République Algérienne Démocratique et Populaire
Université Abou Bekr Belkaid–Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en Informatique

Option: *Réseaux et Systèmes Distribués (R.S.D)*

Thème

TEST DE CONNECTIVITÉ IP DANS LES RÉSEAUX DE CAPTEURS SANS-FIL : UNE APPROCHE VERS L'INTERNET DES OBJETS

Réalisé par :

- **Mme Baba Bendermel Soumia**

Présenté le 04 Novembre 2014 devant le jury composé de MM.

- *Mr. BENAMAR Abdelkrim* *(Président)*
- *Mme. LABRAOUI Nabila* *(Encadreur)*
- *Mr. BENMAMMAR Badr* *(Examinateur)*
- *Mr. BELHOUCINE Amine* *(Examinateur)*

Année universitaire: 2013-2014

Remerciements

En préambule de ce mémoire et avant tout, le grand et le vrai merci à Allah qui m'a donné la volonté et le courage et la patience pour la réalisation de ce travail.

Ces quelques lignes ne pourront jamais exprimer la reconnaissance que j'éprouve envers tous ceux qui, de près ou de loin ont contribué par leurs conseils, leurs encouragements ou leurs amitiés à l'aboutissement de ce travail.

Mes vifs remerciements accompagnés de toute ma gratitude vont tout d'abord à mon encadreur « **Mme LABRAOUI** », pour m'avoir proposé cet intéressant sujet et pour les précieux conseils et orientations qu'elle m'a prodigués. Je la remercie pour sa disponibilité, son aide, ses précieux conseils, ses critiques constructives, ses explications et suggestions pertinentes aussi son soutien moral dans les moments de stress et enfin, pour avoir apporté tant de soins à la réalisation de ce projet de fin d'études.

Je remercie tout particulièrement **Mme KHEDIM Farah** qui m'a beaucoup aidé et soutenue pour réaliser ce laborieux travail, merci pour sa patience, ses conseils et ses encouragements prodigués tout au long de ce mémoire.

Mes vifs remerciements vont également aux membres du jury **Mr BENMAMMAR Badr,** et **Mr BELHOUCINE Amine** pour l'intérêt qu'ils ont porté à mes recherches en acceptant d'examiner mon travail et de l'enrichir par leurs propositions. Je remercie également **Mr BENAMAR Abdelkrim** de m'avoir fait l'honneur de présider le jury.

Je tiens à exprimer mes sincères remerciements à tous les enseignants qui m'ont enseigné et qui par leurs compétences m'ont soutenus dans la poursuite de mes études.

Dédicaces

A mes parents, pour leur patience infinie, leur soutien sans faille et leur amour sans limite. Ce mémoire est autant le fruit de vos efforts que de mon travail.

A ma deuxième moitié, FethAllah que sans lui, ce travail n'aurait vu le jour, que Dieu réunisse nos chemins pour un long commun serein.

A mon petit ange Mohammed Wassim.

A mon adorable grand-maman qui je le sais ma réussite est très importante pour elle .Que Dieu vous paye pour tous vos bienfaits et vos prières.

A mes très chers frères et sœurs Mohammed, Abderrahmen, Asmaa et Narimen Lilia, qui n'ont cessé de m'encourager tout le long de mon travail ainsi qu'à Cherifa et Mustapha, mes frères de cœur ! Je vous souhaite une bonne continuation dans vos études.

A la famille BABA BENDERMEL, SALMI et BOUDIA.

A toutes mes amies et à toute personne qui me connait. A toute personne qui m'a aidé un jour à réussir jusque là, en espérant être toujours à la hauteur de leurs attentes et de leurs espérances.

Que la paix d'Allah soit avec tous Que Dieu nous réunisse dans son vaste paradis incha Allah.

Résumé

Avec les progrès technologiques dans le domaine des réseaux de capteurs sans fil, il ya un intérêt croissant de les connecter à internet pour partager des mesures en temps réel à partir des nœuds pour que "n'importe où, et n'importe quand, quiconque" puisse avoir accès à l'information et pouvoir l'utiliser. L'intégration d'IPv6 dans les réseaux de capteurs est devenue une réalité pour de nombreux industriels. Ces réseaux vont avoir un impact aussi bien sur l'environnement industriel (relevé de compteurs, gestion de l'énergie,...) que sur la domotique. Même si de nombreux protocoles existent déjà, l'utilisation d'IP permet une meilleure interopérabilité et une réduction de coût liées à l'utilisation de standards.

L'objectif de ce mémoire est de configurer et tester la connectivité IP entre des capteurs sans-fil en utilisant la librairie Blip, et aussi de se familiariser avec le domaine des réseaux de capteurs : Telosb, TinyOS, NesC, Blip, ZigBee. L'avantage de l'IP dans ce domaine, serait par exemple de pouvoir récupérer les informations émises par le ou les capteurs choisis (connaissant leur IP) et d'accéder à ce réseau depuis internet.

Mots clés : Réseaux de capteurs sans fil, internet des objets connectivité IP, 6lowpan, Blip, IPV6.

Abstract

As technology in the field of wireless sensor networks progress, there is a growing interest in connecting to the internet to share real-time measurements from the nodes so that "anywhere, and anytime, anyone" to have access to information and be able to use. The integration of IPv6 in sensor networks has become a reality for many manufacturers. These networks will have an impact both on the industrial environment (meter reading, energy management,...) on home automation. Although many existing protocols, the IP makes use of enhanced interoperability and reduced cost associated with the use of standards.

The objective of this paper is to configure and test IP connectivity between wireless sensors using the Blip library, and also become familiar with the field of sensor networks: Telosb, TinyOS, NESC, and Blip. The advantage of IP in this area, for example, would be able to recover the information transmitted by or selected sensors (knowing their IP) and access to the network from the Internet.

Keywords: Wireless sensor networks, internet of things, IP connectivity, 6lowpan, Blip, IPV6.

ملخص

مع التقدم التكنولوجي في شبكات الاستشعار اللاسلكية، هناك اهتمام متزايد في الاتصال عبر الإنترنت لتبادل قياسات الوقت الحقيقي عن طريق العقد بحيث يكون بإمكان "أي شخص، في أي مكان وفي أي وقت " الحصول على المعلومات وتكون قادرة للاستخدام. أصبح تكامل IPv6 في شبكات الاستشعار واقعا لكثير من المصنعين. هذه الشبكات سوف يكون لها تأثير سواء على البيئة الصناعية (قراءة العدادات، وإدارة الطاقة،...) على التشغيل الآلي للمنزل. على الرغم من أن العديد من البروتوكولات موجودة بالفعل، استعمال IP يفيد في تعزيز العمل المشترك وخفض التكاليف المرتبطة باستخدام المعايير.

الهدف من هذا المشروع هو : تكوين واختبار الاتصال IPبين أجهزة الاستشعار اللاسلكية باستخدام مكتبة Blip، وأيضا للتعرف على مجال شبكات الاستشعار:MicaZ, TinyOS, NESC, Blip, ZigBee. على سبيل المثال الاستفادة من الملكية الفكرية في هذا المجال,سوف تكون قادرة على استرداد المعلومات المرسلة من قبل أجهزة الاستشعار المختارة (مع العلم بIP الخاصة بهم) والوصول إلى الشبكة من الإنترنت.

كلمات البحث :شبكات الاستشعار اللاسلكية ,الاتصال IP ,إنترنت الأشياء,6lowpan, Blip ,IPV6 .

Table des matières

Chapitre3 : Mise en œuvre de la connectivité IP

Introduction Générale

En 1999, une technologie a été considérée par le DARPA (Defense Advanced Research Projects Agency) comme « l'une des 21 créations pour le 21ème siècle », en 2003, était « l'une des 10 nouvelles technologies qui ont bouleversé le monde » et en 2009, le IDTechEx (The World's most comprehensive RFID (Radio Frequency IDentification) case studies database)) a scruté que c'est « La technologie qui a réalisé le rêve d'auto-surveiller et de prévenir contre les incendies, les avalanches, les ouragans, les failles des équipements, les accidents de circulation, les hôpitaux et beaucoup d'autres applications sur des zones étendues». Cette technologie révolutionnaire n'est autre que les réseaux de capteurs sans fil (RCSF) ou plus connue sous le nom de wireless sensor networks (WSN) [1].

Depuis leur création, les réseaux de communication sans fil ont connu un succès sans cesse croissant au sein des communautés scientifiques et industrielles [2]. Au cours de son évolution, le paradigme sans fil a vu naître diverses architectures dérivées. Durant cette dernière décennie, une nouvelle architecture a vu le jour : les réseaux de capteurs sans fil. Ce type de réseaux résulte d'une fusion de deux pôles de l'informatique moderne : les systèmes embarqués et les communications sans fil. Ces réseaux sont composés d'un ensemble d'unités de traitements embarquées, appelées "capteurs", communiquant via des liens sans fil. Le but général d'un RCSF est la collecte d'un ensemble de paramètres de l'environnement entourant les capteurs, telles que la température ou la pression de l'atmosphère, afin de les acheminer vers des points de traitement.

Les réseaux de capteurs sans fil (RSCF) exploitent des appareils avec des ressources énergétiques limitées équipés de capteurs afin de récupérer en temps réel des mesures par exemple la température, la radioactivité, ou le CO2. Les réseaux de capteurs sont particulièrement pertinents pour la surveillance, la télémétrie ou la prévention des catastrophes naturelles. Cependant, ce type de réseau pose des problèmes majeurs tels que l'utilisation efficace de ressources énergétiques limitées, la prise en charge transparente de nœuds défaillants sans intervention humaine. L'Internet des Objets ne permettra d'intégrer des réseaux de capteurs autonomes que si les protocoles sont standards et passent à l'échelle.

Au cours de ses cinq ans d'existence, l'organisme industriel s'est fortement engagé dans un soutien indéfectible aux efforts de normalisation menés parallèlement par l'IEEE (Institute of Electrical and Electronics Engineer) et l'IETF (Internet Engineering Task Force) dans le domaine des réseaux de capteurs sur protocole IP. Efforts qui se sont d'abord concrétisés par l'arrivée à maturité du standard 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) qui a réussi à adapter le protocole IPv6 aux communications sans fil entre nœuds à très faible consommation et aux ressources limitées. 6LoWPAN définit en particulier des mécanismes d'encapsulation et de compression d'en-têtes permettant aux paquets IPv6 d'être envoyés ou reçus via le protocole de communication pour réseaux radio IEEE 802.15.4, norme à la base, notamment, de la spécification Zig-Bee. Dans la pratique, la couche d'adaptation 6LoWPAN se glisse entre la couche réseau IPv6 et la couche MAC 802.15.4. L'intégration d'IPv6 dans les réseaux de capteurs est devenue une réalité pour de nombreux industriels [3].

L'objectif principal de ce mémoire est d'établir une connectivité IP entre des capteurs sans-fils en utilisant la librairie Blip.

Ce manuscrit est organisé en trois chapitres à savoir:

Le premier chapitre présente une introduction aux réseaux de capteurs sans fil, leurs architectures, leurs domaines d'application ainsi que leurs principales caractéristiques.

Le deuxième chapitre contient une petite définition sur l'internet des objets. Nous avons commencé par un ensemble de rappels sur IPv4 et nous avons présenté le fonctionnement du protocole internet v6, ainsi que ces principes de base, en introduisant une comparaison entre les deux protocoles (IPv4/IPv6), pour terminer enfin par une idée générale sur 6lowpan.

Le troisième chapitre constitue le cœur de notre travail. Dans ce chapitre nous avons présenté les outils matériels et logiciels nécessaires à la réalisation de notre test, ainsi qu'une architecture complète permettant de réaliser une connectivité IP entre des capteurs sans fil.

Enfin, nous avons conclu notre travail en présentant les résultats obtenus et en donnant quelques perspectives.

CHAPITRE 1

INTRODUCTION AUX RÉSEAUX DE CAPTEURS SANS FIL (RCSF)

Sommaire

1. Introduction

L'essor des technologies sans fil offre aujourd'hui de nouvelles perspectives dans le domaine des télécommunications. En comparaison avec l'environnement filaire, l'environnement sans fil permet aux utilisateurs une souplesse d'accès et une facilité de manipulation des informations à travers des unités de calcul mobiles (PC portable, PDA, capteur…) [4].

La recherche dans le domaine des capteurs est en train de vivre une révolution importante, ouvrant des perspectives d'impacts significatifs dans de nombreux domaines. La plupart du temps, ces capteurs communiquent entre eux en utilisant un protocole propriétaire à l'aide d'une passerelle qui récupère les données et qui les rend disponibles sur le réseau IP.

Dans ce chapitre, nous présentons les réseaux de capteurs sans fil, leurs architectures de communication et leurs applications.

2. Capteur sans fil

Un capteur ou « mote » en anglais est un petit dispositif électronique capable de mesurer une grandeur physique environnementale tel que la température, la pression, l'humidité, etc.., et de la communiquer à un centre de contrôle via une station de base, ses inconvénients sont:

- Faible capacité de calcul.
- Faible capacité de mémoire.
- Faible capacité d'énergie.
- Faible capacité de communication [5].

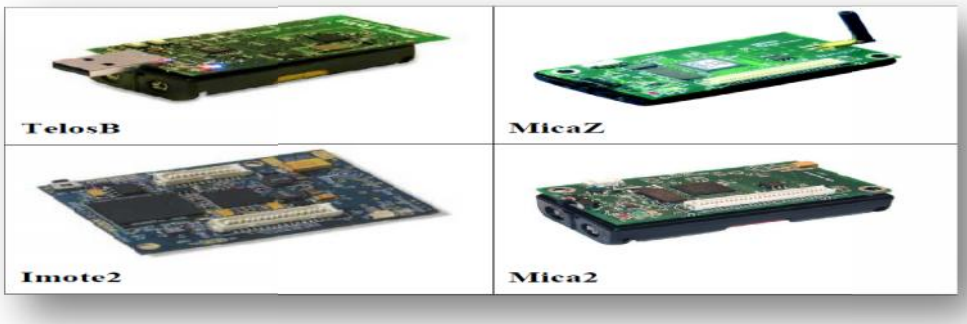

Figure 1. 1 : Quelques modèles de capteurs sans fil [6]

3. Composants d'un capteur sans fil

Un capteur sans fil est doté, principalement, de quatre unités (fig.1.2).

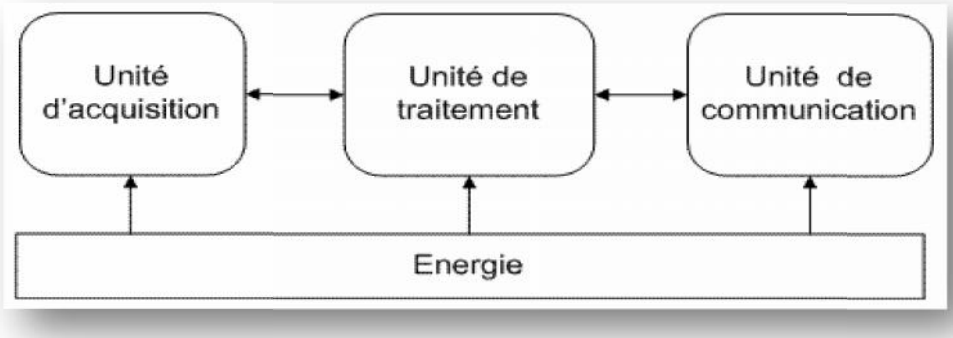

Figure 1. 2 : Composants d'un capteur sans fil [7]

- Unité d'acquisition : composée d'un dispositif qui va obtenir des mesures numériques sur les paramètres environnementaux et les transformer en signaux analogiques, et d'un convertisseur Analogique/Numérique qui va convertir l'information relevée et la transmettre à l'unité de traitement.

- Unité de traitement : composée de deux interfaces, une interface pour l'unité d'acquisition et une interface pour l'unité de transmission. Cette unité est également composée d'un processeur et d'un système d'exploitation spécifique. Elle acquiert les informations en provenance de l'unité d'acquisition et les envois à l'unité de transmission.

- Unité de transmission : responsable de toutes les émissions et réceptions de données via « un médium sans fil » [8].

- Unité de contrôle d'énergie : responsable de la gestion de l'énergie et de l'alimentation de tous les composants du capteur. Elle consiste, généralement, en une batterie qui est limitée et irremplaçable, ce qui a rendu l'énergie comme principale contrainte pour un capteur [7].

Ces capteurs ont 3 fonctions principales : [2]

- Capter des données de type : son, vibration, lumière,...
- Calculer des informations à l'aide de ces valeurs collectées.
- Les communiquer à travers un réseau de capteurs.

4. Types de capteurs

Il existe actuellement un grand nombre de capteurs, avec des fonctionnalités diverses et variées. La plupart de ces capteurs dépendent de l'application pour lesquelles ils ont été conçus (capteurs aquatiques, sous-terrain, etc...).

Figure 1.3 recense les différents composants actuellement disponibles sur le marché. Notons, que bien qu'ils soient différents, ces modèles ont en commun les mêmes composants de base

	Unité de traitement				Unité de transmission	Unité de captage	Unité de puissance
Modèle	Micro-contrôleur	RAM	Flash	EEprom	Type radio		
MICA2 (Crossbow)	ATmega 128L	4 KB	128KB	4 KB	Chipcon CC1000 38kbps	Connecteur pour carte de capteurs externe	2xAA
MICAZ (Crossbow)	ATmega 128L	4 KB	128KB	4 KB	Chipcon CC2420 250kbps	Connecteur pour carte de capteurs externe	2xAA
Imote2 (Crossbow)	Intel PXA271	256KB	32 KB	32KB	Chipcon CC2420 250kbps	Connecteur pour carte de capteurs externe	3xAAA
TeloSB (Crossbow)	TI MSP 430	10KB	48KB	16KB	Chipcon CC2420 250kbps	Connecteur pour carte de capteurs externe	2xAA
TinyNode (Shockfish SA)	TI MSP 430	10KB	48KB	16KB	Semtech XE 1205 153kbps	Connecteur pour carte de capteurs externe	2/3xAA
BTnode3 (ETH)	ATmega 128L	64KB	128KB	4KB	Chipcon CC1000/Bluetooth	Connecteur pour carte de capteurs externe	2xAA
Tmote Sky (Moteiv)	TI MSP 430	10KB	48KB	128KB	Chipcon CC2420	Connecteur pour carte de capteurs externe	2xAA

Figure 1. 3 : Différents types des capteurs [6]

5. Réseaux de capteurs sans fil

5.1. Définition

Un RCSF est un type spécial de réseau ad-hoc défini par un ensemble coopérant de capteurs déployés dans une zone géographique appelée zone de captage ou zone d'intérêt afin de surveiller un phénomène et récolter les données d'une manière autonome [9].

5.2. Architecture d'un RCSF

Un RCSF est composé d'un nombre souvent très important de nœuds qui sont soit posés à un endroit précis, soit dispersés. Ces nœuds capteurs sont organisés en champs « sensor fields » (voir Figure 1.2). Chacun de ces nœuds a la capacité de collecter des données et de les transférer au nœud passerelle ("sink" en anglais ou puits) par l'intermédiaire d'une architecture multi-sauts. Le puits transmet ensuite ces données par internet ou par satellite à l'ordinateur central «Gestionnaire de taches» pour analyser ces données et prendre des décisions [2].

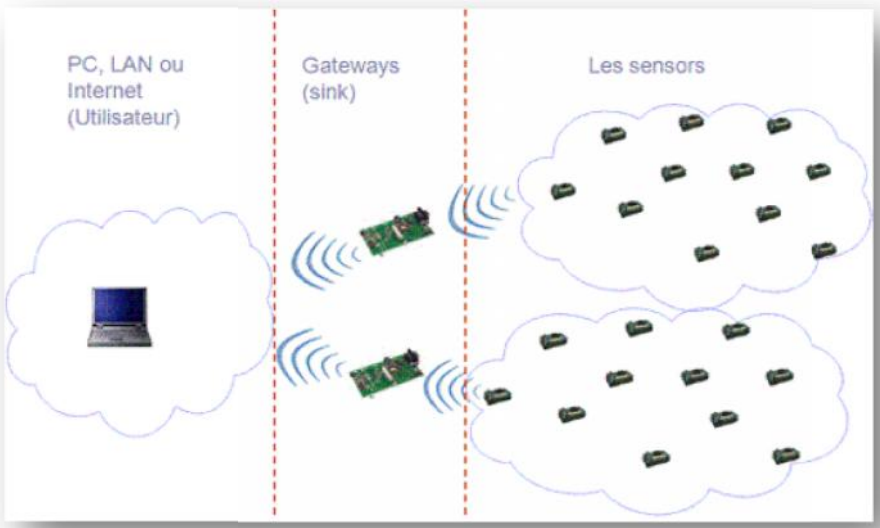

Figure 1. 4 : Architecture d'un réseau de capteurs sans fil [2]

5.3. Caractéristiques des RCSF

Un réseau de capteurs présente les caractéristiques suivantes :

- Énergie limitée : Dans un RCSF l'alimentation de chaque nœud est assurée par une source d'énergie limitée et généralement irremplaçable à cause de l'environnement hostile où il est déployé. De ce fait, la durée de vie d'un RCSF dépend fortement de la conservation d'énergie au niveau de chaque nœud.

- Modèle de communication : Les nœuds dans les RCSF communiquent selon un paradigme plusieurs à un (many to one). En effets, les nœuds capteurs collectent des informations à partir de leur environnement et les envois toutes vers un seul nœud qui représente le centre de traitement.

- Densité de déploiement : Elle est plus élevée dans les RCSF que dans les réseaux Ad Hoc. Le nombre de nœuds capteurs peut atteindre des millions de nœuds pour permettre une meilleure granularité de surveillance. De plus, si plusieurs nœuds capteurs se retrouvent dans une région, un nœud défaillant pourra être remplacé par un autre. Cependant, la densité de déploiement donne naissance à des challenges pour la communication entre les nœuds. En effet, elle provoque des collisions ou des endommagements des paquets transmis.

- Absence d'adressage fixe des nœuds : Les nœuds dans les réseaux sans fil classiques sont identifiés par des adresses IP. Cependant, cette notion n'existe pas dans les RCSF. Ces derniers utilisent un adressage basé sur l'attribut du phénomène capté, on parle donc de l'adressage basé attribut. En effet, les requêtes des utilisateurs ne sont pas généralement destinées à un seul nœud, mais plutôt, à un ensemble de nœuds identifiés par un attribut.

- Limitations de ressources physiques : A cause de la miniaturisation des composants électroniques, les performances des nœuds capteurs sont limitées. Par conséquent, les nœuds capteurs collaborent en traitant partiellement les mesures captées et envoient seulement les résultats à l'utilisateur. Une autre conséquence, ces limitations imposent des portées de transmission réduites contraignant les informations à être relayées de nœud en nœud avant d'atteindre le destinataire. C'est la raison pour laquelle les RCSF adoptent des communications multi sauts [1].

5.4. Domaines d’application

Les capteurs ouvrent de nouveaux horizons à la gestion de l'information. Ils forment une "peau virtuelle" avec le monde réel qui nous informe des événements physiques se déroulant autour de nous. Cela a naturellement attiré plusieurs domaines d'applications qui ont su tirer parti des facilités que les capteurs leur offrent. En voici une liste non exhaustive :

- Le domaine militaire : comme pour beaucoup d’autres domaines, les applications militaires ont été les locomotives de la recherche pour les réseaux de capteurs. Pour les militaires, un réseau de capteurs offre des avantages très précieux. Il s’agit d’un réseau qui s’installe rapidement, dynamiquement et sans aucune infrastructure. Ainsi, il offre un atout de taille pour surveiller les mouvements de l’ennemi, communiquer à bas coût entre les unités avec une logistique peu compliquée [6].

- Le domaine environnemental : la petite taille et les capacités relativement grandes au niveau du calcul et de la communication des capteurs permettent de les placer à des endroits que les humains ne peuvent ou ne veulent pas accéder, comme par exemple les grandes forêts, les volcans, les profondeurs des océans, les régions polaires, ou encore d'autres planètes que la terre [6].

- Les domaines urbains et domotique : le milieu urbain, les capteurs sont déjà utilisés pour la localisation des bus, pour des tickets électroniques et pour la sécurité. Une des applications est la surveillance du trafic routier avec les réseaux de capteurs déployés sur les autoroutes.

- Le domaine médical : En implantant sous la peau de mini capteurs vidéo, on peut recevoir des images en temps réel d'une partie du corps sans aucune chirurgie pendant environ 24h. On peut ainsi surveiller la progression d'une maladie ou la reconstruction d'un muscle [6].

- Le domaine sportif : L'évolution des réseaux de capteurs est utilisée de plus en plus dans le domaine sportif, à savoir les systèmes de surveillance, les systèmes de calcul de trajectoires (comme dans le tennis), systèmes de détection d'erreurs d'arbitrage (comme dans le football indiquent si le balle a franchi la ligne de but) et d'autres applications des réseaux de capteurs sont illustrées dans la figure 1.4 qui suit [9].

Figure 1. 5 : Domaines d'applications de RCSf [1]

6. Conclusion

Dans ce chapitre nous avons parcouru les réseaux de capteurs sans fil, nous avons donné une vue générale en décrivant leurs architecture et leurs applications, puis nous avons décrit les caractéristiques de ces réseaux. Les RCSF est un domaine de recherche très répondu, et devient de plus en plus vaste.

Dans le chapitre suivant nous donnons une petite définition sur l'internet des objets, aussi nous allons présenter quelques protocoles internet, nous commençons par un ensemble de rappels sur IPv4 puis une présentation des principes de base d'IPv6, enfin nous terminons par une idée générale sur le protocole 6lowpan.

CHAPITRE 2

LE CONTEXTE DES SYSTÈMES DISTRIBUÉS DES RCSF DANS UN ENVIRONNEMENT IP

Sommaire

1. Introduction

Les réseaux de capteurs sont l'une des composantes naturelles de l'Internet des Objets. Le déploiement massif des services de communication de machine à machine qui s'appuient sur des réseaux de capteurs (sans fil) est conditionné par l'adoption d'une couche fédératrice IPv6 garante de l'interopérabilité des technologies, mais également par la capacité d'utiliser un protocole de routage performant et susceptible de prendre en compte les caractéristiques (plusieurs milliers de nœuds en réseau, par exemple) et les contraintes (faibles ressources en énergie et en mémoire des composantes réseau) de ce type d'environnement [10].

2. Internet des Objets (IDO)

Il y avait le « web 1.0 » le web des médias, le « web 2.0 », celui des réseaux sociaux, aujourd'hui nous sommes dans le « Web 3.0 » c'est-à-dire l'internet des objets. Ce sont des millions d'objets qui ont une adresse internet et qui vont pouvoir s'interconnecter [11].

2.1. Définition

L'Internet des objets, ou Internet of Things (IoT) en anglais, transformera l'ensemble de la société, y compris nous-mêmes. À première vue, cette affirmation peut paraître exagérée, mais pensez à l'impact qu'a déjà eu Internet sur l'enseignement, les communications, les entreprises, la science, les organismes publics et les hommes. Internet est sans nul doute l'une des inventions les plus importantes et les plus significatives de toute l'histoire de l'humanité [12].

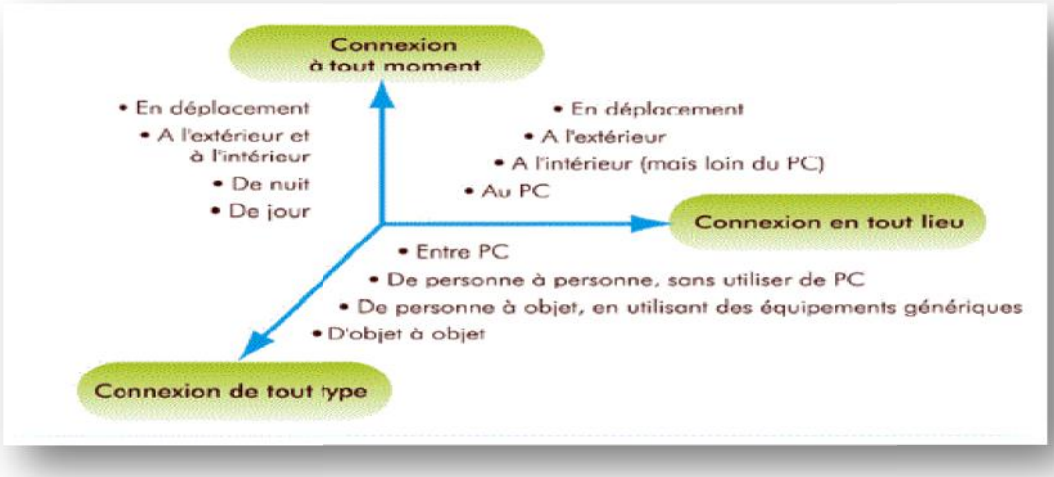

Figure 2. 1 : Internet des objets [13]

Le paradigme de l'Internet des objets réconcilie le virtuel et le réel. En reliant de très nombreux capteurs et objets-interfaces (capables de communiquer sur un réseau) à Internet on ouvre des possibilités très grandes :

- Signaler une personne en détresse.
- Optimiser les processus de production et la chaîne logistique (possibilité de vendre avant de produire).
- Surveiller et piloter les consommations d'électricité et la production d'énergie.
- Réguler le trafic routier. …..

Bien sur ce nouvel Internet implique la multiplication de capteurs, puces, etc qui correspondent à autant d'identifiants. Aucun objet ne peut appartenir et communiquer dans un réseau sans identifiant. A l'heure actuelle on identifie une entité sur un réseau à l'aide d'une adresse IP. Or ces adresses IP sont définies selon le protocole IPv4 et leur nombre est limité. La plupart d'entre elles sont déjà utilisées. Il faut donc un nouveau protocole IP (ou un nouvel identifiant) pour passer à l'Internet des objets. De plus, les objets seront très nombreux, leur coût devra donc être très limité [14].

2.2. Historique

En 2003, la population mondiale s'élevait à environ 6,3 milliards d'individus et 500 millions d'appareils étaient connectés à Internet.3 Le résultat de la division du nombre d'appareils par la population mondiale (0,08) montre qu'il y avait moins d'un appareil connecté par personne. Selon la définition de Cisco IBSG, l'IOT n'existait pas encore en 2003 car le nombre d'objets connectés était relativement faible.

En raison de l'explosion des Smartphones et des tablettes, le nombre d'appareils connectés à Internet a atteint 12,5 milliards en 2010, alors que la population mondiale était de 6,8 milliards. C'est ainsi que le nombre d'appareils connectés par personne est devenu supérieur à 1 (1,84 pour être exact) pour la première fois de l'histoire. Voir Figure 2.2.

En ce qui concerne l'avenir, Cisco IBSG estime que 25 milliards d'appareils seront connectés à Internet d'ici à 2015 et 50 milliards, d'ici à 2020. Il est important de noter que ces estimations ne tiennent pas compte des progrès rapides d'Internet ni des avancées technologiques, mais reposent uniquement sur les faits avérés à l'heure actuelle [12].

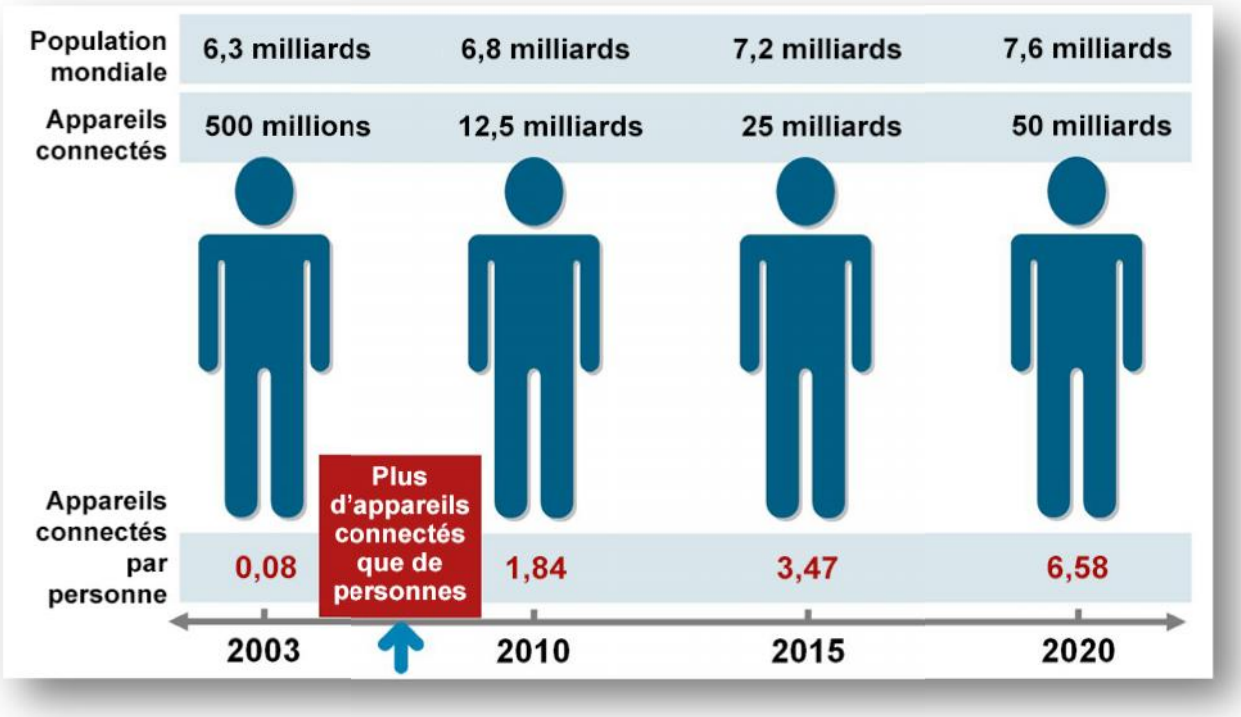

Figure 2. 2 : L'Internet des objets est apparu entre 2008 et 2009 [12]

3. Les protocoles IP

Un protocole de communication est un ensemble de règles et de procédures permettant de définir un type de communication particulier.

3.1. Le protocole IPv4

IPv4 ou « Internet Protocol version 4 » est comme son nom l'indique un protocole qui identifie les adresses dites IP sur internet. Défini dès le début des années 1970 par les créateurs d'Internet. Les adresses IP sont codées sur 32 bits (4 octets) de la forme xxx.xxx.xxx.xxx, Chaque série de xxx correspond à un octet (8 bits) soit un nombre entre 0 et 255. A un moment donné sur internet chaque ordinateur connecté a une adresse IP de cette forme. Par exemple, on peut avoir 85.12.65.124 ou encore 245.111.0.6. Ce protocole permet donc de gérer près de 4 milliards 300 millions d'adresses différentes (2^{32}-2 exactement). A son origine, on pensait que ce serait amplement suffisant pour gérer tous les ordinateurs connectés sur internet mais depuis quelques années, un nouveau protocole IPv6 codé sur 128 bits est en cours d'élaboration car Ipv4 commence à montrer ses limites [15].

3.2. Limites de l'IPv4

IPv4 présente les limites suivantes: [16]

- Épuisement des adresses: Les adresses IP qui risquent d'être rapidement épuisées sont spécifiquement ceux de classes B. C'est pourquoi, on effectue une attribution multiple d'adresses de classe C. Mais ce n'est qu'une solution provisoire.

- Explosion des tables de routage: L'adressage IP est faiblement hiérarchique. Les routeurs des dorsales (Backbones) doivent par conséquence avoir des tables de routages conséquents.

- Absence de type de données: Bien qu'un champ Type de service (TOS) et qu'un champ Options soit présent dans l'IP, le manque de spécifications et l'absence d'implantations dans les routeurs font qu'IP ne peut gérer les priorités (intéressant pour le trafic multimédia), la sécurité, …

- Temps de traitement important: Dans chaque routeur un certain nombre de traitements est effectué pour chaque datagramme: calcul de checksum, calcul de routage... Ceci introduit une gigue importante dans le trafic.

3.3. Pourquoi V6 et non V5?

Dans tout entête IP, les 4 premiers bits sont réservés à la version du protocole. C'est ainsi qu'un numéro de protocole entre 0 et 15 est théoriquement possible. Le 4 est déjà pris pour IPv4. Cependant le 5 est réservé à un autre protocole (le protocole de flux STP). Le numéro libre suivant était donc 6! [17]

3.4. L'IPv6 : la solution aux limites de l'IPv4

Les limites imposées par le protocole IPv4 se font sentir : le stock d'adresses IP autorisé par ce protocole n'est pas infini. Rapidement, un nouveau protocole de substitution est défini par la communauté internationale afin de se substituer à l'IPv4 et de proposer un stock d'adresses : c'est l'IPv6.

La définition de ce nouveau protocole IPv6 a été également une opportunité de corriger certains problèmes inhérents au protocole IPv4. Ces problèmes avaient été mis en exergue par la communauté réseau au cours des dernières années. De nouveaux besoins tels que la

sécurité, la mobilité, une facilitation des mécanismes de configuration sont également apparus et ont pu être pris en compte lors de la standardisation d'IPv6. [18]

3.4.1. Objectifs d'ipv6

Les objectifs principaux de ce nouveau protocole furent de [19] :

- ✓ Supporter des milliards d'ordinateurs, en se libérant de l'inefficacité de l'espace des adresses IP actuelles,
- ✓ Réduire la taille des tables de routage.
- ✓ Simplifier le protocole, pour permettre aux routeurs de router les datagrammes plus rapidement.
- ✓ Fournir une meilleure sécurité (authentification et confidentialité) que l'actuel protocole IP.
- ✓ Accorder plus d'attention au type de service, et notamment aux services associés au trafic temps réel
- ✓ Faciliter la diffusion multidestinataire en permettant de spécifier l'envergure.
- ✓ Donner la possibilité à un ordinateur de se déplacer sans changer son adresse.
- ✓ Permettre au protocole une évolution future,
- ✓ Accorder à l'ancien et au nouveau protocole une coexistence pacifique.

3.4.2. Format des adresses

Les adresses IPv6 sont constituées de 16 octets (128 bits). On dispose ainsi d'environ 3,4 × 1038 adresses, soit plus de 667 millions de milliards d'adresses par millimètre carré de surface terrestre. Elles sont découpées en 8 mots de 16 bits (4 chiffres hexadécimaux) séparés par des « **:** ». En comparaison les adresses IPv4 sont constituées de 4 octets, chaque octet étant noté par sa forme décimale; les différents octets étant séparés par des «.» [18].

Exemple : fe80:0000:0000:0000:0240:96ff:fea7:00d3 est une adresse IPv6

Cette notation pouvant être fastidieuse, les méthodes de simplification suivantes ont été définies :

1. La notation « **::** » permet de représenter plusieurs 0 consécutifs au sein de plusieurs mots de 16 bits. Le nombre de 0 peut être retrouvé en examinant le nombre de mots présents dans l'adresse. Cet élément ne peut être présent qu'une fois au sein de l'adresse.

2. Au sein d'un mot de 16 bits les chiffres hexadécimaux de poids fort positionnés à 0 peuvent être omis.

La méthode de simplification 1 sur l'exemple précédent nous donne fe80::0240:96ff:fea7:00d3.

En appliquant la méthode 2 on obtient l'adresse fe80::240:96ff:fea7::d3, qui est beaucoup plus lisible.

En IPv6 on abandonne le format classique de masque utilisé en IPv4 pour décrire un réseau ou un sous-réseau par le nombre de bits pertinents après le symbole « / ».

Exemple :

- 2a01:e35:2EC0:B6A0::/64 : décrit un réseau IPv6 composé des 64 premiers bits.
- FE80::/64 : décrit également en format simplifié un réseau IPv6 de 64 bits. Il s'agit en fait de FE80:0000::/64 .

Généralement, les 64 premiers bits de l'adresse IPv6 servent à l'adresse de sous-réseau, tandis que les 64 bits suivants identifient l'hôte à l'intérieur du sous-réseau [18].

3.4.3. Adressage IPv6 et nommage

L'évolution la plus visible d'IPv6 concerne l'extension de son espace d'adressage pour palier à la pénurie d'adresse du protocole actuel IPv4 [18].

IPv6 défini 3 type d'adresses :

- **Unicast (point à point) :** destinées à la communication avec une interface unique.
- **Multicast (point à multipoint)** : destinées à la communication avec un groupe d'interfaces.
- **Anycast :** destinées à la communication avec une seule interface d'un groupe donné. Ce type d'adresse indique que le datagramme doit être transmis à un seul membre de ce groupe (par exemple, le plus proche). Ces adresses ne peuvent servir qu'en tant qu'adresses de destination [20].

a. Adressage unicast

Les adresses Unicast sont destinées à la communication avec une interface unique. Ces adresses sont de deux types selon leur portée :

• Les adresses **Lien-local** : destinées à la communication au sein d'un lien.

• Les adresses **globales** : ayant une portée mondiale et destinées aux échanges de l'Internet IPv6.

Similairement à IPv4, on retrouve en plus une adresse de loopback ainsi qu'une adresse indéterminée.

• Adresses de **loopback :** L'adresse de loopback (127.0.0.1 en IPv4) est utilisée pour représenter le nœud lui-même. Elle ne transite jamais sur le réseau. Elle est notée ::1

• Adresses **Indéterminées** : Cette adresse est utilisée par exemple lorsque l'interface n'a pas encore connaissance de son adresse (0.0.0.0 en IPv4). Elle est notée ::

b. Adressage Multicast

En IPv4, on dispose de la notion de broadcast afin de permettre la diffusion de paquets à l'ensemble des interfaces présentes sur un lien. IPv6 raffine cette notion et lui oppose le concept de multicast pour représenter un groupe d'interfaces potentiellement de portée mondiale. Les adresses multicast utilisent le préfixe FF00::/8

Le champ Flag est composé de 4 bits. Les 3 premiers sont réservés et généralement positionnés à 0, le dernier représente la durée de validité de l'adresse et est positionné à 1 si l'adresse est permanente, le cas échéant il est positionné à 0 [18].

Le champ Scope indique la portée de l'adresse selon le tableau 2.1:

valeur	portée
1	Interface local
2	Lien-local exemple fe80 ::64
4	Admin-local
5	Site-local exemple fec0 ::/64
0, 3, F	Réservé
6, 7, A, B, C, D	Non assigné

Tableau 2. 1 : Portée des adresses Multicast [18].

c. Les adresses Anycast

En général, c'est l'interface la plus proche (au sens de la métrique des protocoles de routage : RIPng, OSPF) qui est choisie.

Le principe de l'anycast n'en est encore qu'à son stade de recherche. On ne peut, à ce jour, attribuer une telle adresse qu'à un routeur. Il n'existe, de plus, qu'une seule sorte de groupe qui possède une adresse anycast pour un sous réseau. Un paquet IPv6 ne peur avoir comme adresse source une adresse anycast [21].

d. Adresse particulières

Comme IPv4, le protocole IPv6 défini un certain nombre d'adresses ou de plages d'adresses Dédiées à un usage particulier :

• **::1/128** : la boucle locale

• **FE80** : l'adresse lien-local servant en local à désigner une interface réseau.

• **FF01::** : Nœud local. Un paquet émis sur cette adresse ne quitte jamais l'équipement

• **FF02::1** : Lien local. Sert à désigner tous les nœuds IPv6 situés sur le même lien local que l'interface de connexion. Ils ne doivent pas être routés sur un autre réseau.

• **FF02::2** : Sert à désigner tous les routeurs connectés sur le même lien local que l'interface de connexion.

• **FF02::3** : Sert à désigner tous les hôtes situés sur le lien local.

• **::** désigne l'adresse indéterminée.

• **FF05:: :** Désigne tous les hôtes du réseau local.

• **FEC0::/10** : Adresse de réseau privé [20]

3.4.4. Comparaison entre IPV4 et IPV6

C'est donc lorsqu'on cherche à relier simplement en réseau un grand nombre d'appareils ou de dispositifs et que ceux-ci doivent pouvoir être visibles et directement accessibles depuis l'internet que les avantages d'IPv6 sont les plus manifestes. Une adoption rapide et efficace d'IPv6 permettrait d'innover et de bien se positionner ce qui concerne les progrès futurs de l'internet.

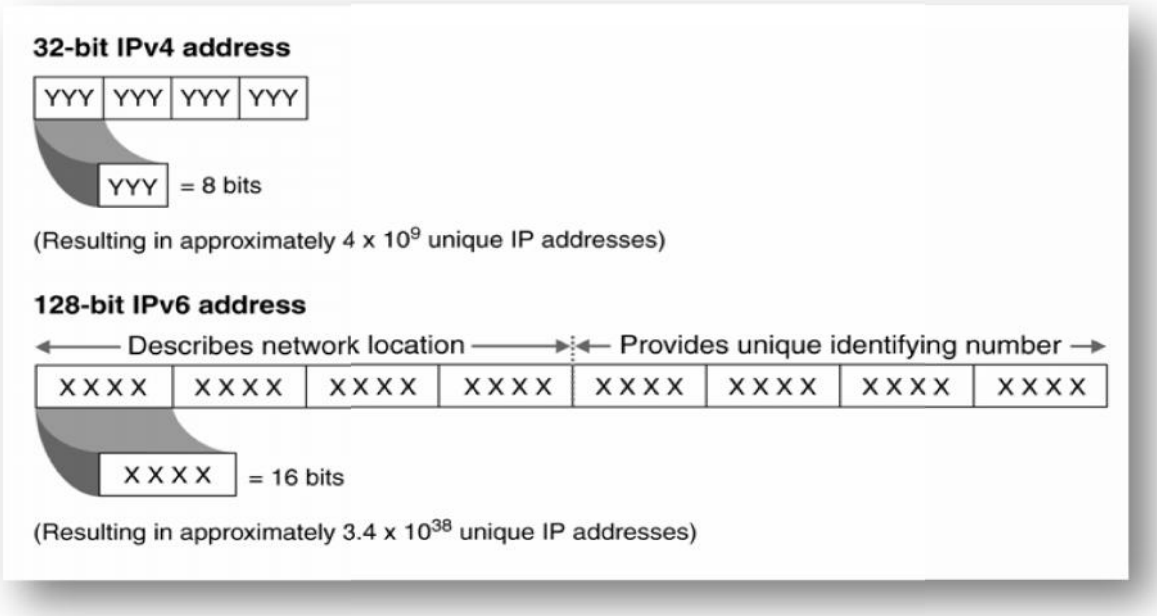

Figure 2. 3 : Comparaison entre adressage ipv4 et ipv6 [22]

Bien que 6 des 12 entêtes IPv4 aient été supprimées, que certains champs aient été transposés sous d'autres noms et enfin que certains nouveaux champs aient été ajoutés pour introduire de nouvelles fonctionnalités, les performances de traitement sont grandement augmentées avec IPv6 (particulièrement pour les architecture 64 bits) [24].

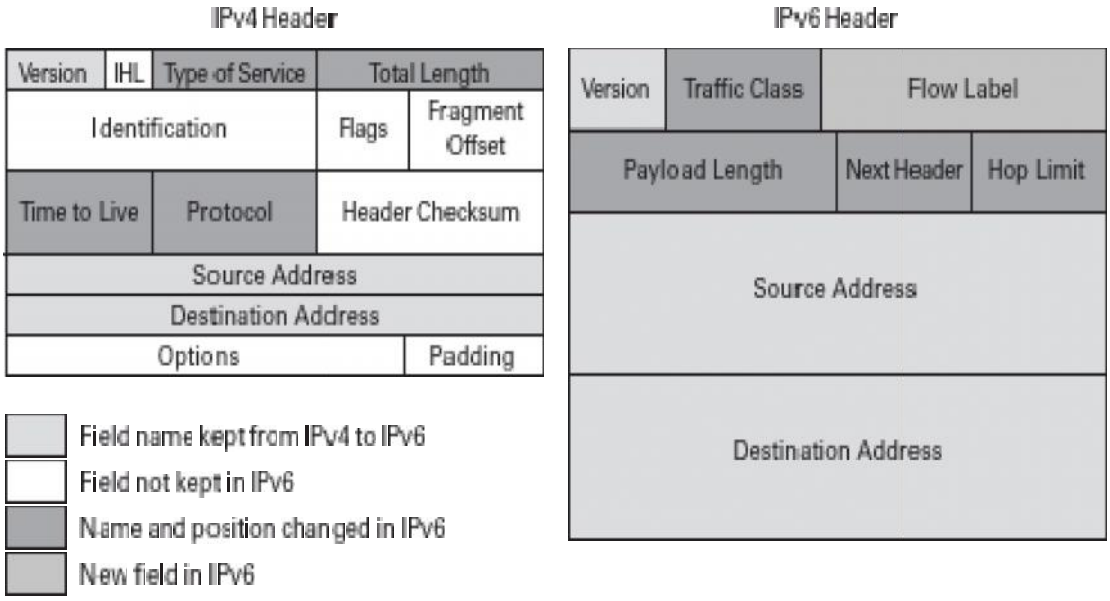

Figure 2. 4 : Comparaison entre les composantes des entêtes IPv4 et IPv6 [23]

La comparaison entre les composants des entêtes IPV4 et IPV6 est illustré dans le tableau 2.1

IPv4	**IPv6**
Header Lenght (IHL)	Supprimé
ToS	Flow Label
ID, Flags et Fragment Offset (FO)	Supprimés
TTL	Hop Limit
Protocol	Next header (mêmes valeurs que dans IPv4)
Header CS	Supprimé
Adresses 32 bits (4octets)	Adresses 128 bits (16 Octets)
Alignement 32 bits	Alignement 64 bits

Tableau 2. 2 : Changement de l'en-tête IPv4 vers IPv6 [21]

Version : 4 bits Décrit la version du protocole. Vaut 6 pour IPv6.

Traffic Class : 8 bits Destiné pour faire de la QoS par priorisation, shaping de trafic … ayant pour but d'offrir des fonctions de qualité de service comme Diffserv.

Flow Label : 20 bits Incomplètement spécifié actuellement. Numéro unique choisi par la source, ayant pour but d'offrir des fonctions de qualité de service comme RSVP.

Payload Length : 16 bits Longueur en octet de la charge utile du paquet. En présence d'extension d'entête, ceux ci sont comptabilisés par ce champ. En IPv4, un champ similaire *Total Length* comptabilise en plus l'entête ce qui finalement est inutile et limite la taille totale de la charge utile du paquet.

Next Header : 8 bits Décrit l'entête de la couche immédiatement supérieure ou la prochaine extension d'entête. Similaire au champ *Protocol* en IPv4.

Hop Limit : 8 bits Décrémenté par chaque routeur présent le long du chemin. Le paquet est jeté si ce champ devient nul permettant ainsi d'éviter que le paquet boucle indéfiniment dans le réseau. Similaire au champ *TTL* en IPv4.

Source Address : 128 bits Contient une adresse *unicast* de l'émetteur du paquet.

Destination Address : 128 bits Contient l'adresse du ou des destinataires du paquet.

L'intégration d'IPv6 dans les réseaux de capteurs est devenue une réalité pour de nombreux industriels. Ces réseaux vont avoir un impact aussi bien sur l'environnement industriel (relevé de compteurs, gestion de l'énergie,...) que sur la domotique. Même si de nombreux protocoles existent déjà, l'utilisation d'IP permet une meilleure interopérabilité et une réduction de coûts liés à l'utilisation de standards [25].

4. Lowpan / IEEE 802.15.4

Un réseau LowPAN c'est un réseau de machines communiquant sans-fil, à faible distance et par radio à l'aide du protocole **802.15.4** qui défini les couches PHY et MAC (Medium Access Control) de données adaptées aux applications à faible débit dont l'autonomie énergétique est une contrainte fort. Ces équipements sont dits "légers" : peu de puissance et de ressources pour un coût faible. Cette dernière caractéristique les rend indispensables à l'Internet des objets qui aura besoin d'un très grand nombre d'objets communiquant sans-fil. Le coût est donc un facteur primordial : il est certain que l'Internet des objets se bâtira sur des LowPAN [14].

Parmi les problèmes des applications sur réseaux 6LoWPAN que l'IETF a définit est que l'utilisation d'UDP dans les LoWPAN est fréquente car TCP est beaucoup plus complexe à mettre en œuvre du fait des limites de certains systèmes et les pertes de paquets sur les LoWPAN.

5. UDP (User Datagram Protocol)

Le protocole UDP (User Datagram Protocol) est une norme TCP/IP obligatoire. Il permet de transporter des datagrammes au-dessus d'IP dans un mode non connecté. C'est un protocole qualifié non fiable. Dans IPv6, le checksum devient obligatoire.

Certains programmes utilisent le protocole UDP à la place de TCP pour transporter rapidement, mais avec une fiabilité non assurée, des volumes de données peu importants entre les hôtes TCP/IP.

UDP fournit un service de datagrammes sans connexion proposant la livraison optimale, ce qui signifie que le protocole UDP ne garantit pas la livraison ou la vérification de la mise en séquence des datagrammes. Un hôte de source nécessitant des communications stables doit

utiliser le protocole TCP ou un programme proposant ses propres services de mise en séquence et d'accusé de réception [27].

Internet est actuellement à un tournant de son histoire. La pénurie d'adresse IP est un problème connu qui dispose d'une solution depuis plus de 20 ans : IPv6. Une tendance, toute récente, est d'amener Internet sur des appareils de plus en plus petits pour pouvoir les contrôler à distance.

Ces deux aspects réunis en un même problème nous donnent comme solution le protocole 6LoWPAN (IPv6 over Low Power Wireless Personnal Area Networks) qui est une couche d'adaptation d'IPv6 pour des systèmes à faibles ressources [24].

6. Protocole 6LowPAN

6.1. Définition

Le 6LoWPAN, ou encore "IPv6 for Low power Wireless Personal Area Networks" rend possible la participation d'objets très limités en ressources à l'Internet des Objets. Ce protocole propose en effet d'étendre l'architecture d'Internet IPv6 aux réseaux de capteurs IEEE 802.15.4, la technologie de communication sans fil à bas débit et basse consommation à la base de standards existants tels que le ZigBee. Le 6LoWPAN se concentre sur la problématique de la transmission de paquets IPv6 sur des trames 802.15.4, en proposant une couche d'adaptation entre couches réseau IPv6 et MAC 802.15.4. En particulier, ce standard proposé par l'IETF définit un format de compression de l'entête IPv6 et permet la fragmentation et réassemblage de paquets IP dépassant les limites imposées par le format de trame 802.15.4 [25]. IPv4 et IPv6 sont efficaces pour la délivrance de données pour les réseaux locaux, les réseaux métropolitains et les réseaux étendus comme l'internet. Cependant, ils sont difficiles à mettre en œuvre dans les capteurs en réseaux et autres systèmes contraints en raison, notamment, de la taille importante des en-têtes. 6LoWPAN devrait permettre à IPv6 d'intégrer ces matériels informatiques contraints et les réseaux qui les interconnectent [28].

6.2. Pourquoi 6LoWPAN?

Les avantages d'IP sont nombreux [29]:

- Interopérabilité extensive (WiFi, Ethernet,GPRS, ATM,...).
- Sécurité : authentification, pare-feux,.
- Adressage, nommage, routage éprouves.
- Services réseau de haut niveau: équilibrage de la charge, cache, mobilité, NAT.
- Services applicatifs de haut niveau: HTTP/XML/HTTP/FTP/SOAP/REST.
- Outils de supervision réseau: ping, SNMP, Trace route.

L'intérêt de 6LoWPAN est [30]:

- Ouvert, durée de vie longue, standards fiables
- Intégration transparente d'Internet
- Stabilité du réseau
- Passage à l'échelle
- Communication de bout-en-bout

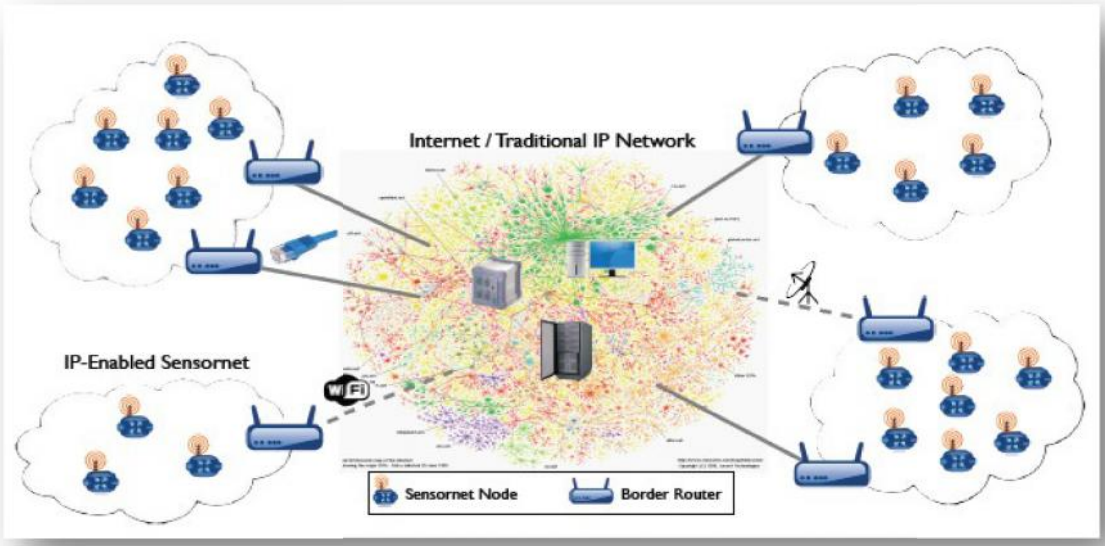

Figure 2. 5 : Relier Internet et un réseau de capteur [29]

6.3. Pourquoi utilise IPv6 et non IPv4?

6LoWPAN soutient juste IPv6 car ce dernier tire largement parti de l'expérience acquise par IPv4. Rationalisation de l'adressage et du routage, auto configuration des équipements sont autant d'atouts. IPv6 assure ensuite la compatibilité avec IPv4 [29].

6.4. Positionnement de La couche 6LOWPAN dans la pile protocolaire

La couche d'adaptation 6LoWPAN se glisse entre la couche réseau IPv6 et la couche MAC 802.15.4. Voir Figure 2.5 :

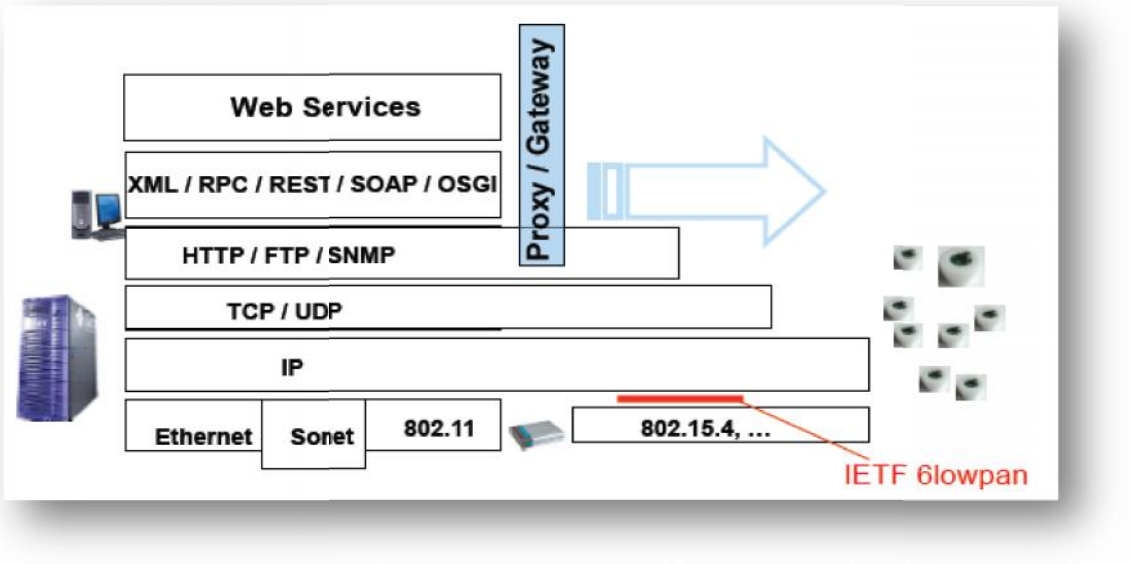

Figure 2. 6 : positionnement dans la pile protocolaire [30]

La technologie 6LoWPAN a réussi à adapter le protocole IPv6 aux communications radio compatibles 802.15.4 entre nœuds à très faible consommation et aux ressources limitées. Mais 6LoWPAN intéresse également les communications CPL (communication par courants porteurs en ligne) à bas débit sur lignes d'électricité, notamment dans les applications de comptage d'énergie intelligent [3].

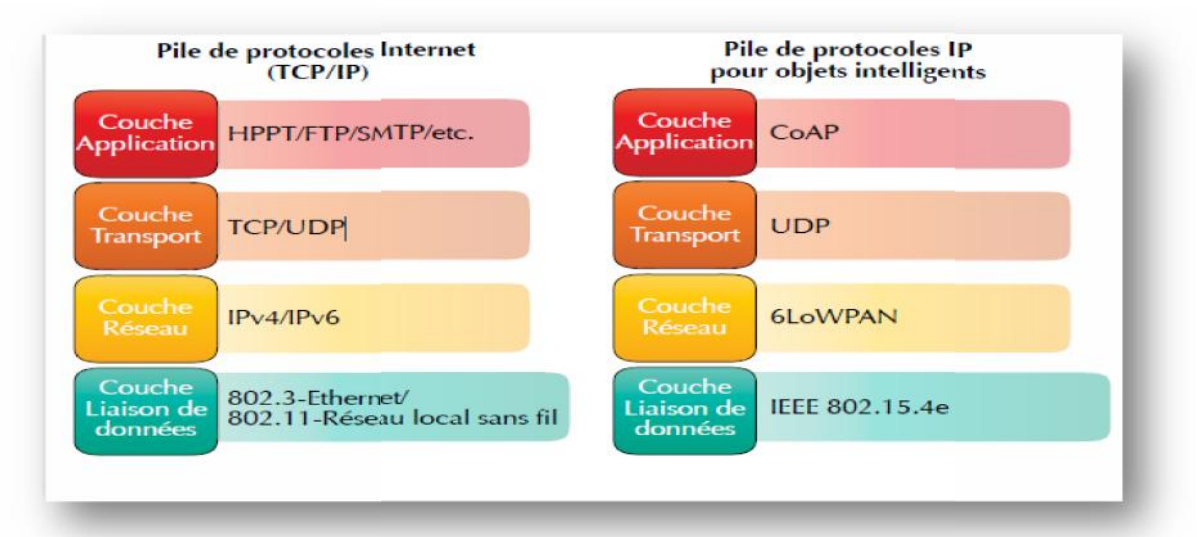

Figure 2. 7 : Comparaison de la pile TCP/IP traditionnelle et de la pile IP pour objets intelligents [3]

6.5. Caractéristique de 6LOWPAN

La propagation entre les différents éléments du réseau est totalement transparente (le protocole "6LowPAN" prenant en charge toutes ces fonctionnalités). Ainsi les données seront automatiquement relayées d'un point à un autre du réseau en nous permettant de créer des réseaux très complexes et étendus tout en augmentant la portée d'action des éléments. Par exemple un capteur de température placé dans le sous-sol d'un bâtiment pourra communiquer avec le système de régulation de la chaufferie placé au dernier étage du même bâtiment (à condition d'avoir pris soin de placer différents modules "Router" à tous les étages intermédiaires) [30].

Caractéristiques générales du protocole "6LoWPAN"	
Fréquences de travail	16 canaux en bande 2,4 GHz
Débit de communication	Jusqu'à 250 Kbps
Topologies supportées	Point-to-point, Star, Tree
Taille max. du réseau	100 nodes (topologie tree)
Gestion réseau	Fin-à-Fin (End-to-end) message d'acquittement La formation de voie automatique et la réparation

Tableau 2. 3 : Caractéristiques générales du 6lOWPAN [30]

7. Conclusion

Un réseau de capteurs est dit connecté si et seulement si, il existe au moins une route entre chaque paire de nœuds.

Dans ce chapitre nous avons commencé par un ensemble de rappels sur IPv4 et nous avons présenté le fonctionnement du protocole internet v6, ainsi que ces principes de base, en introduisant une comparaison entre les deux protocoles (IPv4/IPv6), pour terminer enfin par une idée générale sur 6lowpan.

CHAPITRE 3

MISE EN ŒUVRE DE LA CONNECTIVITÉ IP

Sommaire

1. Introduction

L'avantage de l'IP dans le domaine des RCSF est de pouvoir récupérer les informations émises par le ou les capteurs choisis (connaissant leur adresse IP) et d'accéder à ce réseau depuis internet dont l'Objectif est de simplifier le développement de produits connectables à des réseaux de capteurs sans fil tout-IP et plus globalement, à l'Internet des objets. (Figure (3.1)).

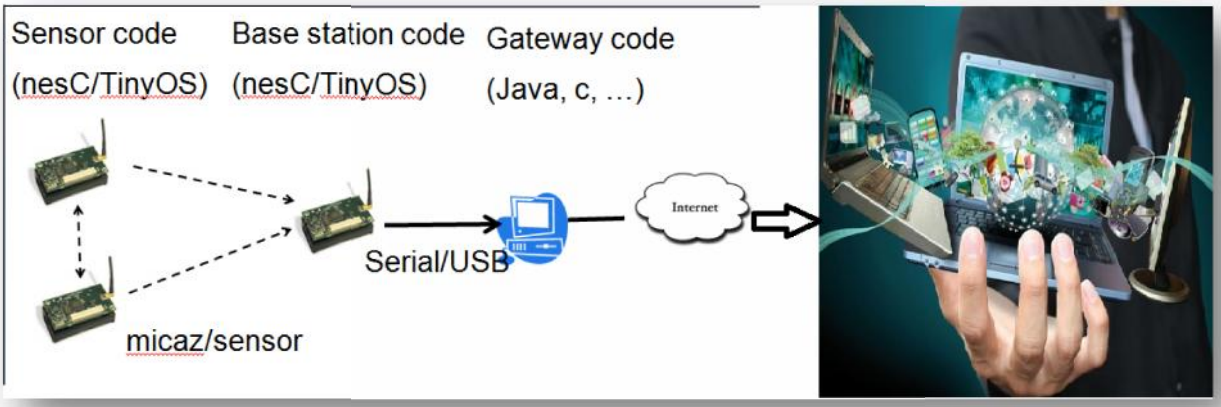

Figure 3. 1 : L'objectif de la connectivité IP dans les RCSF

Dans ce chapitre, nous avons configuré et testé la connectivité IP entre des capteurs sans-fil en utilisant la librairie Blip aussi nous avons capturé et analysé les paquets UDP avec le logiciel wireshark.

Ce chapitre sera divisé en trois parties principales :

Nous présenterons dans la première une description du matériel ainsi que l'environnement logiciel utilisé.

La deuxième partie explique pas à pas le test d'une connectivité IP entre Telosb.

La troisième partie capture et analyse les paquets avec le logiciel wireshark.

2. Environnement de travail

Le modèle de capteurs que nous avons utilisé lors de ce projet est le Telosb (voir la figure 3.2) de la marque Crossbow. D'autres modèles existent chez ce fabriquant tel que le Mica2, MicaZ ou l'Imote2.

2.1. Capteur telosb

La plate-forme TelosB a été élaborée et publiée à la communauté scientifique par l'université Berkeley. Cette plate-forme offre une faible consommation d'énergie, elle est compatible avec la distribution open-source de TinyOs. Alimenté par deux piles AA (1.5 V). Ce type de nœud peut être utilisé dans les applications suivantes [31]:

- Plate-forme à faible puissance pour le développement de la recherche.

- Expérimentation des réseaux de capteurs sans fil.

Figure 3. 2 : Capteur telosb

Dans notre projet nous utilisons une image VM VirtualBox-4.3.12-93733-Win d'une distribution Ubuntu 14.04 disposant d'un environnement TinyOS 2.1.2 qui utilise le langage NesC, nous utilisons aussi une pile IP: blip2.0 pour une connectivité IPv6. Les étapes d'installations du système sont détaillées ci-dessous.

2.2. VirtualBox

C'est un logiciel qui permet de lancer des machines virtuelles, ainsi que l'installation d'un très grand nombre d'OS Guest, disponible sous Linux, MacOS et Windows, il est présenté en deux versions [32]:

✗ Version de base à usage personnel ou éducatif (PUEL) mais payante pour les professionnels.

✗ Version Open Source (OSE).

2.3. Tinyos

TinyOS est un système d'exploitation intégré, modulaire, destiné aux réseaux de capteurs miniatures. Cette plate-forme logicielle ouverte et une série d'outils développés par l'Université de Berkeley est enrichie par une multitude d'utilisateurs. En effet, TinyOS est le plus répandu des OS pour les réseaux de capteurs sans-fil. Cet OS est capable d'intégrer très rapidement les innovations en relation avec l'avancement des applications et des réseaux eux même tout en minimisant la taille du code source en raison des problèmes inhérents de mémoire dans les réseaux de capteurs. TinyOS est en grande partie écrit en C mais on peut très facilement créer des applications personnalisées en langages C, NesC, et Java. Il peut être installé à partir d'un environnement Windows ou bien Linux [2].

2.4. NesC

C’est un langage orienté composant, syntaxiquement proche du C conçu pour incarner les concepts de structure et le modèle d’exécution de TinyOS.

Le langage nesC est le langage utilisé par TinyOS, il permet de déclarer deux types de composants [33] :

Les modules, contenant le code d'un composant.

Les configurations qui permettent de faire le lien entre différents modules.

Les interfaces décrivent les commandes et événements proposés par les composants. Il est possible de les redéfinir.

Un autre grand intérêt à utiliser TinyOS, est sa bibliothèque de composants très complète implémentant des protocoles réseaux, des pilotes de capteur, des outils de capture, et plus particulièrement intéressante pour notre travail, **une pile IP** : **Blip 2.0**.

2.5. Blip

Blip, conçu par Berkeley, est l'implémentation dans TinyOS d'un certain nombre de protocoles base IP [34], dans notre cas nous utiliserons Blip v2.0 pour une connectivité IPv6. TinyOS et Blip donnent la possibilité de créer un réseau IP multi-sauts entre différents capteurs utilisant des protocoles de communication différent. En raison de l'évolution rapide de l'IETF et des normes IEEE, Blip n'est actuellement pas entièrement conforme aux normes, mais offre une importante interopérabilité avec d’autres réseaux IP.

Enfin nous avons installé wireshark au niveau du poste de contrôle pour communiquer avec les capteurs et faire capturer et analyser les paquets.

2.6. Wireshark

Wireshark est un logiciel d'analyse réseau (sniffer) qui permet de visualiser l'ensemble des données transitant sur la machine qui l'exécute, et d'obtenir des informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau PCAP (packet capture), puis regroupés en blocs d'informations et analysés par le logiciel. La dernière version de Wireshark est disponible en téléchargement sur www.wireshark.org [35].

3. Mise en place de la plateforme

La mise en place de la plateforme nécessite deux étapes: l'installation logicielle et l'installation matérielle.

- Installation logicielle : tout d'abord, on a commencé par l'installation de TinyOs 2.1.2 dans Ubuntu 14.04 ce qui nous a pris beaucoup de temps, ensuite nous avons essayé de se familiariser avec les capteurs telosb et le langage NesC, enfin nous avons installé le logiciel wireshark pour capturer et analyser les paquets.

- Installation matérielle : dans notre cas, nous avons utilisé 3 capteurs dont chacun à un rôle bien particulier, une station de base reliée à l'ordinateur via un câble USB comme s'est illustré dans la figure 3.3, et les 2 autres TelosB communiquent avec la station de base via une liaison sans fil alimentés par deux piles AA (1.5 V).

Figure 3. 3 : Environnements de travail

3.1. Architecture du réseau à tester

La configuration et le test de la connectivité IP devrait répondre à quatre impératifs voir figure (3.4):

- Installation et configuration du routeur de bord.
- Installation d'un (des) nœud (s).
- Test de la communication IP.
- capture et analyse avec le logiciel wireshark.

L'utilisation de la librairie Blip doit être déclarée lors de la compilation. La pile IP est chargée au démarrage du routeur sur la machine, elle comprend notamment son adresse IPv6 et le canal sur lequel vont communiquer les capteurs.

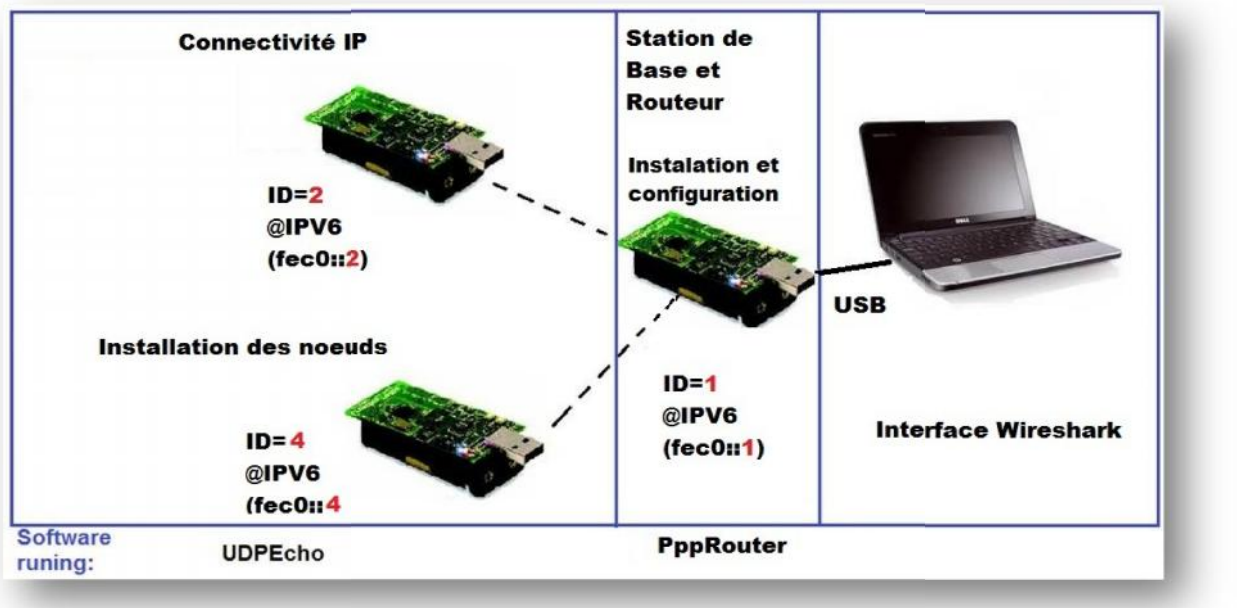

Figure 3. 4 : Architecture de sous-réseau IPV6 basé Blip

3.2. Structure d'adressage

La pile IP fournit la couche réseau une interface de datagramme IPv6.

Afin de pouvoir programmer des sockets, deux structures de données sont très importantes :

{struct in6_addr qui définit le datagramme IP.

{struct sockaddr_in6 qui inclut 'struct in6_addr' et le port afin de définir une socket.

Socket : Outil de communication pour échanger des données entre un client et un serveur en utilisant l'interface de transport (TCP-UDP). Les sockets se situent juste au-dessus de la couche transport du modèle OSI (via le modèle UDP ou TCP).

Exemple : Mettre en place un sockaddr_in6 pour pointer vers FF02 :: 5, le port 10000

```
{
   struct sockaddr_in6 sa6;
   inet_pton6("ff02::5", &sa6.sin6_addr);
   sa6.sin6_port = htons(10000);
 }
```

Blip utilise le socket UDP comme un service de base de transport de l'application.
L'interface UDP est située dans :

```
tos/lib/net/blip/interfaces/UDP.nc
```

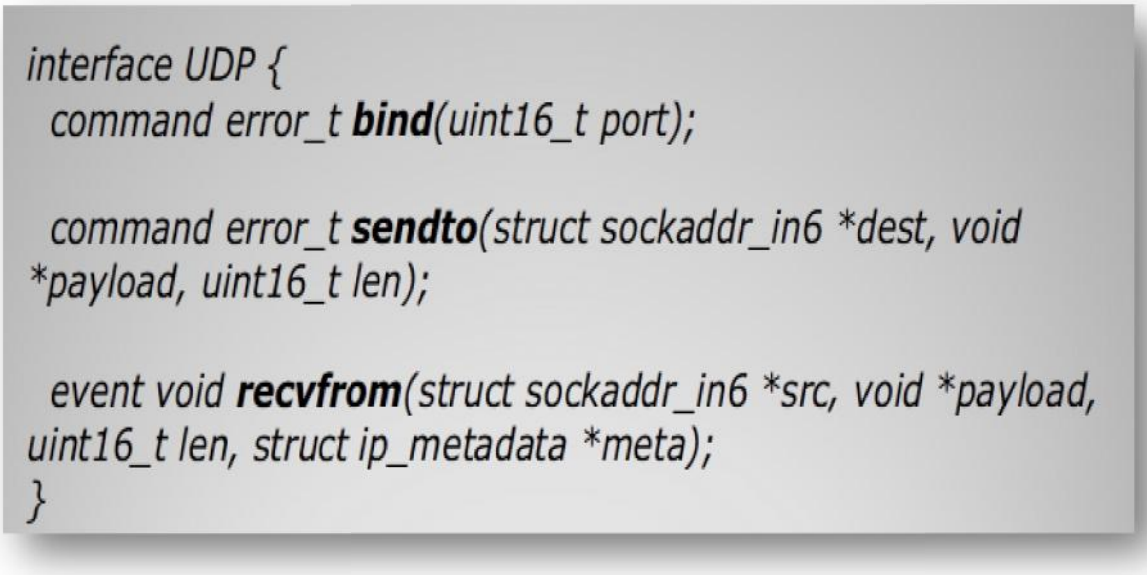

Figure 3. 5 : Interface UDP

Bind : commande pour ouvrir un port et commencer à écouter directement.
Sendto : commande pour envoyer un message.
Recvfrom : notification quand il y a un nouveau message reçu.

3.3. Configuration IPv6 dans Blip 2.0

Dans notre projet, nous avons attribué l'adresse IPv6 statique au moment de la compilation. Par défaut, chaque capteur se configure avec trois adresses: deux adresses lien-local et une adresse globale sur le préfixe fec0::/64. Un adressage statique est sélectionné en définissant la macro IN6_PREFIX au moment de la compilation; ce paramètre est réglé par défaut pour PppRouter et UDPEcho. Une adresse globale est configurée en utilisant le préfixe défini lors de la compilation (IN6_PREFIX). Le préfixe par défaut est fec0::/64, si l'ID de nœud est 1, l'adresse IPv6 est fec0::1.

3.4. Outils d'application utilisés dans Linux

- **Ping**: Ping est un utilitaire d'administration de réseau informatique utilisé pour tester l'accessibilité d'un hôte sur un protocole Internet (IP).
- **Netcat**: Netcat, ou "nc" est un utilitaire Linux simple qui lit et écrit des données à travers les connexions réseau (table de routage).

4. Étapes du Test de la connectivité

La nouvelle version Blip est structurellement similaire à Blip 1.0 sauf que la station de base agit comme un routeur entre le réseau 802.15.4 et une liaison série à un serveur. D'autres nœuds envoient des paquets qui sont reçus par le routeur. La station de base est une application par défaut du routeur appelé '' PppRouter ''.

Avant de commencer les étapes, nous devrions avoir un environnement de travail de TinyOS installé sur une machine Linux, aussi faire la mis à jour de notre chaîne d'outils ; il est particulièrement important que nous utilisons msp430-gcc 4.5.3, puisque c'est la version testée. Il contient également un optimiseur considérablement amélioré qui est nécessaire pour obtenir le code de routeur. La première étape de l'exécution d'un sous-réseau Blip est d'installer un PppRouter connecté à l'aide du démon Linux ppp.

4.1. Étape 1 : installation et configuration du routeur de bord

Avant de compiler et d'installer le routeur de bord, nous devons tester si les capteurs ont été bien détecté et reconnu par le système. Entrez la commande motelist pour lister tous les capteurs branchés : comme le montre la figure 3.10.

Pour changer les droits d'accès on utilise la commande suivante :

```
sudo chmod 666 /dev/ttyUSB0
```

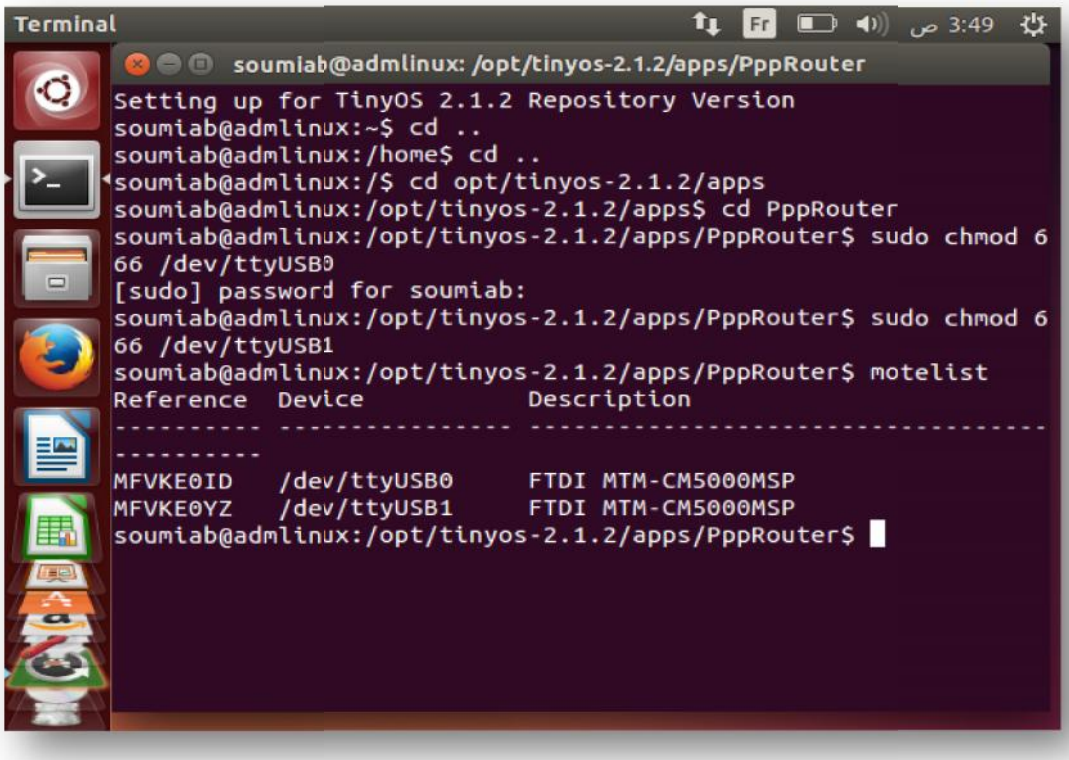

Figure 3. 6 : Vérification du branchement de capteur

Installation de Blip 2.0 sur PppRouterC qui est une application qui dispose de deux interfaces: L'une est une liaison série entre le routeur périphérique et l'ordinateur portable, qui est utilisé comme interface d'écoute pour PPP Wireshark et l'autre est l'interface 6LoWPAN pour la communication sur IEEE 802.15.4. Il ressemble à une «passerelle» pour le réseau de sous-réseau. La figure 3.7 montre les commandes associées:

```
$ cd $TOSROOT/apps/PppRouter
$ make telosb blip install
(L'ID de la station est égale à 1 par défaut)
```

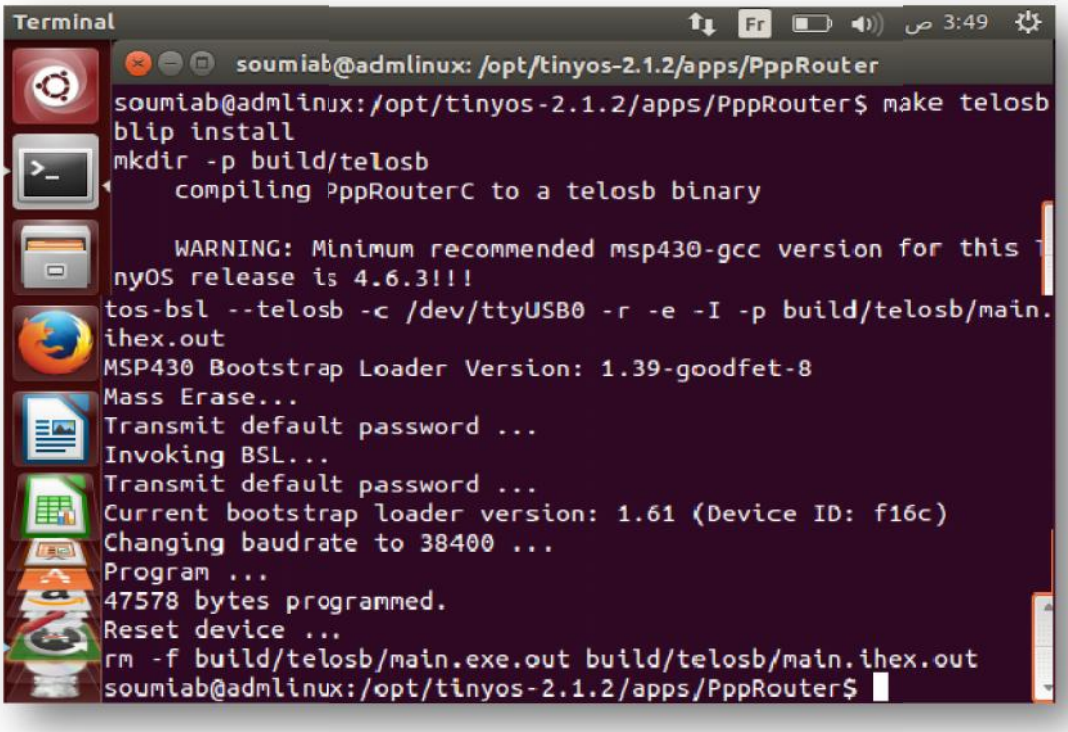

Figure 3. 7 : Installation du routeur de bord

On a connecté « PPP (Point-to-Point Protocol) » avec le nœud précédent (ID=1), pour cela on a affecté deux adresses statiques :: 23 et :: 24 l'une pour la station de base et l'autre pour le routeur. Voir la figure 3.8.

Blip 2.0 utilise " PPP " pour se connecter au réseau 802.15.4. Ceci est utile car il permet de connecter un seul ordinateur à plusieurs réseaux.

Pour lancer la connexion on exécute cette commande:

```
$ pppd debug passive noauth nodetach 115200 /dev/ttyUSB0 nocrtscts
nocdtrcts lcp-echo-interval 0 noccp noip ipv6 ::23,::24
```

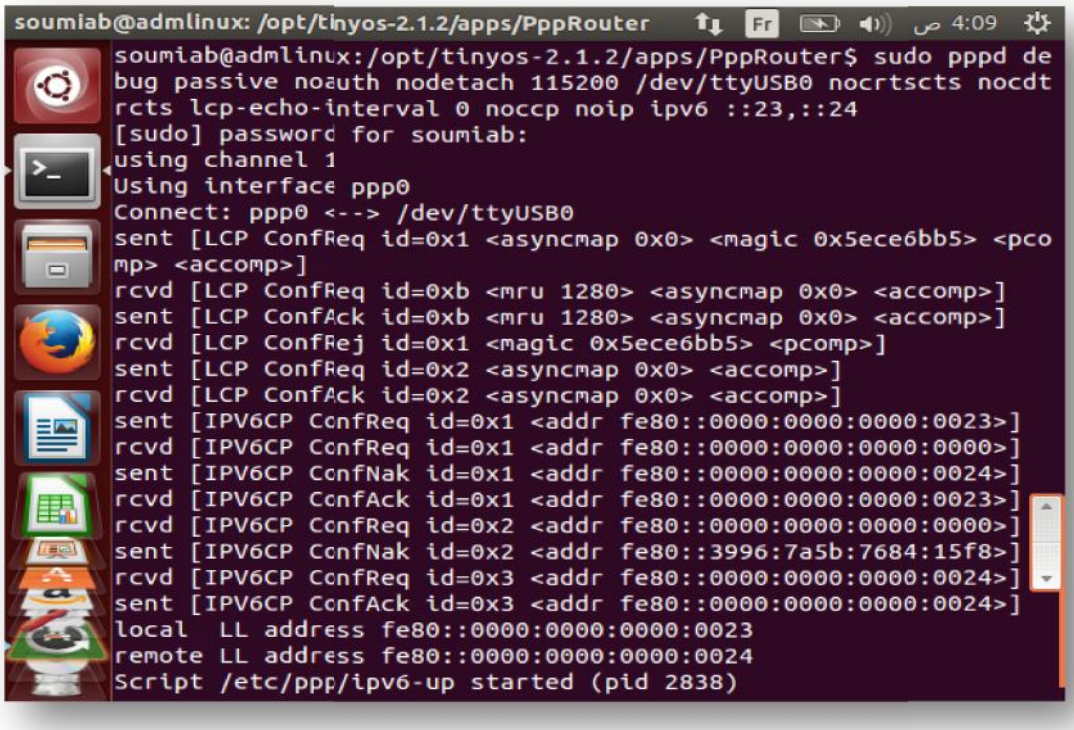

Figure 3. 8 : Connexion entre PPP0 et le routeur de bord

Dans un autre terminal on a exécuté la commande suivante pour donner à notre ordinateur une adresse IPv6 sur le même préfixe:

```
$ ifconfig ppp0 add fec0::100/64
```

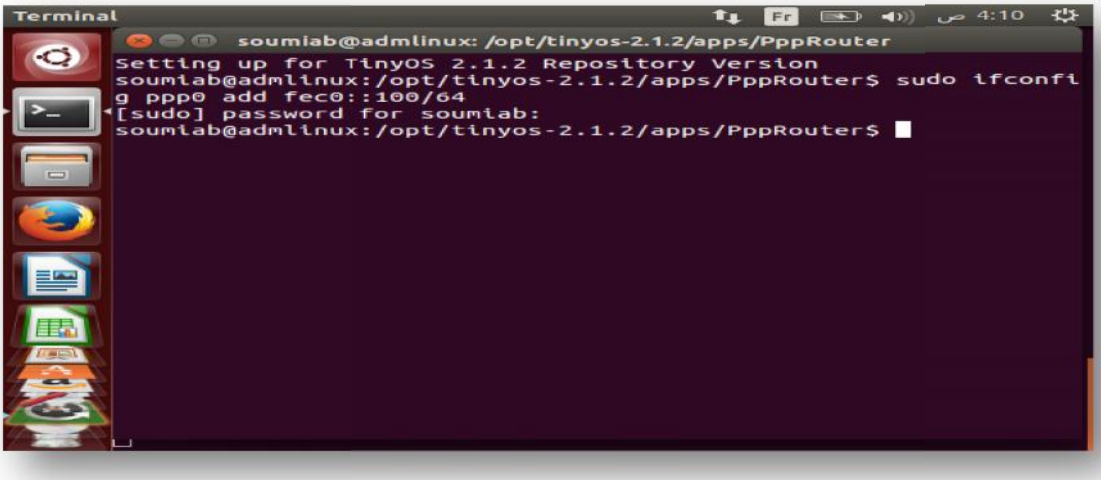

Figure 3. 9 : Configuration du PppRouter

4.2. Étape2 : installation du programme UDPEcho sur plusieurs nœuds

« Echo » est un message ICMP utilisé pour tester la connectivité et le délai de transmission entre deux adresses IP. Il est notamment utilisé par la commande ping.

Après l'installation et la configuration du routeur de bord et la mise en place d'une connexion PPP, nous avons installé le nœud de capteurs sans fil, pour cela TinyOS fournit une application de test dans le dossier /opt/tinyos-2.1.2/apps/UDPEcho. Cette application utilise Blip 2.0 elle permet notamment de tester le ping, afin de voir si le nœud est bien dans le réseau. On a Flashé donc les capteurs (ID=2) et (ID=4) comme précédemment mais avec le programme UDPEcho, Voir Figure 3.10.

```
$ cd $TOSROOT/apps/UDPEcho
$ make telosb blip install.ID bsl,/dev/ttyUSB1 ( ID=2 et 4 dans notre cas )
```

L'**ID** est l'identifiant du nœud, il doit être unique. Il est par défaut **« 1 »** s'il n'est pas précisé lors de l'installation.

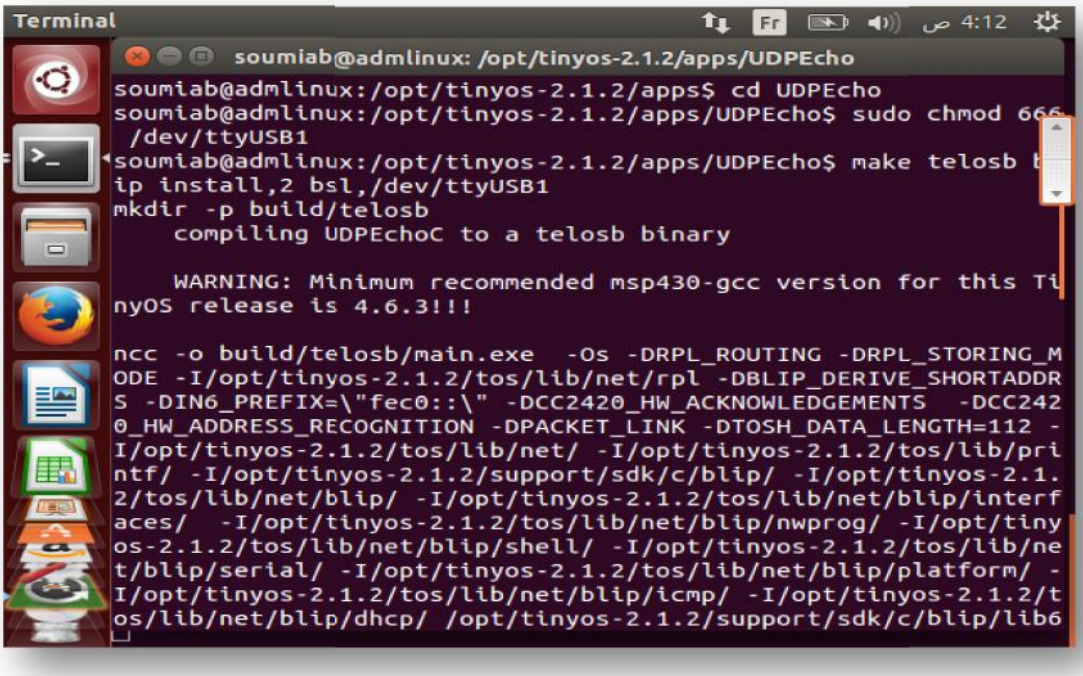

Figure 3. 10 : Installation de nœud (ID=2)

4.3. Étape3 : Test de la communication IP

Maintenant que le routeur de bord et les deux nœuds sont installés, on doit assurer d'avoir lancé le routeur. Puis tester la communication IP avec le capteur en utilisant la commande ping6. Voir le résultat sur la Figure 3.11.

```
$ ping6 fec0::2
```

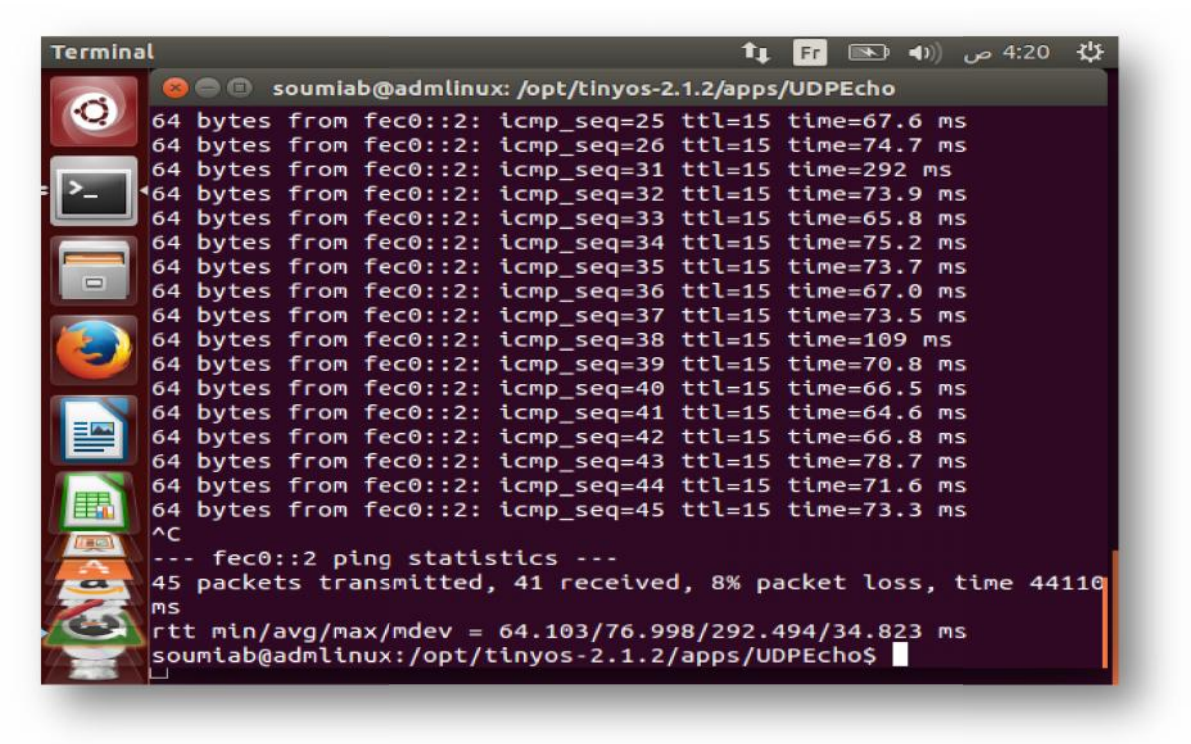

Figure 3. 11 : Test du ping entre le capteur et la station de base

A partir de maintenant, nous pouvons inspecter la table de routage d'un nœud, nous pouvons également utiliser le netcat6 ou (nc6) outil utilitaire pour initialiser le service d'écho UDP dans n'importe quel nœud dont nous avons besoin. L'exemple illustré dans figure 3.12.

```
$ nc6 -u fec0::2 2000
Route
Destination                gateway          iface
::/0              fe80::22:ff:fe00:1               pan
```

```
Ping6 ff02::1
```

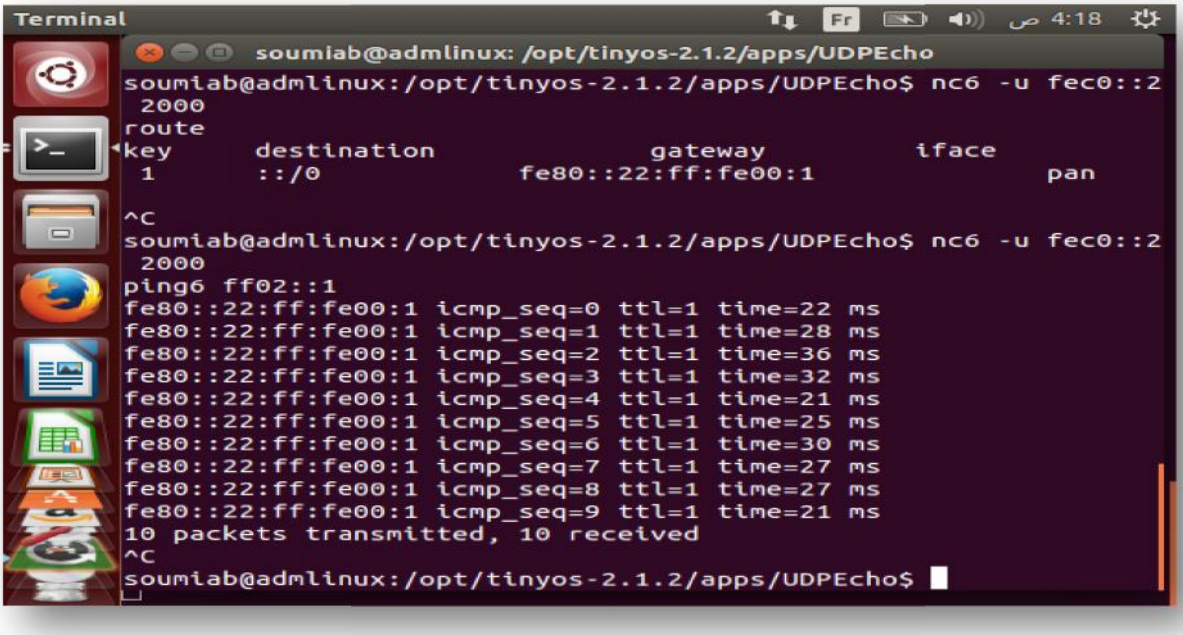

Figure 3. 12 : Table de routage et initialisation du service « echo »

Comme vous pouvez le voir, le Protocole de routage a provisionné une route par défaut via le routeur de bord PPP. Pour plus de détail, vous pouvez faire un ping de tous les nœuds par exemple Figure 3.13.

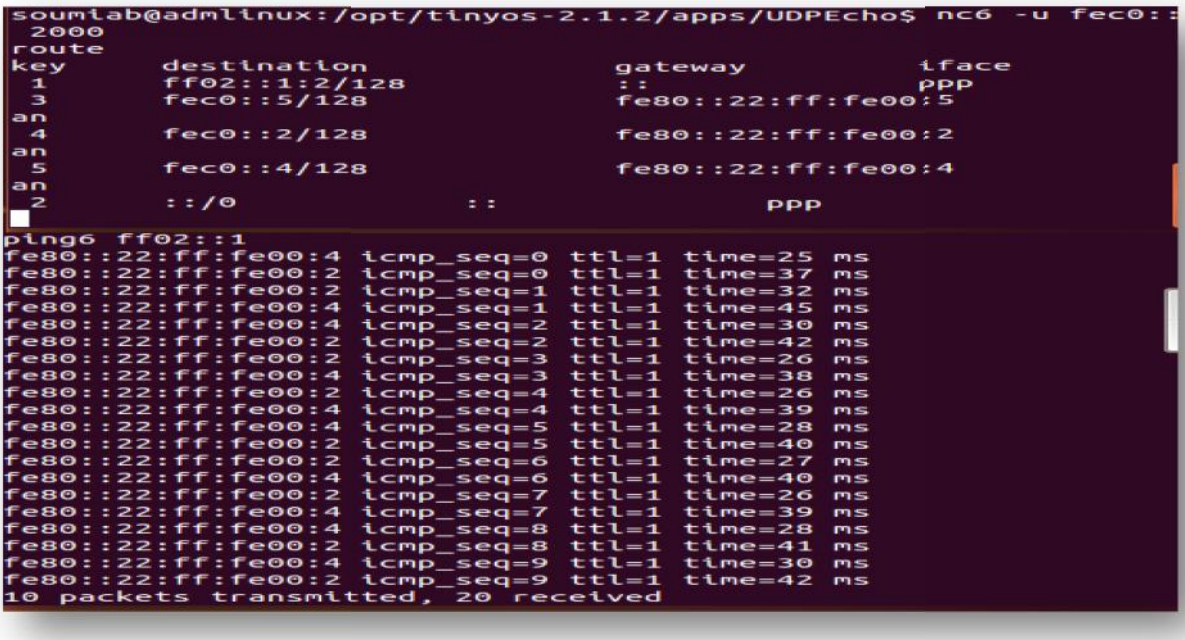

Figure 3. 13 : Table de routage et test du ping après l'installation de tous les nœuds

5. Capture et analyse avec le logiciel wireshark

Wireshark permet d'analyser un trafic enregistré dans un fichier annexe, mais également et surtout le trafic en direct sur des interfaces réseau. Cette seconde fonction nécessite de posséder les droits administrateurs, ou d'appartenir à un groupe possédant ces droits [35].

De nombreuses distributions linux incluent Wireshark dans leur gestionnaire de paquet. Pour installer le logiciel sous ubuntu on tapera simplement la commande :

```
Sudo apt-get install wireshark
```

5.1. Capture

Enfin, nous avons capturé les paquets UDP du nœud de serveur d'écho en utilisant le logiciel wireshark. Voir la figure 3.14, les paquets sont émis à partir du nœud 4.

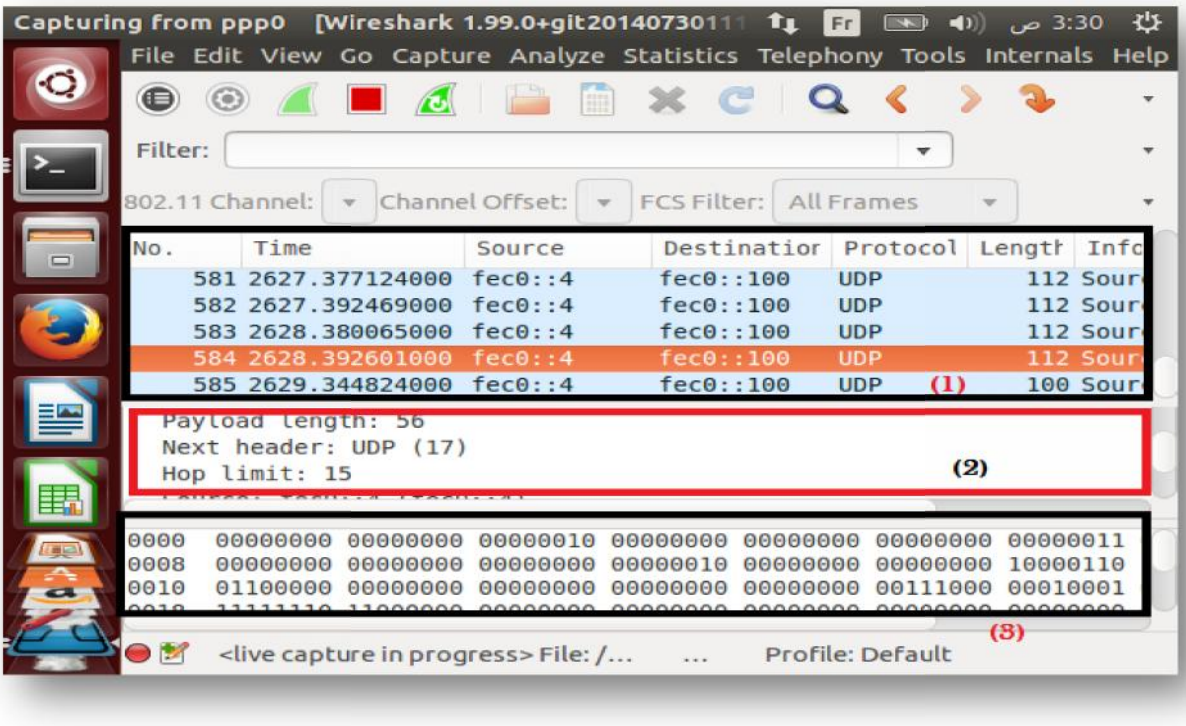

Figure 3. 14 : Interface de l'analyseur

L'interface de l'analyseur est découpée en trois zones :

• **Zone supérieure, numérotée (1)** sur Figure 3.14: liste de l'ensemble des paquets capturés [35].

• **Zone centrale, numérotée (2)** sur Figure 3.14 : affiche le détail d'un paquet sélectionné dans la liste des paquets de la zone supérieure. Les informations présentées y sont de loin les plus pertinentes, puisqu'il est possible de visualiser aisément les différents en-têtes résultant de l'encapsulation d'un message [35].

• **Zone inférieure, numérotée (3)** sur Figure 3.14 : présente l'ensemble du paquet sous forme octale et ASCII. Ces octets contiennent les en-têtes des différentes couches de l'architecture TCP/IP ainsi que les données transmises par le processus à l'origine du message [35].

5.2. Analyse d'un paquet

Il existe une fonction permettant par exemple d'afficher des graphes. Pour cela il faut se rendre dans le menu **Statistics > IO Graphs**.
Par défaut, c'est le filtre d'affichage actuel qui sera affiché avec la couleur noire correspondant au graphe n°1. L'échelle en ordonnée est en nombre de paquets / seconde.

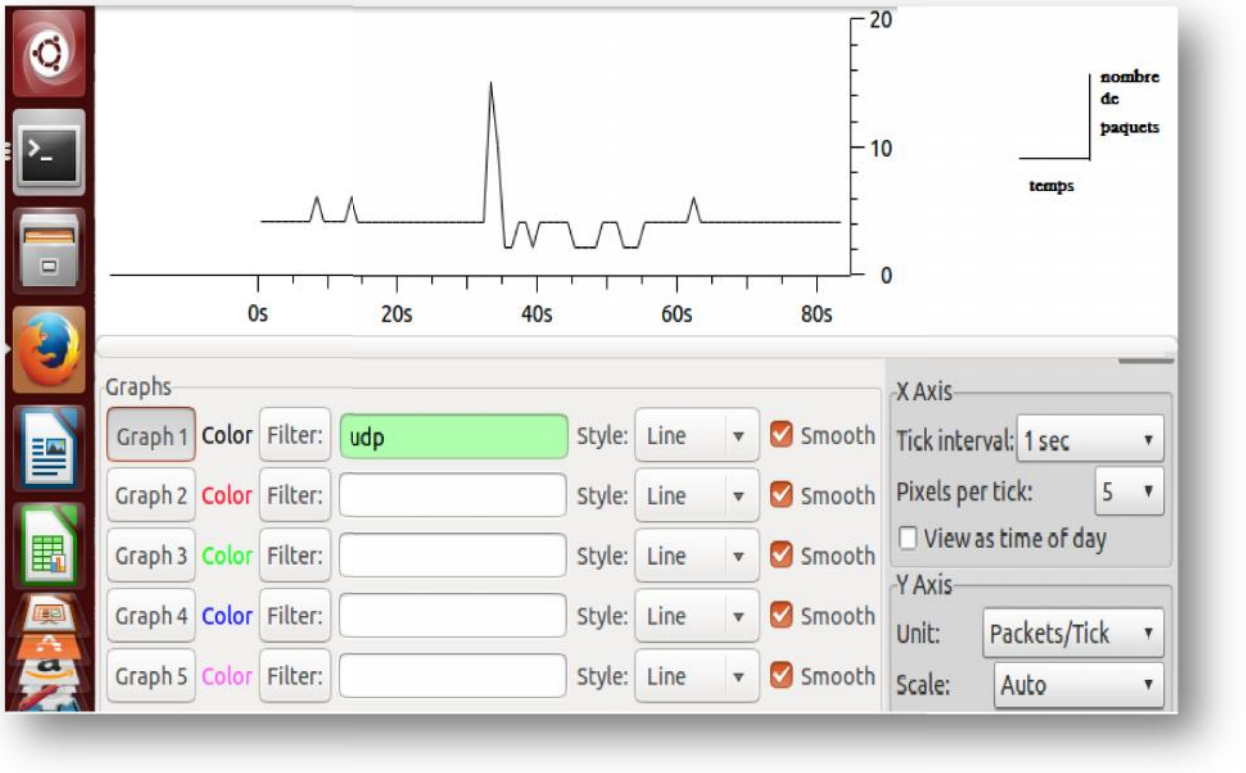

Figure 3. 15 : Graphe des paquets UDP perdus

Il est bien sûr possible d'exporter les graphes dans un format facilement intégrable dans un rapport (BMP, JPG, PNG...) en cliquant sur le bouton "**Enregistrer**", voir figure (3.15).

6. Conclusion

Blip, conçu par Berkeley, est l'implémentation dans TinyOS d'un certain nombre de protocoles basés IPv6. Elle fournit les structures de données nécessaires à la programmation de sockets.

Dans ce chapitre, nous avons présenté les démarches à suivre pour réaliser une connectivité IP entre deux capteurs telosb, pour ça il a fallu utiliser des outils logiciels bien particuliers tels qu’un système d’exploitation léger "TinyOs" et un langage orienté composant "NesC".

Conclusion générale

La création d'un "Internet des Objets", le développement et la diffusion ubiquitaire des technologies basées sur les capteurs, vont à terme brouiller les frontières entre monde virtuel et monde physique et pourraient modifier la nature même de la vie privée [40].

Dans ce projet, il nous a été confié de configurer et de tester la connectivité IP entre des capteurs telosb. Il a fallut pour cela prendre en main beaucoup de nouvelles technologies, comme TinyOS et le nesC.

La mise en œuvre de ce projet nous a permis de découvrir un nouveau domaine, une nouvelle manière de programmer et de concevoir une application, avec des contraintes techniques et matérielles très importantes, nous avons appris à tirer le meilleur de la théorie qui existe afin d'atteindre notre but.

Ce projet est particulièrement intéressant par le fait que les réseaux de capteurs sans-fil sont vraiment en pleine expansion de nos jours, mais encore trop peu connu des personnes extérieures à ce domaine.

Lors de nos expérimentations nous ne disposions que d'une machine et de trois capteurs, dont un servant de passerelle. Il serait peut être intéressant par la suite d'étendre ce projet à un nombre de capteurs beaucoup plus important, afin de couvrir une plus grande zone à étudier. Ainsi l'adressage IP des différents capteurs permettrait de diviser logiquement la zone en différents réseaux indépendants. Mais le plus grand intérêt serait la connexion de ces réseaux de capteur sans-fil avec Internet.

Liste des figures

Chapitre1

Chapitre2

Chapitre3

Liste des Tableaux

Bibliographie

[1] BOUNEGTA Nadia, **«** Approche distribuée pour la sécurité d'un réseau de capteurs sans fils (RCSF) », Ingénieur d'état en informatique, 2010.

[2] CHALLAL Yacine, « Réseaux de Capteurs Sans Fils », support-SIT60, Vol. 103, pp. 14, 17, Novembre 2008.

[3] ARLOT Pierrick, « La pile de protocoles IP se met au goût de l'Internet des objets », L'EMBARQUÉ / N°3 / 2013.

[4] ATHMANI Samir, « Protocole de sécurité Pour les Réseaux de capteurs Sans Fil », mémoire de magister, Aout 2010.

[5] BENCHOUK Imane, BALASKA Ahlem, « Agrégation des données dans les réseaux de capteurs sans fil », Mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique, juin 2013.

[6] LABRAOUI Nabila, «La sécurité dans les réseaux de capteurs sans fil», Thèse pour l'obtention du diplôme de doctorat, 2012.

[7] MERAD Omar, « la sécurité des données agrégées dans les réseaux de capteurs sans fil », mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique, 2010.

[8] SAHRAOUI Belkheyr, « La Géo--localisation dans les Réseaux de Capteurs sans Fil », Mémoire de fin d'études pour l'obtention du diplôme Ingénieur d'État en Informatique, Juillet 2011.

[9] BENAZZOUZ Mohamed, « Surveillance de tout point d'une zone d'intérêt à l'aide d'un réseau de capteur multimédia sans fil », magistère IRM 2013.

[10] JACQUENET Christian, « Routage dynamique et réseaux de capteurs - Bénéfice d'utiliser IPv6 dans les environnements contraints »**,** Référence IN132, Date de publication : 10 févr. 2011.

[11] ROUX Camille, « L'histoire et l'avenir du Web », 2008

[12] EVANS Dave, « L'Internet des objets Comment l'évolution actuelle d'Internet transforme-t-elle le monde », Avril 2011

[14] CATR Olivier, GALERNE Alexandre, « 6LowPAN Working Group », 11 mars 2011.

[18] ROUDAUT Fréderic, « Le protocole IPv6 », 2009.

[21] GRESSIER Yoan, CANAVAGGIO Guillaume, « IPv6 Généralités & état actuel du déploiement », 2002/2003.

[24] SOMMER Marc, « Gestion d'une couche réseau et MAC utilisant le protocole 6LowPAN », 2011.

[28] GELIBERT Anthony, « Simulation de réseaux 6LoWPAN avec OPNET Modeler», 2009

[29] LANTERI Isabelle**,** « 6LOWPAN IPv6 over Low power Wireless Personal Area network», CNAM 2008-2009

[30] RACHEDI Abderrezak, « réseaux sans infrastructure », 2011.

[31] KHEDIM Farah, « Détection des attaques par réplication dans un réseau de capteurs sans fil », Mémoire de fin d'études Pour l'obtention du diplôme de Master en Informatique, juillet 2013.

[32] LETAIEF Wajih, « Virtualisation sous Ubuntu avec VirtualBox », le 20 novembre 2008.

[33] D.Gay, D.Culler, and P.Levis. nesC Language Reference Manual, 2002.

[35] DARTIES Benoit, « Tutoriel d'utilisation de Wireshark ».

Webographie

[13] «L'Internet des objets»,

http://www.itu.int/itunews/manager/display.asp?lang=fr&year=2005&issue=09&ipage=things , Consulté le 03/05/2014

[15] « IPv4-Internet Protocol v4»,

http://www.dicodunet.com/definitions/reseaux/ipv4.htm , Consulté le 18/05/2014

[16] « IPv6: Introduction »,

http://www.httr.ups-tlse.fr/pedagogie/cours/tcp-ip/ipv6/introduction.htm, Consulté le 18/05/2014

[17] « Linux IPv6 HOWTO (fr), Chapitre 2, Les bases »,

http://mirrors.deepspace6.net/Linux+IPv6-HOWTO-fr/x440.html, Consulté le 18/05/2014.

[19] « Le protocole IPv6 »,

http://www.commentcamarche.net/contents/524-le-protocole-ipv6, Consulté le 18/05/2014.

[20] « Protocoles Internet »,

http://www.toubibpc.info/2011/04/protocoles-la-resolution-dadresse.html, Consulté le 25/05/2014.

[22] « IPv6 : qu'est ce que c'est ?, Réseau IPv6 Tunisien »,

http://www.ipv6net.tn/fr/qu-est-ce-que-ipv6.html, Consulté le 25/05/2014.

[23] « Présentation d'IPv6 et différences avec l'IPv4 »,

http://www.awt.be/web/res/index.aspx?page=res,fr,fic,110,002 , Consulté le 25/05/2014

[25] « Réseaux de capteurs et internet des objets »

http://www.telecom-bretagne.eu/formation-continue/architecture-reseaux/stage-fcg48-2014.php , Consulté le 25/05/2014.

[26] « 6LBR »,

https://www.cetic.be/6LBR, Consulté le 29/06/2014

[27] « UDP (User Datagram Protocol) »,

http://msdn.microsoft.com/fr-fr/library/cc785220(v=ws.10).aspx , Consulté le 29/05/2014

[34] Tutoriel officiel de Blip

http://tinyos.stanford.edu/tinyos-wiki/index.php/BLIP_Tutorial , Consulté le 04/06/2014

Annexe

INSTALLATION DE TINYOS 2.1.2 SOUS LINUX 14.04

1. ouvrez le terminal et exécutez cette commande :

$ sudo gedit /etc/apt/sources.list

2. Ajoutez « **deb http://tinyos.stanford.edu/tinyos/dists/ubuntu natty main** » à la fin du fichier

3. Maintenant installez tinyos-2.1.2 en tapant :

$ sudo apt-get update

$ sudo apt-get install tinyos-2.1.2

Il vous faudra environ 5 - 6 minutes, en fonction de votre vitesse d'Internet.

4. Maintenant, vous devez configurer l'environnement pour TinyOS. Ouvrez le fichier :

$ sudo gedit ~/.bashrc

Ajouter les lignes indiquées ci-dessous à la fin de ce fichier :

#Sourcing the tinyos environment variable setup script
source /opt/tinyos-2.1.2/tinyos.sh
export CLASSPATH=$CLASSPATH:.

5. Après tapez:

$ sudo gedit /opt/tinyos-2.1.2/tinyos.sh

Ajouter les lignes suivantes, sauvegardez et quittez.

#! /usr/bin/env bash
 # Here we setup the environment
 # variables needed by the tinyos
 # make system
echo "Setting up for TinyOS 2.1.2 Repository Version"
export TOSROOT=
export TOSDIR=
export MAKERULES=
TOSROOT="/opt/tinyos-2.1.2"
TOSDIR="$TOSROOT/tos"
CLASSPATH=$CLASSPATH:$TOSROOT/support/sdk/java:.:$TOSROOT/support/sdk/java/tinyos.jar

MAKERULES="$TOSROOT/support/make/Makerules"
export TOSROOT
export TOSDIR
export CLASSPATH
export MAKERULES

6. à la fin changez la permission en utilisant cette commande :

$ sudo chown -R <username> /opt/tinyos-2.1.2/

Maintenant pour tester, vous compilez le programme **Blink** :

$ cd /opt/tinyos-2.1.2

$ make telosb