon, an ETSI M2M based NSC Platform.

Video 4: Connecting to the M2M Cloud

Video 4 will present the various REST resources used by ETSI M2M.

Video 5: Analysing ETSI M2M REST Resources

This video will tell you more about the major ETSI M2M REST resources and help you get a better understanding of these resources using a web browser.

Video 6: Understanding Cloud mechanisms & NSC function

This video focuses on the «cloud» function of ETSI M2M : the NSC. The main functionalities of the NSC are discussed in details:

Video 7: Understanding REST drivers for fieldbus protocols : the ETSI TR102966 interworking resources

If you are looking for a generic REST API for your next automation application, don't miss this video ! Most TR102966 drivers are available as open-source on the Cocoon project web site.

Video 8: A ZigBee 1.x primer

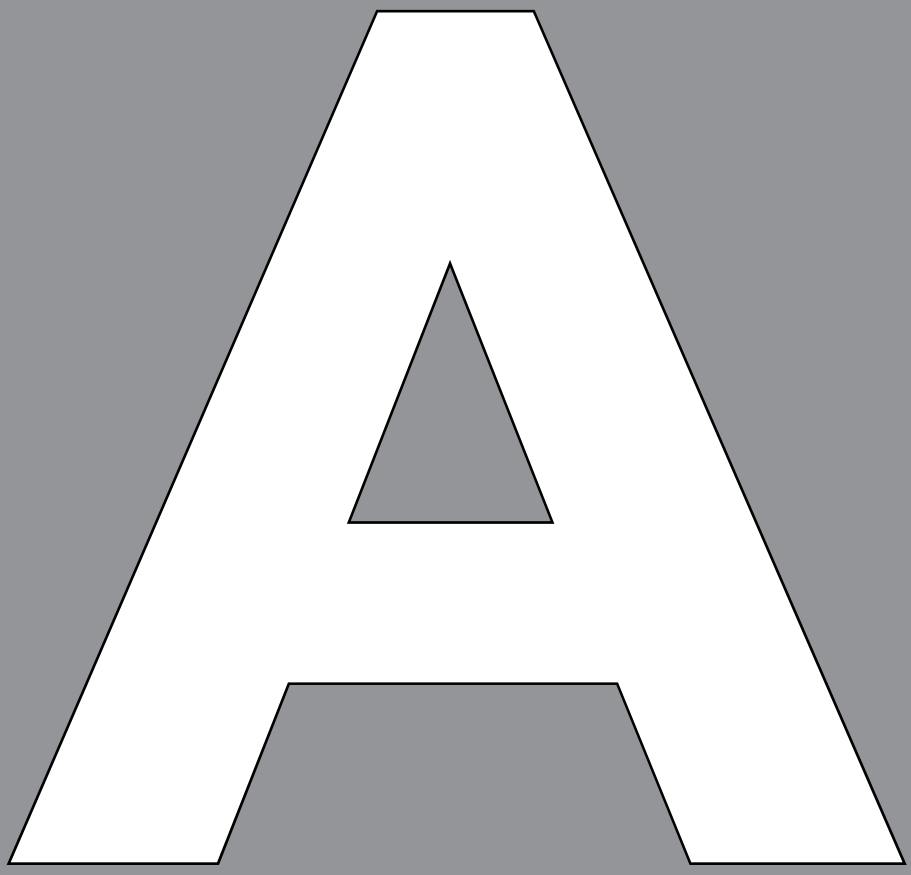
This is a crash course that focuses on the needs of a ZigBee network administrator or ZigBee application developper

Video 9: Cocoon ZigBee driver

This video enables M2M applications to discover the topology of a fieldbus network, or read sensor measurements without bothering about the specific protocol employed.

Video 10: Cocoon ZigBee driver configuration

This video is for the expert user.



LES COUCHES PHYSIQUES POUR RÉSEAUX M2M

1 IEEE 802.15.4

1.1 La famille de normes du comité IEEE 802

Le comité 802 de l'IEEE (*Institute of Electrical and Electronics Engineers*) définit les technologies de la couche physique et de la couche liaison de l'OSI. Cette dernière est elle-même constituée de deux couches secondaires :

- La sous-couche de contrôle d'accès au support (MAC, *Media Access Control*) se place directement au-dessus de la couche physique (PHY) et met en œuvre les méthodes d'accès au réseau, comme la méthode d'accès multiple avec écoute de la porteuse et détection des collisions (CSMA/CD, *Carrier Sense Multiple Access/Collision Detection*), employée par Ethernet, et la méthode d'accès multiple avec écoute de la porteuse et esquive des collisions (CSMA/CA, *Carrier Sense Multiple Access/Collision Avoidance*), employée par les protocoles sans fil de l'IEEE.
- La sous-couche de contrôle de la liaison logique (LLC, *Logical Link Control*), qui construit les trames de données envoyées sur le canal de communication au travers des couches MAC et PHY. L'IEEE 802.2 définit un format de trame indépendant des couches MAC et PHY sous-jacentes et présente aux couches supérieures une interface uniforme.

Depuis 1980, l'IEEE a défini de nombreuses normes MAC et PHY répandues (le tableau 1.1 illustre uniquement les normes sans fil), qui se fondent toutes sur la couche LLC du 802.2.

Le 802.15.4 a été défini par le groupe de travail 4/4b du comité IEEE 802.15 (*http://ieee802.org/15/pub/TG4b.html*). La norme a été initialement publiée en 2003 puis révisée en 2006 et 2011. Ces dernières versions améliorent les débits de données des couches physiques dans les bandes 868 et 900 MHz (jusqu'à 250 kbps, à la place des 20 et 40 kbps, respectivement). Vous pouvez les télécharger gratuitement à partir du site de l'IEEE à l'adresse *http://standards.ieee.org/getieee802/download/*.

Tableau 1.1 Les couches MAC définies par l'IEEE

Couche MAC	Utilisation	Bande
802.11	Wi-Fi	802.11, 802.11b, 802.11g, 802.11n : ISM 802.11a : U-NII
802.15.1	Bluetooth	ISM 2,4 GHz
802.15.4	ZigBee, 6LoWPAN	ISM 2,4 GHz dans le monde entier ISM 902–928 MHz aux USA 868,3 MHz dans les pays européens 802.15.4a : 3,1–10,6 GHz
802.16	Réseaux métropolitains sans fil (WMAN, *Wireless Metropolitan Access Network*) Technologie large bande mobile (BWA, *Broadband Wireless Access*), WiMax	802.16 : 10–66 GHz 802.16a : 2–11 GHz 802.16e : 2–11 GHz pour le fixe et 2–6 GHz pour le mobile

1.2 La couche physique

La conception de la norme 802.15.4 prend en compte les règles d'allocation des fréquences en vigueur aux États-Unis (FCC CFR 47), au Canada (GL 36), en Europe (ETSI EN 300 328-1, 328-2, 220-1) et au Japon (ARIB STD T66). Aux États-Unis, la gestion et l'allocation des bandes de fréquences sont sous la responsabilité de la Commission fédérale des communications (FCC, *Federal Communications Commission*). La FCC a alloué des fréquences pour les applications industrielles, scientifiques et médicales (ISM), qui peuvent être utilisées sans demande d'autorisation préalable lorsque la puissance d'émission est inférieure à 1 W. Par ailleurs, pour les applications à faible puissance, la FCC a réservé la bande U-NII (*Unlicensed National Information Infrastructure*). Le tableau 1.2 recense les fréquences et la puissance d'émission maximale pour chaque bande.

Tableau 1.2 Les bandes ISM et U-NII de la FCC

Bande FCC	Puissance d'émission maximale	Fréquences
Industrielle	< 1 W	902 MHz–928 MHz
Scientifique	< 1 W	2,4 GHz–2,48 GHz
Médicale	< 1 W	5,725 GHz–5,85 GHz
U-NII	< 40 mW	5,15 GHz–5,25 GHz
	< 200 mW	5,25 GHz–5,35 GHz
	< 800 mW	5,725 GHz–5,82 GHz

L'IEEE 802.15.4 peut employer :

- la bande ISM 2,4 GHz (bande S) dans le monde entier, avec un débit de données de 250 kbps (modulation O-QPSK) et 15 canaux (de 11 à 26) ;
- la bande ISM 902–928 MHz (bande I) aux États-Unis, avec un débit de données de 40 kbps (modulation BPSK), 250 kbps (modulation BPSK+O-QPSK ou ASK) ou 250 kbps (modulation ASK) et 10 canaux (de 1 à 10) ;
- la bande de fréquences 868–868,6 MHz en Europe, avec un débit de données de 20 kbps (modulation BPSK), 100 kbps (modulation BPSK+O-QPSK) ou 250 kbps (PSSS : modulation BPSK+ASK) et un seul canal (0 pour la modulation BPSK ou O-QPSK, et 1 pour la modulation ASK).

Dans la pratique, la plupart des mises en œuvre actuelles utilisent la bande de fréquences 2,4 GHz disponible dans le monde entier. Cela évolue actuellement notamment en Europe car les bandes sub-GHz se comportent mieux en habitat dense et constructions de pierre et la norme 802.15.4g a défini de nouveaux canaux sub-GHz rendant les déploiements possibles. Plus récemment, une nouvelle couche physique a été conçue pour la bande ultralarge (3,1 à 10,6 GHz).

Modulation O-QPSK à 2,4 GHz

Les données à transmettre sont découpées en bloc de 4 bits. Chacun de ces blocs est associé à un *symbole* parmi les seize définis. Le symbole est ensuite converti en une séquence de *chips* de 32 bits (étalement de spectre par une séquence pseudo-aléatoire définie pour chaque symbole par le 802.15.4). Les bits pairs sont transmis par modulation de la composante en phase (I) tandis que ceux impairs le sont par modulation de la composante en quadrature (Q), comme illustré à la figure 1.1. Chaque chip est modulé sous forme d'une impulsion semi-sinusoïdale. Le débit des chips émis est de 2 Mchip/s, ce qui correspond à un débit de symboles 32 fois plus lent et un débit de données utilisateur de 250 kbps. La somme des signaux I et Q est ensuite transposée sur la porteuse à 2,4 GHz.

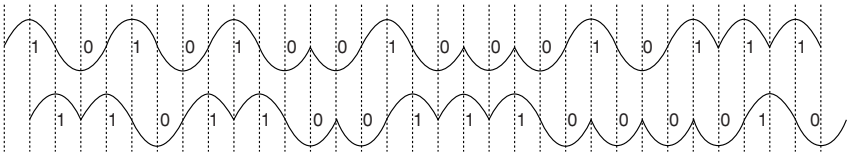


Figure 1.1 Les composantes I et Q de la modulation O-QPSK

Le 802.15.4 met en place un codage sur 32 bits pour faire référence à une bande de fréquences, une modulation et un canal précis. Les cinq premiers bits indiquent un numéro de page tandis que les 27 bits restants servent de numéro de canal dans la

page. Le tableau 1.3 précise les numéros de canaux et les fréquences centrales associés à une bande de fréquences, une modulation et une page.

Tableau 1.3 Bandes de fréquences, modulation et canaux du 802.15.4 :2003

Bande de fréquences	Modulation	Numéro de page	Numéro de canal et fréquence centrale
2,4 GHz	0-QPSK	0	11 : 2 405 MHz
			12 : 2 410 MHz
			13 : 2 415 MHz
			14 : 2 420 MHz
			15 : 2 425 MHz
			16 : 2 430 MHz
			17 : 2 435 MHz
			18 : 2 440 MHz
			19 : 2 445 MHz
			20 : 2 450 MHz
			21 : 2 455 MHz
			22 : 2 460 MHz
			23 : 2 465 MHz
			24 : 2 470 MHz
			25 : 2 475 MHz
			26 : 2 480MHz
915 MHz	BPSK	0	1 : 906 MHz
	BPSKASK	1	2 : 908 MHz
	BPSK+0-QPSK	2	3 : 910 MHz
			4 : 912 MHz
			5 : 914 MHz
			6 : 916 MHz
			7 : 918 MHz
			8 : 920 MHz
			9 : 922 MHz
			10 : 924 MHz
868 MHz	BPSK	0	0 : 868,3 MHz
	BPSK+ASK	1	1 : 868,3 MHz
	BPSK+0-QPSK	2	0 : 868,3 MHz

Interférences avec d'autres technologies

Puisque la bande scientifique (2,4–2,48 GHz) n'exige aucune autorisation préalable dans la plupart des pays, elle est employée dans de nombreuses normes de réseau sans fil, notamment le Wi-Fi (802.11, 802.11b, 802.11g, 802.11n), le 802.15.4 et d'autres appareils tels que les téléphones sans fil et les fours à micro-ondes.

Normes sans fil FHSS

La couche physique du 802.11 se fonde sur l'étalement de spectre par saut de fréquence (FHSS, *Frequency Hopping Spread Spectrum*) et la modulation par étalement de spectre direct. Le Bluetooth (802.15.1) emploie FHSS dans la bande ISM.

La technologie FHSS décompose la bande ISM en 79 canaux de 1 MHz (voir le tableau 1.4). La FCC impose à un émetteur de n'utiliser aucun canal pendant plus de 400 ms (temps de rétention) et d'essayer d'utiliser au moins 75 canaux (mais cela n'est pas toujours possible lorsque certains d'entre eux sont trop perturbés).

Tableau 1.4 Canaux FHSS définis par la FCC dans la bande S

Canal FHSS	Fréquence (GHz)
2	2,401–2,402
3	2,402–2,403
4	2,403–2,404
...	
80	2,479–2,480

Normes sans fil DSSS

Les normes 802.11b et 802.11g se servent uniquement de l'étalement de spectre à séquence directe (DSSS, *Direct Sequence Spread Spectrum*). Onze canaux DSSS ont été définis, chacun avec une largeur de bande de 16 MHz. Les fréquences centrales de canaux adjacents sont séparées de 5 MHz. Seuls trois canaux ne se chevauchent pas (indiqués en gras dans le tableau 1.5) : ils doivent être employés dans l'ordre afin de réduire les problèmes d'interférences dans des déploiements adjacents (trois canaux suffisent à un déploiement bidirectionnel, mais, dans une configuration tridimensionnelle, comme dans un bâtiment, un plus grand nombre de canaux est nécessaire).

Tableau 1.5 Canaux DSSS utilisés par le 802.11b

Canal DSSS	Fréquence (GHz)
1	**2,404–(2,412)–2,420**
2	2,409–(2,417)–2,425
3	2,414–(2,422)–2,430
4	2,419–(2,427)–2,435
5	2,424–(2,432)–2,440
6	**2,429–(2,437)–2,445**
7	2,434–(2,442)–2,450
8	2,439–(2,447)–2,455
9	2,444–(2,452)–2,460
10	2,449–(2,457)–2,465
11	**2,456–(2,462)–2,470**

Choix d'un canal de communication 802.15.4, détection d'énergie et informations de qualité de la liaison

Dans la pratique, la bande de fréquences 2,4 GHz est communément employée par les couches réseau et application situées au-dessus des couches MAC 802.15.4, notamment ZigBee et 6LoWPAN. La puissance d'émission peut être réglée entre 0,5 mW (spécifié par la norme 802.15.4) et 1 W (maximum de la bande ISM). Pour d'évidentes raisons, la puissance d'émission doit être réduite lorsque les liaisons impliquent des appareils fonctionnant sur batterie. Une puissance d'émission de 10 mW fournit une portée d'environ 300 m en extérieur (50 m en intérieur) pour des débits d'information de quelques dizaines de kbit/s.

Puisque le 802.15.4 ne met pas en œuvre le saut de fréquence, le choix du canal de communication est important. Les interférences avec les technologies FHSS ne sont que sporadiques car la source FHSS ne reste pas plus de 400 ms sur une fréquence donnée. Pour réduire les interférences avec les systèmes DSSS, comme un système Wi-Fi (802.11b/g) configuré pour fonctionner sur les trois canaux sans chevauchement 1, 6 et 11, il est généralement conseillé de laisser les applications 802.15.4 opérer sur les canaux 15, 20, 25 et 26 qui se trouvent entre ces trois canaux.

La couche physique du 802.15.4 propose une fonction de détection d'énergie (ED, *Energy Detection*) qui permet aux applications de demander une estimation du niveau d'énergie de chaque canal. En fonction des résultats, un coordinateur de réseau 802.15.4 est capable de sélectionner un canal de façon optimale.

Pour chaque paquet reçu, la couche physique du 802.15.4 fournit également des informations de qualité de la liaison (LQI, *Link Quality Information*) aux couches réseau et application (la méthode de calcul des LQI est propre à chaque fournisseur). En fonction de ces indications, du nombre de retransmissions et du nombre de paquets perdus, les émetteurs peuvent décider d'utiliser une puissance d'émission supérieure et certaines applications, comme ZigBee Pro, disposent de mécanismes pour changer dynamiquement de canal 802.15.4 lorsque celui sélectionné est trop encombré, mais ce basculement doit rester exceptionnel.

Envoi d'une trame de données

Le 802.15.4 exploite la méthode d'accès multiple avec écoute de la porteuse et esquive des collisions (CSMA/CA) : avant d'envoyer une trame, les couches supérieures demandent à la couche physique d'effectuer une évaluation de canal non occupé (CCA, *Clear Channel Assessment*). La signification exacte d'un canal non occupé est configurable : elle peut correspondre à un seuil d'énergie sur le canal quelle que soit la modulation (mode 1), à la détection d'une modulation 802.15.4 (mode 2) ou à une combinaison des deux (mode 3 : niveau d'énergie supérieur à un seuil et modulation 802.15.4).

Après une durée aléatoire conçue pour éviter toute synchronisation des émetteurs, l'appareil vérifie que le canal est toujours vide et transmet une trame de données. Elle est constituée d'un préambule de 30 à 40 bits, suivi d'un délimiteur de début de trame (SFD, *Start Frame Delimiter*) et d'un en-tête minimal de la couche physique indiquant uniquement la longueur de la trame sur 7 bits (voir la figure 1.2).

En-tête de synchronisation (SHR)		En-tête physique (PHR)		Unité de données du service physique
Préambule	SFD 111100101	Longueur de trame (7 bits)	1 bit (réservé)	0 à 127 octets

Figure 1.2 Trame de la couche physique du 802.15.4

1.3 La couche de contrôle d'accès au support

Le standard 802.15.4 fait la distinction entre la partie de la couche MAC responsable du transfert des données – la sous-couche MAC commune (MCPS, *MAC Common Part Sublayer*) – et la partie responsable de la gestion de la couche MAC elle-même – l'entité de gestion de la couche MAC (MLME, *MAC Layer Management Entity*).

La MLME comprend les paramètres de configuration et d'état de la couche MAC, comme l'adresse IEEE sur 64 bits et l'adresse courte du nœud sur 16 bits, le nombre de tentatives d'accès au réseau en cas de collision (en général quatre, mais cinq au maximum), la durée d'attente d'un accusé de réception (en général 54 unités de durée d'un symbole, mais 120 au maximum) ou le nombre de renvois d'un paquet resté sans accusé de réception (0–7).

Dispositifs 802.15.4 à fonctions limitées ou pleines, coordinateurs et coordinateur PAN

Les réseaux 802.15.4 sont constitués de plusieurs types d'appareils :

- L'architecture s'articule autour d'un nœud qui joue le rôle de *coordinateur PAN* (*Personal Area Network*) ou, plus simplement, coordinateur. Pour chaque réseau, il existe un seul coordinateur PAN, identifié par son identifiant (PAN ID). Ce coordinateur est chargé de scanner le réseau et de choisir le canal RF optimal. Il sélectionne aussi le PAN ID du réseau (identifiant sur 16 bits). Pour rejoindre un réseau 802.15.4, les autres nœuds doivent envoyer au coordinateur PAN une demande d'association avec ce PAN ID.
- Les dispositifs qui disposent d'un fonctionnel complet (FFD, *Full Function Device*), également appelés coordinateurs, sont capables de relayer des messages à d'autres FFD, y compris le coordinateur PAN. Le premier coordinateur qui envoie une trame balise (*beacon*) devient le coordinateur PAN. Ensuite, les dispositifs rejoignent le coordinateur PAN en tant que parent et, parmi ces appareils, les FFD commencent également à transmettre périodiquement une trame balise (spontanément si le réseau utilise la méthode d'accès avec balise comme expliqué ci-après, ou en réponse aux demandes de balise dans les autres cas). À ce stade, d'autres dispositifs peuvent rejoindre le réseau, en utilisant le coordinateur PAN ou n'importe quel FFD comme parent.
- Les dispositifs qui disposent de fonctions limitées (RFD, *Reduced Function Device*) ne peuvent pas router les messages. Leurs récepteurs sont généralement éteints, excepté lors de l'émission. Ils ne peuvent être associés au réseau qu'en tant que nœuds feuilles.

Au sein d'un réseau, deux topologies différentes peuvent être employées, chacune avec sa méthode de transfert des données propre :

- *Topologie en étoile* : les transferts de données sont possibles uniquement entre le coordinateur PAN et les dispositifs.
- *Topologie point à point* : les transferts de données sont possibles entre deux appareils quelconques. Toutefois, cette solution ne restera simple que si le réseau comprend uniquement des dispositifs en écoute permanente. Une

communication point à point entre des dispositifs qui peuvent entrer en mode veille nécessite une synchronisation, ce qui n'est pas pris en charge par la norme 802.15.4 de base, mais par des extensions (802.15.4e notamment).

Chaque réseau, identifié par son PAN ID, est appelé *cluster*. Un réseau 802.15.4 peut en théorie comprendre plusieurs clusters, chacun ayant son propre PAN ID, organisés sous forme d'arborescence : le coordinateur PAN racine ordonne à l'un des FFD de devenir le coordinateur d'un PAN adjacent. Chaque coordinateur PAN enfant peut également ordonner à un FFD de devenir un coordinateur pour un autre PAN, et ainsi de suite. En pratique toutefois, les réseaux 802.15.4 se limitent aujourd'hui à un seul cluster.

La couche MAC stipulée par le 802.15.4 définit deux méthodes de contrôle d'accès au réseau :

- La *méthode d'accès coordonné* (ou *Slotted CSMA/CA*). Dans ce mode, le coordinateur PAN structure la communication sous forme d'une *supertrame* constituée d'une trame balise de début et de fin, de 15 slots temporels et d'une période inactive optionnelle au cours de laquelle le coordinateur peut entrer en mode faible consommation (voir la figure 1.3). Les premiers slots temporels définissent la période d'accès avec contention (CAP, *Contention Access Period*), pendant laquelle les autres nœuds du réseau peuvent tenter des transmissions avec CSMA/CA. Les N ($N \leq 7$) derniers slots temporels forment la période sans contention facultative (CFP, *Contention Free Period*), qui peut être utilisée par des nœuds nécessitant un accès déterministe au réseau ou une garantie de bande passante.

  La trame balise commence par le champ de contrôle de la trame de la couche MAC (voir les figures 1.3 et 1.4), puis comprend le PAN ID de source, une liste d'adresses pour lesquelles le coordinateur possède des données en attente, et les paramètres de configuration de la supertrame. Les dispositifs qui souhaitent envoyer des données à un coordinateur commencent par écouter la balise de la supertrame puis se synchronisent avec cette supertrame et transmettent des données au cours de la CAP en utilisant CSMA/CA ou pendant la CFP. Les dispositifs pour lesquels le coordinateur possède des données en attente doivent les lui demander en employant une commande de requête de données MAC (voir le tableau 1.6).

  Lorsque plusieurs coordinateurs transmettent des balises, les périodes d'activité des supertrames ne doivent pas se chevaucher (le paramètre de configuration StartTime permet de s'en assurer).

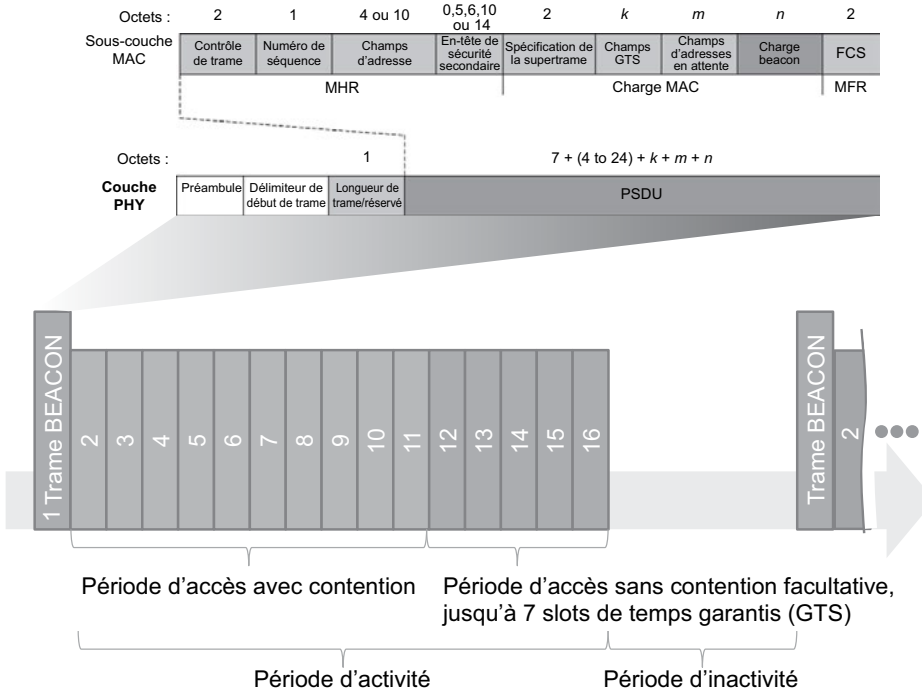


Figure 1.3 Structure de la supertrame 802.15.4

Tableau 1.6 Identifiants des commandes 802.15.4

01	Requête d'association
02	Réponse d'association
03	Notification de dissociation
04	Requête de données
05	Notification de conflit de PAN ID
06	Notification d'état « orphelin »
07	Requête de balise
08	Réalignement du coordinateur
09	Requête GTS

	Octets	
Champ de contrôle de la trame	2	000---------- : trame balise 001---------- : trame de données 010---------- : trame d'accusé 011---------- : trame de commande ---1---------- : sécurité activée sur la couche MAC ----1---------- : trame en attente -----1---------- : demande d'accusé de réception ------1---------- : compression de PAN ID (PAN ID source omis, identique à la destination) -------XXX----- : réservés ----------XX---- : mode adresse de destination *00* : *PAN ID et destination sont absents (adressage indirect)* *01* : *réservé* *10* : *adresses courtes sur 16 bits* *11* : *adresses étendues sur 64 bits* ------------XX-- : version de trame (00 : 2003, 01 : 2006) --------------XX : mode adresse source
Numéro de séquence	1	
PAN ID de destination	0 ou 2	
Adresse de destination	0, 2 ou 8	
PAN ID de source	0 ou 2	
Adresse de source	0, 2 ou 8	
Sécurité secondaire	variable	Comprend un contrôle de sécurité, un compteur de trame et un identificateur de clé
Charge	variable	
FCS	2	CRC sur 16 bis pour le contrôle d'intégrité de la trame

Figure 1.4 Format de la trame de la couche MAC 802.15.4

- La *méthode d'accès non coordonné* (ou *Unslotted CSMA/CA*). Ce mode est utilisé par ZigBee et la plupart des implémentations actuelles de 6LoWPAN. Tous les nœuds accèdent au réseau en utilisant CSMA/CA. Le coordinateur envoie une balise uniquement lorsqu'un nœud le demande et fixe le paramètre Beacon Order (BO) à 15 de manière à indiquer que la méthode d'accès sans balise (*non-beacon*) est employée. Les nœuds, y compris le coordinateur, demandent une balise au cours de la procédure de *scan actif*, lorsqu'ils tentent de déterminer si des réseaux se trouvent dans le voisinage et d'obtenir leur PAN ID.

Les dispositifs n'ont aucun moyen de savoir si le coordinateur possède des données en attente qui leur sont destinées et le coordinateur ne peut pas envoyer simplement les données à des dispositifs qui ne sont pas en écoute permanente et non synchronisés. Par conséquent, les dispositifs doivent demander les données au coordinateur de façon périodique, à une fréquence fixée par l'application.

Association

Pour rejoindre un réseau, un nœud envoie une requête d'association à l'adresse du coordinateur. Cette requête précise le PAN ID que le nœud souhaite rejoindre, ainsi qu'un ensemble d'indicateurs de capacités codés sur un octet :

- *PAN de remplacement (*Alternate PAN*)* : 1 si le dispositif a la capacité de devenir un coordinateur.
- *Type de dispositif (*Device type*)* : 1 pour un appareil capable de devenir un dispositif possédant toutes les fonctions possibles (FFD), comme effectuer des scans actifs du réseau.
- *Source d'alimentation (*Power source*)* : 1 en cas d'utilisation d'une source d'alimentation principale, 0 en cas de fonctionnement sur batterie.
- *Récepteur actif pendant que l'émetteur est inactif (*Receiver on while transceiver is idle*)* : fixé à 1 si le dispositif est en écoute permanente.
- *Capacité de sécurité (*Security capability*)* : 1 si le dispositif prend en charge l'envoi et la réception de trames MAC sécurisées.
- *Adresse d'allocation (*Allocation address*)* : fixé à 1 si le dispositif demande une adresse courte au coordinateur.

Dans sa réponse, le coordinateur affecte une adresse courte sur 16 bits au dispositif (ou le code spécial `0xFFFE` pour indiquer que le dispositif peut utiliser son adresse MAC IEEE sur 64 bits) ou donne la raison de l'échec (accès refusé ou absence de capacité disponible).

Le dispositif et le coordinateur peuvent tous deux émettre une requête de dissociation pour terminer l'association.

Lorsqu'un dispositif perd son association avec son parent, par exemple s'il devient hors de portée, il renvoie des notifications de commande spécifique (une trame constituée d'un en-tête MAC, suivi d'un code de commande spécifique). S'il accepte la réassociation, le coordinateur doit envoyer une trame de réalignement qui comprend le PAN ID, ainsi que les adresses courtes du coordinateur et du dispositif. Cette trame peut également être utilisée par le coordinateur pour signaler un changement de PAN ID.

Dans le cas de réseau IP (6LoWPAN), ces demandes d'association ou de désassociation deviennent redondantes avec les fonctions équivalentes disponibles dans le