ZigBee, de la théorie à la pratique : création d'un réseau ZigBee avec transmission de données

Jackson Francomme, Férial Virolleau, Jiamin Pang, Yan Xin Phang, Thierry Val

ZigBee, de la théorie à la pratique
Création d'un réseau ZigBee avec transmission de données

Résumé

Les technologies de l'informatique sont de nos jours enfouies profondément dans le tissu de notre société à un point tel que nous ne pouvons éviter de passer chaque jour devant un très grand nombre de machines informatiques de toutes natures. Il ne faut pas penser simplement à l'outil informatique posé sur votre bureau, ou dans votre poche qui vous permet de téléphoner. Vous pourriez imaginer par exemple, sans vous projeter dans un film de science-fiction que ces machines informatiques vous ouvrent des portes, vous reconnaissent pour vous guider en toute sécurité vers votre destination, vous aident et vous surveillent si vous êtes à mobilité réduite et âgés, surveillent en continu une forêt pour prévenir rapidement d'un début d'incendie, etc.

Pour de multiples raisons, ces machines sont très souvent amenées à collaborer. Pour cela, elles communiquent via des réseaux câblés ou sans fil. La mise en œuvre de tels réseaux peut être très compliquée, notamment parce qu'elle impose de connaître parfaitement la structure du réseau et les protocoles associés à la communication.

Cet article vous présente une solution concrète de communication sans fil basée sur la technologie ZigBee, qui pour de multiples raisons s'adapte très bien au domaine de l'électronique embarquée, notamment par sa facilité de mise en œuvre, son optimalité en termes de consommation et de coût. Autour d'un scénario simple de fonctionnement, nous illustrerons nos propos avec une présentation des outils matériels et logiciels permettant d'appréhender la mise en place du réseau de capteurs et la vérification de son fonctionnement.

1. Introduction sur les communications sans fil et ZigBee

Dans la course à la miniaturisation et en relation avec des considérations de développement durable, des technologies informatiques s'adaptent et se créent.

Dans le domaine des communications sans fil, aujourd'hui plus particulièrement centré sur la communication entre machines informatiques complexes et en téléphonie, le standard de communication ZigBee apporte une nouvelle dimension des technologies de communication. Force est de constater que la grande majorité des évolutions tendent à décupler les capacités de débit des machines informatiques sans réellement prendre en considération, à leur base, des aspects comme la consommation énergétique, le facteur d'échelle, la simplicité de mise en œuvre des protocoles et des réseaux, etc.

Il est de coutume de commencer par une introduction sur les spécifications du standard et de la norme. Nous ne dérogerons pas à cette règle dans la mesure où beaucoup de réponses à vos questions pourront être trouvées dans les documents que vous trouverez cités.

2. Informations de base sur la technologie ZigBee/IEEE 802.15.4

ZigBee désigne une technologie pour la communication sans fil robuste de type WPAN (*Wireless Personal Areal Network*). Ses caractéristiques en font une technologie à part qui vient compléter et non pas remplacer les offres des standards de communication bien connus tels que le WLAN (*Wireless Local Area Network*) WiFi et le WPAN Bluetooth.

- **La pile protocolaire**

ZigBee regroupe un ensemble de protocoles de hauts niveaux (Fig. 1) utilisés sur une structure matérielle, communiquant sans fil, de petite taille, très économe en énergie. ZigBee appartenant plus particulièrement à la famille des réseaux personnels sans fil désignée en anglais par l'acronyme LP-WPAN (*Low Power - WPAN*), est basé sur le standard *IEEE 802.15.4*[1]. Les spécifications de ce standard sont accessibles sur le Web et sont régulièrement mises à jour depuis 2005, sur le site Internet de l'IEEE [2]. La majorité des ressources que vous retrouvez sur le Web sont des émanations de ces documents ; il ne faut donc pas hésiter à s'emparer de ces documents précieux.

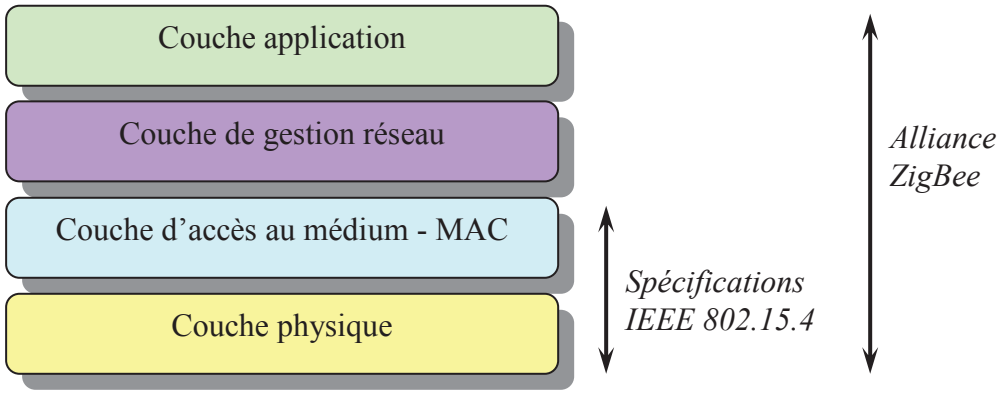

Fig. 1 - Pile de protocoles ZigBee

- La *couche physique* supporte la gestion des fréquences d'émission et de réception, le débit des données envoyées ou reçues, le type de modulation et le codage numérique des informations.
- La *couche d'accès au médium* ou MAC (*Medium Access Control*) s'appuie sur les ressources de la couche physique. C'est la couche principale pour les aspects logiciels qui définit la façon dont un nœud du réseau pourra dialoguer (transmettre ou recevoir). Ces mécanismes sont tous détaillés dans la spécification du standard IEEE 802.15.4 [3].
- La *couche réseau* assure principalement les règles d'établissement d'un réseau, l'association et l'interconnexion de tous les nœuds dans le réseau, le transfert des informations entre les entités de ce réseau via une route, ainsi que la structure des messages (trames) qui seront échangés.
- La *couche application* utilise les couches inférieures pour une application communicante donnée. Elle donne entre autres une signification aux informations échangées dans le réseau.

- **Les domaines d'application**

ZigBee est aujourd'hui utilisé dans de nombreux équipements, très généralement embarqués, qui imposent une très faible consommation, et se suffisent d'un très faible débit de données et une portée de quelques dizaines de mètres (jusqu'à 100m). Ces équipements peuvent être opérationnels dans une maison ou dans l'industrie. Afin de rendre inter-opérationels les équipements des différents fournisseurs, plusieurs normes se sont développées autour de ZigBee : WirelessHART, ISA100.11a, 6LoWPAN, SynchroRF, RF4CE [1]. Nous ne développons pas ces normes dans cet article.

- **Basse consommation ! mais comment ?**

[1] À titre de comparaison, la norme WiFi bien connue est basée sur le standard IEEE 802.11, nuancée par les suffixes a, b, g, n, et bientôt ac...

Le mécanisme permettant d'économiser l'énergie des modules communicants est basé principalement sur leur mise en sommeil lorsque aucune activité d'émission, de réception ou d'écoute radio n'est requise. L'activité de sommeil est ainsi prépondérante. Les modules communicants appelés dans notre jargon « nœuds » se réveillent occasionnellement afin de vérifier si aucun message n'a été enregistré pour eux par le *coordinateur du réseau* ; nous reviendrons plus loin sur les fonctions de ce *coordinateur de réseau*. Les composants électroniques développés par les industriels sont également optimisés afin de consommer le moins possible. Il n'est pas difficile de vérifier cela en consultant les fiches techniques des composants dédiés à cette norme (microcontrôleur, émetteur-récepteur, capteurs, etc). La consommation est également optimisée au niveau de la communication entre les nœuds du réseau ; nous citerons pour exemple les techniques de routage[2] qui élaborent des stratégies sur la recherche et l'utilisation de chemins pour la communication. Ces informations pourront, par exemple, être trouvées dans la première partie (état de l'art) de thèses de doctorat que vous trouverez sur le Web ; elles sont en général simplifiées et très abordables.

- **Quelques données techniques sur le protocole sans-fil ZigBee/IEEE 802.15.4**

Nous ne nous étendrons pas dans ce paragraphe ; vous retrouverez toutes les informations utiles dans les spécifications du standard IEEE 802.15.4 [3] ainsi que dans une version simplifié en langue française [4].

Le standard IEEE 802.15.4 initial peut utiliser 3 bandes de fréquences différentes et propose 27 canaux de communication. (Fig. 2). Vous remarquerez que le débit n'est en rien comparable à celui du WiFi ou Bluetooth (en particulier dans va version 4). ZigBee/IEEE 802.15.4 dédié aux réseaux de capteurs sans fil n'est amené à transmettre que de petites quantités de données (ie. quelques octets), liées notamment à des grandeurs physiques acquises (température, pression, lumière, etc.).

A l'inverse, ce standard peut supporter un très grand nombre de machines interconnectées (plus de 65000) dans le même réseau, ce qui est loin d'être le cas de WiFi et Bluetooth.

Bande de fréquence	Débit possible	Nombre de canaux
2,4 GHz	250 Kbits/s	16
915 MHz	40 Kbits/s	10
868 MHz	20Kbits/s	1

Fig. 2 - IEEE 802.15.4 dans la bande radio ISM

- **Les topologies réseau avec le protocole ZigBee/IEEE 802.15.4**

Le protocole IEEE 802.15.4 supporte les topologies *réseau étoile* (Fig. 3a) et *maillé* (Fig. 3b). La topologie indique la façon dont est associé un nœud dans le réseau et la forme géométrique de l'architecture globale des liens ; le nœud capteur peut être dépendant d'un nœud principal dans le réseau que l'on nomme *coordinateur*. Dans la topologie étoile, toutes les communications passent par le *nœud coordinateur* qui assure le rôle de relais entre les *nœuds terminaux*. Dans la topologie maillée, certains nœuds assurent le relais au même titre que le nœud coordinateur ; ces nœuds se nomment *routeurs*. Dans ce dernier cas, certaines

[2] Routage : procédé qui consiste à trouver un chemin de communication dans un réseau entre un nœud émetteur et un nœud récepteur (couche réseau).

communications doivent donc réaliser plusieurs *sauts* avant de pouvoir atteindre leur destination.

Les flux de communication sont dépendants de la distance entre les nœuds, du mode d'association des nœuds dans le réseau et de la qualité du signal au voisinage des nœuds.

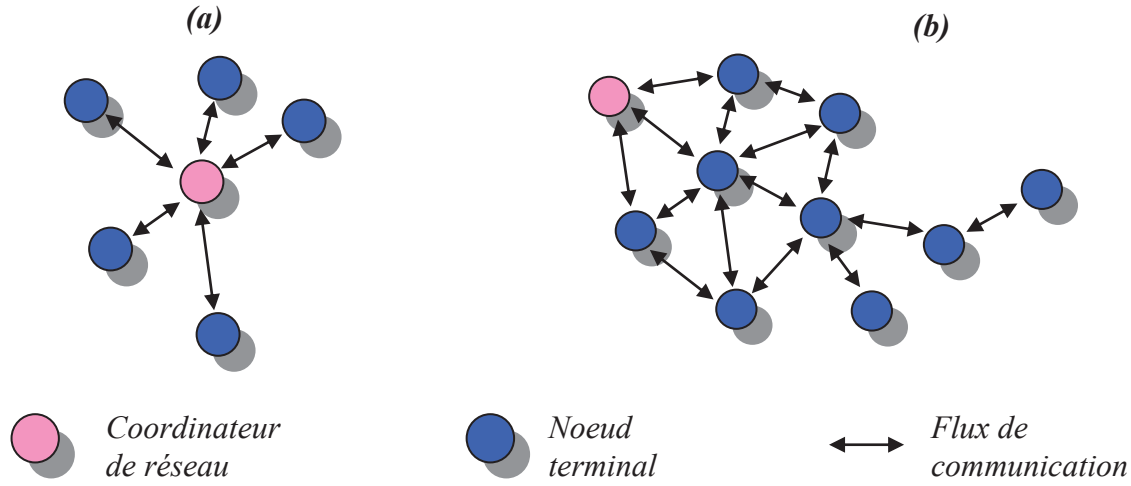

Fig. 3 - Topologies des réseaux ZigBee

- **Illustration d'un réseau maillé simplifié**

Pour comprendre à quoi correspond un réseau maillé, vous pouvez imaginer un immeuble comportant 5 étages (Fig. 4).

- Le coordinateur (en rouge) est placé au 3^{ième} étage, ce qui lui permet théoriquement d'être à portée radio de presque tous les autres nœuds terminaux.
- Au 4^{ième} étage, nous avons un routeur (en bleu) qui permet d'étendre le réseau vers le 5^{ième} étage. Le nœud terminal du 5^{ième} étage est donc joignable depuis le coordinateur via le routeur.
- Par contre, nous n'avons aucun routeur sur le second étage ; la distance étant trop grande, le nœud terminal du 1er étage ne peut pas être joint par le coordinateur.

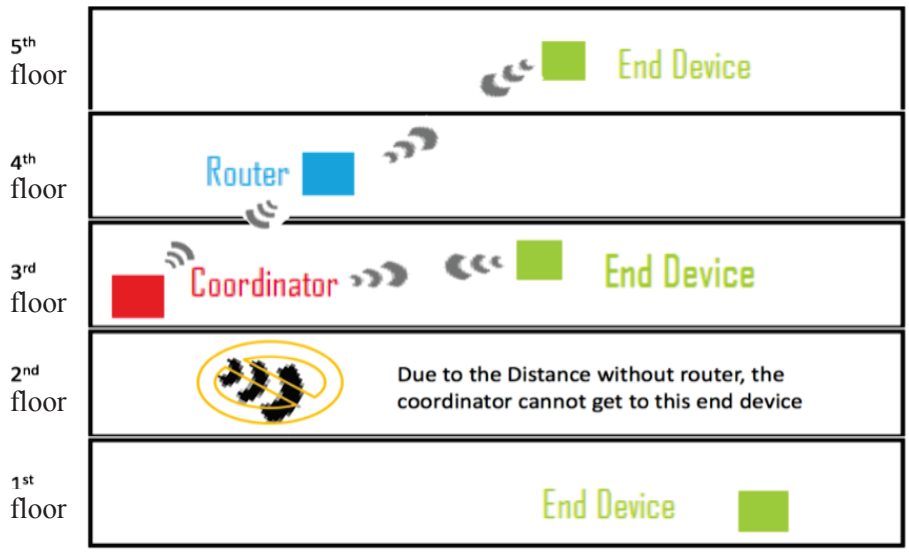

Fig. 4 - Représentation d'un réseau maillé simplifié

3. Mise en place expérimentale du réseau ZigBee

Préambule : Les illustrations pour cette partie expérimentale ont été réalisées par 2 étudiants de l'école d'ingénieurs de Nanyang de Singapour en stage à l'ESIEE-Paris. Vous trouverez donc sur les figures des commentaires en langue anglaise.

– Scénario et choix des matériels

Nous nous donnons pour objectif de réaliser un réseau maillé, typiquement celui représenté sur la Fig. 4. Notre choix sur le matériel s'oriente sur une solution à base de contrôleur MICROCHIP et émetteur-récepteur radio CHIPCON. Ceux-ci sont présents sur une carte de développement vendue dans le commerce sous la dénomination « *PICDEMZ Demonstration kit* ». Ce kit est composé de :

- 2 cartes mères PICDEMZ alimentées par batterie
- 2 cartes filles « émetteur-récepteur 2.4GHz » MRF24J40MA
- Une carte ZENA pour l'analyse des communications ZigBee
- Un câble USB
- 1 CDROM de ressources pour les cartes PICDEMZ, dont le logiciel MPLAB et la pile de protocoles ZigBee2006
- 1 CDROM de ressources pour l'analyseur de réseau.

Fig. 5 – PICDEMZ : Solution matérielle retenue

La carte PICDEMZ comporte pour élément principal un microcontrôleur PIC 18LF4620 de MICROCHIP ; la programmation de celle-ci se fera à l'aide du logiciel MPLAB, gratuit, téléchargeable sur Internet [5].

Pour la construction de notre réseau, nous utiliserons la pile protocolaire IEEE 802.15.4 simplifiée. Les étudiants ont disposé d'une application de base qu'ils ont complétée afin de prendre en compte les liaisons multi sauts. Nous ne décrirons pas le logiciel dans cet article.

Notre choix a été guidé par le coût de la structure à installer ainsi que par la possibilité de disposer d'une structure logicielle que nous pouvions modeler à notre convenance, mais il existe bien d'autres des solutions concurrentes équivalentes, nous y reviendrons dans la conclusion.

Il est tout à fait possible de développer un réseau ZigBee sans pratiquement aucune connaissance en informatique réseau. Chez vos distributeurs, vous trouverez par exemple les modules XBEE et les logiciels associés [6], qui vous permettrons de transmettre des données respectant le standard IEEE 802.15.4 pour quelques dizaines d'euros. Pour la création de votre application, vous pourrez par exemple choisir des architectures Arduino [7] ou Mbed [8] pour lesquels la programmation se fait en langage commun tel que le C.

- **Description de la carte PICDEMZ**

La carte mère et le module de communication RF sont représentés Fig. 6. Les 2 cartes sont séparées ; lors de la connexion de la carte fille RF, il faut faire attention de ne pas la mettre à l'envers.

Le cœur de la carte est un microcontrôleur PIC18LF4620. Il est alimenté avec une source de tension de 3,3V. Il est programmable à l'aide de l'interface MPLAB C18. La connexion avec l'ordinateur se fait à travers un module ICD2 connecté sur le port ICSP (Fig. 6). Le port série RS232 sera utilisé pour le suivi de l'exécution de l'application et le déverminage. La carte peut être alimentée avec une batterie ou avec une alimentation secteur.

La carte mère possède 2 DEL, D_1 et D_2. D_1 indique que le nœud appartient à notre réseau. D_2 clignote lorsque que le nœud reçoit un message d'un nœud non associé au réseau.

Les boutons-poussoirs permettent la réinitialisation de la carte (MCLR). L'envoi d'un message à tous les nœuds du réseau (diffusion ou *broadcast*) se fait par un appui sur PB_5. PB_4 permet d'associer le nœud au réseau.

La carte possède également un capteur de température Microchip TC77, connecté sur la liaison série SPI. Nous utiliserons cette ressource comme producteur de la donnée à transmettre.

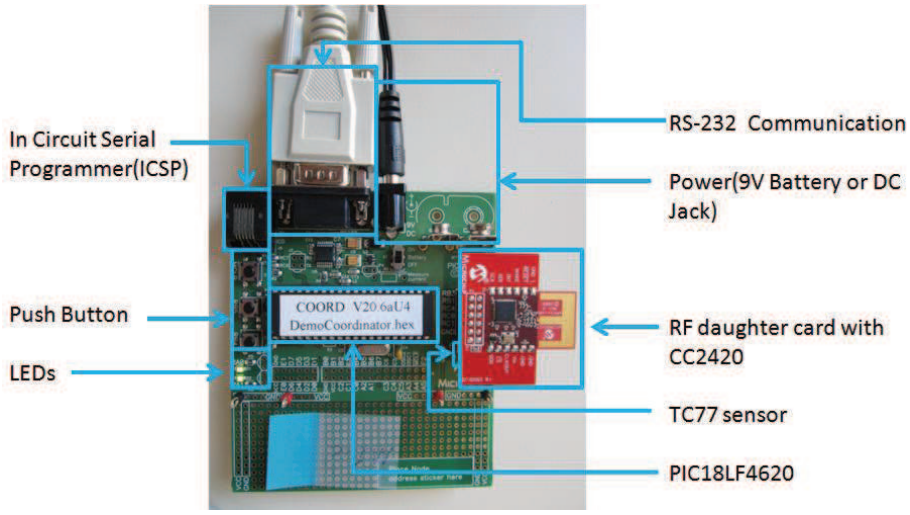

Fig. 6 - Carte mère PICDEMZ et sa carte fille pour l'émission-réception HF 2.4GHz

La carte radio fille supporte un circuit intégré CC2420 (*transceiver* radio Texas Instruments). Elle est parfaitement compatible avec le standard IEEE 802.15.4. Sa couche physique utilise la bande de fréquence de 2,4 GHz. Le débit des données sera de 250 Kbits/s. Cette carte peut être utilisée pour les routeurs, le coordinateur ou les nœuds terminaux[3].

[3] La distinction entre coordinateur, routeur et nœud terminal réside essentiellement au niveau logiciel, qui intégrera plus ou moins de fonctionnalités.

- **ZENA : Analyseur de réseau**

La carte ZENA connectée à un PC via un câble USB (Fig. 7), et associée à son logiciel permet de capturer et visualiser toutes les trames ZigBee dans son voisinage. L'alimentation se fait par le câble USB. Les paquets de données reçus par l'antenne *patch* (gravée sur le circuit imprimé) sur le canal choisi sont envoyés au PC via la liaison USB. Cette carte et son logiciel seront présentés plus loin dans cet article.

Fig. 7 - Carte ZENA pour l'analyse des communications ZigBee

- **Module de mise au point MPLAB ICD2**

MPLAB ICD2 (*In Circuit Debugger*) (Fig. 8) connecté entre la carte mère et le PC permet de déverminer les programmes ainsi que de programmer les processeurs supportés.

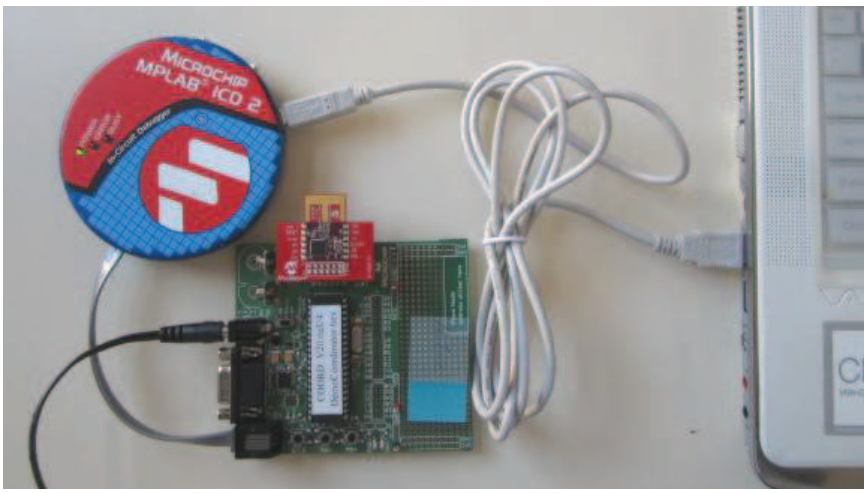

Fig. 8 - Module ICD2 pour le débogage et la programmation du microcontrôleur

4. Procédures pour l'initialisation et l'utilisation des logiciels et matériels

Vous trouverez dans cette section les instructions nécessaires pour l'utilisation des matériels associés à l'environnement de programmation et d'évaluation.

- **Chargement de l'application sur la carte-mère à partir de MPLAB**

Les codes de base utilisés sont présents dans le CD livré avec la carte. Vous pouvez également les télécharger depuis Internet. Vous téléchargerez également la note d'application

[9] qui vous donnera les indications pour l'utilisation de cet environnement. Vous disposez ainsi de 2 exécutables ; l'un pour le coordinateur et l'autre pour un nœud terminal du réseau ZibBee. La procédure est donnée pour le coordinateur. Vous effectuerez la même démarche pour le nœud terminal, avec le code approprié.

a) Connectez le module ICD2 entre le connecteur approprié de la carte-mère et le port USB de votre PC. La DEL verte sur le boîtier ICD2 indique que la connexion USB est parfaite.
b) Lancez l'application MPLAB (notre version : v8.76)
c) Sélectionnez « *Configure >> Select Device* » puis choisissez PIC 18F4620.
d) Sélectionnez « *File >> Import* » et choisissez l'application « DemoCoordinator.hex ». Cette application possède toutes les fonctionnalités pour assurer la fonction de coordinateur du réseau ZigBee.
e) Sélectionnez « *Programmer >> Select programmer* » et choisissez « *MPLAB ICD2* »
f) Sélectionnez « *programmer >> program* »
g) Appuyez puis relâchez le bouton Reset de la carte. Vous pouvez fermer l'application MPLAB IDE et déconnecter la carte-mère du boîtier IDC2.

- **Configuration de l'application sur la carte-mère du coordinateur**

À la suite de l'étape précédente, vous disposez de 2 cartes programmées que vous aurez pris soin d'annoter pour reconnaître le coordinateur et le nœud terminal. Pour la création d'un réseau, il vous suffit d'un coordinateur et d'au moins un nœud terminal.

a) Mettez sous tension les 2 cartes mères.
b) Appuyez sur le bouton Reset du coordinateur de réseau pour le démarrer. Attendez que D_1 et D_2 s'allument ; cela signifie que le réseau a été créé avec succès.
c) Appuyez maintenant sur le bouton Reset du nœud terminal. D_1 et D_2 doivent également s'allumer ; cela signifie que le nœud terminal s'est associé au réseau créé par le coordinateur avec succès. Si cela n'est pas le cas, répétez la démarche.
d) Appuyez ensuite sur BP_4 de chacune des cartes pour les associer au groupe 4 ; cette manipulation est liée à l'application. Un nouvel appui sur ce bouton-poussoir enlève le nœud du groupe et éteint la DEL D_1.
e) Maintenant que les 2 nœuds font partie du même groupe 4, ils peuvent s'échanger des données. Un appui sur le bouton-poussoir PB_5 d'un des nœuds inverse l'état de la DEL D_2 de l'autre nœud ; ce qui prouve que la transmission a été réalisée avec succès.

Vous venez de créer votre premier réseau. Afin de surveiller le fonctionnement du réseau en visualisant les trames échangées entre ces 2 noeuds, vous pouvez utiliser le logiciel *Hyperterminal* ou le *moniteur ZENA* que nous décrirons plus loin.

- **Configuration de l'outil logiciel MPLAB IDE et son compilateur MPLAB C18**

Afin de pouvoir obtenir un exécutable de votre application, il est nécessaire de disposer du compilateur capable de délivrer le code pour le microcontrôleur de votre carte. Si le compilateur C18 n'est pas installé sur votre machine, téléchargez le depuis le site de Microchip et installez-le.

- **Compilation du code source de l'application pour un nœud du réseau**

a) Sélectionnez « *File >> Open workspace* »
b) Choisissez « *DemoPIC18RFD.mcw* » dans le répertoire de votre PC (c'est un exemple de projet fourni par Microchip avec la pile protocolaire ZigBee 2006).

c) Sélectionnez « *Project >> Select language tool suite* » et choisissez l'emplacement pour tous les outils (Fig. 9).

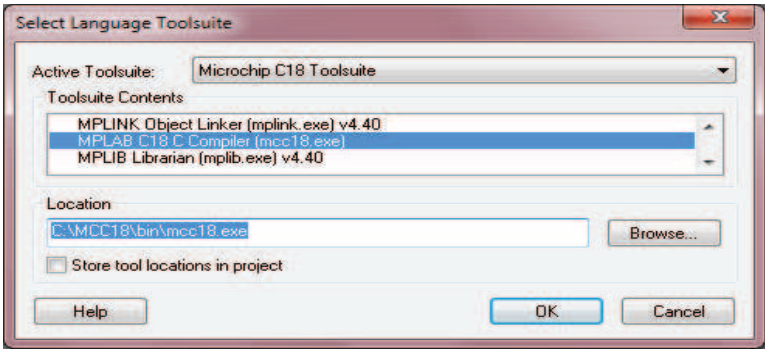

Fig. 9 - Initialisation de MPLAB IDE pour le compilateur C18

d) Sélectionnez « *Project >> Build all* » Vous pourrez ainsi voir la fenêtre suivante (Fig. 10).

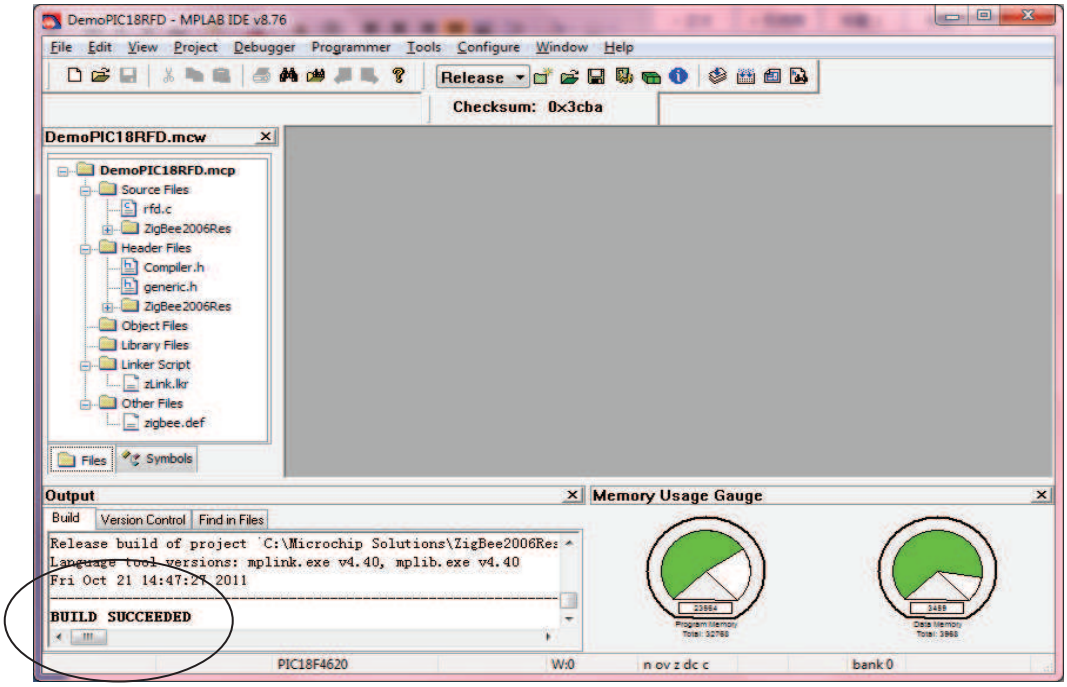

Fig. 10 - Echo de MPLAB IDE pour une compilation réussie de l'application

- **Initialisation de l'hyperterminal (ou *Tera Terminal*) pour la transmission série**

Nous proposons de créer un réseau de 3 nœuds, comportant un coordinateur, un routeur et un nœud terminal.

Les cartes PICDEMZ peuvent être connectées à un ordinateur. L'application de la carte PICDEMZ envoie sur la ligne série RS232, une aide à l'exécution ainsi qu'un écho de toutes les actions relatives à l'émission et à la réception sur le réseau ZigBee. Dans cette section, nous décrivons les étapes d'initialisation des terminaux (*Tera Terminal*) permettant de suivre l'exécution de l'application sur les ordinateurs PC.

Vous disposez normalement sur votre machine informatique sous Windows d'une application nommée *Hyperterminal*. Si ce n'est pas le cas, vous pourrez facilement télécharger une application équivalente sur Internet. La procédure d'initialisation est donnée ci-dessous.

a) Connectez les cartes PICDEMZ à vos ordinateurs en utilisant un câble série RS232. Mettez vos cartes sous tension.
b) Ouvrez autant de fenêtre « *Hyperterminal* » que vous utilisez de ports série sur votre ordinateur. La suite de la procédure décrit l'initialisation pour un seul port série.
c) Pour commencer, nommez par exemple votre connexion « *test* » (Fig. 11). Validez en cliquant sur le bouton *OK*. Sélectionnez ensuite le port série sur lequel vous êtes connecté : « *COM1* » par exemple. *Remarque : si vous utilisez un ordinateur portable souvent dépourvu maintenant de port série, vous aurez probablement besoin d'utiliser un adaptateur RS232/USB ; il sera nécessaire que vous installiez un driver avant l'étape b. Pour connaître le numéro de votre port série, vous accèderez au panneau de configuration : « Control panel >> System >> Hardware >> Device Manager >> Port (COM&LPT) »*

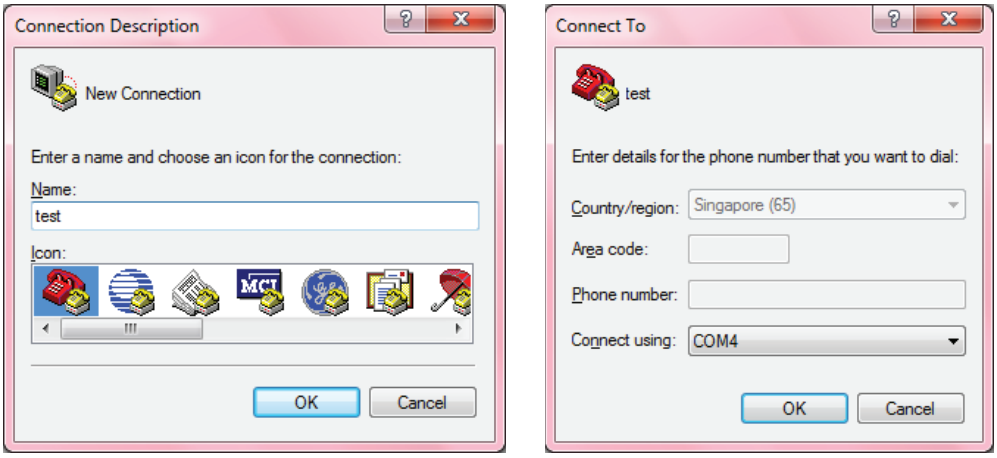

Fig. 11 - Initialisation pour *Hyperterminal*

Le visuel pour l'initialisation de l'application *Tera Terminal* diffère un peu. Les paramètres sont toutefois identiques (Fig. 12).

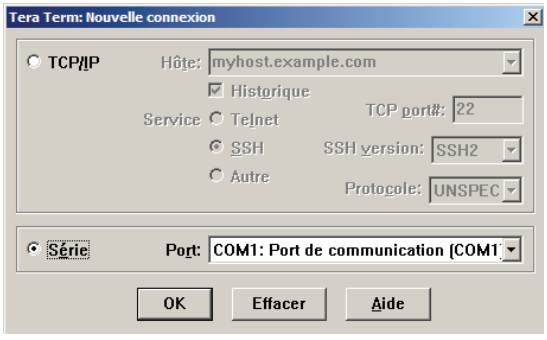

Fig. 12 - Initialisation pour l'application *Tera Terminal*

d) Paramétrez ensuite votre terminal pour qu'il affiche localement les caractères que vous entrez au clavier et qui seront envoyés sur la ligne série (Fig. 13)

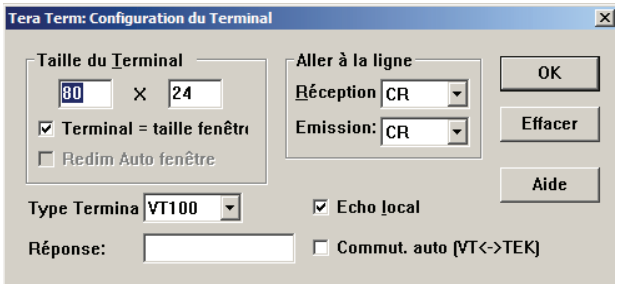

Fig. 13 - Paramétrage de *Tera Terminal*

e) Configurez le port série avec les paramètres suivants : 19200 bits par seconde, 8 bits de données, pas de parité, 1 bit de stop, pas de contrôle de flux (Fig. 14)

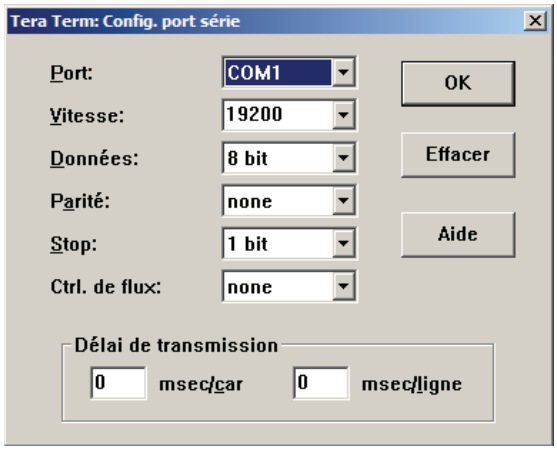

Fig. 14 - Paramétrage de la communication série

- **Suivi de l'activité des nœuds sur le réseau ZigBee**

a) Faites un RESET de chacune de vos cartes connectées sur vos ordinateurs et vous verrez apparaître pour chacune des fenêtres *Hyperterminal* l'un des contenus illustré sur les figures Fig. 15 et Fig. 16. Attention ! *Le coordinateur doit bien sûr être démarré le premier comme présenté au chapitre précédent, avant le nœud routeur et le nœud terminal*.

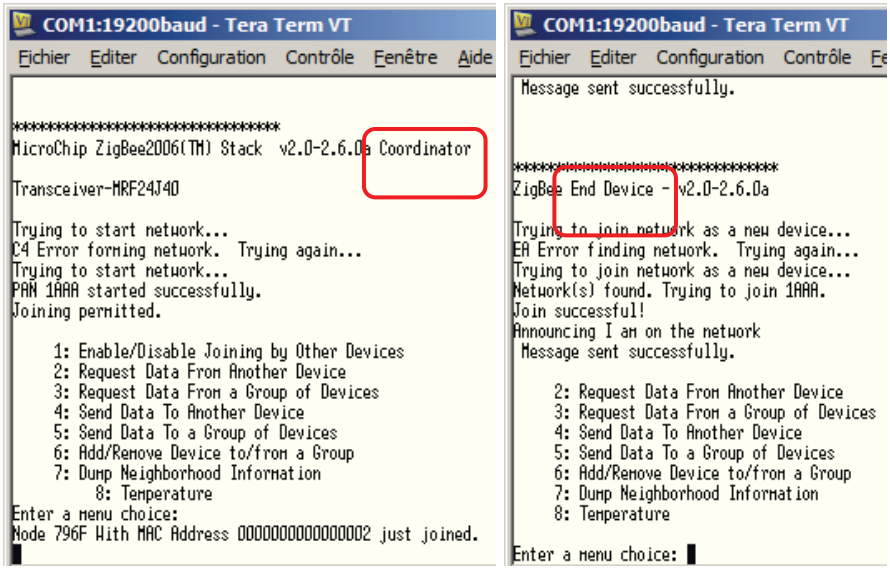

Fig. 15 - Écho de l'exécution de nœuds sur l'écran de l'*Hyperterminal*

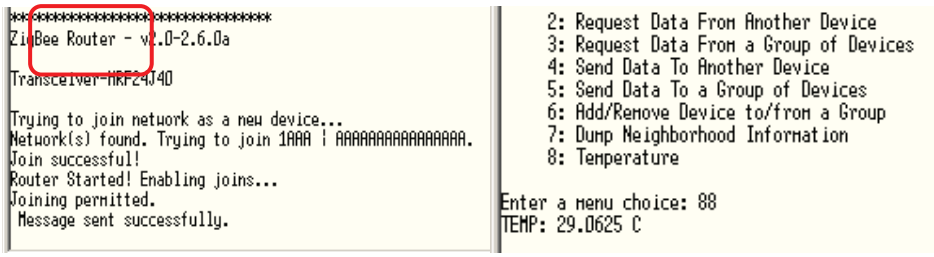

Fig. 16 - Écho de l'exécution des nœuds sur l'écran de l'*Hyperterminal*

b) Appuyez sur le bouton-poussoir BP_4 pour que toutes les cartes fassent partie du même groupe. Si vous ne voyez pas apparaître le menu sur un des terminaux, cela signifie que l'association a échoué. Appuyez de nouveau sur le bouton-poussoir BP_4 pour résoudre le problème.

c) En choisissant l'option *7*, sur l'écran du coordinateur, vous obtenez les informations d'adresse de tous les nœuds associés au réseau qu'il a créé.

d) Le choix *2* sur l'écran du nœud terminal permet de demander des données d'un autre nœud. Vous entrerez l'adresse du coordinateur et la quantité de données attendue. Ainsi, le nœud terminal recevra un message du coordinateur incluant la quantité de données (*length*), l'adresse et le buffer de données (arbitraire dans l'exemple). Ce message contiendra par exemple *00 00 01 02 03* si la longueur que vous avez tapée est *4*. Le premier octet indique que le message a été reçu correctement. Ainsi, les données effectives sont *00 01 02 03*.

e) Le choix *8* sur le nœud terminal permet l'acquisition de la température (Fig. 16). *Cette fonctionnalité n'est pas incluse dans le pack logiciel de Microchip et a été rajouté par les étudiants*.

f) Le choix *2* sur le coordinateur a été modifié pour recevoir la température d'un nœud terminal (Fig. 17). Vous remarquerez que les températures *émise et reçue* sont identiques.

g) Vous pouvez ensuite tester les autres fonctionnalités de cette application.

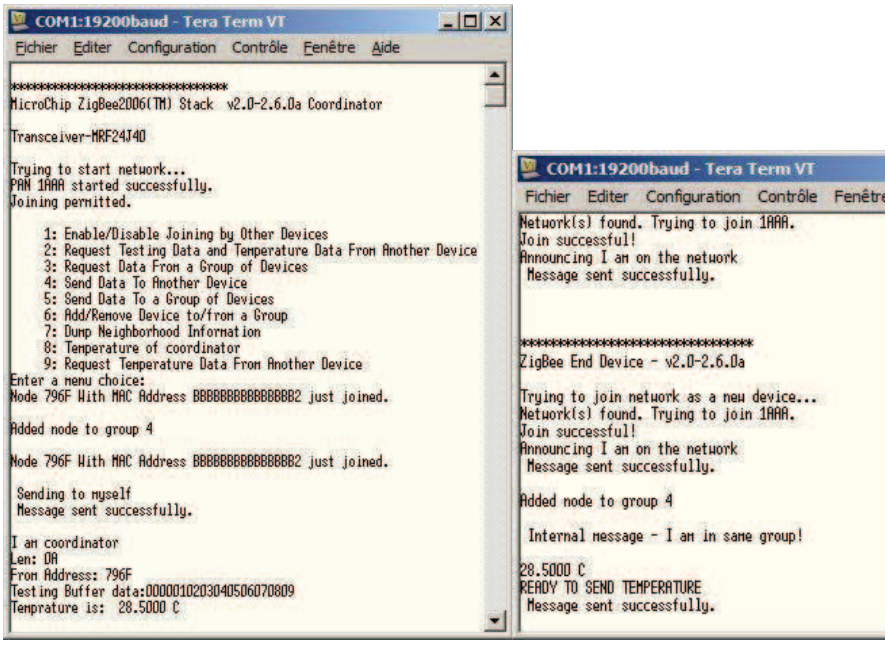

Fig. 17 - Requête pour l'envoi de données du nœud terminal vers le coordinateur

- **Outil d'analyse du réseau sans fil ZigBee**

ZENA est un logiciel qui permet l'analyse de toutes les communications respectant la norme ZigBee disposant des couches physique et MAC 802.15.4 standards. Il peut être considéré comme un espion (*SPY* ou *sniffer*) sur le réseau étant donné qu'il ne fait que lire les trames et qu'il ne participe pas aux communications. Il est comparable à des outils bien connus pour Ethernet et WiFi tels que *wireshark* par exemple.

Il est nécessaire d'installer le logiciel ZENA (Fig. 18) avant de pouvoir utiliser la carte. Cette application est disponible sur le CD du kit PICDEMZ et peut également se télécharger sur Internet. Pensez également à télécharger son guide d'utilisation nommé en anglais (*ZENA™ Network Analyzer User's Guide*)

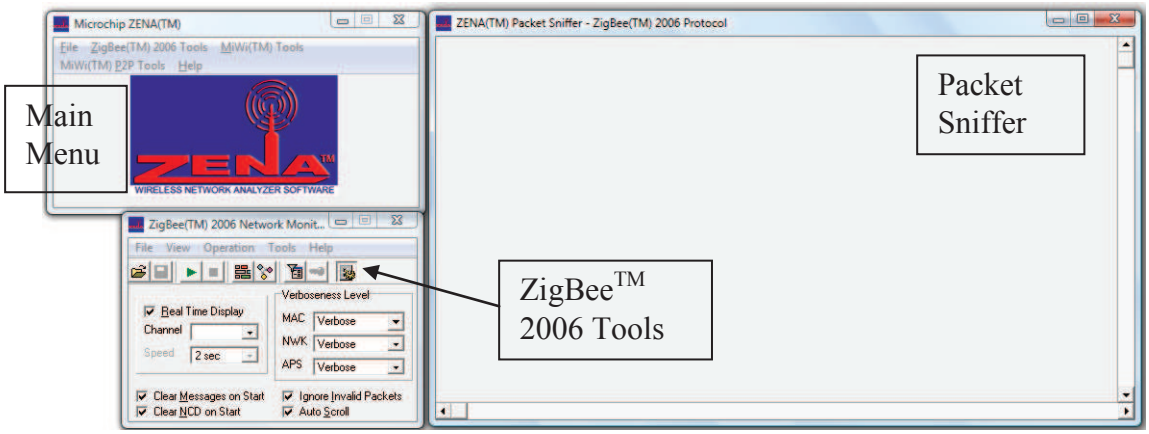

Fig. 18 - Outil d'analyse des communications sans fil respectant la norme ZigBee

Vous trouverez sur la Fig. 19 un exemple de capture de trames de la carte ZENA. Cette illustration est composée de 11 trames qui ont été lues sur le réseau. Pour chaque trame, vous disposez de plusieurs informations organisées avec des couleurs différentes. Le code vous est donné dans le tableau de la Fig. 20. Toutes les trames sont marquées d'un numéro et d'un temps.

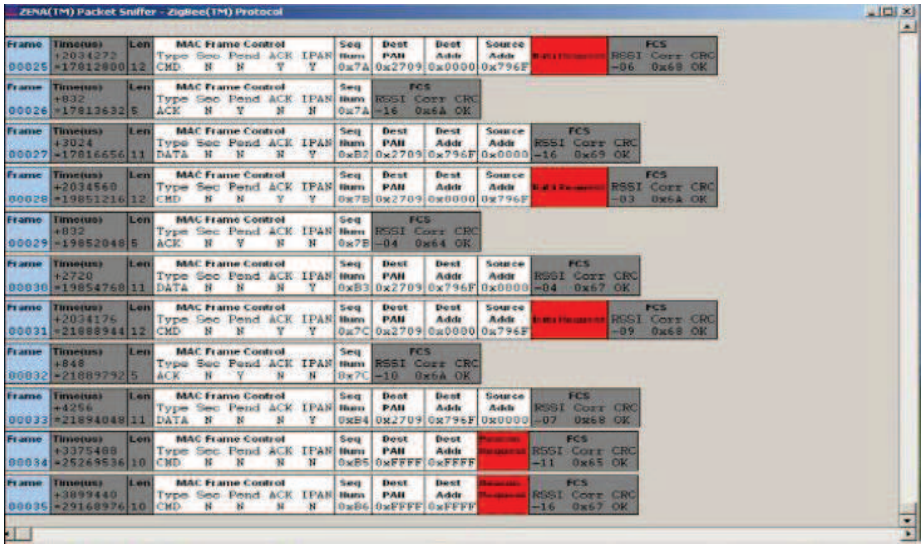

Fig. 19 - Exemple d'une capture de trames pour les communications à portée radio de la carte ZENA

Désignation	Couleur
Entête trame MAC	Blanc
Trame MAC de commande et balise	Rouge
Entête trame NWK (*NetWorK* ou réseau)	Beige
Trame de commandes NWK	Fushia
Entête trame APS (APplicationS)	Jaune
Charge utile *ou Payload* APS	Bleu clair
Entête trame sécurité et données cryptées	Bleu
Inconnu ou invalide	Brun olive

Fig. 20 - Code des couleurs pour les trames affichées par ZENA

Vous suivrez les étapes suivantes pour l'initialisation et l'utilisation du logiciel ZENA.

a) Lancez le logiciel ZENA (Notre version v3.0)
b) Sélectionner le canal de communication approprié
c) Sélectionnez dans le menu « *ZigBee 2006 Tools >> Network traffic monitor* ». Vous ouvrirez automatiquement le *sniffer* de paquets.
d) Vous pouvez visualiser l'organisation de réseau avec tous les nœuds présents. Pour cela sélectionnez le menu « *ZigBee 2006 Tools >> Network traffic monitor >> View >> Configuration display* ». Si à l'ouverture aucune activité n'a eu lieu, vous n'avez qu'un élément inconnu affiché. Dans le cas contraire, l'affichage intègre toutes les connexions existantes dans le réseau. Vous trouverez un exemple d'organisation simple obtenu à partir des trames reçues par le *sniffer* de paquets sur la Fig. 21.

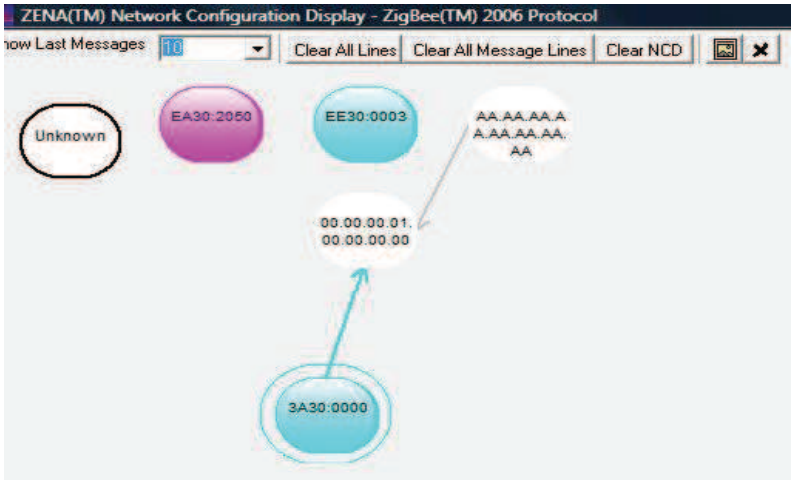

Fig. 21 - ZENA - Exemple d'organisation réseau

e) Afin de démarrer l'acquisition, vous devez cliquer sur le bouton « *Start* » ou sélectionner le menu *« Operation >> Start sniffing/Playback* » (Fig. 22).

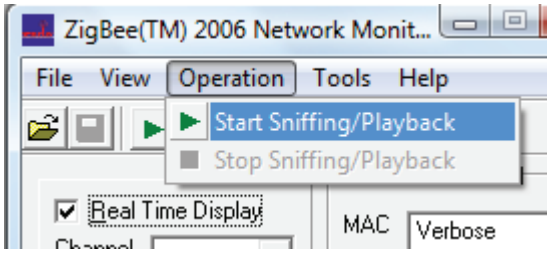

Fig. 22 - Lancement de l'acquisition des trames avec ZENA

Vos outils sont maintenant prêts à vous afficher l'activité de votre réseau composé des 3 nœuds décrits précédemment. Nous vous proposons de visualiser l'organisation du réseau ainsi que toutes les trames transmises à la suite d'une requête de transmission de données du coordinateur à un nœud terminal.

Nous visualisons donc la configuration du réseau avec l'outil adapté de ZENA (Fig. 23). Nous retrouvons notre réseau maillé comprenant 2 nœuds terminaux, un routeur et le coordinateur.

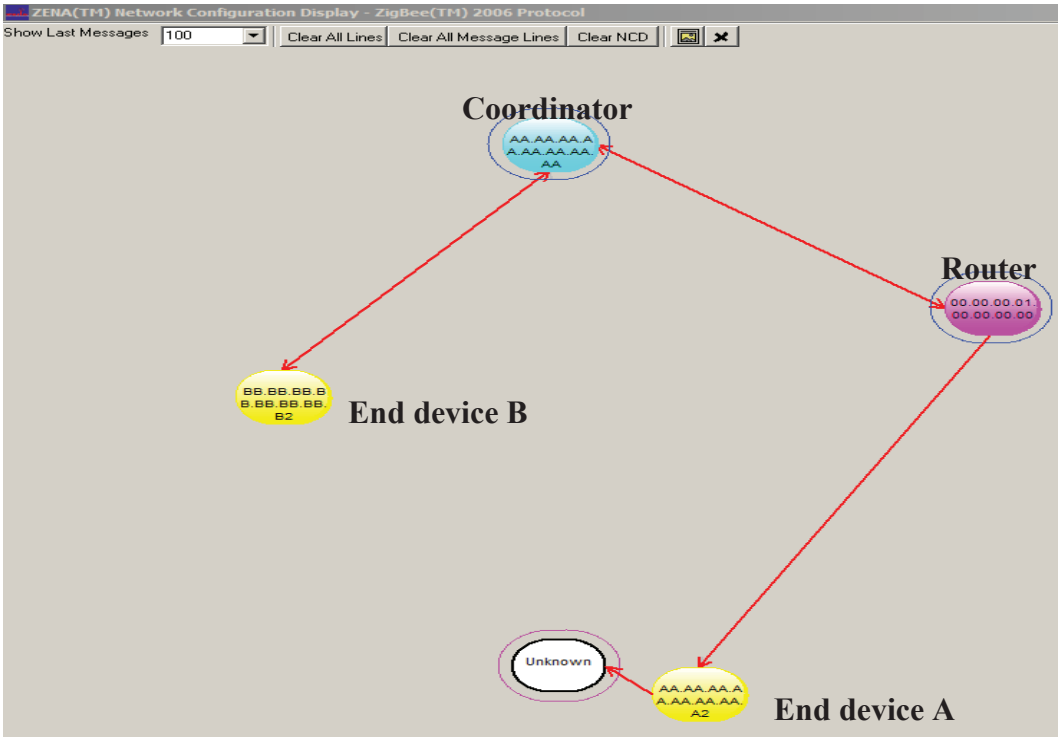

Fig. 23 - Topologie du réseau mise en oeuvre

Les trames échangées lors de la requête de demande de données du coordinateur au nœud terminal sont illustrées sur la Fig. 24.

Les 3 plus longues trames sont celles qui nous intéressent. Dans l'ordre d'apparition, nous avons :

- la trame de requête de données envoyée par le coordinateur au nœud terminal,
- la trame pour l'acquittement de la requête du coordinateur envoyée par le nœud terminal pour indiquer qu'il a bien reçu la demande d'envoi de données. Il prend le temps nécessaire pour répondre,
- enfin, la trame réponse du nœud terminal. Celle-ci contient notamment les données que le coordinateur lui a demandé, en l'occurrence la valeur de la température au voisinage du capteur du nœud terminal.

Dans ces trames, nous retrouvons plus particulièrement les adresses du coordinateur et du nœud terminal sollicité pour l'envoi des données sur la température, puis les données qui seront affichées sur l'écran de *l'Hyperterminal* du coordinateur.

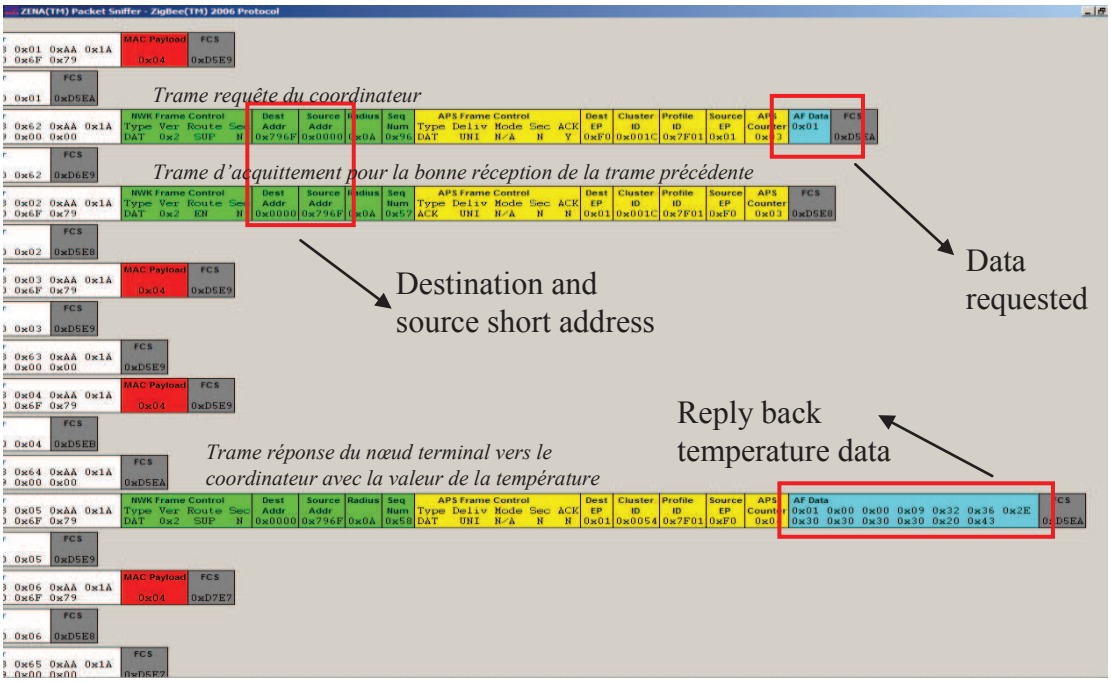

Fig. 24 - Trames détaillées relatives à la requête du coordinateur

5. Conclusion

L'utilisation de la technologie ZigBee/IEEE 802.15.4 telle qu'elle est présentée dans cet article s'adresse à toutes les personnes désirant découvrir cette technologie de communication sans fil. La diversité des produits supportant la norme, la simplicité de mise en oeuvre et l'encombrement réduit en font un outil privilégié pour des problématiques embarquées.

Les 2 étudiants de niveau Bac+2 ayant travaillés sur ce projet n'avaient pour commencer que peu ou pas de connaissance sur les technologies de communication sans fil. La création d'un réseau avec des communications simples entre les nœuds ne leur a pas posé de problème. La documentation est abondante, notamment en langue anglaise.

Le problème de la communication peut être abordé avec plusieurs niveaux de difficulté : de simple utilisateur à utilisateur expérimenté. Le premier fournit à la carte de transmission les données qui seront envoyées en respectant le standard. L'utilisateur plus expérimenté pourra lui-même formater ses trames (*payload*) et y inclure tout ce qui lui semble utile pour son application. Ce dernier niveau nécessite un minimum de connaissances de la programmation en langage évolué (langage C). Les étudiants ont abordé ce deuxième niveau avec l'acquisition de la température sur la carte mère et la création de leur propre trame. Il est même ensuite possible de passer à une analyse encore plus détaillée du réseau ZigBee, en particulier en visualisant et analysant les trames échangées lors de la construction du réseau, étape par étape, ou le retrait d'un nœud suite à une panne ou un éloignement radio, mais ceci est une « autre histoire » !

La transposition de cette démarche sur une autre plateforme n'est pas insurmontable. N'hésitez pas à utiliser les kits de découverte des différents constructeurs. Nous pouvons par exemple citer les produits proposés par la société CLEODE [10], en particulier le kit orienté pédagogie *EduBee*. Ce kit complet dispose d'une clé USB coordinateur (*UBee*), d'une prise de courant *ZBee* pilotable par radio et permettant également des remontées de consommation énergétique, d'une télécommande *ZRC* à 5 boutons poussoirs, remontant également la

température de la pièce, et comme le kit utilisé dans cet article, d'un espion *PacketSniffer* associé ici à une clé USB équipée d'un CI CC2531 de *Texas Instrument*.

6. Sources bibliographiques

[1] Adrien VAN DEN BOSSCHE, Thierry VAL, Eric CAMPO, « La technologie sans fil 802.15.4 : son héritage protocolaire et ses applications », Techniques de l'Ingénieur, France - Novembre 2011

[2] Groupe de travail IEEE TG4 : http://www.ieee802.org/15/pub/TG4.html

[3] IEEE 802.15.4™ – 2011, IEEE Standard for local and metropolitan area networks – Part 15.4 : Low-Rate Wireless Personnal Area Networks (LR-WPANs) - http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf

[4] Cyril ZARADER, « Le protocole sans-fil ZigBee/IEEE 802.15.4 et ses applications », REE N°10, pp91-98, Revue de l'Electricité et de l'Electronique, novembre 2004.

[5] Logiciel MPLAB IDE – lien pour le téléchargement : http://www.microchip.com

[6] Modules XBEE et logiciels associés : http://www.matlog.com/wireless/modules-zigbee-et-802154/

[7] Modules ARDUINO : http://www.arduino.cc/

[8] Modules Mbed de NXP : http://mbed.org/nxp/lpc1768/

[9] Derrick P. LATTIBEAUDIERE, MICROCHIP Inc., « AN132 – Microchip ZigBee-2006 Residential Stack Protocol », 2008.

[10] Kit d'évaluation ZigBee domotique et pédagogique de la société CLEODE : http://www.cleode.fr

Coauteurs

Jackson FRANCOMME – Enseignant en BTS SE / ERAEI / PhD en Informatique – Paris
Férial VIROLLEAU – Ingénieur en Informatique – ESIEE Paris
Jiamin PANG & Yan Xin PHANG – Nanyang Polytechnic (Singapour)
Thierry VAL – Professeur des Universités – Université de Toulouse