2010-2011

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU
FACULTÉ DE GÉNIE ÉLECTRIQUE ET INFORMATIQUE
DÉPARTEMENT INFORMATIQUE

MEMOIRE

Pour l'obtention du

Grade de Master de l'UMMTO
Spécialité Systèmes Informatiques

Prise en charge d'un grand nombre de capteurs sans fil dans 6LoWPAN

Réalisé par

Ali OUBAZIZ

Dirigé par

Mehammed DAOUI

MEMOIRE

Pour l'obtention du

Grade de Master 2 de l'UMMTO
Spécialité Systèmes Informatiques

Prise en charge d'un grand nombre de capteurs sans fil dans 6LoWPAN

Réalisé par

Ali OUBAZIZ

Dirigé par

Mehammed DAOUI

Remerciements

Mes premiers remerciements et ma grande gratitude s’expriment envers Dr Mehammed DAOUI, mon directeur de projet. Je le remercie chaleureusement pour sa pédagogie, sa patience, sa disponibilité et son dévouement. Faire mon projet sous sa direction était pour moi un grand honneur et un immense bonheur.

J’adresse également mes sincères remerciements à ma famille ; parents, frères et ma petite sœur de m’avoir aidé à surmonter tous les obstacles et à me forger à travers les difficultés vécues durant toute cette période de travail.

Mes remerciements à tous ceux qui ont été continuellement présents, qui m’ont épaulée par leur aide, soutien et encouragement. Soyez assurés de mon profond respect et amour.

Un grand MERCI à ceux qui ont aidé de prés ou de loin à la réalisation de ce travail.

Table des matières

Liste des figures

Liste des Tableaux

Introduction générale

Les avancées récentes dans le domaine de la communication sans fil et les technologies « MEMS » (Micro Electro Mechanical Systems) ont permis le développement des micro-composants qui intègrent des dispositifs de captages et de communication sans fil dans un seul circuit, à dimension réduite, et avec un coût raisonnable. Ces composants, communément appelés micro-capteurs, ont favorisé l'idée de développer les réseaux de capteurs basés sur l'effort collaboratif d'un grand nombre de nœuds opérant d'une façon autonome et communiquant entre eux via des transmissions à courte portée.

L'objectif de ce travail est d'explorer un certain nombre de technologies concernant la mise en œuvre des réseaux de capteurs en particulier le déploiement d'un grand nombre de capteurs. 6LoWPAN est un protocole visant à intégrer l'adressage IPv6 dans les réseaux de capteurs. Toute fois, ce protocole utilise toujours un Hop limit à 8 bits qui limite le nombre de capteurs à déployer. Nous proposons une extension du Hop limit permettant la prise en charge d'un grand nombre de capteurs dans les RCSFs. Ainsi, nous avons organisé le rapport en 4 chapitres :

Le chapitre 1 récapitule les différentes technologies sans fil et l'objectif des réseaux de capteurs, leurs architectures, leurs caractéristiques et contraintes ainsi que leurs domaines d'applications.

Dans le chapitre 2 nous présentons une étude théorique approfondie du protocole IPv6, de ses spécificités techniques, les différents avantages apportés par ce protocole et les différentes translations existantes.

Le chapitre 3 définît le protocole 6LoWPAN conçu afin de pouvoir interfacer la norme IEEE 802.15.4 avec IPv6 et la manière de compression proposée par ce protocole.

Enfin, le chapitre 4 est consacré à détailler notre problématique et définir ensuite la solution proposée.

Nous finalisons cette étude par une conclusion synthétisant le travail réalisé, tout en proposant des perspectives.

Chapitre I

Présentation des réseaux de capteurs sans fil

I. Introduction

Au cours des dernières décennies, nous avons assisté à une miniaturisation du matériel informatique. Cette tendance à la miniaturisation a apporté une nouvelle génération de réseaux informatiques et télécoms présentant des défis importants. Les réseaux de capteurs sans fil sont l'une des technologies visant à résoudre les problèmes de cette nouvelle ère de l'informatique embarquée et omniprésente. Nous allons retracer dans le présent chapitre le fonctionnement des réseaux de capteurs en se focalisant sur les mécanismes et les principes proposés pour économiser de l'énergie, la sécurité, la QoS, l'intégration de grand nombre de capteurs, etc.

La mise en œuvre de simples possibilités de traitement, de stockage, de détection et de communication dans des dispositifs à petite échelle, à faible coût et leur intégration dans ce qu'on appelle des réseaux de capteurs sans fil ouvrent la porte à une multitude de nouvelles applications. Les réseaux de capteurs constituent une catégorie de réseaux sans fil comportant un très grand nombre de nœuds. Ils sont également caractérisés entre autre par un déploiement très dense et à grande échelle dans des environnements souvent limités en terme de ressources. Ces nœuds déployés autour ou dans une zone à observer sont utilisés pour l'acquisition de données et leur transmission à une station de traitement appelée communément « Station de Base ». Les spécificités les plus frappantes de ces nœuds sont leurs capacités d'auto-organisation, de coopération, leur rapidité de déploiement, leur tolérance aux erreurs et leur faible coût.

Dans ce qui suit, nous étudierons ce type de réseaux sans fil, ses principales caractéristiques, les différences qui les distinguent des réseaux ad hoc traditionnels ainsi que les éventuelles applications de ce type de réseaux très prometteur. En outre, l'architecture de communication dans les réseaux de capteurs sera détaillée ainsi que l'ensemble de facteurs influençant sur sa conception. Nous présenterons à la fin un ensemble de contraintes conceptuelles dans ce type de réseau.

II. Les réseaux sans fil

Le développement rapide dans le domaine de la technologie sans fil, connu par la facilité de déploiement et le coût relativement faible, a permis à un usager muni d'unité portable (Laptops, PDA, Pen Tablet, capteurs,…etc.), d'accéder à

l'information indépendamment de la position géographique et du facteur de temps, en lui permettant une libre mobilité, sans l'astreindre à une localisation fixe.

II.1. Définition

Un réseau sans fil (wireless network) est, comme son nom l'indique, un réseau dans lequel les terminaux peuvent communiquer sans liaison filaire. Les terminaux du réseau se déplacent librement, tandis que le système doit assurer toutes les fonctionnalités et tous les services d'un réseau classique. **[1]**

La communication sans fil permet une grande flexibilité d'emploi. En particulier la mise en réseau des sites dont le câblage serait trop onéreux à réaliser dans sa totalité, voire même impossible. En effet, la mise en place des réseaux sans fil n'exige pas de lourds aménagements des infrastructures comme c'est le cas dans les réseaux filaires (creusement de tranchées pour acheminer les câbles, équipement des bâtiments en câblage, goulottes et connecteurs,…etc.).

Néanmoins, ils présentent des inconvénients étant donné qu'ils sont caractérisés par une faible puissance d'émission et qu'ils n'offrent pas le même niveau de sécurité que les réseaux câblés, vu la nature contraignante de l'environnement sans fil, qui leur impose plusieurs défis que doivent surmonter les unités mobiles.

Les réseaux avec câbles n'ont pas disparu avec l'apparition des réseaux sans fil. Par conséquent, ces deux types de réseaux cohabitent en donnant naissance aux réseaux hybrides.

II.2. Caractéristiques des réseaux sans fil

- **Fiabilité :** La propagation des signaux subit des perturbations (microcoupures, erreur de transfert, timeout,…etc.) dues à l'environnement qui détériore l'information transmise.
- **Débit :** L'une des limitations principales vient de la faiblesse en bande passante. Ceci est dû au type du média utilisé. On distingue des réseaux utilisant, par exemple, des communications radio qui peuvent atteindre 20 Mbps et des communications Bluetooth avec 3Mbps à 10Mbps **[2]**.
- **Sécurité :** Plus qu'elle ne l'est dans les réseaux filaire, la sécurité est d'une importance primordiale dans les réseaux sans fil. Cela est dû à l'absence du

câblage dont résulte la diffusion de l'information facilitant l'interception à distance et la sensibilité au brouillage augmentant les interférences dans le réseau.

- **Topologie dynamique :** Elle change d'une manière fréquente suite à la mobilité continue des nœuds qui forment la topologie du réseau.

II.3. Classes des réseaux sans fil

Les réseaux sans fil peuvent être classés selon l'architecture de communication adoptée en deux catégories : les réseaux cellulaires avec infrastructure et les réseaux Ad Hoc sans infrastructure fixe. Plusieurs technologies sont apparentées aux réseaux cellulaires comme : GPS, WiMax, GPRS,…etc., et aux réseaux Ad Hoc comme les RCSF. Dans ce qui suit, ces deux classes de réseaux sans fil seront décrites en détail.

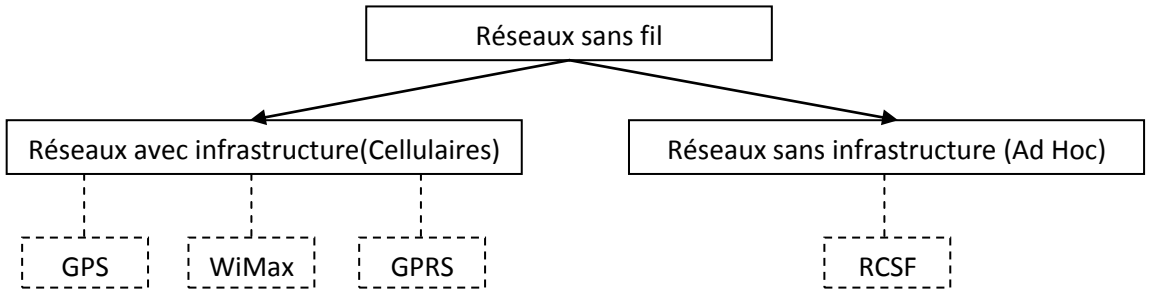


Figure 1. Classification des réseaux sans fil. **[3]**

III. Les réseaux cellulaires

Un réseau cellulaire est un système de communication basé essentiellement sur l'utilisation des réseaux filaires et la présence des stations de base qui couvrent les différentes unités mobiles du système **[4]**.

Un réseau cellulaire est un réseau dont l'architecture de communication est déterminée au préalable. Il est composé de sites fixes interconnectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé. Parmi les sites fixes, on retrouve les stations de bases SB. Chacune d'elles définit une région appelée cellule et administre un ensemble d'unités mobiles UM (nœuds) qui communiquent entre elles par une liaison sans fil possédant une bande passante limitée qui réduit sévèrement le volume des informations échangées.

Une cellule correspond à une zone de couverture où les nœuds communiquent avec d'autres nœuds de l'intérieur ou de l'extérieur de la cellule.

La figure 2 schématise l'architecture de communication des réseaux cellulaires.

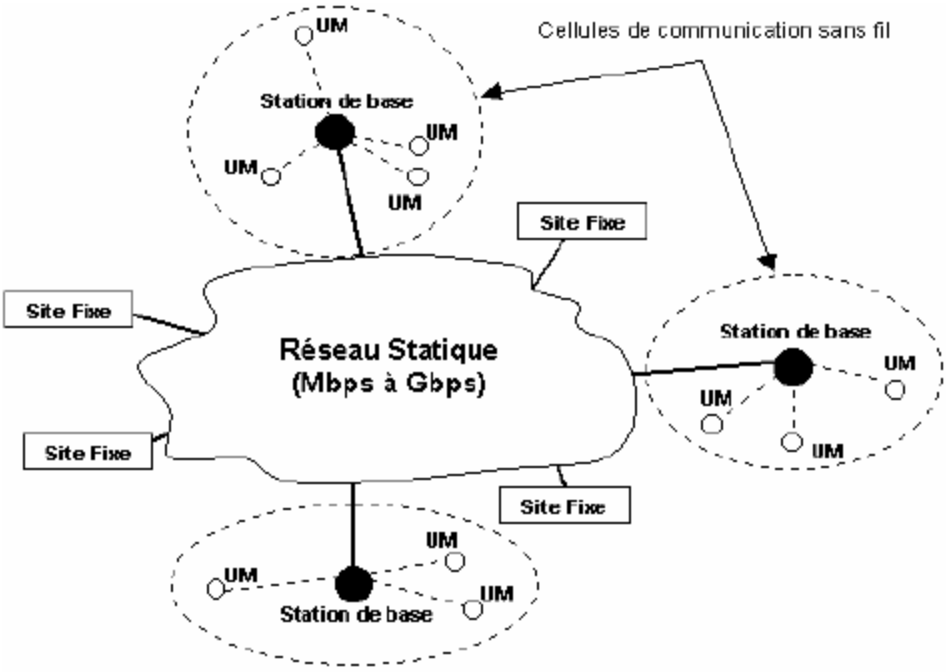


Figure 2. Architecture de communication d'un réseau cellulaire

La communication entre deux unités mobiles connectées, passe forcément par les stations de base. Par exemple, si une unité mobile UM1 (reliée à la station de base SB1) veut communiquer avec l'unité mobile UM2 (reliée à la station de base SB2) alors UM1 devra envoyer le message à SB1 qui va le transmettre à son tour à SB2. Cette dernière le transmettra à UM2.

IV. Réseaux Ad hoc

IV.1. Définition

Un réseau mobile Ad Hoc, appelé généralement MANET (Mobile Ad hoc NETwork), consiste en un ensemble d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou administration centralisée.

Les nœuds de ce type de réseau peuvent servir de routeurs et de serveurs fonctionnant sur le principe de pair-à-pair [1]P2P (Peer to Peer**).** Dans les réseaux Ad

[1] Modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur.

Hoc qui ont cette propriété, la défaillance d'un nœud ne met pas en péril l'accès à la ressource, contrairement à un réseau client-serveur où la donnée est fournie par le serveur. Par conséquent, si le serveur devient inaccessible par le réseau, les nœuds seront bloqués. **[5]**

Client-serveur *pair-à-pair*

Figure 3. Comparaison des topologies client-serveur et P2P

Si dans le passé, la notion des réseaux Ad Hoc était associée à la communication sur des champs de combat et à l'emplacement des zones dévastées, aujourd'hui, ce n'est plus le cas. En effet, l'utilisation de ce type de réseaux est devenue dans le domaine civil (opérations de secours, incendies, tremblements de terre, missions d'exploration, réseaux de communication,…etc).

IV.2. Caractéristiques des réseaux Ad Hoc

En plus des caractéristiques des réseaux sans fil en général, les réseaux Ad Hoc ont les caractéristiques suivantes:

- **Architecture décentralisée**: Cela fait référence à un système sans entité centralisée et sans contrôle extérieur. Par conséquent, les nœuds interagissent, analysent et traitent les données sans faire appel à d'autres dispositifs exotiques.
- **Auto-organisation**: Les nœuds découvrent automatiquement et d'une manière autonome les différents paramètres leur permettant de s'intégrer dans l'environnement et de s'autoconfigurer pour devenir opérationnels.
- **Sécurité**: L'absence d'infrastructure fixe pénalise l'ensemble du réseau dans la mesure où il faut faire abstraction de toute entité centrale de gestion pour l'accès aux ressources. Cela fait que la sécurité dans les réseaux Ad Hoc soit plus pénible à assurer. De plus, les nœuds d'un réseau Ad Hoc assurent la fonction de reconfiguration contrairement à un réseau avec infrastructure où la gestion du rapport de confiance ne se fait qu'entre le nœud et la station. Dans

les réseaux Ad Hoc, cette gestion de confiance mutuelle se fait sur tout l'ensemble des nœuds. Par ailleurs, les nœuds Ad Hoc étant fortement mobiles, leur sécurité physique est moins assurée que pour un poste de travail fixe, dans un bureau par exemple. Leur valeur marchande peut être d'une importance non négligeable.

V. Réseaux de capteurs sans fils

Les domaines scientifiques et techniques exigent d'observer et de contrôler certains phénomènes physiques tels que la pression atmosphérique, la température, le degré de pollution de l'air,…etc. Et cela est devenu plus simple grâce aux réseaux de capteurs.

Ces réseaux présentent un intérêt considérable pour le secteur industriel et militaire, mais aussi pour les organisations civiles où la surveillance et la reconnaissance de phénomènes physiques sont une priorité. Les réseaux sans fil trouvent un intérêt tout particulier dans ce type d'applications. En effet, ces réseaux d'utilisation très fréquente procurent de nombreux avantages tels que la flexibilité et l'affranchissement du câblage. Notons que les réseaux de capteurs font partie de la famille des réseaux ad hoc, c'est à dire des réseaux sans infrastructure.

V.1. Description physique d'un capteur

Un capteur est composé de quatre éléments principaux :

- Un élément qui se charge de mesurer l'environnement extérieur (unité de capture),
- Une unité de calcul,
- Un élément émetteur / récepteur,
- Une alimentation.

Trois composants additionnels peuvent être implantés dans un capteur :

- Un système de recherche d'emplacement,
- Un générateur d'alimentation,
- Une unité mobile (permettant de faire bouger le capteur).

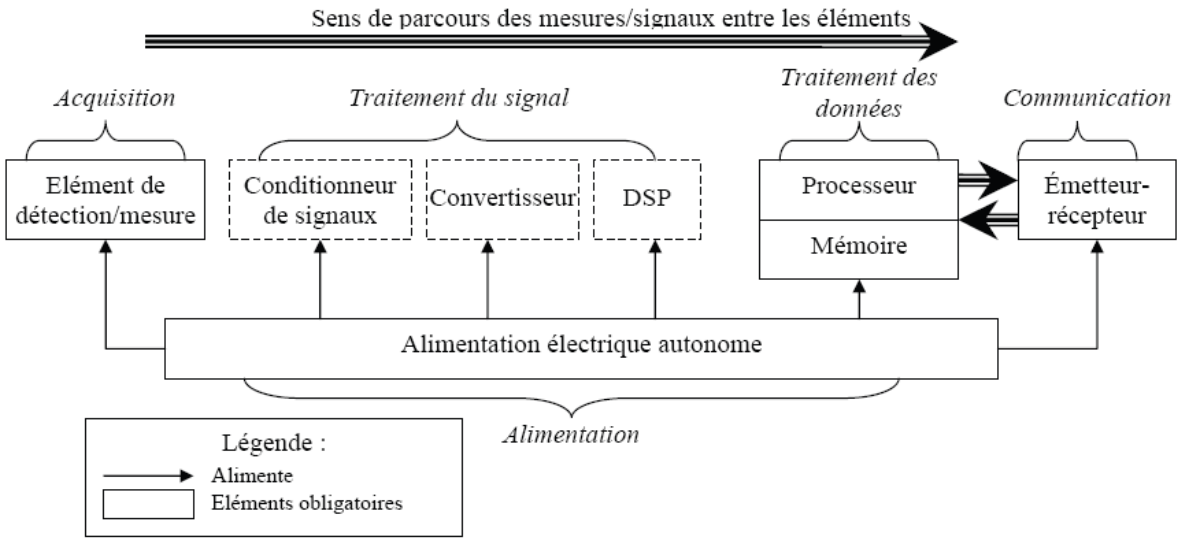


Figure 4. Architecture de base d'un capteur **[6]**

- **Capteur :** L'unité de capture ou élément capteur est composée de deux sous éléments :
  - Le capteur récupérant des données analogiques,
  - Un convertisseur faisant passer les données analogiques du capteur a des données numériques (appelée ADC pour analog to digital convertor) envoyées a une unité de calcul.
- **Unité de calcul :** Le composant regroupe :
  - Un processeur,
  - Une unité de mémoire réduite :

  Il permet de stocker les données, exécute les taches de perception qui lui sont assignées.
- **Emetteur/Récepteur :** élément permettant de connecter le capteur au réseau.
- **Alimentation :** la source d'énergie pour le capteur, comme tout dispositif embarqué, ils disposent d'une alimentation autonome telle qu'une batterie.

V.2. Description d'un réseau de capteurs

Les réseaux de capteurs sans fil "Wireless Sensor Networks (WSN)" sont considérés comme un type spécial de réseaux ad hoc. Les nœuds de ce type de réseau consistent en un grand nombre de micro-capteurs capables de récolter et de transmettre des données environnementales d'une manière autonome. La position de ces nœuds n'est pas obligatoirement prédéterminée. Ils sont dispersés

aléatoirement à travers une zone géographique, appelée champ de captage, qui définit le terrain d'intérêt pour le phénomène capté. Les données captées sont acheminées grâce à un routage multi-saut à un nœud considéré comme un "point de collecte", appelé nœud puits (ou sink). Ce dernier peut être connecté à l'utilisateur du réseau via Internet ou un satellite. Ainsi, l'usager peut adresser des requêtes aux autres nœuds du réseau, précisant le type de données requises et récolter les données environnementales captées par le biais du nœud puits (station de base).
Il existe deux grands types de réseaux de capteurs sans fil :

- **Avec capteurs mobiles :** Le réseau est constitué d'un ensemble de capteurs mobiles évoluant dans un environnement statique. Ce type de réseaux est, la plupart du temps, utilisé pour l'exploration de zones inaccessibles ou dangereuses.
- **avec capteurs fixes :** Le réseau est constitué de capteurs fixes servant à la surveillance d'occurrence d'évènements sur une zone géographique. Ici, le réseau n'effectue que la surveillance, les données mesurées sont transmises en mode multi sauts à un nœud spécifique appelé « puits » qui est chargé, après réception, de mettre en œuvre les actions nécessaires. Ce puits peut être connecté, de manière filaire par exemple, à un autre réseau.

  Il existe des réseaux hybrides qui sont constitués de capteurs fixes lors du déploiement (au départ) et qui décident de se déplacer après auto-organisation des nœuds pour certaines raisons tel que l'inadaptation à l'environnement ou le changement de la cible à détecter. **[7]**

V.3. Caractéristiques d'un réseau de capteurs

Les caractéristiques d'un réseau de capteurs sont **[8]**:

- **Absence d'infrastructure** : Les réseaux ad hoc, en général, se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructure préexistante et de tout genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue.
- **Un grand nombre de capteurs** : Des réseaux de 1 000 000 nœuds peuvent être envisagés.

- **Contrainte d'énergie** : Dans plusieurs applications, les nœuds capteurs sont placés dans des surfaces distantes. Ce qui favorise une plus grande consommation d'énergie pour la communication, par conséquent une durée de vie limitée.
- **Topologie dynamique** : Les capteurs peuvent être attachés à des objets mobiles qui se déplacent d'une façon libre et arbitraire rendant ainsi, la topologie du réseau fréquemment changeante. Nous pouvons citer comme exemple celui du GPS d'une voiture qui fait office de capteur de position mobile des déplacements de la voiture.
- **Auto organisation du réseau** : Ceci peut être nécessaire dans plusieurs cas. Un réseau comportant un grand nombre de nœuds placés dans des endroits hostiles où la configuration manuelle n'est pas faisable, il doit être capable de s'auto organiser, i.e. que les nœuds décideront par eux même de la fonctionnalité de chacun et de la hiérarchie à adopter. Un autre cas est celui où un nœud est inséré ou retiré (à cause d'un manque d'énergie ou destruction physique), ainsi le réseau doit être capable de se reconfigurer pour continuer sa fonction.
- **Sécurité physique limitée** : Les réseaux de capteurs sans fil mobiles sont plus touchés par le paramètre de sécurité que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

V.4. Domaines d'application des réseaux de capteurs sans fil

Les RCSF peuvent avoir beaucoup d'applications. Parmi elles, nous citons :

V.4.1. Applications militaires

Le déploiement rapide, l'auto-configuration et la tolérance aux pannes des réseaux de capteurs sont des caractéristiques qui font de ce type de réseaux un outil appréciable dans un tel domaine. Déploiement sur un endroit stratégique ou difficile d'accès, afin de surveiller toutes les activités des forces ennemies ou d'analyser le terrain avant d'y envoyer des troupes (par la détection d'agents chimiques, biologiques ou de radiations, par exemple). **[9]**

V.4.2. Applications liées à la sécurité

Les altérations dans la structure d'un bâtiment, suite à un séisme ou au vieillissement, pourraient être détectées par des capteurs intégrés dans les murs ou dans le béton, sans alimentation électrique ou autres connexions filaires. Les capteurs doivent s'activer périodiquement et peuvent ainsi fonctionner durant des années, voire des décennies. Un réseau de capteurs de mouvements peut constituer un système d'alarme distribué qui servira à détecter les intrusions sur un large secteur.

Déconnecter le système ne serait plus aussi simple, puisqu'il n'existe pas de point critique. La surveillance de voies ferrées pour prévenir des accidents avec des animaux et des êtres humains peut être une application intéressante des réseaux de capteurs. La protection des barrages pourrait être accomplie en y introduisant des capteurs. La détection prompte de fuites d'eau permettrait d'éviter des dégâts. Les êtres humains sont conscients des risques et attaques qui les menacent. Du coup, ils mettent à disposition toutes les ressources humaines et financières nécessaires pour leur sécurité.

Cependant, des failles sont toujours présentes dans les mécanismes de sécurisation appliqués aujourd'hui, sans oublier leur coût très élevé. L'application des réseaux de capteurs dans le domaine de la sécurité pourrait diminuer considérablement les dépenses financières consacrées à la sécurisation des lieux et à la protection des êtres humains tout en garantissant de meilleurs résultats. **[10]**

V.4.3. Applications environnementales

Des thermo-capteurs dispersés à partir d'un avion sur une forêt peuvent signaler un éventuel début d'incendie dans le champ de captage; ce qui permettra une meilleure efficacité pour la lutte contre les feux de forêt. Dans les champs agricoles, les capteurs peuvent être semés avec les graines. Ainsi, les zones sèches seront facilement identifiées et l'irrigation sera donc plus efficace. Sur les sites industriels, les centrales nucléaires ou dans les pétroliers, des capteurs peuvent être déployés pour détecter des fuites de produits toxiques (gaz, produits chimiques, éléments radioactifs, pétrole,…etc.) et alerter les utilisateurs dans un délai suffisamment court pour permettre une intervention efficace. Une grande quantité de capteurs peut être déployée en forêt ou dans un environnement de conservation de

la faune afin de recueillir des informations diverses sur l'état du milieu naturel et sur les comportements de déplacement. **[11]**

V.4.4. Applications médicales

Surveillance permanente des patients et une possibilité de collecter des informations physiologiques de meilleure qualité facilitant ainsi le diagnostic de maladies grâce à des micro-capteurs qui pourront être intègres ou implantes sous la peau.

- Les micros-cameras qui peuvent être ingérées et sont capables, sans avoir recours à la chirurgie, de transmettre des images de l'intérieur d'un corps humain,
- La création d'une rétine[2] artificielle composée d'une centaine de micro-capteurs pour améliorer la vision de l'œil.

V.4.5. Applications écologiques

L'intégration de plusieurs micro-capteurs dans le système de climatisation et de chauffage des immeubles. Ainsi, la climatisation ou le chauffage ne sont déclenches qu'aux endroits où il y a des personnes présentes et seulement si c'est nécessaire. Le système distribué peut aussi maintenir une température homogène dans les pièces. Utilisée à grande échelle, une telle application permettrait probablement de réduire la demande mondiale en énergie. **[9]**

V.4.6. Applications de traçabilité et de localisation

Suite à une avalanche il est nécessaire de localiser les victimes enterrées sous la neige en équipant les personnes susceptibles de se trouver dans des zones à risque par des capteurs. Ainsi, les équipes de sauvetage peuvent localiser plus facilement les victimes. Contrairement aux solutions de traçabilité et de localisation basées sur le système de GPS (Global Positionning System), les réseaux de capteurs peuvent être très utiles dans des endroits clos comme les mines par exemple.

[2] Organe sensible de la vision.

V.4.7. Applications commerciales

Il est possible d'intégrer des nœuds capteurs au processus de stockage et de livraison. Le réseau ainsi formé, pourra être utilisé pour connaître la position, l'état et la direction d'un paquet ou d'une cargaison. Il devient alors possible pour un client qui attend la réception d'un paquet, d'avoir un avis de livraison en temps réel et de connaître la position actuelle du paquet. Pour les entreprises manufacturières, les réseaux de capteurs permettront de suivre le procédé de production à partir des matières premières jusqu'au produit final livré. **[11]**

V.5. Architecture des réseaux de capteurs sans fil

Les nœuds capteurs sont habituellement dispersés dans un champ de captage. Ils ont la capacité de rassembler des données et les routées vers la station de base "Sink". Ce routage se fait en multi saut comme montré dans la figure figue 5. Le Sink peut ainsi communiquer les données vers un gestionnaire de tâches (pour le traitement de données) par Internet (liaison filaire) ou satellite.

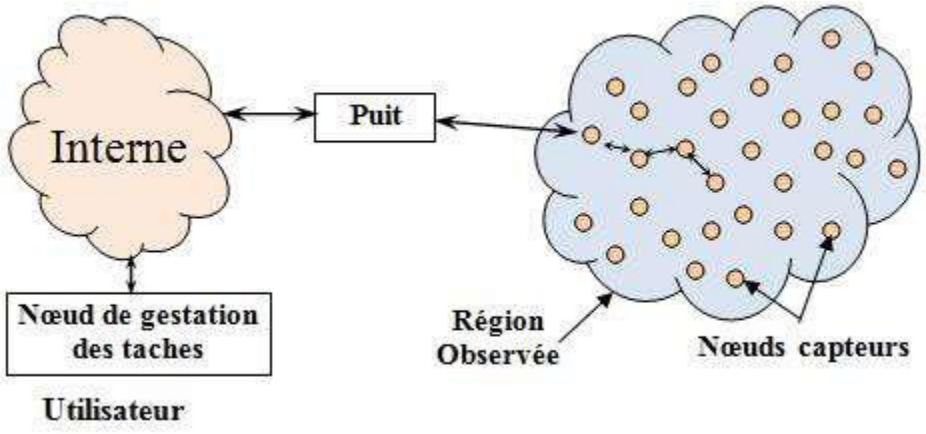


Figure 5. Architecture d'un réseau de capteurs

Il existe deux schémas de configuration des nœuds (illustré dans la figure 6) qui influent étroitement sur les protocoles de communication :

V.5.1. Les réseaux de capteurs sans-fil plats

Dans ce type de configuration, tous les nœuds ont un même niveau et peuvent communiquer avec tous les autres nœuds. On peut distinguer deux schémas:

- **Centralisé:** dans lequel, toutes les données capturées par les nœuds capteurs sont envoyées vers un nœud central qui fait le traitement et la fusion des données pour les transmettre à la station de base. Ce schéma est très simple et il est utilisé seulement pour des réseaux de petite densité.
- **Distribué:** il est plus compliqué. Plusieurs nœuds de traitement de données existent et peuvent communiquer entre eux. Un groupe de nœuds récoltent chacun de leur côté les données du réseau et les communiquent entre eux jusqu'à acheminement à la station de base.

V.5.2. Les réseaux de capteurs sans-fil hiérarchiques

Le réseau est découpé en clusters, dans chaque cluster un Cluster-Head est élu pour gérer les communications inter et intra cluster. Toutes les données reçues d'un niveau inférieur sont traitées et agrégées par les cluter-heads de ce niveau avant d'être transmises vers le niveau supérieur.

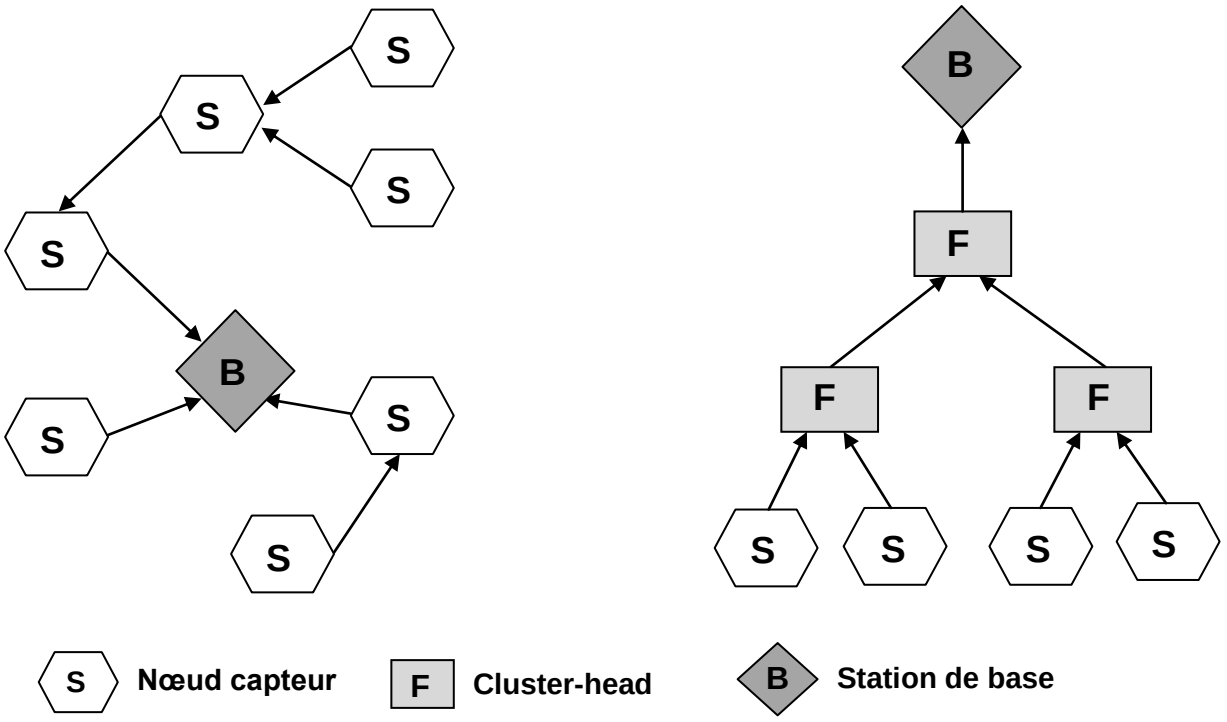


Figure 6. Types d'architectures des réseaux de capteurs

V.5.3. Architecture géographique

Dans certains types d'applications les nœuds peuvent être mobiles et la connaissance de la position géographique des nœuds est nécessaire. Cette position peut être calculée par les méthodes de triangulation ou obtenue par un système GPS (Global Positioning System). Une telle architecture est baptisée architecture géographique.

V.6. Communication dans les réseaux de capteurs

V.6.1. Modèle en couches [12]

Après le déploiement des nœuds capteurs sur une certaine zone de captage, ceux-ci commencent par la découverte de leurs voisins afin de construire la topologie de communication. Ainsi, ils deviennent capables d'accomplir les tâches qui leur sont affectées.

Dans le but d'un établissement efficace d'un RCSF, une architecture en couches est adoptée afin d'améliorer la robustesse du réseau. Une pile protocolaire de cinq couches est donc utilisée par les nœuds du réseau. Citons la couche application, la couche transport, la couche réseau, la couche liaison de données et la couche physique.

De plus, cette pile possède trois plans (niveaux) de gestion : le plan de gestion des tâches qui permet de bien affecter les tâches aux nœuds capteurs, le plan de gestion de mobilité qui permet de garder une image sur la localisation des nœuds pendant la phase de routage, et, le plan de gestion de l'énergie qui permet de conserver le maximum d'énergie.

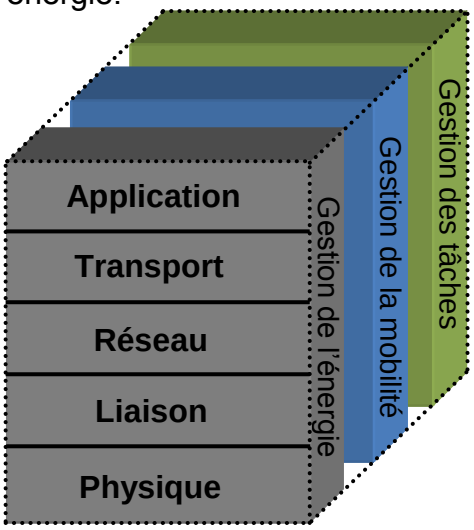


Figure 7. La pile protocolaire dans les réseaux de capteurs

- **La couche application :** Elle assure l'interface avec les applications. Il s'agit donc de la couche la plus proche des utilisateurs, gérée directement par les logiciels. Parmi les protocoles d'application, nous citons : SMP (Sensor Management Protocol) et TADAP (Task Assignement and Data Advertisement Protocol).
- **La couche transport :** Elle vérifie le bon acheminement des données et la qualité de la transmission. Dans les RCSF, la fiabilité de transmission n'est pas majeure. Ainsi, les erreurs et les pertes sont tolérées. Par conséquent, un protocole de transport proche du protocole UDP et appelé UDP-Like (User Datagram Protocol Like) est utilisé.

  Cependant, comme le protocole de transport universel est TCP (Transmission Control Protocol), les RCSF doivent donc posséder, lors d'une communication avec un réseau externe, une interface TCP-spliting pour vérifier la compatibilité entre ces deux réseaux communicants.
- **La couche réseau :** Elle s'occupe du routage de données fournies par la couche transport.Elle établit les routes entre les nœuds capteurs et le nœud puits et sélectionne le meilleur chemin en termes d'énergie, délai de transmission, débit,…etc.

  Les protocoles de routage conçus pour les RCSF sont différents de ceux conçus pour les réseaux Ad Hoc puisque les RCSF sont différents selon plusieurs critères comme :
  - L'absence d'adressage fixe des nœuds tout en utilisant un adressage basé-attribut.
  - L'établissement des communications multi-sauts.
  - L'établissement des routes liant plusieurs sources en une seule destination pour agréger des données similaires,…etc.

  Parmi ces protocoles, nous citons : LEACH (Low-Energy Adaptive Clustering Hierarchy) et SAR (Sequential Assignement Routing).
- **La couche liaison :** Elle est responsable de l'accès au media physique et la détection et la correction d'erreurs intervenues sur la couche physique. De plus, elle établit une communication saut-par-saut entre les nœuds. C'est-à-dire, elle détermine les liens de communication entre eux dans une distance d'un seul saut.

Parmi les protocoles de liaison de données, nous citons: SMACS (Self-organizing Medium Access Control for Sensor networks) et EAR (Eavesdrop And Register).

- **La couche physique :** Elle permet de moduler les données et les acheminer dans le media physique tout en choisissant les bonnes fréquences.

V.6.2. Les réseaux de capteurs standards

Plusieurs gammes de produits sont actuellement commercialisées, mais la normalisation pourrait encore modifier les choses. Les groupes de travail qui se chargent de cette normalisation proviennent de l'IEEE aux Etats-Unis et de l'ETSI en Europe. La figure 8 décrit les normes existantes et différentes catégories de réseaux suivant leur étendue.

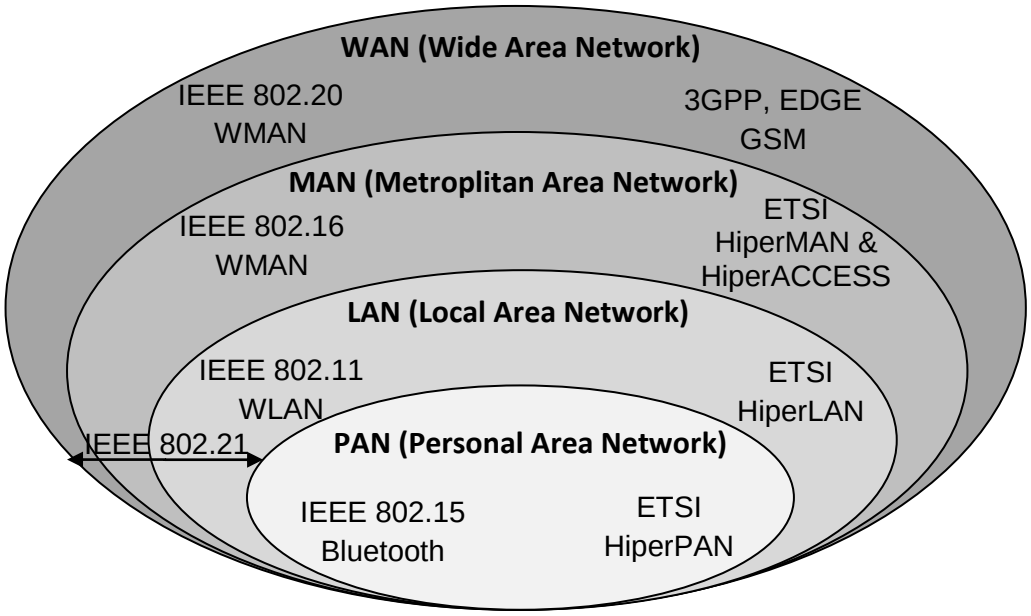


Figure 8. Catégories des réseaux sans-fil **[13]**

Les principales normes sont IEEE 802.15, pour les petits réseaux personnels d'une dizaine de mètres de portée, IEEE 802.11, ou Wi-Fi (Wireless-Fidelity), pour les réseaux WLAN (Wireless Local Area Network), IEEE 802.16, pour les réseaux WMAN (Wireless Metropolitan Area Network) atteignant plus de dix kilomètres, et IEEE 802.20, pour les réseaux WWAN (Wireless Wide Area Network), c'est-a-dire les tares grands réseaux.

Dans ce qui suit, nous allons présenter les RCSFs standards :

- **V.6.2.1. IEEE 802.15.1/BLUETOOTH**

IEEE 802.15.1, le plus connu, prend en charge la norme Bluetooth, aujourd'hui largement commercialisée. Mais cette norme est rarement utilisée dans RCSFs à cause de sa consommation importante d'énergie.

- **V.6.2.2. IEEE 802.15.3/UWB (ULTRA WIDE BAND)**

IEEE 802.15.3 définit la norme UWB (Ultra-Wide Band), qui met en œuvre une technologie très spéciale, caractérisée par l'émission à une puissance extrêmement faible, sous le bruit ambiant, mais sur pratiquement l'ensemble du spectre radio (entre 3,1 et 10,6 GHz). Les débits atteints sont de l'ordre du gigabit par seconde sur une distance de 10 mètres. **[13]**

- **V.6.2.3. IEEE 802.15.4/ZigBee Alliance**
  - **V.6.2.3. IEEE 802.15.4**

Les réseaux micro-capteurs sans-fil ont été l'objet de recherches intensives ces dernières années, ils émergent maintenant dans des applications industrielles. Une étape importante dans cette transition a été le dégagement de la norme d'IEEE 802.15.4 qui indique l'interopérabilité dans la couche physique et la couche MAC (Medium Access Control) visant la radio de transmission du nœud capteur. L'IEEE 802.15.4 standard supporte différentes topologies de réseaux. Dans cette norme, deux types de topologies sont discutes : la topologie en étoile "Star" et la topologie paire a paire "Peer-to-peer". La norme d'IEEE 802.15.4 présente deux types de nœuds : un nœud avec une charge complète (Full Function Device (FFD)) et un nœud avec une charge réduite (Reduced Function Device (RFD)).

La norme indique que le réseau est coordonné par un des FFDs, ce dernier peut router des données (contrairement au RFD). Dans cette norme, la topologie en étoile met l'accent sur la durée de vie des batteries puisque chaque RFD est relie directement au coordonnateur. Par contre la topologie paire a paire s'intéresse a la fiabilité et a la sociabilité puisque tous les nœuds sont des FFDs et peuvent donc être relies ensemble. La norme IEEE 802.15.4 peut supporter d'autres topologies, par exemple la topologie arbre de cellules "Cluster tree" qui combine les deux topologies précédentes (étoile et paire a paire ou maille "Mesh"). Les différentes topologies du réseau supportées par IEEE 802.15.4 sont montrées dans la figure 9 suivante **[14]** :

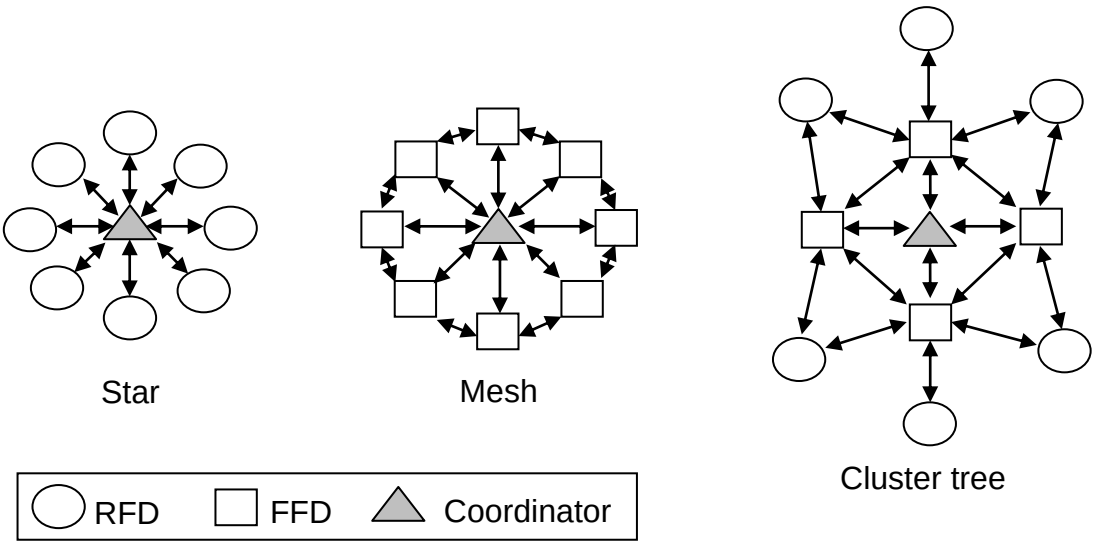


Figure 9. Les topologies du réseau supportées par IEEE 802.15.4

- **ZigBee Alliance**

En 2002, ZigBee Alliance a été constituée par une association d'entreprises. Le but de ZigBee Alliance est de développer des produits de contrôle fiables avec un cout réduit, et qui ne demandent pas beaucoup d'énergie. Ces produits doivent pouvoir être gères par un réseau sans-fil en utilisant une norme standard globale. Zigbee Alliance fonctionne globalement sur la bande de fréquences des 2,4 GHz mais également à 915 MHz en Amérique et à 868 MHz en Europe. Les débits offerts sont : 250 Kbits/s à 2.4 GHz (10 canaux), 40 Kbits/s à 915 MHz (6 canaux) et 20 Kbits/s à 868 MHz (1 canal). ZigBee Alliance permet de connecter jusqu'à 255 matériels par réseau sur une portée allant jusqu'à 100 mètres. ZigBee Alliance a été ratifiée en Aout 2003 sous la norme IEEE 802.15.4 **[15]**

V.7. Facteurs et contraintes conceptuelles des RCSFs

La conception des RCSFs, leurs protocoles et algorithmes sont guides par plusieurs facteurs:

V.7.1. La tolérance aux fautes

Le réseau doit être capable de maintenir ses fonctionnalités sans interruption en cas de défaillance d'un de ses capteurs. Cette défaillance peut être causée par une perte d'énergie, dommage physique ou interférence de l'environnement. Le degré de tolérance dépend du degré de criticité de l'application et des données

échangées. Un premier défi sera donc d'identifier et de modéliser formellement les modes de défaillances des capteurs, puis de repenser aux techniques de tolérance aux fautes à mettre en œuvre sur le terrain.

V.7.2. L'échelle (Scalabilité)

Une des caractéristique des RCSFs est qu'ils peuvent contenir des centaines voir des milliers de nœuds capteurs. Le réseau doit être capable de fonctionner avec ce nombre de capteurs tout en permettant l'augmentation de ce nombre et la concentration (densité) des nœuds dans une région (pouvant dépasser 20 nœuds/m3).

Un nombre aussi important de nœuds engendre beaucoup de transmissions inter nodales (implémentation d'une détection d'erreur, d'un contrôle de flux,…etc.) et nécessite que le puits soit équipé de beaucoup de mémoire pour stocker les informations reçues.

V.7.3. Système d'exploitation

TinyOS est parmi les systèmes d'exploitation open-source pour les réseaux de capteurs conçu par l'université américaine de BERKELEY. Le caractère open-source permet à ce système d'être régulièrement enrichie par une multitude d'utilisateurs. Sa conception a été entièrement réalisée en NesC, langage oriente composant syntaxiquement proche du C. Il respecte une architecture basée sur une association de composants, réduisant ainsi la taille du code nécessaire à sa mise en place. Cela s'inscrit dans le respect des contraintes de mémoires qu'observent les capteurs pourvus de ressources très limitées dues à leur miniaturisation. Pour autant, la bibliothèque de composants de TinyOS est particulièrement complète puisqu'on y retrouve des protocoles réseaux, des pilotes de capteurs et des outils d'acquisition de données. Un programme s'exécutant sur TinyOS est constitue d'une sélection de composants systèmes et de composants développes spécifiquement pour l'application a laquelle il sera destiné (mesure de température, du taux d'humidité,…etc.). TinyOS s'appuie sur un fonctionnement événementiel, c'est-a-dire qu'il ne devient actif qu'a l'apparition de certains événements, par exemple l'arrivée d'un message radio. Le reste du temps, le capteur se trouve en état de veille,

garantissant une durée de vie maximale connaissant les faibles ressources énergétiques des capteurs.

V.7.4. Sécurité physique limitée

Les réseaux de capteurs sans-fil sont plus touchés par le paramètre de sécurité que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

V.7.5. Cout de production

Le cout de production d'un seul capteur est très important pour l'évaluation du cout global du réseau. Si ce dernier est supérieur a celui nécessaire pour le déploiement des capteurs classiques, l'utilisation de cette nouvelle technologie ne serait pas financièrement justifiée. Par conséquent, réduire le cout de production jusqu'à moins de 1 dollar par nœud est un objectif important pour la faisabilité de la solution des réseaux de capteurs sans-fil.

V.7.6. L'environnement

Les nœuds capteurs peuvent être déployés a proximité ou a l'intérieur du phénomène observé. Ils peuvent ainsi, opérer dans des régions géographiques éloignées et sous certaines contraintes, telles que: des intersections encombrées, des tornades, des surfaces contaminées biologiquement ou chimiquement, attaches a des animaux,…etc.

V.7.7. La topologie du réseau

Le déploiement d'un grand nombre de nœuds nécessite une maintenance de la topologie. Cette maintenance consiste en trois phases :

- Déploiement
- Post-déploiement (les senseurs peuvent bouger, ne plus fonctionner,…etc)
- Redéploiement de nœuds additionnels. **[16]**

V.7.8. Les contraintes matérielles

Comme nous l'avons mentionné précédemment, un nœud capteur peut contenir d'autres unités dépendantes de l'application du réseau. En effet, la plupart des opérations de capture et des algorithmes de routage dans les réseaux de capteurs sans-fil requièrent la connaissance de la localisation des nœuds avec une grande précision, car ces nœuds sont déployés d'une manière aléatoire et fonctionnent d'une façon autonome. Ceci rend l'intégration d'une unité, consacrée au système de localisation, très commune dans un nœud capteur. C'est la raison pour laquelle souvent ces nœuds possèdent un système de localisation GPS, bien qu'il ait été montré que cette solution n'est pas fiable pour les réseaux de capteur sans-fil. Une autre approche proposée dans consiste à doter un nombre limité de nœuds avec le système GPS, et aider les autres nœuds à trouver leurs positions d'une manière terrestre. La conception des nœuds capteurs peut aller jusqu'à prévoir un système de mobilité du capteur pour le déplacer en cas de nécessité. Toutes ces unîtes peuvent exiger leur intégration dans un boitier de taille minimale inferieure a un centimètre cube, et avec un poids très léger qui permet aux nœuds de rester suspendus dans l'air, si l'application l'exige. [**17**]

V.7.9. Media de transmission

Les nœuds communicants sont reliés de manière sans-fil. Ce lien peut être réalisé par radio, signal infrarouge ou un media optique. **[16]**

Il faut s'assurer de la disponibilité du moyen de transmission choisi dans l'environnement de capture afin de permettre au réseau d'accomplir la totalité de ses tâches. Pour les liens de communication via les fréquences radio, les bandes ISM[3] (Industrial Scientific Medical bands) peuvent être utilisées. Pour les réseaux de capteurs, les unîtes de transmission intégrées au niveau des nœuds doivent être de petite taille et a faible consommation d'énergie. En effet, les contraintes matérielles associées aux nœuds, ainsi que le compromis existant entre l'efficacité des antennes et la consommation d'énergie, limite le choix de la bande de fréquence utilisée sur les bandes a hautes fréquences. **[18]**

[3] Bandes de fréquence qui ne sont pas soumises à des réglementations nationales et qui peuvent être utilisées librement.

V.7.10. La connectivite

Un réseau de capteurs est dit connecté si et seulement si, il existe au moins une route entre chaque paire de nœuds. La connectivite dépend essentiellement de l'existence des routes. Elle est affectée par les changements de topologie dus à la mobilité, la défaillance des nœuds, les attaques,… etc. Ce qui a pour conséquences: la perte de liens, l'isolement des nœuds, le partitionnement du réseau, la mise a jours des routes (le routage),…etc. **[19]**

V.7.11. La consommation d'énergie

Comme les nœuds capteurs sont des composants micro-électroniques, ils ne peuvent être équipés que par des sources limitées d'énergie (<0.5 Ampère-heure, 1.2 V). De plus, dans certaines applications, ces nœuds ne peuvent pas être dotes de mécanismes de rechargement d'énergie, par conséquent, la durée de vie d'un nœud capteur dépend fortement de la durée de vie de la batterie associée. Sachant que les réseaux de capteurs sont basés sur la communication multi-sauts, chaque nœud joue à la fois un rôle d'initiateur de données et de routeur également. Le dysfonctionnement d'un certain nombre de nœuds entraine un changement significatif sur la topologie globale du réseau, et peut nécessiter un routage de paquets différent et une réorganisation totale du réseau. C'est pour cela que le facteur de consommation d'énergie est d'une importance primordiale dans les réseaux de capteurs. La majorité des travaux de recherche mènes actuellement se concentrent sur ce problème afin de concevoir des algorithmes et protocoles spécifiques a ce genre de réseau qui consomment le minimum d'énergie.

Dans les réseaux de capteurs, l'efficacité en consommation d'énergie représente une métrique de performance significative, qui influence directement sur la durée de vie du réseau en entier. Pour cela, les concepteurs peuvent, au moment du développement des protocoles, négliger les autres métriques de performances telles que la durée de transmission et le débit, au profit du facteur de consommation d'énergie. **[18]**

VI. Conclusion

Les réseaux de capteurs sans fil se propagent dans plusieurs domaines d'application. Ils sont devenus indispensables pour les mesures de température, humidité, vibration,…etc.

Bien qu'ils présentent des concepts généraux comme étant des réseaux MANET, ils s'avèrent différents des réseaux sans fil conventionnels dû à un ensemble de caractéristiques; entre autre, le facteur d'énergie limitée, les contraintes matérielles ou encore le concept de tolérance aux pannes. Ce dernier dévoile un large domaine de recherche dans les WSN

Les réseaux de senseurs restent une nouvelle technologie peu accessible au grand publique. Elle est principalement répandue dans les laboratoires de recherches. Des progrès sont encore à réaliser dans ce domaine. Néanmoins ils correspondent à une certaine vision du futur et permettront des améliorations dans d'innombrables domaines de la vie quotidienne.

Dans ce chapitre, nous avons présenté les réseaux sans fil en général. Nous avons décrit ensuite les RCSF qui sont apparentés aux réseaux Ad Hoc.

Les RCSF sont appelés à s'intégré dans une architecture globale du réseau internet, la monté en échelle impose l'utilisation d'adressage supportant un certain nombre de nœud. Le protocole IPv6 s'impose comme alternative au procédés d'adressage.

Le prochain chapitre sera consacré à l'étude de l'IPv6.

Chapitre II

Etude de l'IPv6

I. Introduction

Internet fut créé à la fin des années 60. Conçu au début pour des besoins militaires et de recherche, il s'est développé de façon exponentielle ce qui a conduit à une saturation des ressources Internet comme l'espace d'adressage disponible et les tables de routages ainsi que la bande passante offerte sur le réseau.

A l'initiative de l'IETF, un nouveau protocole baptisé IPv6 a vu le jour qui répond par divers mécanismes à cette réduction des ressources comme l'apparition d'un nouveau format d'adresse qui augmente de façon significative l'espace d'adressage disponible et introduit les notions d'adressage hiérarchique et de qualité de service accrue.

Dans un premier temps ce chapitre s'attachera à montrer les solutions apportées à la réduction drastique des ressources par le protocole IPv6. Dans un deuxième temps sera proposé un état des lieus des réseaux IPv6 existants dans le monde ainsi qu'une description détaillé d'adressage dans ces types de réseaux.

II. Pourquoi IPv6 ?

Le changement d'échelle de l'Internet, passé d'une petite communauté d'utilisateurs à un réseau mondial constitué lui-même de réseaux au service de plus d'un milliard d'utilisateurs, est une réussite remarquable. En l'espace d'une courte période, l'Internet est aussi devenu une infrastructure fondamentale pour les économies et les sociétés du monde entier. En même temps, le modèle initial d'interconnexion à partir du grand système d'une université ou d'une grande société a laissé la place à un modèle d'interconnexion d'ordinateurs individuels, puis à un environnement constitué de dispositifs informatiques et de systèmes variés permettant une utilisation étendue et diversifiée et autorisant toutes les formes d'accès. On peut penser que dans l'avenir, d'avantage d'appareils seront connectés à l'internet.

II.1. Limitations d'IPv4

II.1.1. Adressage

L'Internet Protocol version 4 est la première version du protocole IP à avoir été largement déployée, et constitue encore la base de l'Internet. Elle est décrite dans la RFC[4] 791 de septembre 1981. IPv4 utilise une adresse IP sur 32 bits, soit 4 294 967 adresses possibles. Depuis quelques années avec l'explosion de l'internet, le nombre d'utilisateurs ne cessant de s'accroitre exponentiellement, il est évident que l'adressage IPv4 a atteint sa limite quant aux nombres d'adresses valables. Le stock d'adresses IPv4 non attribuées pour les nouvelles utilisations est en train de se réduire rapidement. Selon des prévisions, si la tendance actuelle se poursuit, cet espace utilisable d'adresses IPv4 non attribuées devrait se réduire à néant entre 2010 et 2015. Cependant, les concepteurs de normes ayant anticipé ce problème ont mis en place des techniques afin de freiner ce déficit exigeant des contraintes telles que la QoS, la sécurité et la mobilité et l'avènement des Réseaux de Nouvelle Génération (NGN).

II.1.1.1. Inégalités géographiques

Le peu d'adresses disponibles sous IPv4 commence à constituer un réel problème. En effet, le stock est aujourd'hui très entamé, et si près de 47% des adresses sont non attribuées (parmi le stock total d'adresses), la répartition géographique en est très inégale. Les adresses allouées (destinées à être utilisées par un registre régional ou par des organisations pre-RIR[5]) représentent la majorité du stock et sont destinées essentiellement à la zone américaine au dépend de l'Asie qui présente pourtant un important potentiel de développement (Chine, Inde).

Il est également à noter, que parmi le total des adresses IPv4 disponibles, 53% ont été attribuées directement à des organisations (américaines pour la plupart), avant l'apparition des RIR et ces adresses ne sont donc pas aujourd'hui sous le contrôle de ces derniers.

[4] requests for comments: sont une série numérotée de documents officiels décrivant les aspects techniques d'Internet.

[5] Un registre Internet régional (RIR, de l'anglais Regional Internet Registry) est un organisme qui alloue les blocs d'adresses IP (adressage IPv4, IPv6) et des numéros d'Autonomous System dans sa zone géographique.

Ainsi, en tenant compte de ces organisations pre-RIR, on peut estimer fin 2001 que 74% des adresses allouées le sont pour l'Amérique du Nord, 17% pour l'Europe et 9% pour l'Asie. **[20]**

II.1.1.2. Explosion des besoins

Outre la croissance encore forte d'internet dans le monde entier (et particulièrement en Asie où le potentiel de croissance est très élevé et les ressources en adresses très faibles), nombre d'applications nouvelles, consommatrices d'adresses IP devraient se développer.

Ainsi, l'Internet mobile, avec notamment GPRS[6] et UMTS[7] pourraient agir en levier de croissance des besoins. Les objets connectés, notamment dans le domaine de l'électronique grand public, de la domotique, des véhicules communicants, les réseaux de capteurs connectés, développement du mode de connexion à haut débit et des applications "bout-en-bout",...etc. Autant de facteurs de croissance des besoins en adresses IP, même si le fameux "killer application[8]" qui fera croître fortement et brutalement le besoin en adresses IP n'a pas encore été identifiée. **[20]**

II.1.2. Protocole non pensé pour l'usage commercial

Prévu à l'origine pour des usages non commerciaux, IPv4 n'a pas été conçu pour assurer les Fonctions de QoS attendues aujourd'hui, ni non plus pour assurer les fonctions Multicast, ou plug and play, ou encore la sécurité, essentielles dans l'Internet commercial moderne. Des solutions ont été trouvées, alourdissant le protocole de couches supplémentaires, ou pour doper artificiellement la durée de vie du stock d'adresses, faisant exploser la complexité des tables de routage.

II.1.2.1. Explosion des tables de routage

L'anarchie relative qui a pu régner un temps sur l'attribution des adresses, a mené à une perte de possibilité d'adressage hiérarchique. La désorganisation

[6] Norme pour la téléphonie mobile dérivée du GSM permettant un débit de données plus élevé.

[7] Universal Mobile Telecommunications System : est l'une des technologies de téléphonie mobile de troisième génération (3G) européenne.

[8] Programme informatique si attrayant qu'il justifie à lui seul, pour de nombreux consommateurs, l'achat ou l'adoption d'un type particulier d'ordinateur, de console de jeu, de système d'exploitation ou de téléphone portable.

relative, ainsi que les solutions (type CIDR[9] puis NAT[10]) permettant de reculer l'échéance de la pénurie d'adresses ont eu pour effet d'alourdir les Chemins de routage et de surcharger les tables de routage.

II.1.2.2. Sécurité perfectible

Des outils sécuritaires existent sous IPv4 comme IPSec[11] Avec les développements des échanges commerciaux sur Internet, des échanges de données confidentielles, le besoin en sécurité s'est fortement accru. IPv4 n'est pas conçu à l'origine pour un niveau de sécurité maximal et les solutions proposées sont optionnelles et fonctionnent sous forme de couches supplémentaires et optionnelles par rapport au protocole initial, ou sur la base d'éléments "pares-feux".

II.1.2.3. Mobilité non prévue initialement

La mobilité d'un terminal dans un réseau et à fortiori la mobilité entre réseaux hétérogènes, n'a pas été prévue à l'origine par IPv4. Dans le contexte actuel de développement de l'Internet mobile, mais également de développement des applications et objets mobiles utilisant IP, il devient critique de pouvoir assurer cette fonction. Des couches supplémentaires, comme Mobile IPv4 ont été développées, mais restent optionnelles et non optimales : elles ne sont pas identifiées comme des solutions d'avenir. Par ailleurs Mobile IPv4 n'est pas utilisé dans les réseaux cellulaires par exemple, qui préfèrent, même s'ils utilisent IP, avoir recours à d'autres protocoles de gestion de la mobilité, comme GTP. En outre, le routage n'est pas optimal et est même complexe (routage triangulaire) dans le cadre de la mobilité dans IP version 4. **[20]**

II.1.2.4. QoS non prévue à l'origine

La QoS est un élément essentiel de l'Internet commercial. Opérateurs et utilisateurs attendent un fonctionnement optimal du réseau et souhaitent mesurer cette QoS. IPv4 n'a pas été à l'origine prévu pour un usage "commercial" intense et

[9] Classless Inter-Domain Routing : Mis au point en 1993[1] afin de diminuer la taille de la table de routage contenue dans les routeurs.

[10] Network Address Translation: Mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4.

[11] Internet Protocol Security: défini par l'IETF comme un cadre de standards ouverts pour assurer des communications privées.

ne prend pas en charge de façon native la gestion de la QoS, qui est gérée selon des politiques et avec des outils créés en addition d'IPv4 (DiffServ, IntServ, MPLS,…etc.)

II.1.2.5. Autres

- Des lourdeurs dans la gestion des réseaux IP sous IPv4
- L'absence de possibilités d'auto configuration sous IPv4

Les attentes des utilisateurs modernes d'IP ont en outre évolué. Aujourd'hui, et notamment dans un contexte commercial où l'efficacité est cruciale, la lourdeur de configuration d'un réseau IPv4 est un handicap. En effet, même si quelques solutions ont pu être développées, IPv4 n'est pas prévu à l'origine pour assurer la configuration automatique d'un terminal dans un réseau : il faut configurer les serveurs, numéroter manuellement,…etc. Le concept de plug and play (par ailleurs essentiel dans le développement des objets grand public connectés) est totalement ignoré.

La fonction multicast, qui se développe aujourd'hui, monopolise une classe complète d'adresses, et n'est pas une fonction native d'IPv4, mais fonctionne grâce à un "add on".

Même si actuellement, tout est envisageable avec IPv4, la lourdeur imposée par ces manques constitue un frein au développement des nouvelles applications. Du fait des nombreux ajouts et des "options" disponibles, la complexité s'est fortement accrue, tant du point de vue de la compréhension du protocole et de ses nombreuses options, que de la gestion des réseaux : tables de routage surchargées, lourdeur d'administration des réseaux d'utilisateurs, complexité de la gestion des adresses privées/publiques,…etc.

Aujourd'hui, IPv4 est souvent décrit par ses détracteurs comme une "usine à gaz", héritage des ajouts et améliorations successives d'une base ancienne.

Tout ceci a poussé l'IETF[12] à mettre en place un groupe de réflexion sur la mise en œuvre d'un système d'adressage qui pallierait aux insuffisances et limites du système d'adressage IPv4. **[20]**

[12] Internet Engineering Task Force: groupe informel, international, ouvert à tout individu, qui participe à l'élaboration de standards pour Internet.

II.2. Avantages d'IPv6

II.2.1. Avantages techniques

II.2.1.1 Adressage

- **Adressage sur 128 bits**

IPv6 dispose d'un adressage sur 128 bits et non plus sur 32 comme dans IPv4. On dispose ainsi d'un stock de 2^{128} adresses, soient 2^{96} fois plus qu'avec IPv4. Ce stock très important permet d'envisager l'avenir avec sérénité, et de considérer qu'il sera ainsi possible de faire face à la croissance d'Internet dans toutes les zones géographiques, mais aussi de faire face aux besoins induits par l'apparition de nouvelles applications consommatrices d'adresses IP. La suppression du recours aux NAT est alors possible restaurant le mode end-to-end et améliorant le potentiel d'applications déjà existantes, comme notamment, les applications temps réel (type VoIP) qui sont actuellement freinées par les NAT. **[20]**

- **Adressage hiérarchique**

Un adressage hiérarchique qui structurera plus proprement l'Internet et améliorera le routage IPv6, réduisant le nombre de routes envisagées par les routeurs de cœur de réseau IP. Cet adressage hiérarchique permet de simplifier les agrégations d'adresses (par fournisseur ou par nœud d'échange). Dans IPv6, il y a séparation entre l'adresse du terminal et l'identification du réseau. Cette séparation permet de renuméroter un réseau très simplement (auto configuration).

L'intérêt du nouveau format d'adresses, outre son allongement, est son organisation hiérarchique. L'utilisation de préfixes séparés pour les adresses affectées à un fournisseur et les adresses affectées à une zone géographique constitue un compromis entre deux différentes visions du futur réseau Internet (à savoir, une gestion 100% par zone géographique et une gestion 100% par prestataire de service).

Le modèle géographique est le même que celui du réseau Internet actuel, dans lequel les fournisseurs d'accès ne jouent pas un grand rôle. Dans ce cadre, IPv6 peut gérer 2 types d'adresses, locales ou globales.

Les adresses de liens et de sites locaux n'ont qu'une spécification locale. Elles peuvent être réutilisées par d'autres organisations sans qu'il y ait de conflit. Elles ne peuvent pas être propagées hors des limites des organisations, ce qui les rend bien

adaptées à celles qui utilisent des gardes-barrières pour protéger leur réseau privé du réseau Internet.

Les conséquences de l'adressage hiérarchique sur les modes d'attribution ne sont donc pas extrêmement visibles. Toutefois, on peut noter que les politiques mises en œuvre sont particulièrement rigoureuses et structurées, afin d'éviter de reproduire la confusion survenue avec IPv4.

Ainsi, l'adressage hiérarchique permet de structurer "proprement" la répartition des adresses, notamment du fait que l'adressage IPv6 est encore neuf et n'hérite pas d'un adressage anarchique comme ce fut le cas avec IPv4. Les procédures d'agrégation en seront donc simplifiées, par voie de conséquence, les tables de routage allégées. La gestion globale de l'adressage étant correctement et rationnellement ordonnée, c'est l'ensemble du monde IP qui fonctionnera mieux. **[20]**

- **Multicast et anycast**

La fonctionnalité (Multicast) est prévue en natif dans IPv6. Cette fonction va de pair avec le nouvel adressage et simplifie le routage des données. Globalement, le routage est simplifié, fluidifié et donc amélioré.

IPv6 a prévu une autre fonction Anycast, qui permet de diffuser largement des données et de réaliser simplement des fonctions de type broadcast[13].

II.2.1.2 Auto configuration et gestion de la mobilité

Des possibilités d'auto configuration :

- Très utiles pour des applications domotiques ou d'électronique connectée.
- Très utiles pour la gestion/renumérotation de réseaux IP d'entreprises.

IPv6, contrairement à IPv4, prévoit la possibilité pour un terminal IPv6 (ou nœud IPv6) de s'auto configurer dans un réseau. On parle alors d'un mode "plug and play". Cette fonctionnalité est particulièrement utile en vue du développement des réseaux privés, et des applications domotiques et nomades, qui s'accommodent mal de lourdes procédures d'administration. La gestion et l'administration des réseaux IP en général est simplifiée, au bénéfice des utilisateurs : la renumérotation des réseaux

[13] Est employée par les techniciens en informatique et réseaux, il s'agit à proprement parler, de transmission ou de liaison.

est alors automatique en cas de fusion ou de scission du réseau, l'introduction d'un nouveau nœud est également automatique,…etc.

La fonctionnalité a en outre une utilité en termes de gestion de la mobilité, elle-même prévue en natif dans IPv6 : même si Mobile IPv6 est une couche supplémentaire de protocole, celle-ci est envisagée dès la spécification d'IPv6 et l'auto configuration vient jouer un rôle. En effet, lorsqu'un terminal mobile vient se brancher dans un réseau visité, il doit prendre une adresse dans ce réseau : l'auto configuration et le mode "neighbour discovery[14]" permettent de rendre cette opération plus simple.

- Mobile IPv6 est mieux adapté à la gestion de la mobilité; les premières utilisations de ce protocole avec des technologies WLAN le confirment.

Outre donc les avantages de l'auto configuration en termes de gestion de la mobilité, Mobile IPv6 présente un certain nombre d'avantages par rapport à la version 4, présentés dans le tableau suivant :

Tableau 1. Tableau récapitulatif des différences entre Mobile IPv4 et Mobile IPv6

	Mobile IPv4	Mobile IPv6
Mécanisme général	Mécanisme d'encapsulation des paquets IP et de transfert vers l'adresse IP temporaire dans le réseau visité	Suppression du foreign agent, devenu inutile grâce aux fonctionnalités de gestion de la mobilité intégrées dans IPv6
Routage	Routage triangulaire lors de la réception des paquets par le terminal mobile L'optimisation du routage est développée et disponible comme une option	Support intégré de l'optimisation du routage ("Route Optimisation")
Adressage	Seule l'adresse IP du réseau d'origine est connue du correspondant ; le foreign agent assure la correspondance entre l'adresse IP d'origine et celle dans le réseau visité	Les 2 adresses IP (dans le réseau d'origine et dans le réseau visité) sont codées dans l'adresse IPv6, permettant à l'équipement distant de connaître directement l'adresse de destination et d'éviter l'encapsulation.

Pour autant Mobile IPv6 ne devrait pas être le protocole utilisé dans les réseaux cellulaires, même si IPv6 est utilisé. En revanche, il s'impose comme le protocole idéal pour la connexion de terminaux au travers de réseaux hétérogènes notamment WLAN (802.11). Le fait que les produits Microsoft ne prévoient pas de Mobile IP client en IPv4 implique que Mobile IPv6 deviendra incontournable à terme.

[14] Est une méthode de découvert de voisin.

Le chantier de Mobile IPv6 reste ouvert à l'heure actuelle, l'optimisation n'étant pas encore réalisée.

II.2.1.3 Sécurité

L'apparition du protocole IPSec en mode natif, par défaut, permettra d'améliorer le niveau de sécurité global des échanges. Grâce à la profusion d'adresses qui devrait permettre d'éliminer les NAT (qui nuisent au fonctionnement des protocoles de sécurité de bout-en-bout), la sécurité tout le long de la route sera assurée.

Il faut toutefois nuancer cet apport: en effet, déjà sous IPv4, IPSec, outre son aspect optionnel, est gêné par l'absence de réelles infrastructures PKI[15] : cette absence, a priori persistante avec IPv6, constitue une nuisance pour le bon fonctionnement d'IPSec, même si celui-ci est natif.

II.2.1.4. Potentiel de QoS

- IPv6 présente plusieurs avantages permettant de mieux gérer la QoS mais qui ne sont pas encore significatifs.
- De manière générale, on considère que dans un premier temps, la QoS sera gérée de la même façon sous IPv6 que ce que l'on connaît aujourd'hui sous IPv4
- La non définition du champ "Flow Label" : un outil potentiel de gestion de la QoS sous IPv6

IPv6 présente par rapport à IPv4 un certain nombre d'améliorations qui permettent à priori d'améliorer la gestion de la qualité de service. Ci-dessous, sont listées les améliorations principales apportées au protocole IPv6 :

- **Simplification du format de l'en-tête**
- **Support amélioré des options et des extensions futures**
- **Fonctionnalité d'étiquetage de flux d'informations**
- **Dans le processus de routage :**

[15] PKI (Public Key Infrastructure) est un système de gestion des clefs publiques qui permet de gérer des listes importantes de clefs publiques et d'en assurer la fiabilité, pour des entités généralement dans un réseau. Elle offre un cadre global permettant d'installer des éléments de sécurité tels que la confidentialité, l'authentification, l'intégrité et la non-répudiation tant au sein de l'entreprise que lors d'échanges d'information avec l'extérieur. Une infrastructure PKI fournit donc quatre services principaux :
- fabrication de bi-clés.
- certification de clé publique et publication de certificats.
- Révocation de certificats.
- Gestion la fonction de certification.

A part une exception, les en-têtes d'extension ne sont pas examinés ou traités par un quelconque nœud le long du chemin emprunté par le paquet (packet's delivery path), jusqu'à ce que le paquet atteigne le nœud (ou l'ensemble des nœuds, dans le cas du multicasting) identifié par le champ "Adresse Destination" de l'en-tête IPv6.

L'exception à laquelle fait allusion le précédent paragraphe est l'en-tête des options sauts après sauts (Hop-by-Hop Options Header), qui transporte les options qui doivent être examinées et traitées par chaque nœud le long du chemin emprunté par le paquet, incluant les nœuds source et destination.

- **Problème de la longueur des paquets[16]:**

IPv6 exige que chaque lien inter-réseaux ait un MTU[17] supérieur ou égal à 1 280 octets. Sur tout lien qui ne peut pas transporter un paquet de 1 280 octet en un seul morceau, les services de fragmentation et d'assemblage spécifique au lien doivent être fournis par la couche en-dessous d'IPv6.

Cette fonctionnalité permet d'homogénéiser et de rendre plus efficace la transmission des paquets sur le réseau.

- **Labels relatifs aux flux[18] d'informations : Flow Label**

Le champ Label du Flux sur 22 bits dans l'en-tête IPv6 peut être utilisé par une source pour nommer des séquences de paquets pour lesquels un traitement spécial de la part des routeurs IPv6 est demandé. Ce traitement spécial pourrait être une qualité de service différente par défaut ou un service "temps réel".

- **Classes de trafic :**

Le champ Classe du Trafic sur 8 bits dans l'en-tête IPv6 a été créé pour être utilisé par des nœuds origines et/ou des routeurs transmetteurs pour identifier et distinguer différentes classes ou priorités de paquets IPv6.

- **Durée de vie maximale d'un paquet :**

Contrairement à IPv4, les nœuds IPv6 ne sont pas obligés d'imposer un temps de vie maximum des paquets. On peut ainsi envisager une réduction des pertes d'information du fait d'une absence de paquets jetés à la fin de leur durée de vie.

[16] Paquet (packet) : un en-tête IPv6 avec sa "charge utile" (ce qu'il transporte).

[17] MTU de lien (link MTU) : l'unité maximum de transmission (Maximum Transmission Unit), i.e., la taille maximale en octets d'un paquet qui peut être transmis sur le lien.

[18] Un flux est une séquence de paquets envoyée par une source particulière vers une destination particulière (unicast ou multicast)

La QoS passant également par la gestion de la sécurité, on peut ajouter que des extensions prévues pour gérer l'authentification, l'intégrité des données ou une (optionnelle) confidentialité de celles-ci sont spécifiées pour IPv6.

Tableau 2. Synthèse des critères de QoS et des apports d'IPv6 par rapport aux solutions IPv4

Critère de QoS	Apport d'IPv6	Solutions IPv4
Délai	Simplification du format de l'en-tête Support amélioré des options et extensions Fonctionnalité d'étiquetage du flux d'informations, label des flux Amélioration du processus de routage	Modification de l'en-tête du paquet par chaque routeur d'accès pour indiquer le niveau de service Définition d'un flux à travers une suite de routeurs et marquage des paquets en tant que composant de ce flux WRED, WFQ
Gigue	Support amélioré des options et extensions Amélioration du processus de routage	Gestion des files d'attente Trafic Shaping
Bande passante	Simplification du format de l'en-tête Longueur des paquets Classes de trafic	Trafic Shaping Techniques de prévention de la congestion RSVP
Disponibilité	Fonctionnalité d'étiquetage du flux d'informations, label des flux Classes de trafic Durée de vie maximale d'un paquet Gestion de la sécurité	RSVP IPSec et autres Modification de l'en-tête du paquet par chaque routeur d'accès pour indiquer le niveau de service

II.2.2. Impacts sur les acteurs: avantages économiques

II.2.2.1. Equipementiers

Le passage des réseaux vers IPv6, quel que soit le scénario retenu, présente l'avantage pour les équipementiers d'inciter au renouvellement du matériel. Les mises à niveau des matériels récents sont offertes (Software), mais les matériels anciens devront être changés pour assurer la compatibilité (Hardware). Certes, ce changement peut entrer dans le cycle de renouvellement du matériel, mais le passage à IPv6 peut éventuellement accélérer ce cycle.

En outre, l'en tête plus importante ralentit le temps de traitement : ainsi, à prix égal, les routeurs IPv6 seront plus lents donc moins performants que les mêmes routeurs en IPv4. Pour conserver le même niveau de performance, les matériels de

cœur de réseaux devront être eux-mêmes mis à niveaux (plus de mémoire, de capacité de calcul,…etc.) : ceci peut constituer un levier de ventes.

Pour l'instant les équipementiers IP leaders ne peuvent justifier avec précision auprès de leurs clients le passage à IPv6 du point de vue du retour sur investissement. Les paramètres essentiels du business case[19] d'IPv6 pour ces équipementiers sont notamment : les coûts liés aux équipements IPv6 et à la formation des équipes techniques, l'évaluation des gains de productivité avec une gestion moins complexe des réseaux IP (NAT), les gains en termes de services rendus aux clients (ISP[20]).

IPv6 est également une opportunité pour des "outsiders" de se positionner par rapport aux leaders du marché : c'est le cas des équipementiers japonais ou de certaines start-ups[21] qui basent leur stratégie sur IPv6.

Sur le plan de l'équipement du grand public, le développement de nouvelles applications connectées correspond à l'ouverture de nouveaux marchés pour ces équipementiers : de nouveaux produits pour les équipementiers grand public et des relais de croissance pour les équipementiers spécifiques IP qui peuvent pénétrer de nouveaux environnements.

II.2.2.2. Opérateurs

L'intérêt pour les opérateurs est dans la possibilité de fournir des adresses en nombre et ainsi de répondre au développement des connexions "always-on". IPv6 doit permettre d'alléger la gestion des réseaux IP et VPN[22] IP, et éventuellement de fournir des services à valeur ajoutée supplémentaires (accroissement potentiel des marges). L'abondance d'adresses correspond également à la fin de la domination des grands opérateurs sur le domaine des adresses et à la possibilité pour des opérateurs alternatifs d'affirmer leur indépendance. De nouvelles applications (end-to-end, temps réel,…etc.) et de nouveaux modèles économiques sont à imaginer.

[19] En management est une proposition structurée, qui marque un changement dans la conduite des affaires. Ce changement se trouve justifié en termes de coûts et bénéfices.

[20] Est un organisme (généralement une entreprise) offrant une connexion au réseau informatique Internet. Le terme en anglais désignant un FAI est *Internet Service Provider* (ISP) ou *Internet Access Provider* (IAP).

[21] Est une entreprise en construction qui ne s'est pas encore lancée sur le marché commercial (ou seulement à titre expérimental)

[22] Réseau privé virtuel, une connexion inter-réseau permettant de relier deux réseaux locaux différents de façon sécurisée par un protocole de tunnelisation.

En outre, les disparités géographiques introduites par la pénurie d'adresses IPv4 devrait disparaître au profit des opérateurs des zones les plus "défavorisées" par la répartition actuelle des ressources.

Signalons cependant que beaucoup d'opérateurs se tiennent prêts, mais restent attentistes, leur priorité étant actuellement de se renforcer dans un contexte de compétition exacerbée, avant de se lancer dans de nouvelles aventures technologiques.

II.2.2.3. ISP

L'arrivée d'IPv6 offre des possibilités aux ISP (Internet Access Provider) en termes d'allocations d'adresses IP permanentes, ce qui est très difficile actuellement dans une période de gestion de la pénurie d'adresses IPv4. En effet l'avantage introduit par IPv6 consiste essentiellement en la possibilité pour un ISP d'allouer un préfixe IPv6 permanent offrant à l'utilisateur final des adresses permanentes ou temporaires. On trouve déjà des exemples du côté des ISP japonais : IIJ, NTT ou eAccess assignent par exemple un /64 si un seul LAN est connecté ou un /48 si plusieurs LAN sont connectés ; à partir de là les machines peuvent avoir une adresses IPv6 permanentes et bien connue ou aléatoires (pour des raisons de vie privée par exemple).

L'affectation de préfixe et adresses IPv6 permanentes de la part des ISP sont nécessaires pour le déploiement de serveurs et d'applicatifs P2P.

II.2.2.4. Utilisateurs

Pour les utilisateurs "entreprises", IPv6 doit permettre, en allégeant la gestion des réseaux (fin du NAT notamment) de redonner une plus grande indépendance vis-à-vis des prestataires. L'adressage hiérarchique et l'auto configuration doivent permettre de changer de prestataire sans craindre la renumérotation des réseaux. La "géométrie" des réseaux peut être modifiée sans intervention lourde.

De nouvelles applications sont simplifiées (VoIP, Visio conférences,…etc.) et la sécurité doit être améliorée (IPSec possible en natif et de bout en bout).

Les utilisateurs individuels pourraient être les moteurs inconscients du déploiement d'IPv6, en consommant les nouvelles applications connectées (électronique, jeux en réseaux,…etc.) et en promouvant le nomadisme (Internet

mobile, véhicule communiquant,…etc.). Les nouveaux modèles économiques basés sur IPv6 pourraient leur permettre d'accéder plus facilement et moins cher à de nouveaux services.

III. Structure des en-têtes IPv6

III.1. Changements de l'en-tête IPv4 vers IPv6

- **IPv4**

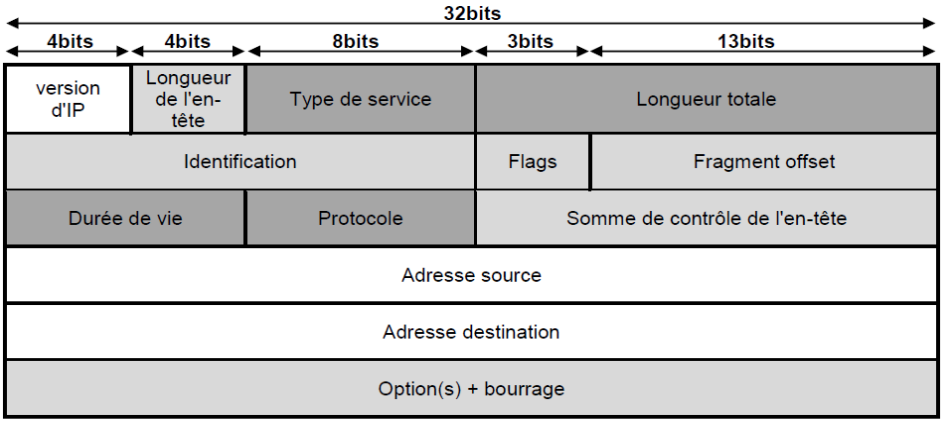


Figure 10. Format d'un datagramme IPv4

Version d'IP illustre le format du paquet IPv4. Après la valeur 4, pour le numéro de version, est indiquée la **longueur de l'en-tête**, qui permet de connaître l'emplacement du début des données du fragment IP.

Type de service, précise le type de service des informations transportées dans le corps du paquet. Ce champ n'a jamais été réellement utilisé avant l'arrivée des nouveaux protocoles de gestion relatifs à la qualité de service, comme DiffServ (Differentiated Services). Vient ensuite la **longueur totale** (Length). Le champ suivant « **Identification** » identifie le message auquel appartient le paquet.

Le drapeau (**Flag**) porte plusieurs notifications. Il précise, en particulier, si une segmentation a été effectuée. Si oui, la place du segment, provenant de la segmentation du message de niveau 4, est indiquée dans le champ **Fragment offset**.

TTL (Time To Live), ou **durée de vie**, spécifie le temps après lequel le paquet est détruit. Si le paquet ne trouve plus son chemin ou effectue des allers-retours, il est éliminé au bout d'un certain temps. Dans la réalité, cette zone contient une valeur

entière, indiquant le nombre de nœuds qui peuvent être traversés avant destruction du paquet.

Protocole indique le protocole qui a été encapsulé à l'intérieur du paquet.

Somme de contrôle de l'en-tête permet de déterminer si la transmission du paquet s'est effectuée correctement ou non. Enfin, les adresses de l'émetteur et du récepteur sont précisées dans la dernière partie de l'en-tête. Elles prennent une place de 4 octets chacune.

- **IPv6**

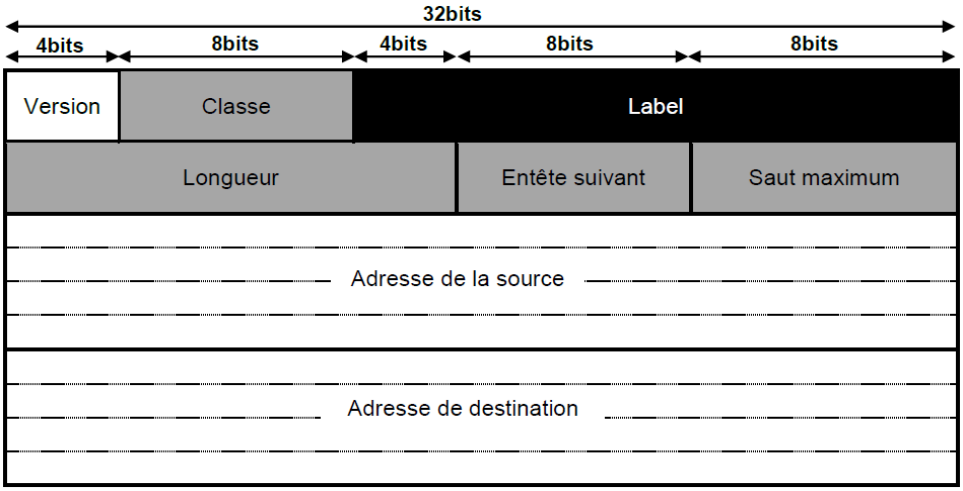


Figure 11. Format d'un datagramme **IPv6**

Nom du champ gardé de l'IPv4

Champ non conservées dans

Les changements de nom et la position dans IPv6

Nouveau champ dans IPv6

Version : Le champ est codé sur 4 bits. Il représente le numéro de version du Protocole Internet. Sa valeur est donc égale à 6.

Classe (Traffic Class) : Il est codé sur 8 bits. Il définit la priorité du datagramme afin que des nœuds origines et des routeurs transmetteurs puissent identifier et distinguer la classe ou la priorité du paquet IPv6.

Label (Flow Label) : Ce champ est codé sur 20 bits. Il peut être utilisé par une source pour nommer des séquences de paquets pour lesquels un traitement spécial de la part des routeurs IPv6 est demandé.

Longueur (Payload Length) : Il est codé sur 16 bits. Il indique le nombre d'octet des données qui suivent l'entête IPv6. Il faut noter que les options de l'entête IPv6 sont considérés comme de la donnée et font donc partie du calcul du champ Longueur.

Entête suivante (Next Header) : Il est codé sur 8 bits. Il identifie le type de donnée ou de l'option qui se trouve derrière l'entête IPv6.

Saut maximum (Hop Limit) : Il est codé sur 8 bits. Il indique le nombre de routeur maximum que le datagramme pourra traverser et est décrémenté de un (1) par chaque nœud que le paquet traverse.

Adresse source (Source Address) : Ce champ est codé sur 128 bits. Il représente l'adresse IP de l'émetteur.

Adresse destination (Destination Address) : Ce champ est codé sur 128 bits. Il représente l'adresse IP du destinataire.

III.2. ICMPv6 et l'auto-configuration [21]

III.2.1. ICMPv6 (Internet Control Message Protocol version 6)

ICMPv6 est la nouvelle version du protocole ICMP, le protocole de contrôle d'IP, correspondant à IPv6. Définit par le RFC 2463, il intègre en plus des fonctions de gestion des groupes de Multicast, réalisées jusqu'alors par le protocole IGMP[23], les fonctions du protocole ARP[24] et gère les messages de découverte du voisinage (sollicitation d'un voisin, annonce de routeur,…etc.). Chaque message ICMPv6 est précédé par une en-tête IPv6 au minimum. L'entête ICMPv6 est identifié par une valeur du champ « Next Header » à 58 dans l'entête du datagramme IPv6. La figure 12 ci-dessous donne le format d'un message ICMPv6.

[23] Est un protocole qui permet à des routeurs IP de déterminer de façon dynamique les groupes multicast qui disposent de clients dans un sous-réseau.

[24] Est un protocole effectuant la traduction d'une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse MAC (typiquement une adresse ethernet), ou même de tout matériel de couche de liaison. Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

Type	Code	Checksum
Messages		

Figure 12. Format d'un message ICMPv6

On distingue plusieurs types de messages ICMPv6 qui se différencient par la valeur du champ « type » comme le montre le tableau suivant.

Tableau 3. Les différents types de messages ICMPv6

Type	Signification
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

III.2.2. La découverte de voisinage (Neighbor Discovery Protocol)

Le protocole de découverte des voisins permet à un équipement de s'intégrer dans l'environnement du réseau local, c'est à dire le lien sur lequel sont physiquement transmis les paquets IPv6. Il possède plusieurs fonctionnalités :

- **La résolution d'adresses :** Le principe est très proche du protocole ARP d'IPv4. La principale différence vient de l'emploi de messages standards ICMPv6 à la place de la définition d'un autre protocole. Comme pour ARP,

une table de correspondance entre les adresses physiques et les adresses IPv6 est construite.

- **La détection d'inaccessibilité des voisins :** Cette fonction appelée aussi "NUD" (Neighbor Unreachability Detection) n'existe pas en IPv4. Elle permet d'effacer dans le cache des voisins les entrées correspondants aux voisins inaccessibles (panne, changement d'adresse,…etc.)

III.2.3. La configuration automatique

L'auto-configuration est l'un des principaux atouts d'IPv6. Il se fait en deux modes. Le mode **Stateful** (auto-configuration avec état) et le mode **Stateless** (auto-configuration sans état).

- **Le mode Stateful :** Il consiste soit en une configuration manuelle de l'équipement, soit une configuration automatique avec DHCPv6[25].
- **Le mode Stateless :** Il est utilisé pour une configuration des nœuds simples uniquement. Ce mode d'auto-configuration se base sur le protocole NDP[26], avec en particulier les sollicitations et annonces de routeurs qui permettent de véhiculer les informations concernant le préfixe, la passerelle par défaut,…etc.

III.2.4. Découverte de MTU (Maximum Transmission Unit)

Avec IPv6 les routeurs ne doivent plus fragmenter les paquets qui sont transmis. Le MTU minimum doit être de 1280 octet pour un lien souhaitant supporter IPv6. Si n'est pas le cas, des mécanismes de fragmentation et de réassemblage doivent être effectués par les couches inférieures à la couche réseau. La nécessité d'adapter la taille des paquets à transmettre pour un flot important de données existe quand même. Si elle n'est pas réalisée par les routeurs, la fragmentation doit donc se faire à la source. Un algorithme de découverte permet de connaître la taille optimale des paquets à transmettre, cet algorithme est appelé Path MTU Discovery et se présente comme suit :

[25] Un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau

[26] Protocole utilisé par IPv6. Il opère sur la couche 3 et est responsable de la découverte des autres hôtes sur le même lien

(1) Le nœud source considère que le MTU du chemin considéré est égal au MTU du premier saut de ce chemin.

(2) Envoi d'un paquet à la destination.

(3) Si réception d'un message ICMPv6 de type « Packet To Big», la source réduit le MTU courant. Retour à (2).

(4) Si pas de réponse de la destination, retourne à (2).

(5) Si réponse de la destination, le MTU du chemin est le MTU courant.

Sur certains liens, le MTU peut varier au cours de la communication. Afin de tirer partie d'une augmentation de MTU, la source reprendra l'algorithme à intervalles réguliers.

IV. Le système d'adressage IPv6 [22]

IV.1. Structure des adresses IPv6

L'adressage IPv6 propose des adresses d'une longueur de 128 bits. La représentation textuelle d'une adresse IPv6 se fait en découpant le mot de 128 bits de l'adresse en 8 mots de 16 bits séparés par le caractère «:», chacun d'eux étant écrit en hexadécimal.

Nous avons par exemple :

FEDC:0000:0000:0000:0400:A987:6543:210F

Dans un champ, il n'est pas nécessaire d'écrire les zéros placés en tête :

FEDC:0:0:0:400:A987:6543:210F

En outre plusieurs champs nuls consécutifs peuvent être abrégés par «::».

Ainsi l'adresse précédente peut s'écrire comme suit :

FEDC::400:A987:6543:210F

Pour éviter toute ambiguïté, l'abréviation «::» ne peut apparaître qu'une seule fois au plus dans une adresse.

La représentation des préfixes IPv6 est similaire à celle utilisée pour les préfixes IPv4. Un préfixe IPv6 est donc représenté par la notation :

adresse-IPv6 / longueur-du-préfixe-en-bits

Nous avons par exemple les représentations suivantes :

3EDC:B198:7654:3210:0000:0000:0000:0000 / 64 ou encore

3EDC:B198:7654:3210:0:0:0:0 / 64

Toutes ces représentations des adresses IPv6 peuvent apparaître beaucoup plus complexes qu'avec IPv4, mais leur attribution répond à des règles strictes, ce qui favorise leur mémorisation. De plus, les fonctions d'auto-configuration font qu'il est très rare, même pour un ingénieur réseau, de les manipuler.

IV.2. Les différents types d'adresses IPv6

Contrairement à l'adressage IPv4 qui utilise des adresses par classe, IPv6 dispose de 3 grands groupes d'adresses ayant chacun des spécificités bien définies. Nous avons les adresses Unicast, les adresses Multicast et les adresses Anycast.

IV.2.1. Les adresses Unicast

Les adresses Unicast sont les plus simples. Une adresse de ce type désigne une interface unique. Un paquet envoyé à une telle adresse, sera donc remis à l'interface ainsi identifiée.

Il existe différents types d'adresses Unicast classés selon leur portée.

IV.2.1.1. Les adresses globales Unicast

Ce sont des adresses Unicast ayant une portée globale. Elles permettent de désigner sans ambigüité une machine sur le réseau Internet. Elles représentent les $1/8^{eme}$ de l'espace d'adressage d'IPv6. Elles sont caractérisées par le préfixe 2000::/3.

Les adresses Unicast globales sont ouvertes à la réservation depuis 1999. Ces adresses sont allouées par bloc /23 à /12 par l'IANA à un registre Internet régional. Certains blocs sont réservés à un usage particulier c'est le cas par exemple du bloc 2002::/16 utilisé pour mettre en œuvre les tunnels broker 6to4. **[25]**

La figure ci-dessous illustre la structure d'une adresse globale Unicast telles que définie dans le RFC 3587. **[23]**

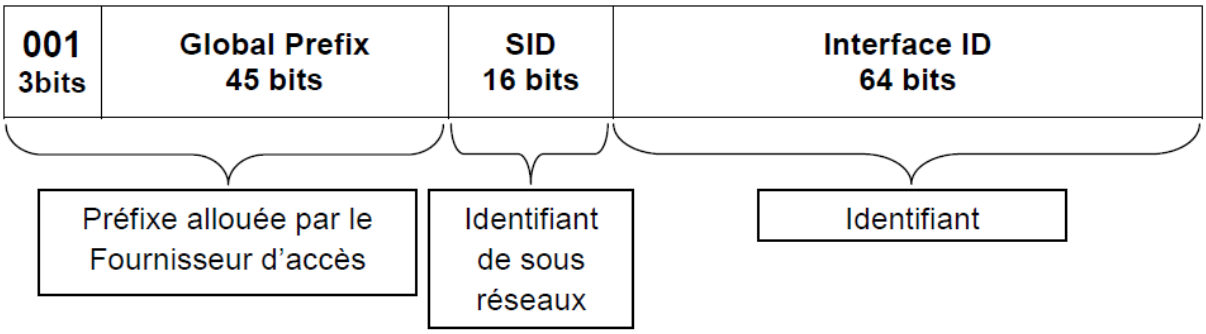


Figure 13. Structure d'une adresse globale Unicast

IV.2.1.2. Les adresses locales uniques

Elles sont utilisées pour les communications locales et ne sont routables que sur les sites qui le souhaitent.

1111	1110	11	0	ID Subnet	ID Interface

Figure 14. Structure d'une adresse locale unique

Les 48 premiers bits sont toujours fixes pour ce type d'adresse et commencent par FEC0::/48

Subnet ID (16 bits) représente l'identifiant d'un sous réseau à l'intérieur du site.

Interface ID (64 bits) représente l'identifiant d'interface.

IV.2.1.3. Les adresses locales de lien

Les adresses de type lien-local (link local use address) sont des adresses dont la validité est restreinte à un lien, c'est-à-dire l'ensemble des interfaces directement connectées sans routeur intermédiaire comme par exemple des machines branchées sur un même réseau Ethernet. Les adresses lien-local sont configurées automatiquement à l'initialisation de l'interface et permettent la communication entre nœuds voisins. L'adresse est obtenue en concaténant le préfixe FE80::/64 aux 64 bits de l'identifiant d'interface. L'identifiant d'interface est généralement basé sur l'adresse MAC. Contrairement aux adresses globales, les adresses lien-local ne sortent jamais du réseau local où elles sont utilisées. Elles sont caractérisées par le préfixe fe80::/64 .

La figure 15 ci-dessous donne la structure d'une adresse locale de lien.

FE80 10 bits	0...0 54 bits	Interface ID 64 bits

Figure 15. Structure d'une adresse locale de lien

Les adresses locales de lien et locales de site ne sont pas routables sur Internet. Au niveau des adresses Unicast, le champ Interface ID peut être configuré automatiquement à partir de l'adresse MAC du poste. Cependant, il est souhaitable d'imposer manuellement une valeur à ce champ au niveau des routeurs et des serveurs. Cet identifiant, lorsqu'il est attribué automatiquement, porte le nom de **EUI-64** (Extended Unique Identifier sur 64 bits). Le principe d'obtention de l'EUI est très simple. Supposons une interface ayant pour adresse physique AA:BB:CC:DD:EE:FF. Elle aura pour identifiant EUI-64 le suffixe 0002**:AABB:CCDD:EEFF.**

Ainsi, toute interface ayant pour adresse MAC AA:BB:CC:DD:EE:FF aura par exemple pour adresse IPv6 Link Local: FE80::0002**:AABB:CCDD:EEFF** De la même façon que l'adresse MAC est unique, l'EUI-64 est unique.

IV.2.2. Les adresses Multicast

Une adresse de type Multicast désigne un groupe d'interfaces qui en général appartiennent à des nœuds différents pouvant être situés n'importe où dans l'Internet. Lorsqu'un paquet a pour destination une adresse de type Multicast, il est acheminé par le réseau à toutes les interfaces membres de ce groupe. Il faut noter qu'il n'y a plus d'adresses de type Broadcast comme sous IPv4, elles sont remplacées par des adresses de type Multicast qui saturent moins un réseau local constitué de commutateurs.

Les adresses Multicast sont caractérisées par le préfixe ff00::/8

1111	1111	000T	Scope	ID Group

Figure 16. Structure d'une adresse Multicast

Cette adresse peut être permanente (T=0) ou temporaire(T=1), le bit T marque cette différence. L'étendue de la diffusion est définie par le champ scope de

l'adresse. Par exemple pour une vidéoconférence, sa diffusion peut être confinée au lien local, au site ou au-delà selon la valeur du champ scope.

IV.2.3. Les adresses Anycast

Une adresse de type Anycast désigne un groupe d'interfaces, la différence avec l'adresse Multicast réside dans le fait que lorsqu'un paquet a pour destination une telle adresse, il est acheminé à un des éléments du groupe et non pas à tous. Nous avons ci-dessous la structure d'une adresse Anycast.

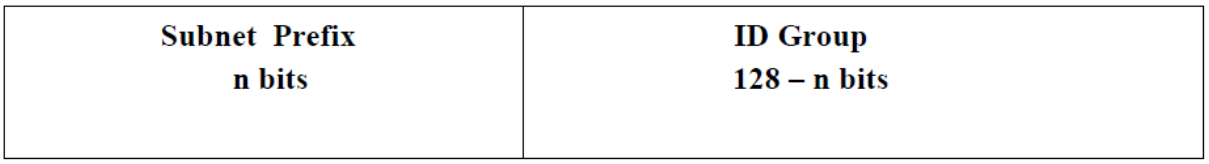


Figure 17. Structure d'une adresse Anycast

V. Le routage dans un réseau IPv6

Le routage est un processus très important dans les réseaux IP. Avec l'apparition du protocole IPv6, plusieurs changements ont été observés au niveau du routage au sein des réseaux. Ces changements sont essentiellement liés à la prise en compte du format de l'adresse IPv6, ainsi qu'à l'ajout d'une nouvelle table de routage dédiée à IPv6. Nous passerons en revue tous les types de routage à savoir le routage statique, le routage interne et le routage externe.

V.1. Le routage statique

Le routage statique en IPv6 est identique à celui d'IPv4 avec le préfix et l'adresse du tronçon suivant qui sont en IPv6.

Dans ce type de routage, l'administrateur se charge lui-même d'indiquer les différentes routes pour transférer les paquets d'un réseau à un autre. Il est souvent utilisé dans les architectures où le nombre de routeurs à relier est moins important.

V.2. Le routage dynamique

Le routage dynamique comme en IPv4 se base essentiellement sur des algorithmes de routage. En IPv6, ces algorithmes de routage qui existaient sous IPv4 n'ont pas vraiment changé. Cependant, ils profitent des propriétés maintenant

incluses dans la nouvelle version du protocole IP comme l'authentification ou le Multicast. **[24]**

Nous avons alors les protocoles de routage IPv6 suivant :

- **RIPng :** C'est le premier protocole de routage dynamique proposé pour IPv6 par le RFC 2080.
- **OSPFv3 :** Il est basé sur l'algorithme du plus court chemin et est plus difficile à mettre en œuvre que RIPng. Il est plus efficace dans les détections et la suppression des boucles dans les phases transitoires. OSPF a été adapté à IPv6 par le RFC 2740.
- **IS-IS:** Il est comme OSPF un protocole interne de routage à états de liens. La particularité de IS-IS est qu'il n'utilise pas IP comme protocole réseau pour l'échange de ses messages. Cette caractéristique lui permet donc d'être totalement indépendant des protocoles qu'il route.
- **BGP :** Dans les réseaux IPv6, le protocole BGP joue le même rôle, il permet le routage des paquets entre Système Autonomes ou domaine de routage. Ainsi, la version pour IPv4 nommée BGP-4 a été plus ou moins transformé pour donner un nouveau protocole appelé MP-BGP.

VI. Les mécanismes de transitions IPv4 vers IPv6

VI.1 La double-pile IP (Dual Stack)

La double pile IP consiste à équiper un équipement du réseau d'une double pile protocolaire (Dual Stack) et à lui affecter une adresse IPv4 et une adresse IPv6. Cela peut s'appliquer sur la plupart des systèmes d'information. Les serveurs doivent alors avoir deux sockets, l'une correspondant à une écoute via IPv4, et l'autre correspondant à une écoute via IPv6. Il faut donc garder en mémoire que, dans ce cas là, les deux protocoles sont installés sur le même système. Ils communiquent directement entre eux et séparément avec l'extérieur.

VI.2 Transport d'IPv6 dans IPv4

Il n'est pas toujours possible d'avoir une double pile IP ou un réseau IPv6 de bout-en-bout. Cependant, les trames IPv6 doivent pouvoir être transmises, même si un réseau intermédiaire ne supporte qu'IPv4. Plusieurs solutions sont disponibles

pour former un tunnel. Les paquets IPv6 transitent alors encapsulés dans IPv4, ce qui s'appelle autrement un tunnel IPv4. Nous distinguons les tunnels statiques et les tunnels automatiques.

A. Les tunnels statiques

La solution la moins souple consiste à établir un tunnel par le protocole GRE[27] (Generic Routine Encapsulation), comme cela se fait déjà sous IPv4 pour d'autres protocoles. Le tunnel est statique, et il faut alors effectuer des modifications aux deux extrémités du tunnel. Il n'y a par ailleurs, tel quel, aucune garantie de sécurité.

Au lieu de configurer manuellement chaque extrémité des tunnels, il est aussi possible d'automatiser un peu la procédure, tout en maintenant la structure statique du tunnel. Le principe est très similaire à celui d'un VPN. Des serveurs, nommés IP Tunnel Brokers servent pour la transition. Il faut se connecter à l'un d'eux en IPv4 pour obtenir une adresse et accéder à la configuration du tunnel vers un réseau IPv6. Ce procédé est bien statique (ou semi-dynamique), dans la mesure où il nécessite de connaître et de configurer correctement IPv4 au niveau du Tunnel Broker. Ce dernier se charge du routage et des configurations des extrémités des tunnels.

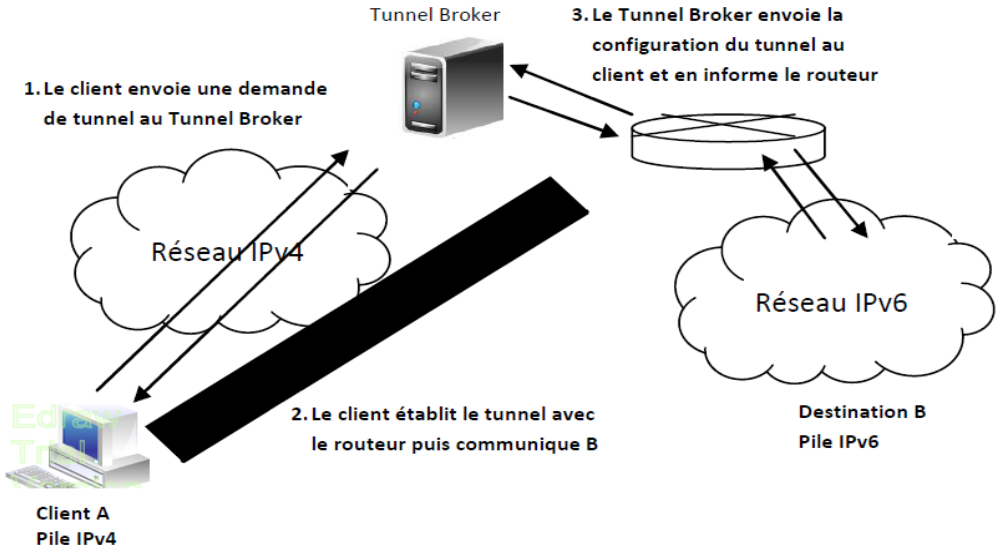


Figure 18. Exemple de tunnel statique sous la tutelle du Tunnel Broker

[27] Est un protocole de mise en tunnel qui permet d'encapsuler n'importe quel paquet de la couche réseau.

B. Tunnels automatiques : IPv6 dans IPv4

Dans le cas d'un tunnel automatique, une liaison fixe point à point est établie entre les machines impliquées. Ce tunnel formé fragmente les paquets selon IPv4 et met en œuvre les mécanismes de découverte des voisins. Si une erreur survient au cours de l'acheminement IPv4, un paquet ICMPv4 est envoyé. Idéalement, le point à la source du tunnel devrait récupérer ce message, puis le traduire en un paquet ICMPv6 équivalent afin de le retourner vers la source du datagramme IPv6. Le transport de datagrammes IPv6 dans une trame IPv4 est précisé dans le RFC 2893. Il existe à l'heure actuelle trois mises en œuvre majeures pour effectuer l'acheminement d'IPv6 sous IPv4 : 6to4, ISATAP, Teredo. **[25]**

VII. Conclusion

A travers ce chapitre, on peut conclure plusieurs points qui sont :

- IPv4 : un protocole non pensé pour un usage commercial mais qui a su s'adapter au fur et à mesure des demandes du marché.
- De nombreux outils et protocoles ont été développés pour pallier les limitations d'IPv4.
- L'espace d'adressage restreint d'IPv4 conduira à des difficultés techniques de plus en plus difficiles à gérer (La prolifération des NAT en est un exemple).
- L'immense espace d'adressage qu'offre IPv6 justifie à lui tout seul le passage au nouveau protocole.
- IPv6 offre de plus d'autres fonctionnalités intéressantes : auto configuration, adressage hiérarchique, QoS,…etc.
- Parmi les acteurs, ce sont les équipementiers qui voient le plus d'intérêt à un passage à IPv6 : levier de croissance.

Chapitre III

L’intégration d’IPv6 dans les RCSF (6LoWPAN)

I. Introduction

Dans les normes en développement qui concerne les applications à bas débit et à basse consommation, on trouve le standard IEEE 802.15.4. Ce standard favorise une très faible consommation de l'interface radio et offre des débits relativement faibles. Il offre également une bonne sécurité au niveau de la protection des données (cryptage des données au niveau MAC). Ce futur standard ouvert est d'ailleurs en train d'être complété par une association de plusieurs compagnies sous le nom de Zigbee™ et 6LoWPAN. Leur but étant de proposer un standard pour réseau sans fil à basse consommation et à bas coûts en normalisant les couches supérieures aux fonctionnalités MAC et Physique déjà décrites par le standard IEEE 802.15.4.

Le groupe de travail 6lowpan de l'IETF travaille actuellement pour adapte IPv6 sur le protocole radio IEEE 802.15.4. La réussite de 6lowpan permettra le développement d'un véritable Internet d'objets, connectant des équipements qui ne sont pas en général classés parmi les ordinateurs comme les capteurs et les autres dispositifs de surveillance et de détection,…etc. **[26]**

II. IEEE 802.15.4 [27]

II.1. Introduction à 802.15.4

La norme IEEE 802.15.4 est récente et concerne uniquement les deux premières couches du modèle OSI, à savoir la couche physique et la couche liaison de données. C'est un standard de communication à bas débit qui fait partie des réseaux locaux personnels (PANs). Elle a été conçue pour garantir une facilité d'installation, un maximum de fiabilité de transfert de données, une opérabilité à court terme, un faible coût et une consommation d'énergie optimisée. La conception reste aussi simple et flexible.

Voici quelques caractéristiques générales du réseau :

- Les débits de données de 250, 100, 40, 20 kb / s.
- Configuration réseaux étoile ou peer to peer
- Allocation d'adresses de 16 bits ou 64bits
- Accès multiple au canal avec CSMA /CA
- Protocole entièrement reconnu pour la fiabilité de transfert

- Faible consommation
- Indication de qualité du lien

Les types de dispositifs qui constituent le cœur du réseau Pan (Personal Area Network) 802.15.4 sans fil sont :

- **Le coordinateur**, élément central du réseau.
- **Le Fully Functional Devices (FFD)**, élément se liant à un coordinateur, mais pouvant effectuer quelques opérations de routages.
- **Le Reduced Functional Devices (RFD),** élément terminal du réseau.

II.2. Topologies de réseaux

Les nœuds du réseau peuvent être connectés des façons suivante : a) topologie en étoile, b) topologie peer to peer selon les spécifications d'application. En topologies en étoile un dispositif FFD coordonne le réseau puisque tous les nœuds communiquent par son intermédiaire. Chaque nœud du réseau dispose d'une adresse 64 bits ou une adresse de 16 bits (court) qui est délivrée par le coordinateur de PAN. Des exemples d'applications qui pourraient tirer profit de ce type de topologie sont : L'automatisation personnelle, les appareils de jeux et les dispositifs de soins de santé,…etc.

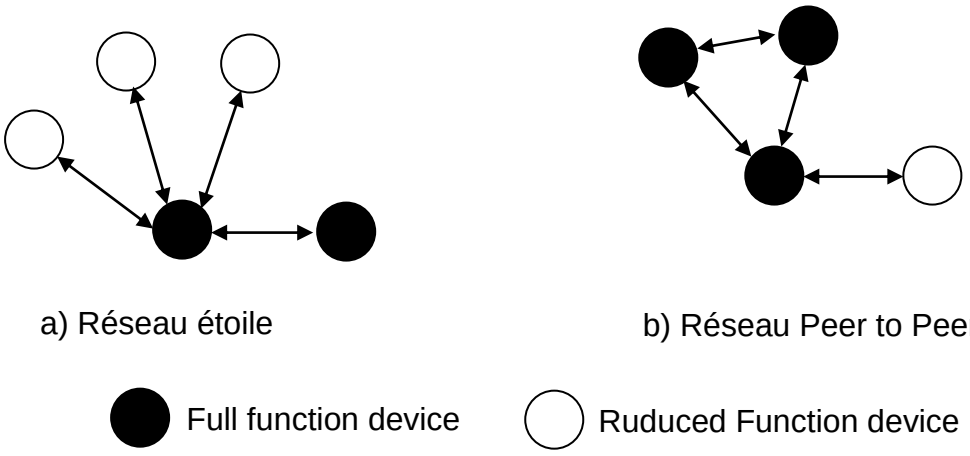


Figure 19. Topologies de réseaux pris en charge par 80.15.4

Dans un réseau peer to peer, les dispositifs communiquent les uns avec les autres tant qu'ils peuvent s'atteindre. Ces topologies de réseau nécessitent l'auto-

organisation et permettent l'utilisation des protocoles de routage. Ces protocoles ne sont pas définis dans la norme 802.14.5.

Dans la topologie en étoile, les FFD (coordinateurs) choisissent un identifiant unique PAN qui n'est pas utilisé par les autres réseaux PAN à proximité. L'identifiant PAN permet aux autres dispositifs d'être connecté dans le même réseau. Dans les réseaux peer to peer des groupes peuvent êtres formés, chaque groupe a un coordinateur qui fournit des mécanismes de synchronisation. Ces groupes sont hiérarchisés et leur structure impose qu'il existe seulement un coordinateur global offrant des mécanismes de synchronisation pour le reste des coordinateurs. C'est possible que le coordinateur donne le contrôle à un autre nœud du système.

La norme *IEEE 802.15.4* est utilisée dans les applications embarquées comme le monitoring environnemental pour l'agriculture, le monitoring de structure pour les bâtiments et l'état des ponts, le contrôle industriel,…etc. Cette norme définit une couche physique (PHY) et une couche *Media Acces Control* (MAC) qui sont utilisées dans *LowPower Personal Area Network* (6LoWPAN).

II.3. Principes de la couche physique définie par 802.15.4

II.3.1. Caractéristiques générales

La couche physique de 802.15.4 est parfaitement adaptée aux besoins des topologies réseaux de faible coût, faible consommation et faible débit. Les services de base qu'elle fournit sont la transmission et la réception des données, l'indication de qualité de lien (IQT), l'activation et la désactivation du récepteur de radio, de sélection de fréquence et la détection d'énergie (ED) dans le canal actuel. Les principales caractéristiques de la couche physique sont :

Bande de fréquence [MHz]	Numéro du canal	Modulation	Bit rate [kb/s]	Symbol rate [kb/s]
868 - 868.6	0	BPSK	20	20
902 - 928	1,2,... 10	BPSK	40	40
2400 - 2483.5	11,12,... 26	O-QPSK	250	62.5

Tableau 4. Caractéristiques de la couche PHY

La norme réunie en réalité deux couches physiques pratiquement identiques, chacune d'elles pouvant être combinées avec la couche MAC. La différence

fondamentale entre les deux couches physiques est la bande de fréquence utilisée. L'une utilise la bande ISM 2.4 GHz et l'autre les bandes ISM 868 MHz (Europe) ou 915 MHz (Etats-Unis). La solution 2.4 GHz offre les meilleures performances. La solution 868/915 MHz est plutôt présente comme alternative si l'espace utilisé est déjà très encombré par d'autres appareils utilisant déjà la bande 2.4 GHz.

Il existe un degré de flexibilité dans le choix du régime de modulation appropriée pour l'application requise. La modulation BPSK implique de faibles débits et de la complexité émetteur-récepteur tandis que ASK, QPSK impliquent des débits et des complexités plus élevés.

La couche physique contient plusieurs fonctions de bas niveau permettant l'implémentation d'une sélection dynamique de canaux qui se fait aux couches supérieures :

- Détection d'énergie à la réception
- Indication de qualité du lien
- Gestion de la commutation de canal

Ces fonctions sont surtout utilisées lors de l'établissement de la connexion initiale au canal et pour les commutations de canaux.

II.3.2. Structure générale d'un paquet PHY

La structure des deux couches physiques est la même afin d'avoir une compatibilité unique avec la couche MAC, cette structure de trames est présente à la figure 20.

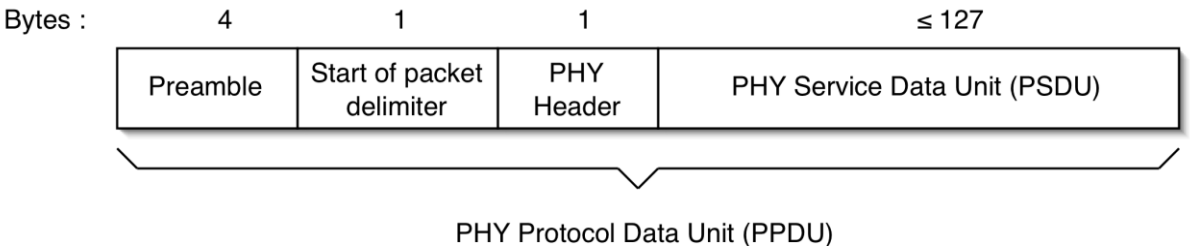


Figure 20. Structure générale d'une trame PHY

L'ensemble de la trame est appelé PPDU (PHY Protocol Data Unit). Les 5 premiers bytes de la trame correspondent à un en-tête de synchronisation (Preamble

+ Start of packet delimiter). Le Byte « Start of packet delimiter » permet de spécifier la fin du préambule. Sinon, les 32 bits du préambule sont notamment prévus pour :

- Acquisition des symboles
- Synchronisation des « Chips »
- Ajustement de la fréquence (dans certain cas seulement)

Le champ « PHY Header » sert principalement à connaître la longueur de la cargaison avec un codage sur 7 bits des 8 disponibles. Le bit restant n'étant pas utilisé (réservé).

II.4. Principes de la couche MAC du 802.15.4

II.4.1. Rôles et services

La couche MAC a plusieurs rôles importants à réaliser :

- Mécanisme d'accès au canal
- Ordonnancement des données
- Délivrèrent des trames d'acquittement (ACK)
- Entretien des « time slot »
- Gestion des « Beacons » (signaux balises)
- Garantir l'intégrité des données

La couche MAC fournit deux services aux couches supérieures : SAP (Service Access Point) :

- Service de données : MCPS-SAP (MAC Common Part Sublayer)
- Service de gestion : MLME-SAP (MAC Layer Management Entity)

La couche MAC reçoit deux services de la couche physique qui est la couche inférieure :

- Service de données : PD-SAP (PHY Data service)
- Service de gestion : PLME-SAP (PHY Layer Management Entity)

II.4.2. Structure générale des paquets

Il existe 4 structures de paquet au niveau MAC :

- Trame de données
- Trame « Beacon » (trame phare)
- Trame d'acquittement (ACK)
- Trame de commande

Les trames de données et de Beacon peuvent contenir des informations qui proviennent ou qui sont destinées aux couches supérieures. Les deux autres structures de trames sont générées et ne sont utilisées que par la couche MAC. Néanmoins, les trames Beacon peuvent ne contenir aucune information venant des couches supérieures et donc, n'être utilisées également que par la couche MAC.

A. Structure d'une trame de données

La structure générale d'une trame MAC de donnée est visible à la figure 21.

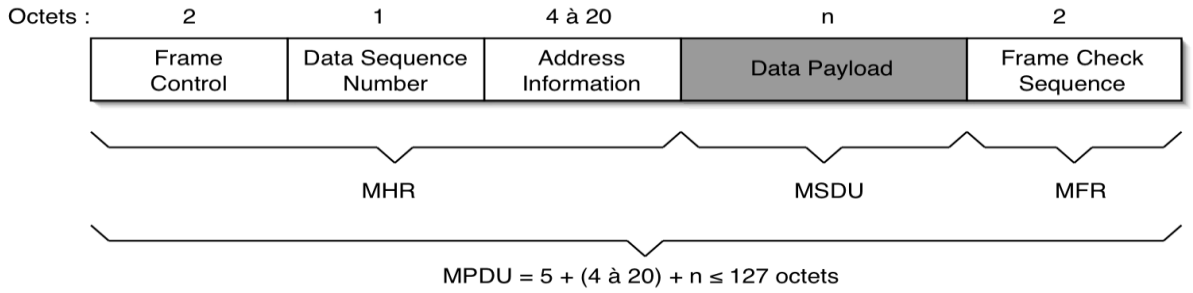


Figure 21. Structure d'une trame MAC de donnée

La trame complète est appelée MPDU (MAC Protocol Data Unit) et ne peut posséder plus de 127 octets. Elle contient un en-tête (MHR), des données provenant des couches supérieures (MSDU) et une fin de séquence (MFR). Voici la description des différents champs contenus dans l'en-tête et la fin de séquence.

- **Frame Control (2 ou 3 octets) :** Ce champ de 16-24 bits d'informations est commun à tous les types de trames et sert à spécifier la structure et le contenu du reste de la trame.
- **Data Sequence Number (1 octet) :** Ce champ défini une numérotation de trames sur 8 bits, qui est notamment utilisée lors des acquittements afin de connaître quelles trames ont été acquittées. Sa valeur correspond à la variable PIB *macBSN*, qui est initialisée aléatoirement puis, pour chaque trame, elle est incrémentée d'une unité. Ce champ est utilisé pour les trames de type de données, de commande et d'acquittement.

- **Address Info (4 à 20 octets):** Spécifie l'adresse de l'émetteur et de récepteur à qui les trames sont envoyées. L'adresse peut être courte (16 bits) ou étendue (64 bits).
- **Data Payload (cargaison) :** Ce champ a une longueur variable. Néanmoins, une trame MAC total (MPDU) ne peut dépasser 127 octets de longueur. Le contenu de la cargaison est appelé MSDU et dans le cas d'une trame de données, celle-ci provient toujours des couches supérieures.
- **Frame Check Sequence (2 octets) :** Ce champ, qui s'ajoute après la cargaison, sert à contrôler l'intégrité des en-têtes et des données de la trame. Il est obligatoire pour tous les types de trames. Aucune correction n'est faite, si des bits erronés sont détectés, il doit y avoir retransmission.

B. Fonctions des trames Beacon

Les trames « Beacon » ne peuvent être transmises que par un dispositif possédant toutes les fonctionnalités (FFD). Les informations qu'elles contiennent servent à la gestion du réseau en décrivant les caractéristiques du PAN. C'est à l'aide de Beacons que la définition d'un mode de transmission que l'on appelle Superframe (réseau « Beacon Enabled ») est possible, ce mode de transmission va servir à la synchronisation du réseau. C'est-à-dire que le coordinateur du PAN envoie régulièrement des Beacons et que les dispositifs utilisent la réception régulière des Beacons pour tenir une base temps commune. Une autre fonctionnalité des Beacons concerne les transmissions indirectes, c'est-à-dire que le Beacon peut contenir des adresses de dispositifs qui indiquent que des données sont en attente chez le coordinateur du PAN et qu'il faut aller les récupérer.

C. Fonctions des trames d'acquittement

Une autre fonction de la couche MAC est d'acquitter la réception de données ou de commandes. C'est dans le champ « Frame Control » de l'en-tête de la trame que l'on indique s'il doit y avoir acquittement ou pas. La trame d'acquittement est envoyée immédiatement après la réception de la trame à acquitter.

D. Fonctions des trames de commande

Les trames de commande sont utilisées pour réaliser des demandes des différentes fonctionnalités MAC.

II.4.3. Méthodes d'accès au canal

L'une des tâches principales de la couche MAC est de proposer une méthode d'accès au canal. La norme contient deux méthodes d'accès, la principale est la méthode CSMA-CA qui est implémentée en deux versions, l'une non synchronisée (utilisé dans un réseau « Non Beacon Enabled ») et une synchronisée sur des Backoffs (utilisé dans un réseau « Beacon Enabled »). La deuxième méthode d'accès est une forme de polling par réservation de temps qui est obtenu grâce à un mode de transmission spécifique que l'on appelle Superframe. Cette dernière méthode ne peut-être obtenue que dans un réseau synchronisé par un coordinateur (réseau « Beacon Enabled »).

A. CSMA-CA

Le principe du CSMA-CA (Carrier Sense Multiple Access - Collision Avoidance) est de détecter l'activité du réseau avant de transmettre, afin d'éviter des collisions. Si le canal de transmission n'est pas libre, on attend qu'il se libère.

Il existe deux versions de l'algorithme du CSMA-CA dans la description du standard, la principale différence est que l'un est synchronisé pour l'accès au canal, tandis que l'autre ne l'est pas :

- CSMA-CA slotted (synchronisé sur des Backoffs)
- CSMA-CA unslotted

Avec la version du CSMA-CA « slotted », la couche MAC doit s'assurer que la couche PHY commence toutes ses transmissions pile sur le début d'une période de Backoff. Tous les dispositifs d'un même PAN sont donc exactement alignés entre eux lorsqu'ils doivent transmettre ou recevoir.

Avec la version du CSMA-CA « unslotted », les périodes de Backoff d'un dispositif n'ont aucun lien temporel avec les périodes de Backoff d'un autre dispositif associé au même PAN.

B. Structure d'une Superframe

Une Superframe ne peut être générée qu'avec la topologie en étoile où un coordinateur PAN est présent. C'est ce dernier qui synchronise le PAN et gère les réservations de temps en envoyant des Beacons.

Une Superframe est délimité par deux trames Beacon (signal balise). La partie active de la Superframe est toujours constituée de 16 slots de durée équivalente. Cette partie active est généralement divisée en deux, une période avec contention (CAP) et une période sans contention (CFP). La Superframe peut également contenir une partie inactive (non obligatoire) qui permet alors au coordinateur PAN d'entrer dans un mode de basse consommation. La structure générale d'une Superframe est à la Figure x.

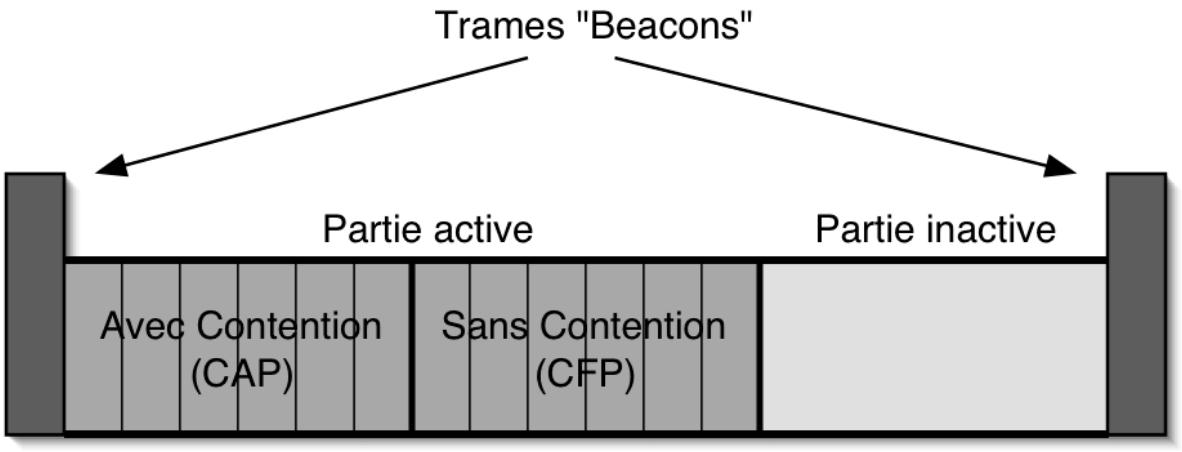


Figure 22. Structure générale d'une Superframe

La norme 802.15.4 définit deux modes d'adressages locaux, soit le 64 bits IEEE EUI mode, soit le mode 16 bits (court) d'adressage. Ces adresses sont employées directement par la couche 6LoWPAN afin de produire directement les adresses IP. En outre le mode 16 bits permet davantage de compression des en-têtes d'IP, même s'il y a certains cas où les adresses ne peuvent pas être utilisées.

III. Problèmes d'implémentation d'IPv6 sur 802.15.4

- **Fortes contraintes sur le MTU :** IPv6 requiert un MTU de 1280 octets et indique que tout lien ne remplissant pas cette contrainte doit implémenter de la fragmentation de niveau liaison afin que celle-ci soit transparente du point de vue d'IPv6.
- **Coût de l'entête IPv6:** Le protocole possède une taille d'en-tête minimum de 40 octets auxquels s'ajouteront les 8 octets d'UDP. Ainsi pour un paquet 802.15.4 auquel on appliquerait un chiffrement (natif pour 802.15.4), l'en-tête IPv6 et l'en-tête UDP…etc. Il resterait seulement 33 octets de disponibles. Existe-t-il des solutions ?

- **Fragmentation de niveau liaison:** L'obligation de fragmentation transparente pour la couche réseau va conduire à une très forte charge de découpage/ reconstruction pour des éléments n'ayant clairement pas le potentiel.
- **Loose Source Routing :** IPv6 a réintroduit le support de cette technique de routage. C'est un moyen permettant à un hôte de spécifier explicitement le chemin que va emprunter son paquet. Cela conduit à un certain nombre de problèmes, et spécialement en termes de sécurité. L'exemple nous concernant est celui permettant à un hôte de pouvoir indiquer une boucle dans son paquet (échange continu entre un routeur R1 et un routeur R2) qui va conduire à une surcharge artificielle du réseau (particulièrement dans les réseaux de capteurs). Comment s'affranchir de ce problème ?
- **Définition de la « qualité de service » :** Elle est l'une des principaux objectifs d'IPv6. Évidemment pour les réseaux de types *LAN Ethernet* ou apparentés, la vitesse, la couverture du réseau, le taux d'erreur, la différenciation de services, etc. sont des critères évidents. Mais qu'en est-il pour les réseaux de capteurs sans fil?
- **Les protocoles utilisés :** Lors de la transition d'*IPv4* à *IPv6*, un grand nombre de protocoles ont été mise à jour afin de respecter la structure des nouvelles trames. Cependant, pour le passage d'IPv6 à *6LoWPAN* certains protocoles ne conviennent toujours pas, plus pour des notions de structures, mais pour des problèmes de fonctionnement.
- **La mobilité :** *IPv6* introduit la notion de mobilité avec le *RFC3775*. La mobilité pour IPv6 implique des éléments qui se déplacent et qui doivent garder leurs connexions et leurs adresses même lorsqu'ils changent de réseaux,...etc. On conçoit aisément la différence de mobilité que vont être les *WSNs* où les objets ne se déplacent pas, mais peuvent « s'endormir » et donc apparaître/disparaître subitement du réseau sans mouvement.
- **Le routage :** Les protocoles de routages pour *IPv6* mobiles ne conviennent pas pour différentes raisons : utilisation massive de paquets, du multicast,…etc. Comment réaliser le routage sur des réseaux où ces méthodes sont proscrites?

IV. 6LoWPAN [28]

IV.1. Introduction

La norme 6lowpan (IPv6 sur réseaux personnels de faible puissance) définit le format des "frames" pour la transmission de paquets IPv6, ainsi que les adresses locales IPv6 et les adresses auto-configurés au dessus des réseaux IEEE 802.15.4. Puisque la taille de MTU de l'IP est de 1280B et la taille de MTU du protocole 802.15.4 est seulement de 127B, il est impossible d'encapsuler un paquet IP dans un paquet 802.15.4 sans un mécanisme d'adaptation. 6LowPAN se concentre sur les mécanismes nécessaires de compression, de fragmentation et d'adaptation. 6LoWPAN permet l'interopérabilité de réseaux internes (PAN) avec les réseaux extérieurs en respectant la norme IPv6 et en même temps en conservant les fonctionnalités clés des réseaux sans fil comme la fiabilité, la sécurité, et la consommation d'énergie limitée, au sein de ressources fortement limitées. La combinaison des normes mentionnées ci-dessus est dénommée "6LOWPAN" et permet l'insertion de milliards de dispositifs connectés à Internet au service de nombreuses applications comme l'automatisation du bâtiment, les compteurs intelligents, l'automatisation industrielle ou personnelle.

IV.2. Pourquoi 6LoWPAN? [29]

Dans ce cadre, plutôt difficile, sur quoi peut compter le concepteur de protocole pour 6lowpan ?

- Le réseau devra utiliser IP, système déjà déployé, connu, et pour lequel il existe d'innombrables applications et plein d'outils de gestion du réseau.
- Contrairement aux concurrents comme Zigbee, IP est ouvert, et accessible à tous.
- Le fait d'utiliser IP permet des interconnexions relativement faciles avec le reste de l'Internet.

Mais il y a aussi des problèmes concrets à résoudre comme :

- Vu le nombre d'objets attendus dans un LoWPAN, il faut disposer de beaucoup d'adresses, ce qui impose IPv6, avec son immense espace d'adressage.

- Comme il n'est pas question de gérer tous ces objets à la main, il faut un système d'auto-configuration, là encore, IPv6 a tout ce qu'il faut.
- La faible capacité du lien va nécessiter la compression des en-têtes.
- Le protocole de routage devra à la fois gérer des topologies variées et ne pas être trop bavard, pour économiser la capacité du réseau. Il devra également tenir compte de l'exigence d'économie et d'énergie (les protocoles existants ont été conçus pour des systèmes très différents de ceux d'un LoWPAN).
- Les équipements du LowPAN doivent autant que possible se configurer tout seuls : en effet, ils seront très nombreux (trop pour être configurés à la main un par un), avec des moyens d'entrée/sortie très limités, et souvent planqués dans des endroits difficiles d'accès.

IV.3. Caractéristiques de 6LoWPAN [30]

- Paquets de petite taille, le maximum de 802.15.4 étant de 127 octets. Avec les différents en-têtes obligatoires (notamment de chiffrement), il n'y a parfois plus que 81 octets libres pour IP.
- Les adresses des machines d'un LoWPAN peuvent être des adresses de 64 bits mais aussi des adresses abrégées de seulement 16 bits.
- Capacité très faible : à 868 Mhz (une des fréquences normalisées), il n'y a que 20 kb/s.
- Les machines d'un LoWPAN peuvent s'organiser en étoile ou bien dans un réseau maillé.
- Grand nombre de machines connectées, bien plus élevé que le nombre d'ordinateurs.
- Machines peu fiables, souvent en panne, déplacées, à la batterie qui se vide...etc.
- Connectivité d'une machine souvent interrompue par ses périodes de sommeil (pour économiser l'energie).

IV.4. Transmission des données

Le contraste entre la taille d'un paquet 802.15.4 (127 octets) et le fait que le MTU (Maximum Transmit Unit) de IPv6 est de 1280 octets, conduit à la nécessité de

la fragmentation et la compression d'en tête afin de transporter des paquets IP sur les paquets 802.15.4. Le RFC IETF 4944 explique comment créer un paquet 6LoWPAN en détail afin d'effectuer un traitement uniforme de logiciel sans avoir des contraintes.

Les paquets 6LoWPAN sont transportés par les paquets 802.15.4 comme charge utile. Ils se composent d'un en-tête de pile qui est semblable à celui de l'IPv6. Dans IPv6 la pile d'en-tête définit les attributs suivants : l'adressage, options hop-by-hop, le routage, la fragmentation, les options de destination, et enfin la charge utile. En 6lowpan l'en-tête est composé dans l'ordre suivant : adressage L2 (soit 64 bit soit 16 bit), options hop-by-hop (y compris la diffusion L2 / multicast), la fragmentation, et enfin la charge utile.

L’en-tête d'adressage 6LoWPAN utilise un type du niveau L2 (MAC) alors, soit 64 ou 16 bits d'adresse locale qui est obtenu pour chaque nœud après un processus de "nommage". Le coordinateur de PAN est responsable de cet événement. Par exemple, tous les nouds partageant les mêmes PAN ont le même préfixe 64 bits d'adresse IPv6, il n'y a aucune raison pour insérer la longueur totale de 128 bits à l'adresse de destination dans un paquet qui est interne au réseau PAN. Bien sûr, cela implique l'existence d'un "Gateway" qui traduira l'adresse IPv6 de 128 bits en une adresse de destination 6LoWPAN comprimée (64 ou 16 bits). Quand le "Gateway" reçoit un message avec une destination externe en mode local 64/16 bits, il peut la traduire en IPv6 (128 bits). L'interopérabilité sera mentionnée au paragraphe suivant. Bien sûr, l'en-tête d'adressage 6LoWPAN est facultatif et est utilisée lorsque le routage est nécessaire à l'intérieur du réseau PAN, ou quand un nœud à l'extérieur du réseau PAN doit être atteint. Il n'y a aucune signification en ajoutant cette adresse quand les valeurs de destination de couche L2(MAC) et de destination 6LoWPAN sont identiques.

L'en-tête de fragmentation définit la taille totale du paquet au niveau IP qu'il faut fragmenter, le décalage du fragment en cours et la valeur de la variable qui associe tous les fragments au paquet IP initiale (tag). La taille du paquet à fragmenter a pu être envoyée seulement sur le premier paquet fragmenté afin de permettre l'allocation de tampon. Mais l'arrivée dans l'ordre n'est pas assurée, il est conseillé de contenir la taille dans chaque paquet de la fragmentation.

IV.4.1. Interopérabilité de 6LoWPAN

Deux types de flux de communication IP existent : 1) Communication lancée à partir d'un nœud appartenant à l'extérieur du réseau PAN, s'adressant à un nœud à l'intérieur du réseau PAN et 2) de la communication initiée à partir d'un nœud du réseau PAN s'adressant à un nœud de l'extérieur du réseau PAN. Un "Gateway" est nécessaire pour effectuer la traduction IPv6 à 6LoWPAN afin de relier ces deux mondes. Ce genre de « traduction » ou de compression / décompression doit consister en la suppression / ajout de 64 bits de préfixe IPv6 quand un paquet entre ou sort du PAN. Le Gateway peut également comprimer l'adresse de 64 bits à 16 bits en utilisant une table de cartographie...etc.

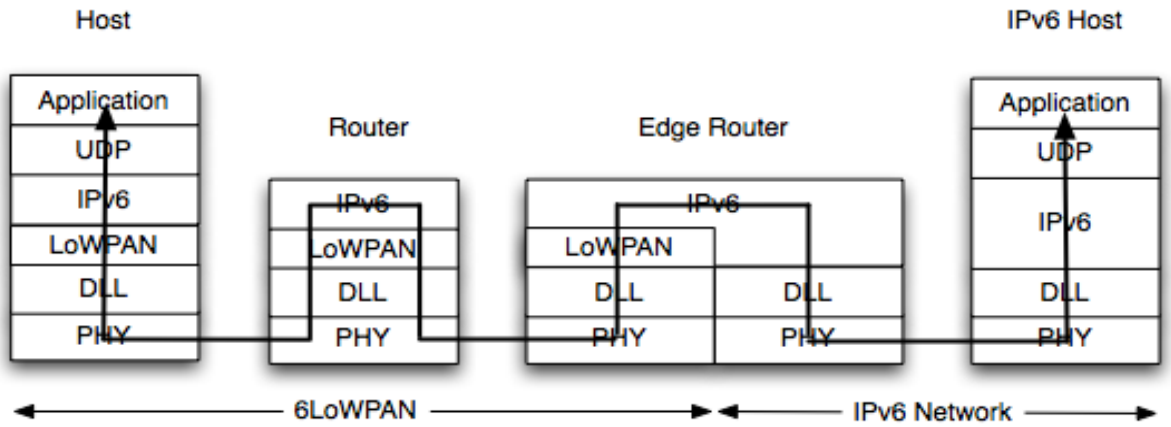


Figure 23. Le passage d'un réseau 6LoWPAN vers un réseau IPv6

IV.4.2. Routage de 6LoWPAN [29]

Le routage dans un réseau 6LoWPAN est une procédure assez délicate car la mémoire et les ressources de traitement sont limitées. En plus, des facteurs comme la distance de transmission limitée et les nœuds Pan "en sommeil" compliquent les mécanismes de routage. Par conséquent il n'y a pas de mécanismes absolument définis pour le routage proposés pour 6LowPan. Cependant, il existe les deux grandes catégories de routage 6LoWPAN : 1) Mesh under. 2) Route over.

En routage "Mesh under", un message est transmis, de proche en proche « plus proche » jusqu'au destinataire final. Une fois que le message arrive à un nœud dont l'adresse de couche MAC est égale à l'adresse de destination encapsulée, le paquet 6LoWPAN est reçu avec succès. En "Route over", les tables de routage et les en-têtes hop by hop sont utilisés afin de déterminer le chemin du

paquet. Il a été mentionné que dans le cas des données fragmentées, le "route over" est plus fiable que le "Mesh under".

V. Plan de Compression de l'en-tête d'IPv6 de 6LoWPAN

Tous les champs de l'en-tête IPv6 peuvent être compressés sauf la limite de bond le champ (de 8 bits). Par exemple :

- La version sera *IPv6* et n'a pas besoin d'être indiquée
- Inférer les adresses de niveau *IP* grâce aux adresses *MAC* permet de ne pas les indiquer dans l'en-tête réseau (champ « Address Info »)
- La taille du paquet peut également être inférée dans l'en-tête *MAC*
- Aucune *QoS* et donc pas de champs *Traffic Class* ou *Flow Label*
- Le champ *Next Header* peut prendre seulement 4 valeurs :
  - Pas d'en-tête
  - *ICMP*
  - *DP*
  - *TCP*

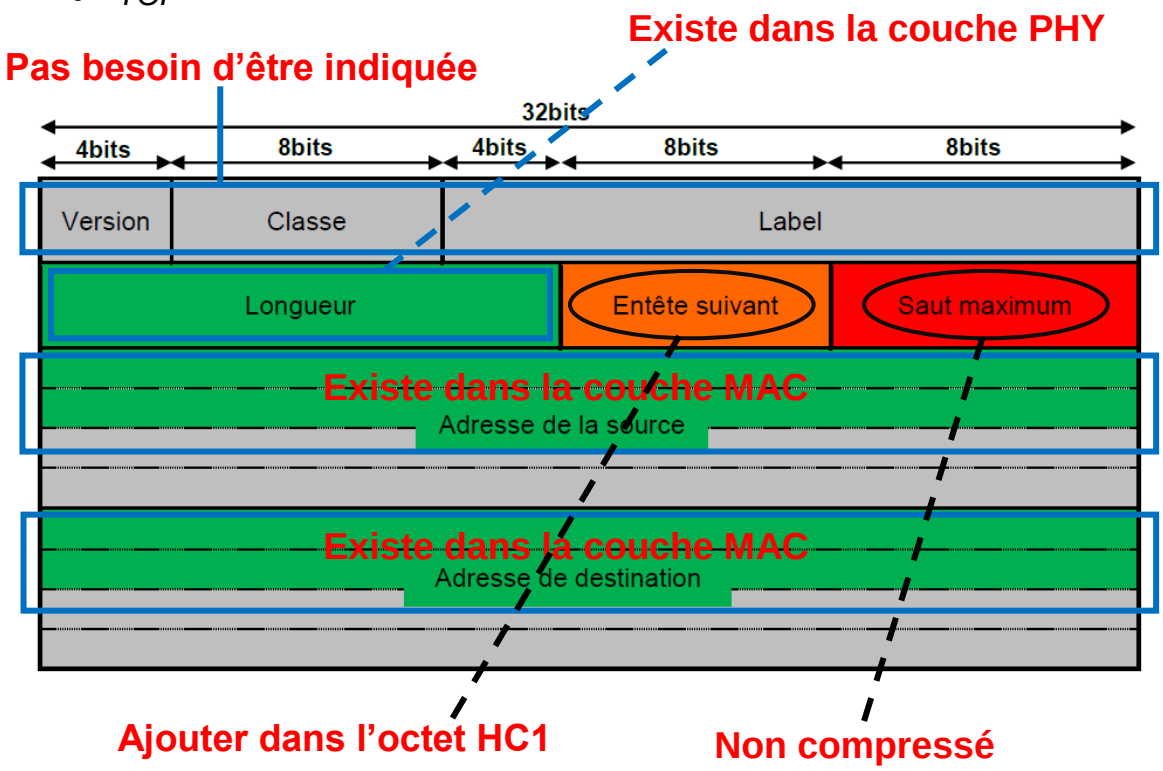


Figure 24. Plan de Compression de l'en-tête d'IPv6 de 6LoWPAN

Cependant, le champ *Next Header est* simplifié à 2bits ajouté dans un champ en produisant HC1 (Compress Header) de 8 bits. Ainsi, nous avons une structure de 40 octets que l'on a réduite à seulement 2 octets. Le premier pour HC1 et le deuxième pour le champ Hop Limit qu'on doit conserver. **[31]**

Enfin, le *RFC 4919* propose une compression de l'en-tête précédente et notamment une méthode pour faire passer l'en-tête *UDP* de 8 à 4 octets. On a donc une en-tête de 48 octets compressés en seulement 6 octets…etc

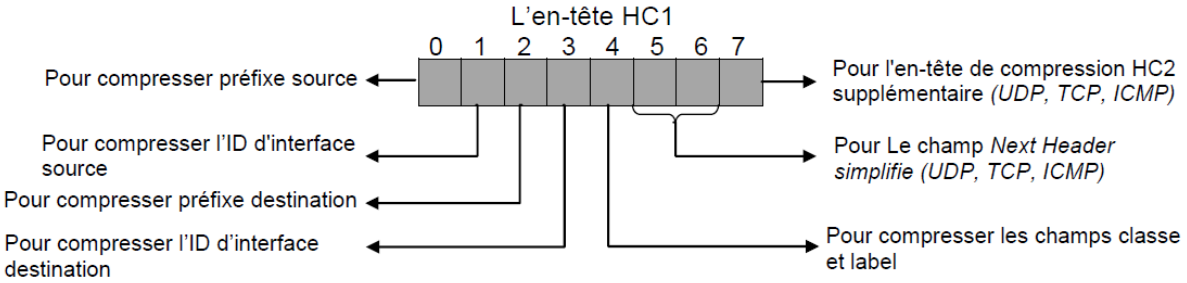
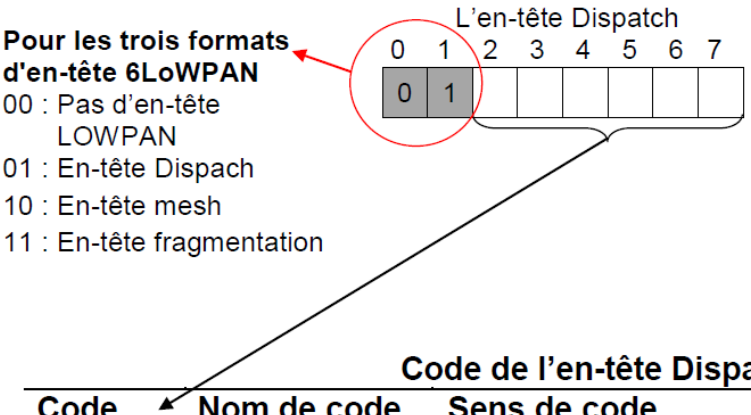


Figure 25. L'en-tête HC1

Le Format de l'octet type en-tête (exemple avec le type Dispatch) :



Code de l'en-tête Dispatch

Code	Nom de code	Sens de code
01000001	IPv6	Adresses d'IPv6 non compressées
01000010	LOWPAN_HC1	LOWPAN_HC1 a compressé IPv6
01000011	LOWPAN_MH	LOWPAN_MH a compressé l'en-tête de mobilité IPv6
…	Reserved	Réservé pour l'utilisation future
01010000	LOWPAN_BC0	LOWPAN_BC0 broadcast
…	Reserved	Réservé pour l'utilisation future
01111111	ESC	L'octet de Dispatch supplémentaire suit

Figure 26. L'en-tête Dispatch

VI. Format de Paquet 6LoWPAN [31]

Il y a trois types de formats d'en-tête 6LoWPAN :

- En-tête Dispach : Indique l'information de l'en-tête suivante. Par exemple, une compression d'en-tête (HC1) la Dispach indique l'information d'IP ou en-tête UDP.
- En-tête mesh : Est utilisée dans l'acheminement.
- En-tête fragmentation : indique l'information pour la fragmentation et le réassemblage des paquets.

Quand plus d'une en-tête LoWPAN est utilisée, l'en-tête de Dispach apparaît avant chaque en-tête.

La figure X montre la structure entière de format IEEE 802.15.4 en incluant un paquet 6LoWPAN. La dimension maximum du paquet est 127 octets. L'en-tête IPv6 est complètement compressé par HC1 et l'en-tête UDP est aussi complètement compressé par l'en-tête HC2.

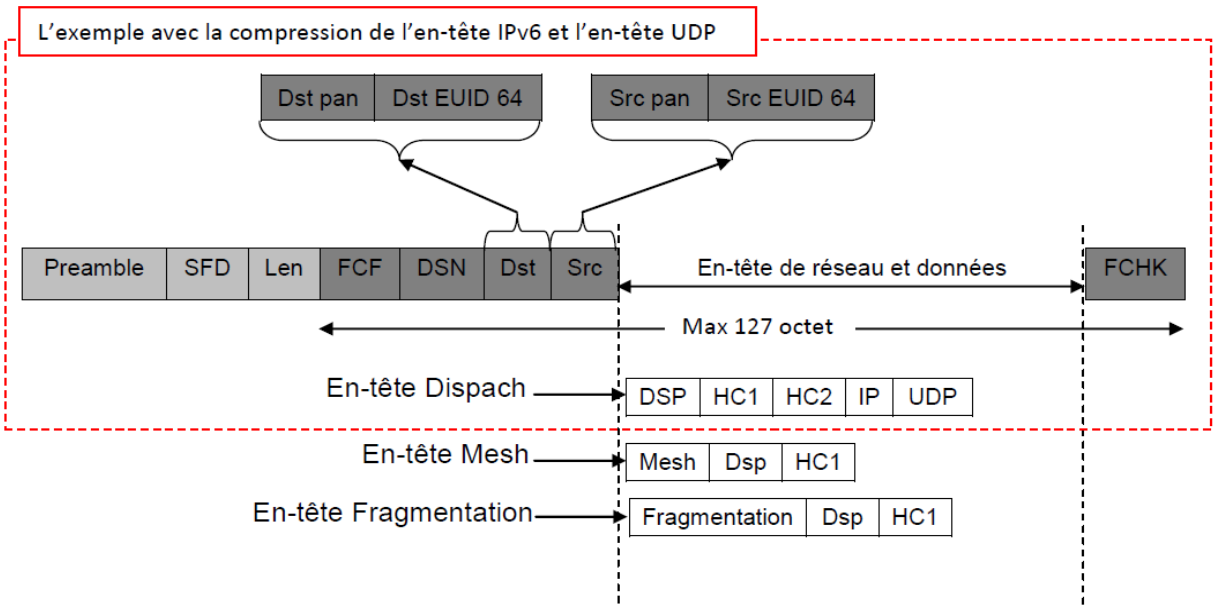


Figure 27. La structure entière d'IEEE 802.15.4 cadre en incluant le paquet 6LoWPAN

VII. Conclusion

Nous avons consacré ce chapitre à l'étude et l'analyse du protocole 6LoWPAN conçue pour les réseaux de capteurs sans fil. En s'appuyant sur une norme couramment utilisée dans les réseaux de capteurs IEEE 802.15.4, nous avons effectué une étude détaillé sur les principaux apports de se protocole pour les réseaux de capteurs sans fil.

A l'origine 6LoWPAN était fait pour être implémenté dans les réseaux IEEE 802.15.4. A partir de l'année 2010 6LoWPAN à tendance d’être utilisent sur d'autres supports (par exemple Bluetooth). Tous les travaux de l'IETF, sont opérationnels mais ceux-ci ne sont pas encore standardises. Ils sont actuellement en perpétuel évolution pour optimiser l'utilisation de 6LoWPAN.

Malgré les nombreux apports offerts par le protocole 6LoWPAN pour les réseaux de capteurs, toutefois, celui-ci présente quand même quelques inconvénients.

Chapitre IV

Problème de 6LoWPAN et la solution proposée

I. Introduction

Bien qu'ils fassent partie du domaine des réseaux ad-hoc, Les réseaux de capteurs sans fil forment une branche de recherche à part. En effet, les contraintes liées à ce type de réseaux sont très différentes de celles du domaine classique, ce qui explique le fait que tous les protocoles et les algorithmes déjà développés pour les réseaux sans fil classiques ne soient pas adaptés aux réseaux de capteurs sans fil.

Le nombre de capteurs déployés pour étudier un phénomène est généralement de l'ordre de centaines ou de milliers, voir même des millions avec une densité très élevée. Ainsi les algorithmes développés et les protocoles existant comme IPv6 doivent avoir un très bon facteur d'échelle : c'est la plus grande différence avec les réseaux sans fils classiques où le nombre de stations ne dépasse généralement pas une centaine.

Afin d'étendre le protocole IPv6 classique pour qu'il soit opérationnel et efficace jusque dans les réseaux de capteurs, le groupe de travail 6LoWPAN a défini des mécanismes d'encapsulation et de compression d'entêtes IPv6 permettant aux paquets d'être envoyés ou reçus via le protocole de communication IEEE 802.15.4. Cela dit, malgré les nombreux apports d'IPv6 surtout en termes d'espace d'adressage qui permet d'avoir un grand nombre de capteurs, un problème inhérent dans la nouvelle en-tête 6LoWPAN concernant la taille du champ *hop Limit* semble être une contrainte pour le routage multi-sauts dans les réseaux de capteurs.

II. Hop limite dans Ipv6 et 6LoWPAN

Le champ "Hop Limit" de taille de 1 octet maintenu dans le protocole 6LoWPAN, Similaire au champ « Time To Live » d'IPv4 (dont l'unité était la seconde) caractérisé par :

- Une durée vie des paquets limités a cause :
  - Des paquets fantômes qui errent sans fin : erreur de routage
  - Limitation (grossière) du domaine atteignable par un paquet
- Une décrémention à chaque routeur (ou nœud capteur pour 6LoWPAN) : -1 à chaque traversée d'un équipement.
- Et si la valeur atteint 0, le paquet est détruit.

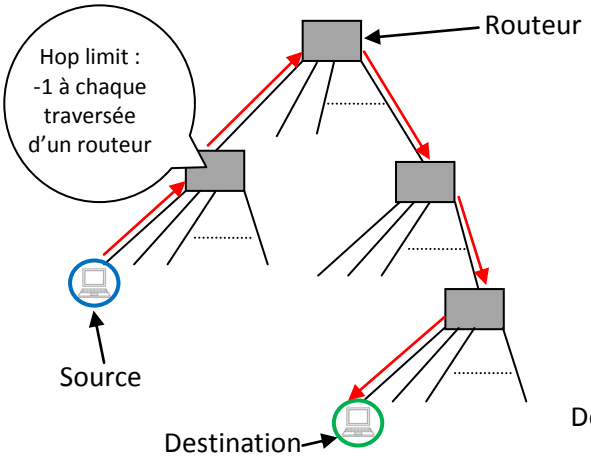


Figure 28. Le routage dans les Réseaux classiques

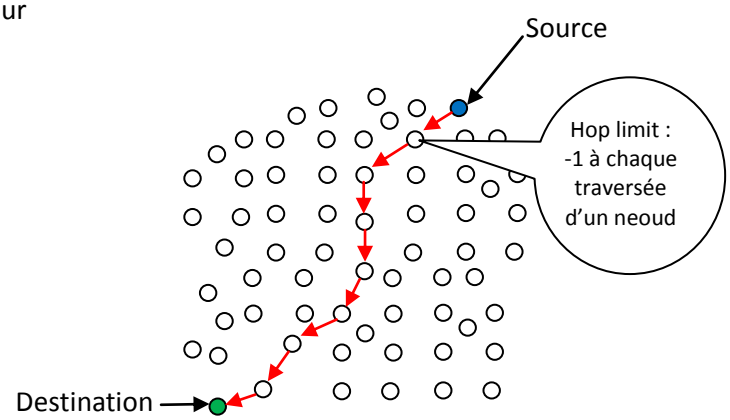


Figure 29. Le routage dans les Réseaux de capteurs

III. Problème de champ hop limite dans les réseaux de capteur 6LoWPAN

Comme la taille du champ Hop limit est de 8 bits, alors deux capteurs séparés par plus de 2^8 (256 sauts) capteurs ne peuvent communiquer car le paquet ne peut pas atteindre le nœud destinataire, il sera déjà détruit avant. Cela veut dire qu'un capteur peut communiquer avec d'autre sur un rayon de 256 sauts (256 capteurs).

Dans ce qui suit, on a envisagé d'étudié deux cas de figure respectivement une représentation sous forme de cercle et de sphère pour mieux illustrer cette problématique.

III.1. Cas d'un cercle

Dans un réseau avec une topologie en deux dimensions un nœud capteur ne peut recevoir des données que par les nœuds qui l'entoure sur un rayon de saut de taille égale à la valeur maximale du champ hop limit. Avec cette topologie et ce rayon on forme un réseau de capteurs limité par un cercle qui à un rayon égale $(2)^{\text{nbr bite de champ hop limit}}$.

Pour trouver le nombre maximum de nœud qu'on peut déployé à l'intérieur d'un cercle qui à un rayon de $(2)^8$ capteurs, on calcule la surface de ce dernier avec la formule suivante:

$$\textbf{Nombre de nœud} \approx \left(\frac{\text{rayon}}{2}\right)^2 \text{X } \pi$$

Avec 8 bits de champ hop limit on a :

nbr nœud ≈ $(2^8)^2$ x π ≈ 205 783 capteurs

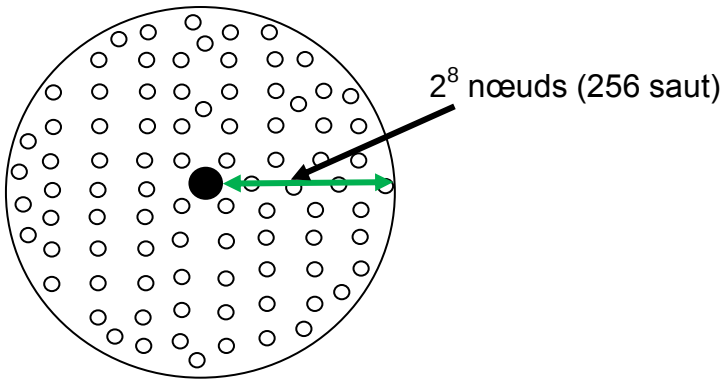


Figure 30. Limite des sauts dans les réseaux de capteurs avec une topologie à deux dimensions

Par ailleur, le calcule du nombre de nœud maximum qu'on peut déployer dans un réseau de capteurs qui utilise le protocole 6LoWPAN, selon la formule suivante : $2^{\text{nbr bite de champ adresse}}$ qui égale à 2^{64} adresses (18 446 744 073 709 551 616 capteurs)

a. Problème

A travers les résultats trouvés précédemment, le nombre maximale de machine avec un Hop limit de 8bits est égale à 205 783 alors que le nombre maximale avec un adressage de 64bits est 18 446 744 073 709 551 616.

La différence de puissance d'adressage est donnée dans la figure suivant:

Nbr max de machine avec un hop limit de 8bits : ? 205 783

Nbr max de machine avec un adressage de 64bits: 18 446 744 073 709 551 616

On constate que le nombre de capteurs déployés est limité par le nombre de sauts et cela pose problème si l'on veut déployer un grand nombre de capteurs. En effet, quand le nombre de capteurs déployés dépasse celui qu'on peut déployer a l'intérieur de ce cercle (205 783 capteurs), les paquets des capteurs qui ce trouvent a l'extérieur ne pourront jamais atteindre la destination, car le nombre de saut est limité au rayon du cercle.

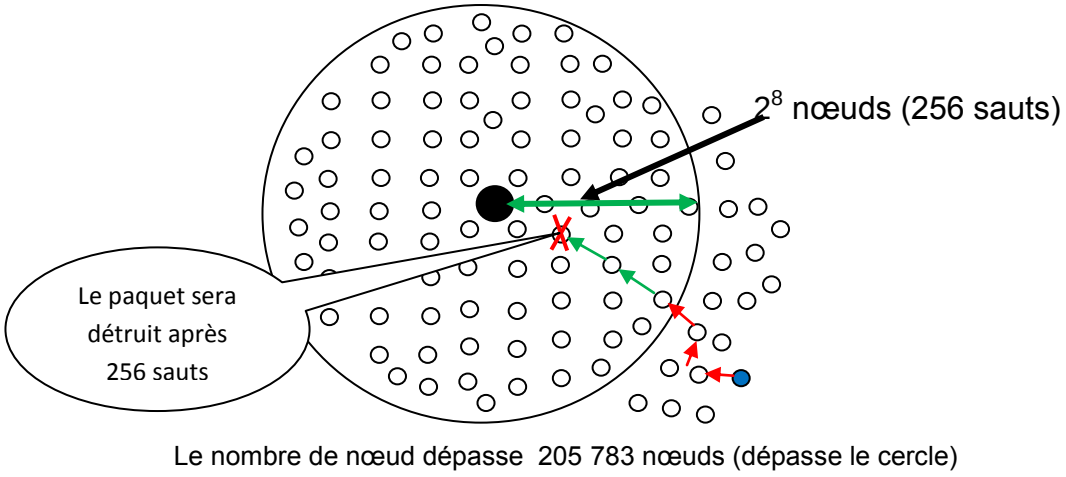


Figure 31. Problème des sauts dans les réseaux de capteurs avec une topologie à deux dimensions

b. Solution

Pour résoudre la problématique posée, on propose d'augmenter le nombre de sauts pour agrandir le rayon de notre cercle de t'elle sorte à ce que le nombre maximum de capteurs déployés soit supérieur ou égale au nombre maximum d'adresses. L'idée est de trouver le nombre de sauts en utilisant le nombre maximum de nœuds déployés avec le protocole 6LoWPAN:

Le nombre maximal de machines avec un adressage de 64 bits est de
18 446 744 073 709 551 616 machines.
Donc le rayon des sauts R de réseaux est :

$(R^2) \times \pi = 18\,446\,744\,073\,709\,551\,616$ capteurs

$$R = \sqrt{\frac{18\,446\,744\,073\,709\,551\,616}{\pi}}$$

$R = 4\,294\,967\,296$ sauts

Pour atteindre ce rayon de sauts il faut 32 bits (4 octet)

Pour vérifier la fiabilité de cette solution on compare le nombre de sauts qu'on peut atteindre en utilisant la nouvelle taille de champ Hop limit (32 bilts) avec le nombre d'adresse maximum.

Nbr max de saut avec un hop limit de 32bits: 4 294 967 296

Nbr max de saut avec un adressage de 64bits: 4 294 967 296

A trévère cette comparaison, on remarque qu'il n'y a pas de perte d'adresse avec la nouvelle taille du champ hop limit (32 bits).

III.2. Cas d'une sphère

Avec les mêmes constatations que précédemment le nombre de capteurs à déployer est limité par une sphère qui à un rayon égale (2)$^{\text{nbr bite de champ hop limit}}$:

On calcule le nombre maximum de nœuds qu'on peut déployer à l'intérieur d'une sphère qui a rayon égal à 2^8 comme suit :

Nombre de nœud $\approx \frac{4}{3}\pi$ **(rayon)**^{3}

Avec 8 bits de champ hop limit on a :

nbr nœud $\approx \frac{4}{3}\pi\ (8^2+8^2)^3 \approx$ **561 924 887** capteurs

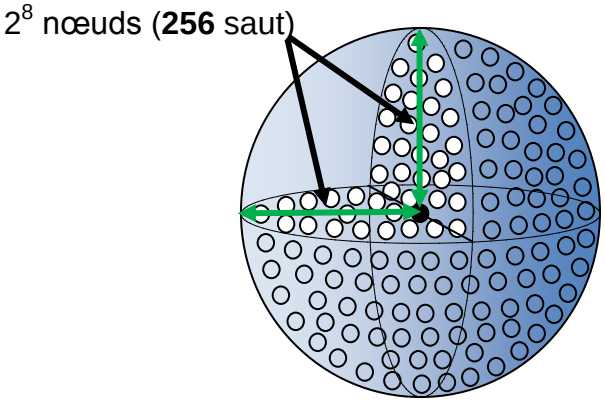


Figure 32. Limite des sauts dans les réseaux de capteurs avec une topologie à trois dimensions

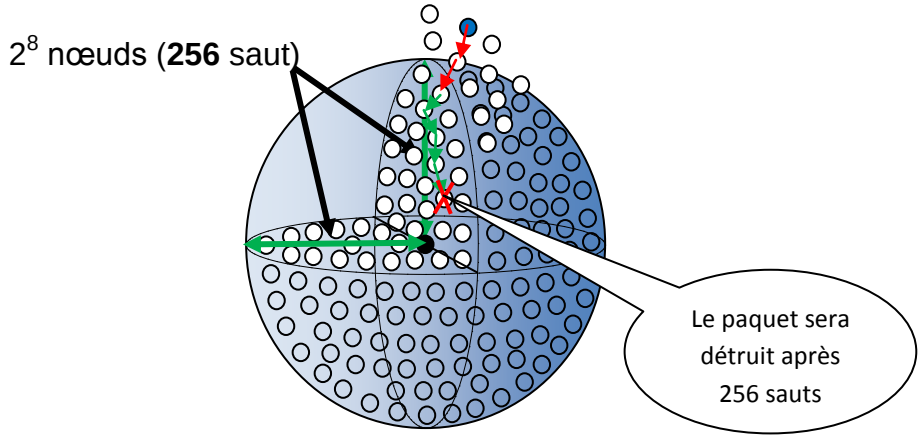
a. Problème

A travers les résultats calculés précédemment on la différence de puissance d'adressage est donnée dans la figure suivant:

Nbr max de machine avec un hop limit de 8bits : ? 561 924 887

Nbr max de machine avec un adressage de 64bits: 18 446 744 073 709 551 616

Dans ce cas de figure, on trouve le même problème qu'avant, concernent le nombre de saut.



Le nombre de nœud dépasse 561 924 887 nœuds

Figure 33. Problème des sauts dans les réseaux de capteurs avec une topologie à trois dimensions

b. Solution

On calcule le nombre de sauts comme on l'à calculé dans le cas d'un cercle:

Le nombre maximal de machines avec un adressage de 64 bits est de

18 446 744 073 709 551 616 machines.

$\frac{4}{3}$ X π $(\frac{R}{2})^3$ = 18 446 744 073 709 551 616 capteurs

Donc rayon des sauts R de réseaux est :

$$R = \sqrt[3]{\frac{6\ X\ 18\ 446\ 744\ 073\ 709\ 551\ 616}{\pi}}$$

R = 3 278 791 saut

Pour avoir ce rayon de sauts il faut 22 bits (3 octet)

Pour vérifier la fiabilité de cette solution on compare le nombre de sauts qu'on peut atteindre en utilisant la nouvelle taille de champ Hop limit (22 bilts) avec le nombre d'adresse maximum.

Nbr max de saut avec un hop limit de 22bits: 4 194 304

Nbr max de saut avec un adressage de 64bits: 3 278 791

En comparant les deux nombres, on remarque qu'il n'y a pas de perte d'adresse avec la nouvelle taille du champ Hop limit (22 bits).

Il se trouve que le déploiement en cercle est fréquent que le déploiement en sphère. Par ailleurs le nombre de bits utilisé pour prendre en charge du cercle couvre celui de la sphère. Pour cela nous avons opté pour une nouvelle taille du Hop limit à 32bits.

IV. Solution proposé

Le standard 6LoWPAN actuel n'a pas été conçu pour une compression avec le champ Hop limit sur 32 bits. Pour répondre à notre problématique de départ, on propose un nouveau format de compression de l'en-tête IPv6 pour permettre à 6LoWPAN d'étendre la taille du Hop Limit à 32 bits au lieu de 8 bits. Pour inclure ce format dans 6LoWPAN, nous avons besoin de définir un nouveau format d'en-tête LoWPAN_HCH32 dans la table des types d'en-tête 6LoWPAN qui utilise une des valeurs des codes réservés (01000100). Le tableau 5 montre les différents formats d'en-tête Dispach incluant le nouveau format LoWPAN_HCH32 :

Tableau 5. Les différents formats d'en-tête Dispach avec le nouveau format LoWPAN_HCH32

Code	Nom de code	Sens de code
01000001	IPv6	Adresses d'IPv6 non compressées
01000010	LOWPAN_HC1	LOWPAN_HC1 a compressé IPv6
01000011	LOWPAN_MH	LOWPAN_MH a compressé l'en-tête de mobilité IPv6
01000100	LOWPAN_HCH32	LOWPAN_HC1 a compressé IPv6 avec Hop limit 32b
…	Reserved	Réservé pour l'utilisation future
01010000	LOWPAN_BC0	LOWPAN_BC0 broadcast
…	Reserved	Réservé pour l'utilisation future
01111111	ESC	L'octet de Dispatch supplémentaire suit

Le nouveau format de paquet proposé pour une compression avec 32bits de champ Hop limit.

Exemple de message 6LoWPAN avec le type de format LoWPAN_HC1 (hop limit = 8bits) :

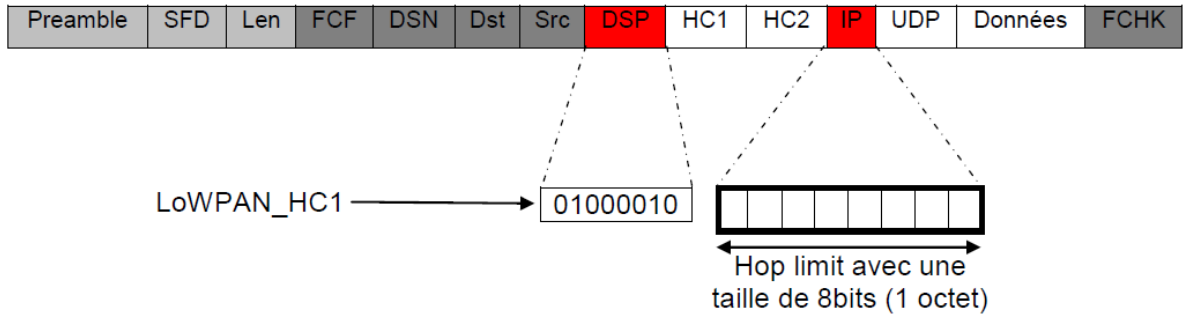


Figure 34. Exemple de message 6LoWPAN avec le type de format LoWPAN_HC1

Exemple de message 6LoWPAN avec le type de format qu'on à proposé LoWPAN_HCH32 (hop limit = 32bits) :

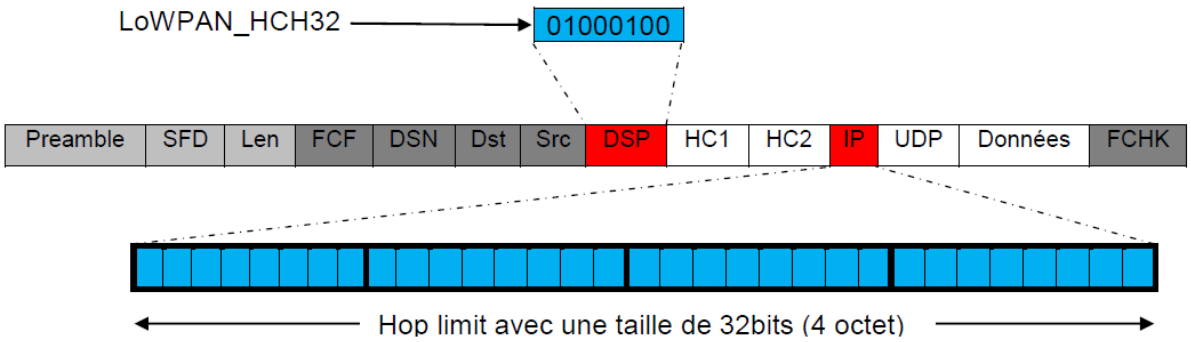


Figure 35. Exemple de message 6LoWPAN avec le type de format qu'on à proposé LoWPAN_HCH32

V. Conclusion

Dans ce chapitre on a exploité les observations de l'étude du protocole cité dans le chapitre précédent afin de proposer des stratégies et des améliorations. Le problème du protocole 6LoWPAN, basé sur la compression d'IPv6 utilise toujours un champ Hop limit de 8bits qui est insuffisant dans un réseau de capteurs a forte densité.

Nous avons présenté une solution à ce problème permettant la prise en charge d'un nombre important de capteurs dans les RCSF. Nous estimons que la solution apportera des performances meilleures que la solution actuelle.

Conclusion générale

Les réseaux de capteurs sont composés d'un très grand nombre de dispositifs de communication ultra petits, autonomes avec des ressources de calcul et d'énergie limitées. Ils sont actuellement considérés comme l'une des technologies qui bouleverseront notre façon de vivre, grâce à leur utilisation dans différents domaines d'application. Les réseaux de capteurs ont le potentiel de révolutionner la manière même de comprendre et de construire les systèmes physiques complexes. Parmi les domaines où ces réseaux peuvent se révéler très utiles, nous citons les domaines suivants: militaire, environnemental, domestique, santé, sécurité,…etc.

Flexibilité, tolérance aux pannes, hautes capacités de captage, coût réduit, installation rapide sont les caractéristiques qui ont permis aux réseaux de capteurs d'avoir des nouveaux domaines d'applications multiples et excitants. Ce large étendu d'applications fera de cette technologie émergeante une partie intégrante de nos vies futures.

Dans ce document, nous avons étudié l'intégration IPv6 dans les réseaux de capteurs sans fil pour prendre en charge un grand nombre de capteurs. Intégrant ce protocole dans les RCSF, un nouveau protocole a vue le jour sous le nom 6LoWPAN. Ce dernier a connu un intérêt auprès de plusieurs chercheurs et a pris une bonne considération parmi l'ensemble des protocoles existant dans les réseaux de capteurs sans fil; grâce à la simplicité de son principe basé sur la compression de l'en-tête IPv6, plusieurs intérêts se présentent pour l'utilisateur car IPv6 est un système déjà déployé, connu, et pour lequel il existe d'innombrables applications et plein d'outils de gestion.

Après avoir analysé le protocole 6LoWPAN et pris connaissance de ses points forts et de ses limites en particulier le nombre de sauts, nous avons défini une solution dont l'idée de base est d'augmenter le nombre de sauts on utilisant un nouveau format d'en-tête 6LoWPAN avec un champ Hop limit plus grand. Nous avons calculé la taille idéale du champ Hop limit qui s'adapte le mieux à la capacité d'adressage de 6LoWPAN.

Comme perspective de recherche de ce travail nous pensons qu'il y a lieu d'étudier d'autres scénarios comme par exemple trouver une solution permettant d'ajuster la taille du champ Hop limit en condition du nombre de capteurs déployés.

Références bibliographiques

[1] Séverine Sentilles, "Architecture logicielle pour capteurs sans-fil en réseau", Master TI 2eme année, Mälardalen University, Sweden, Janvier-Juin 2006

[2] www.Kelkoo.fr , "Cle USB Bluetooth pc", 2008

[3] Lyes Khelladi, Nadjib Badache "Les réseaux de capteurs: état de l'art", Rapport de recherche, Algérie, Février 2004

[4] Tayeb Lemlouma, "Le routage dans les réseaux mobiles Ad Hoc", Mini projet, Institut National de Recherche en Informatique et Automatique INRIA, 2000

[5] Magnus Frodigh, Per Johansson, Peter Larsson, "Wireless ad hoc networking – The art of networking without a network", Review homepage: http://www.ericsson.com , Page(s): 248-263, 2000

[6] Khemapech, I. Duncan and A. Miller. A survey of wireless sensor networks technology. In PGNET, Proceedings of the 6th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting, June 2005

[7] Zhao, Q. et L. Tong. "Distributed opportunistic transmission for wireless sensor networks" Proceedings of the international conference on acoustics, speech and signal processing. New York: IEEE magazine, 2004. 833-836

[8] Metthey, Brice "Simulateurs de réseaux de capteurs sans fils" Université de Pau et des pays de l'Adour, 2006

[9] Séverine Sentilles "Architecture logicielle pour capteurs sans-fil en réseau" Rapport de recherche, Université de Pau et des Pays de l'Adour, juin 2006

[10] Yacine Challal, "Réseaux de Capteurs Sans Fils", Cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France, 17 Novembre 2008.

[11] Noureddine LASLA "La gestion de clés dans les réseaux de capteurs sans-fil" mémoire de magister, Institut National de formation en Informatique (I.N.I) Oued-Smar, Alger.

[12] Bouabdellah Kechar, "Problématique de la consommation de l'énergie dans les réseaux de capteurs sans fil", Séminaire LIUPPA, Université de Pau et des Pays de l'Adour, 14 Octobre 2007

[13] Guy Pujolle. "Les Reseaux". 5eme edition, 2006, ISBN : 2-212-11987-9

[14] A. Delye, V. Gauthier, M. Marot, and M. Becker. "Etat de l'art sur les reseaux de capteurs". Rapport de Recherche INT N-05001RST GET-INT, UMR5157 SAMOVAR, Institut National des Telecommunications, Evry, France, 2005.

[15] http://www.zigbee.org

[16] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. "Wireless sensor networks: a survey". Computer Networks 38, Elsevier Science, pp. 393–422, 2002.

[17] A. Savides, C. C. Han, and M. B. Srivastava. "Dynamic fine-grained localization in adhoc networks of sensors". Proceedings of ACM MOBICom and Networking, Rome, Italy, p.166-179, July 2001.

[18] L. Khelladi and N. Badache. "Les reseaux de capteurs : etat de l'art". Rapport de Recherche, Faculte Electronique et Informatique Bab Ezzouar-Algerie, Fevrier 2004

[19] D. Culler, D. Estrin, and M. Srivastava. "Overview of Sensor Networks". In IEEE Computer, vol. 37, no. 8, pp. 41–49, august 2004.

[20] Les enjeux du déploiement du protocole IPv6

[21] http://fr.wikipedia.org/wiki/ICMPv6 consulté le 5 mai 2011

[22] memoire etude et mise en oeuvre des services reseau de base et de voix sur ip dans un reseau ipv6 (P.38)

[23] http://fr.wikipedia.org/wiki/IPv6

[24] http://livre.g6.asso.fr

[25] Migration IPv6 : enjeux de sécurité, www.certa.ssi.gouv.fr/.../CERTA-2006-INF-004.html

[26] http://tools.ietf.org/wg/6lowpan

[27] VERNEZ Jérôme "Adaptation de la couche MAC du standard IEEE 802.15.4 à une couche physique Ultra Wide Band" description.

[28] ach Shelby and Carsten Bormann "6LoWPAN: The WirelessEmbedded Internet"

[29] Travaux d'Études et de Recherches *Janvier 2009 – Mai 2009*"Simula'on de réseaux 6LoWPAN avec OPNET Modeler"

[30] RFC 4919 : IPv6 over Low-PowerWireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals

[31] Jin Ho Kim, Choong Seon Hong, and Taeshik Shon "A Lightweight NEMO Protocol to Support 6LoWPAN"