Institut Supérieur des Etudes Technologique en communications de Tunis

PROJET DE FIN D'ETUDE

Définition et Implantation d'un protocole pour le standard Home Plug Networking

Réalisé par :

Hana MANSOUR
Rim REZGUI

TS-Télécommunication

Encadrées par :

M.Adel GHAZEL
M. Kamel BOULEIMEN

2001-2002

Dédicace

Je dédie ce travail

à ma mère

à mon père

en témoignage de mon affection et de ma profonde gratitude pour leur soutien moral et financier et leurs encouragements;

à mes sœurs

à toute ma famille proche soit elle ou lointaine

à tous mes ami(e)s et en particulier à Faker, Sana, Najeh, Afef et Nedra

en leur souhaitant le succès dans leurs études et leur vie.

Hana

AVANT-PROPOS

Le travail présenté dans ce rapport a été effectué dans le cadre d'un projet de fin d'études pour la préparation du Diplôme de Technicien Supérieur en Télécommunications options : Transmission et Commutation à l'Institut Supérieur des Etudes Technologiques en Communications de Tunis (ISET'COM).

Ce projet a pour thème l'étude et l'implantation d'un protocole pour le standard Home Plug Networking relatif à la communication haut débit sur les lignes d'énergie.

Au terme de ce travail, nous tenons à remercier tout particulièrement :

Monsieur Adel Ghazel Directeur du Département Electronique, Physique et Propagation à l'Ecole Supérieure des Communications (SUP'COM) et Monsieur Kamel Bouleimen enseignant universitaire à l'ISET'COM, pour leur encadrement, leur disponibilité, pour les conseils qu'ils nous ont prodigués tout au long du travail ainsi que leur sympathie et soutien moral.

Tous nos professeurs qui ont contribué à notre formation ainsi qu'aux responsables de l'ISET 'COM pour les moyens qu'ils nous ont offerts afin de mener à terme ce travail.

Nos vifs remerciements s'adressent aussi à tous ceux qui nous ont encouragé de près ou de loin tout au long de ce travail.

RESUME

Ce travail concerne l'étude, la configuration et le test d'un protocole de communication sur les lignes d'énergie selon le standard Home Plug. Une première partie du travail a été consacrée à l'analyse de la technique CPL afin de dégager les particularités du canal de transmission qu'il faut en tenir compte dans la définition du protocole. En deuxième partie nous avons montré que les protocoles standards de transmission de données restent insuffisants pour compenser la sévérité du canal CPL. Ainsi un protocole amélioré a été configuré. Le travail est complété par une étude pratique de test de protocole.

Mots–clés : technique CPL, protocole d'accès, couche MAC, CSMA.

CAHIER DE CHARGE

Titre de projet

"Définition et Implantation d'un protocole pour le standard Home Plug Networking"

Position du problème

La technique courants porteurs de ligne (CPL) pour la transmission des données à travers les lignes d'énergie devient de plus en plus une solution très intéressante vue la disponibilité de l'infrastructure du réseau. Le développement d'une telle technique pour les applications multi-utilisateurs à haut débit se trouve confrontée aux différentes contraintes de transmission présentes dans la ligne d'énergie (bruit, atténuation, variation d'impédance,.). De ce fait les protocoles classiques de communication s'avère insuffisants pour garantir une qualité de service convenable. Il est alors indispensable de chercher à définir de nouveaux protocoles ou modifier les protocoles existants. C'est pour répondre à cette problématique que vient la définition du sujet de ce projet.

Travail demandé

Il est demandé d'effectuer le travail suivant :

- Etude du principe et de la configuration des réseaux CPL pour la transmission de données.
- Définition des spécifications des applications des protocoles classiques pour les techniques CPL.
- Choix et configuration du protocole MAC pour le standard Home Plug.
- Définition d'une technique de formatage des données et validation pour des tests pratiques de communication entre deux PC.

INTRODUCTION GENERALE

Ces dernières années, on observe une prolifération exceptionnelle du nombre d'utilisateurs des systèmes informatiques qui font preuve d'un développement technologique incessant. En effet, la technologie joue un grand rôle dans la conception et la vie des réseaux. Sa diversité et sa rapidité d'évolution sont de plus en plus grandes. En parallèle, on remarque une montée invraisemblable dans le volume de données échangées entre ces systèmes informatiques. D'où la naissance de la téléinformatique domaine de recherche alliant ces deux besoins.

La concurrence pèse de plus en plus fortement sur l'évolution des réseaux. Les performances "traditionnelles" des réseaux pourraient perdre un peu d'importance, alors qu'une notion telle que la "scalabilité", c'est à dire la capacité à grossir rapidement sans changement de structure pour faire face à l'augmentation rapide du trafic, devient assez fondamentale. Les nouvelles caractéristiques recherchées sont la flexibilité, l'évolutivité, la robustesse face aux divers aléas, en plus les performances économiques.

Il n'apparaît pas de trajectoire type pré–déterminée d'évolution des réseaux. La dynamique des besoins et des usages, des techniques et des coûts conduit à chercher en permanence la meilleure solution malgré l'incertitude engendrée par le contexte technique et économique.

Une solution se trouve être la suivante : pourquoi ne pas exploiter pour la transmission des données les moyens de bord, d'autant plus faciles à installer qu'économiques et viables, à savoir le réseau de distribution électrique étant donné que ce réseau présente une infrastructure existante et très étendue géographiquement.

Pour justifier la fiabilité et l'efficacité de cette technique, nous sommes dans l'obligation de définir les bases d'un système de télécommunications bien particulier. Cette définition doit inclure, l'architecture de ce réseau, ses caractéristiques et le mode d'accès à ce système.

C’est dans ce repère que nous situons notre projet de fin d’étude intitulé "Définition et Implantation d’un protocole pour le standard Home Plug Networking".

Ce rapport se compose de trois chapitres. Dans le premier chapitre nous nous intéressons à la configuration d’un réseau CPL, nous présentons la technique CPL ainsi que des exemples illustrant l’architecture de ce réseau, ensuite nous introduisons les caractéristiques d’un protocole de transmission et enfin nous spécifions le standard Home Plug.

Dans le deuxième chapitre, nous mettons l’accent sur la mise en œuvre du protocole CPL. Nous étudions la couche MAC pour la technique CPL ainsi que sa configuration pour le standard Home Plug.

L’implantation et le test du protocole sont présentés dans le troisième chapitre. Nous commençons par introduire le protocole SNAP ensuite nous présentons les différentes techniques de validation de protocole et enfin, nous décrivons le prototype de test.

Chapitre I :

CONFIGURATION D'UN RESEAU CPL

I-1 Introduction

A l'instar des téléréseaux, le réseau électrique se profile aujourd'hui comme une alternative au réseau téléphonique, en particulier pour les services à haut débit ciblant les utilisateurs résidentiels.

Dans ce Chapitre, nous nous intéressons tout d'abord à la présentation de la technique CPL (Courant Porteur de Ligne). Ensuite, nous présentons quelques exemples d'architectures de réseau CPL. Puis nous allons spécifier les caractéristiques d'un protocole de communication. Enfin nous définissons le standard Home Plug.

I-2 Présentation de la technique CPL

I-2-1 Principe de transmission

La transmission en technique CPL consiste à utiliser une ligne d'alimentation électrique, transportant un courant basse fréquence, sur laquelle on injecte un signal de fréquence supérieure, mais d'amplitude beaucoup plus faible dit onde porteuse.

Cette porteuse peut être modulée en amplitude (ASK), en fréquence (FSK) ou en phase (PSK) de façon à adapter le signal à transmettre à la bande allouée dans le canal CPL.

La réception de la porteuse et sa démodulation permet la reconstitution de l'information utile en bande de base.

Avec cette nouvelle technologie, le raccordement habituel des foyers à la prise de téléphone peut être remplacé par le branchement d'un modem sur n'importe quelle prise de courant. Cette configuration apporte aux usagers une mise en réseau à moindre coût de tous leurs équipements domestiques (ordinateurs, imprimante, téléviseur, modems, alarmes, graveur de CD,…). Toute la maison bénéfice alors des services apportés par les réseaux d'accès employés sans accroître leur facture d'électricité ni occuper leur ligne téléphonique.

La technique courant porteur de ligne (CPL) a donc pour objectif l'utilisation du réseau électrique pour véhiculer tout type de signal dont la voix et les données.

Deux types de réseaux sont envisagés pour l'utilisation de la technique CPL :

- Réseau d'accès extérieur (out door access) : Le signal est par exemple injecté dans le transformateur du réseau local et transmis aux utilisateurs finaux connectés selon le principe point-multipoint sur le réseau de distribution basse tension 220 V/380 V.

- Réseau domestique interne (indoor) : desservant jusqu'à 1000 utilisateurs internes se trouvant dans un rayon maximal de 100 mètres à un débit de 1 à 2 Mbps partagé entre eux et une fréquence entre 10 MHz et 30 MHz. La communication de données se fait ici par les installations basse tension 220 V à l'intérieur de la maison (ou de l'appartement). C'est ce qu'on appelle également "Home Networking".

Un système CPL complet est composé de ces deux systèmes partiels, mais chaque partie peut théoriquement fonctionner indépendamment [1].

Afin de mieux comprendre le mode de fonctionnement de la technologie CPL et notamment son domaine d'application, on se propose de rappeler la structure générale d'un réseau électrique.

Ce dernier est en effet subdivisé en trois niveaux hiérarchiques distincts :

- La haute tension ($\geq$ 60KV) utilisée pour le transport de l'énergie sur de longues distances.

- La moyenne tension (3-60 KV) qui sert à amener l'énergie aux ports de liaison des quartiers.

- La basse tension (220-380V) pour amener l'électricité chez les usagers.

Le passage d'un niveau à l'autre est assuré par des transformateurs. Ceux-ci présentent toutefois la caractéristique fâcheuse de bloquer les hautes fréquences propres à une transmission à haut débit de l'information. Seul le réseau basse tension en aval de la sous-station transformatrice peut donc être utilisé pour offrir des services de télécommunications

évolués. Chaque sous-station dessert entre 100 et 200 usagers pour des distances de l'ordre de 300 à 500 mètres. La topologie du réseau est de type arborescent.

Dans ce contexte, le système à mettre en œuvre pour transmettre des données sur le réseau électrique comprend les éléments suivants (figure I-1) :

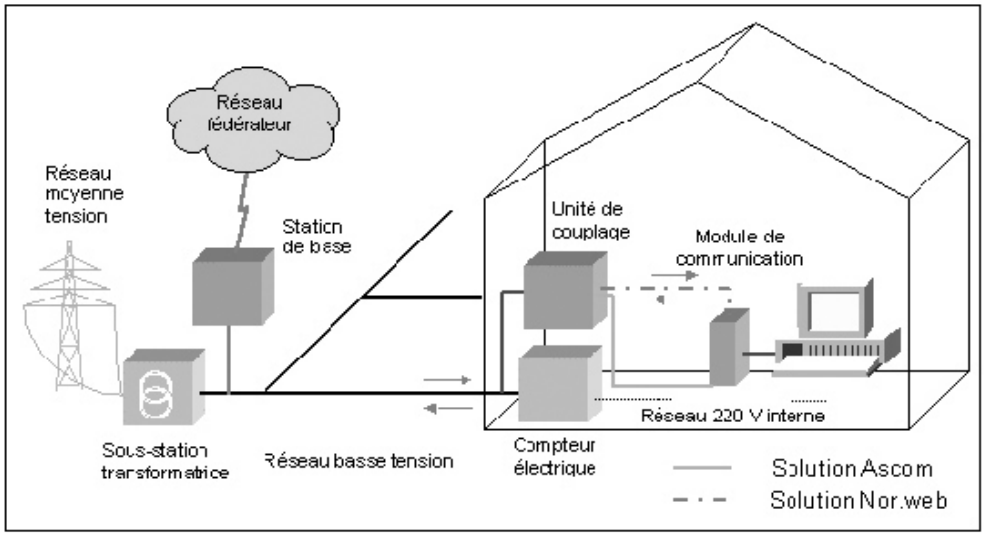


Figure I-1 : Architecture générale du système CPL

- Une station de base, située à la sous-station transformatrice, qui injecte et récupère les signaux sur le câble électrique. D'où, on définit deux sens de transmission dans le réseau CPL :

  - Liaison descendante (Downlink\downstream) : la transmission s'effectue de la station de base vers le réseau des utilisateurs. Le signal est transmis pour toutes les subdivisions de tout le réseau. Donc il est reçu par tous les utilisateurs de ce réseau.

  - Liaison montante (Uplink\upstream) : la transmission s'effectue à partir de l'utilisateur vers la station de base. Le signal envoyé par l'utilisateur est transmis à la station de base et à tous les autres utilisateurs du réseau [2].

- Une unité de couplage située près du compteur électrique, ce dispositif extrait les données du câble électrique et les transmet sur un câble coaxial dédié (dans

le cas du système Norweb), respectivement via le réseau électrique interne (solution Ascom), vers l'équipement terminal de l'utilisateur.

- Un module de communication (carte interne ou modem externe) connecté à un PC pour délivrer l'information à l'utilisateur.

I-2-2 Applications CPL

Le transport des données permet d'envisager des domaines d'applications multiples tels que l'accès aux réseaux des opérateurs ou à des réseaux privés de type intra-entreprises. Toutefois, aujourd'hui, les domaines porteurs et prometteurs sont :

- Les demandes en télécommunications de base comme l'accès Internet, le transport de la voix sur IP, la vidéo à la demande ou encore l'usage de webcam.

- Des possibilités de gestion de l'énergie comme l'analyse des courbes de charges pour des consommateurs importants, permettant de mieux gérer leurs besoins en électricité, la gestion des pompes à chaleur, la domotique (activation ou désactivation de certains interrupteurs et contacteurs) ou encore la télérelevé des compteurs.

- Le domaine de la sécurité comme la vidéo-surveillance ou encore la gestion des alarmes [1].

I-3 Exemples d'architectures de réseaux CPL

I-3-1 Réseau téléphonique

Pour bénéficier de l'application de la technique CPL en téléphonie, chaque usager doit disposer d'un modem CPL connecté à un module H 323 /SIP qui présente une interface avec un poste téléphonique ou un PC. Le CuPLUS représente une unité d'interfaçage entre le réseau téléphonique commuté et le réseau électrique. Les usagers sont disposés en parallèle et partagent le même support (figure I-2) .

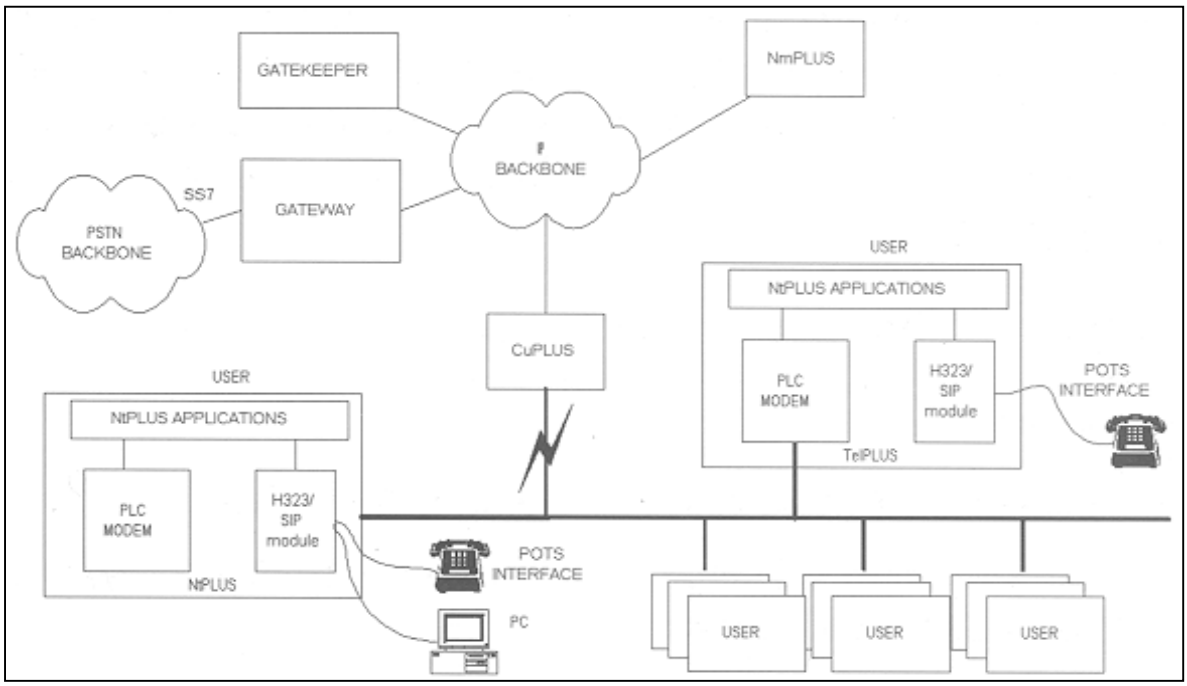


Figure I-2 : Réseau CPL pour téléphonie

I-3-2 Réseau de télérelève

La télérelève permet la lecture à distance des valeurs de la consommation de l'énergie électrique grâce à un compteur qui communique avec un modem CPL. Ainsi, elle permet d'éviter le déplacement chez l'abonné ce qui réduit le coût et assure la confidentialité des informations (figure I-3) [3].

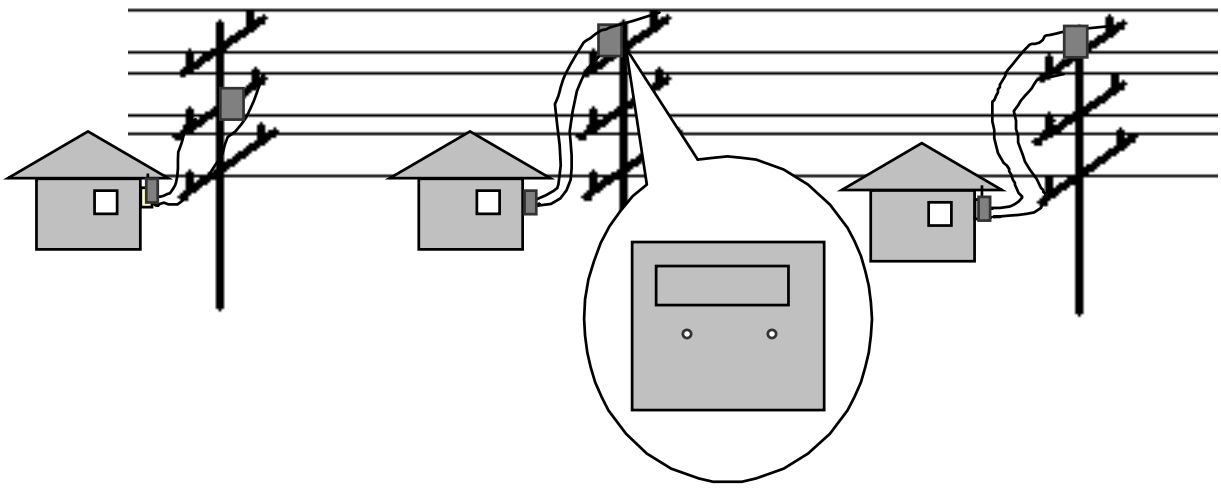


Figure I-3 : Réseau CPLpour télérelève des compteurs d'énergie électrique

I-3-3 Réseau de transmission de données et d'images

La transmission de données et d'images utilise le réseau électrique existant comme installation de base du réseau local (figure I-4).

Les signaux de données et d'images en provenance de la station de base sont injectés sur le câble électrique par l'intermédiaire d'un modem courant porteur de ligne à grande vitesse appelé Head End (HE) qui est installé à proximité du transformateur moyenne tension / basse tension (MT/BT) Chaque habitation possède un modem courant porteur de ligne CPE (Customer Premises Equipement) qui est un module de communication permettant de délivrer l'information à l'utilisateur. Le Home Gatway permet l'interconnexion de réseaux différents.

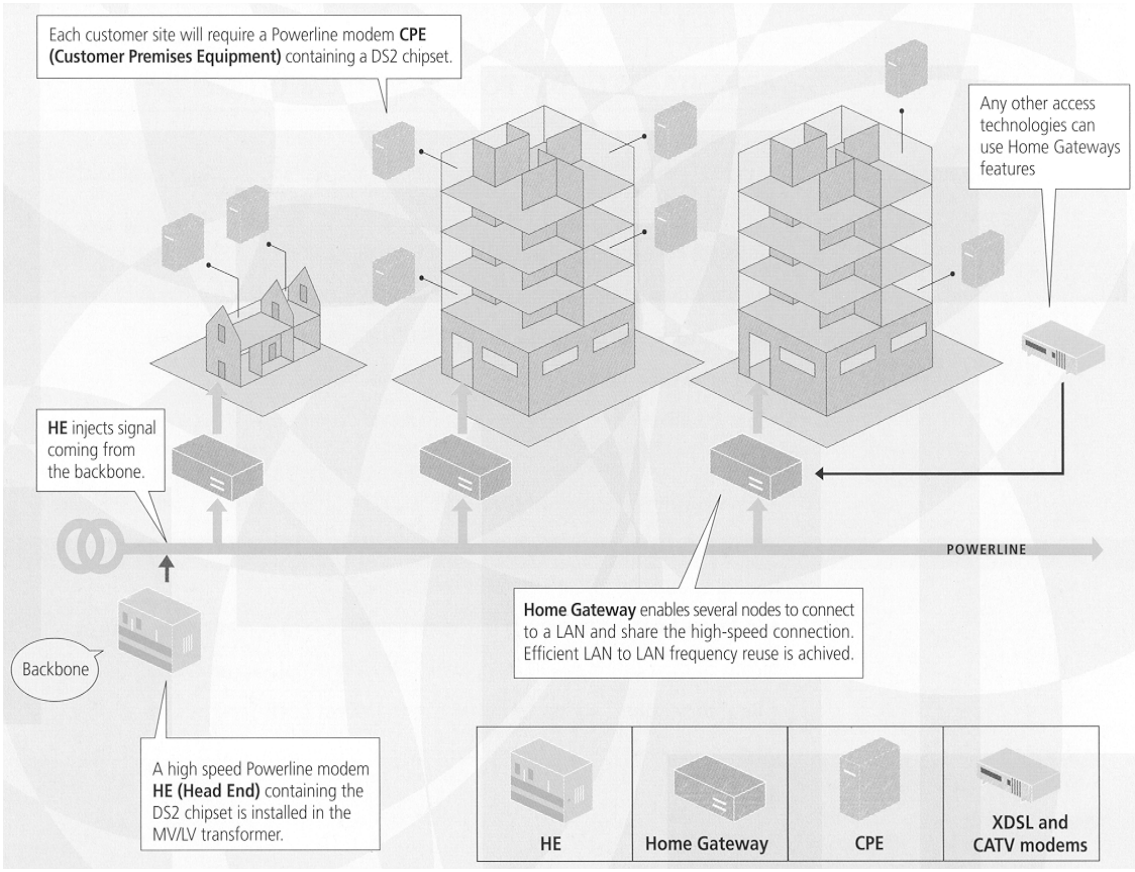


Figure I-4 : Réseau CPL pour transmission de données et d'images

I-4 Caractéristiques d'un protocole de transmission

I-4-1 Définition d'un protocole

Le protocole est un ensemble de règles et de procédures à respecter qui déterminent la façon d'envoyer et de recevoir des données, plus précisément la façon dont l'émetteur doit envoyer et partager les données et comment le récepteur doit les recevoir et les reconstituer.

Il existe des protocoles qui sont spécialisés dans l'échange de fichiers et d'autres qui permettent de gérer simplement l'état de la transmission et des erreurs.

Un protocole permet donc de mettre tout le monde «sur la même longueur d'onde». Ceci afin de remédier à des situations d'incommunicabilité entre les interlocuteurs [5].

I-4-2 Modèle OSI

L'International Standard Organization (ISO) a défini un modèle de base appelé modèle OSI. Ce modèle définit sept niveaux différents pour le transfert de données.

A chacun de ces niveaux, on encapsule une entête et une fin de trame qui comporte les informations nécessaires suivant les règles définies par le protocole utilisé.

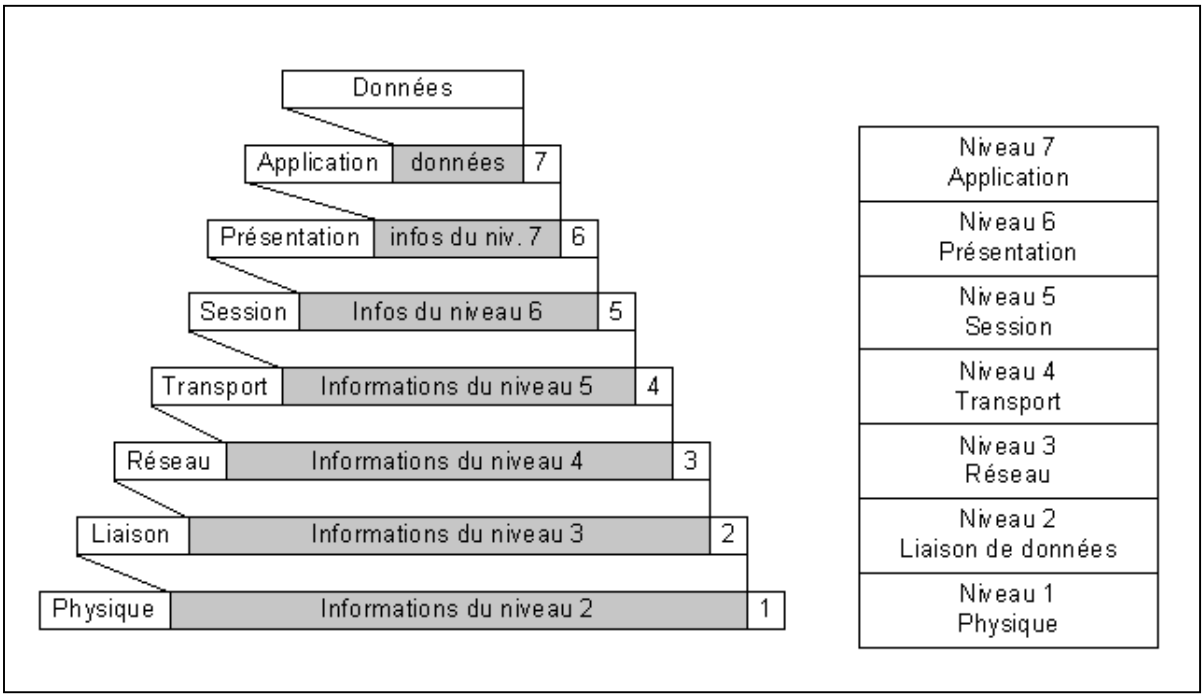


Figure I-5 : Modèle OSI à sept couches

a) Couche physique

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1.Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie...), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.

L'unité d'information typique de cette couche est le bit, représenté par une certaine différence de potentiel.

b) Couche liaison de données

Son rôle consiste à transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données.

La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

L'unité d'information de la couche liaison de données est la trame qui est composée de quelques centaines à quelques milliers d'octets maximums.

c) Couche réseau

C'est la couche qui permet de gérer le sous-réseau, le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques...).

La couche réseau contrôle également la congestion du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat. L'unité d'information de la couche réseau est le paquet.

d) Couche transport

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les fragments arrivent correctement de l'autre côté. Cette couche effectue aussi le réassemblage du message à la réception des morceaux.

Ce niveau est également responsable de l'optimisation des ressources du réseau, en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session.

Cette couche est également responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau par exemple service en mode connecté ou non, avec ou sans garantie d'ordre de délivrance, diffusion du message à plusieurs destinataires à la fois... Elle est responsable de l'établissement et la libération des connexions sur le réseau. Un des tous derniers rôles à évoquer est le contrôle de flux.

C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est par ailleurs elle qui gère l'ensemble du processus de connexion, avec toutes les contraintes qui y sont liées. L'unité d'information de la couche réseau est le message.

d) Couche session

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande

leur dialogue (qui doit parler, qui parle...). La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

e) Couche présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.

Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

f) Couche application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, exemple de service, on cite le transfert de fichier, la messagerie...

I-5 Présentation du standard Home Plug

I-5-1 Caractéristiques générales

Home Plug est une norme qui permet de définir toutes les spécificités et les caractéristiques de transmission sur une ligne d'énergie.

Ce standard permet de supporter un certain nombre d'applications à haut débit (l'accès internet, voie sur IP (VOIP), application multimédia…) tout en offrant plusieurs performances qui sont :

- Le transfert d'un fichier d'un nœud à un autre peut être effectué avec un débit >5 Mbits/s pour 80% des connexions.
- Le transfert de fichiers dans les deux directions, lorsque 5 nœuds partagent le réseau, peut se faire à un débit >3 Mbits/s dans 80% des cas et >500 Kbits /s dans 98% des cas.
- Lorsqu'on a 4 appels VOIP simultanés, le délai de transfert de fichier dans un seul sens est <10ms et le taux d'erreur binaire est <1% dans 98% des connexions.

- La technologie doit supporter 3 ressources média fonctionnant simultanément avec un débit >250Kbits/s et un taux d'erreur <1% et un délai<20 ms pour 98% des connexions.

La norme Home Plug est caractérisée par :

- Une topologie point à point (peer to peer): Le réseau Home Plug adapte une topologie qui permet à un nœud de communiquer avec un autre sans avoir besoin d'un hub ou d'un nœud intermédiaire.

- Technique de transmission Orthogonal Frequency Division Multiplexing (OFDM) : Cette technique permet la transmission des données à haut débit en les divisant en des flots de faible débit binaire modulés séparément, l'espace entre sous porteuse est très étroit.

- Technique de codage : Utilisation d'un codeur convolutif concaténé avec un Reed Salomon en passant par des entrelaceurs pour la correction d'erreur ou aussi Turbo Product Coding(TCP) pour contrôler les champs de données de la trame.

- Le mode d'accès : Le protocole CSMA/CA est utilisé dans la couche MAC [5].

I-5-2 Définition de la couche MAC

Home Plug utilise le mécanisme d'écoute de la porteuse VCS (virtual carrier sense) pour minimiser le nombre de collision.

Le récepteur détecte le préambule et extrait l'information de la trame de contrôle. Cette dernière spécifie le type de délimiteur qui peut être :

- Start Delimiter : Il inclut la durée de charge utile, le type de modulation, le codage et le nombre de porteuse.

- End Delimiter : Il définit la fin de la trame.

Si le récepteur peut décoder la trame de contrôle, il peut déterminer la durée de la transmission et s'il n'arrive pas à décoder ce champ alors il suppose que la longueur du paquet maximale va être transmise et fixe son VCS jusqu'à la réception de plus d'information.

Avant tout échange entre nœud, il faut envoyer un message de demande d'estimation du canal. A cet effet la destination répond en indiquant le type de modulation et le type de codage que la source doit respecter durant la transmission. Parfois, il arrive que la source ne reçoive pas un accusé de réception ACK, elle suppose alors qu'il y a eu une collision pendant la transmission et elle retransmet de nouveau.

I-6 Conclusion

Cette partie avait pour objectif de présenter les principales caractéristiques de la technique CPL et la norme Home Plug et comprendre le principe de fonctionnement basé sur le partage du support de transmission et l'accès multiple.

Ces notions seront utiles dans le chapitre suivant pour la mise en œuvre d'un protocole CPL qui permet de garantir une qualité de service satisfaisante tout en tenant compte des contraintes de transmission sur la ligne d'énergie.

Chapitre II :

MISE EN ŒUVRE DU PROTOCOLE CPL

II-1 Introduction

La technique CPL exige un accès multiple au support de transmission qui doit être contrôlé et géré par la couche MAC. Pour atteindre cet objectif, nous nous intéresserons dans la première partie de ce chapitre aux considérations de la conception du protocole CPL. La deuxième partie est consacrée à l'étude de la couche MAC alors que dans la dernière partie nous nous occupons de la configuration de la couche MAC.

II-2 Considérations de conception

II-2-1 Spécifications des applications visées

II-2-1-1 Application d'accès Internet

L'accès Internet est considéré comme l'application la plus importante de la technique CPL. En effet avoir Internet sur le réseau électrique est une idée lumineuse et bénéfique vu la disponibilité du support physique partout dans la maison. Ainsi, on pourra accéder au web depuis chaque prise électrique [6].

Pour supporter un accès Internet à l'intérieur des bâtiments, le Modem CPL doit présenter les spécifications suivantes :

- Débit de données : 2 à 14 Mbps.
- Portée sans répéteur : 100 m.
- Bande de transmission : 4 à 20 MHZ.
- Type de modulation : OFDM ou DS-SS.
- Type de porteuse : DQPSK ; DBPSK.
- Type d'accès : CSMA/CA.
- Norme : ETSI –ES 201 867 V.1.1.1 (2000).

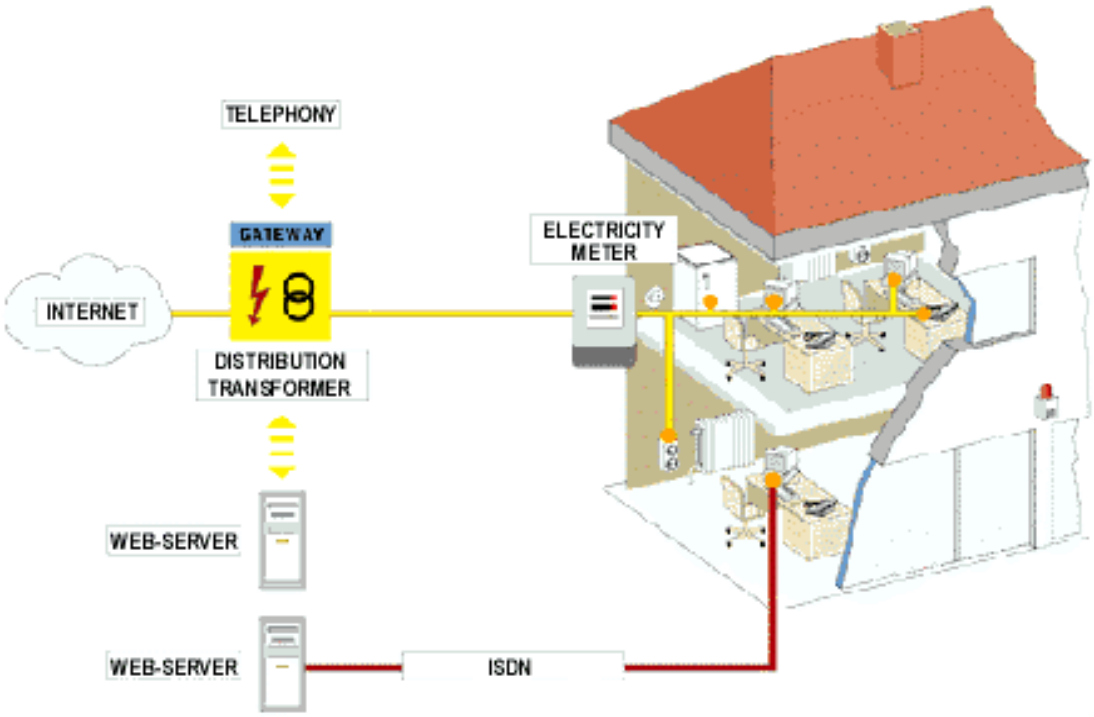


Figure II-1 : Architecture d'un réseau Internet domestique

II-2-1-2 Application de la télédomotique

La télédomotique consiste à commander à distance plusieurs installations domestiques à la maison à travers un support de transmission local, de ce fait l'offre domotique se caractérise par un ensemble d'équipements internes à l'habitat (capteurs, détecteurs, sirènes, centrale) reliés par des moyens de communication locaux (réseau domotique, réseau radio). En les associant à des moyens de télécommunications (modem, ligne téléphonique..) . On assure la possibilité de surveillance et de pilotage à distance.

Les moyens de communications locaux peuvent être des lignes filaires indépendantes, des liaisons Infra Rouge (IR), des liaisons radio. Mais dernièrement, le réseau d'énergie est exploité dans la domotique tenant compte des avantages majeurs qu'il nous offre par rapport aux autres supports déjà cités.

La transmission par CPL regroupe toutes les fonctions qui interviennent dans ce domaine citant : La mesure qui est faite par des capteurs qui identifient les conditions instantanément

(température, position..) et la commande qui est réalisée par l'intervention des signaux haute fréquence émis par une unité centrale et véhiculée sur le réseau BT [7].

Cette application est du type bas débit et présente les spécifications suivantes :

- Débit de données : de 300 bps à 9600 bps
- Portée sans répéteur : 100 m
- Bande de transmission : 95 à 148,5 KHZ
- Type de modulation : bande étroite
- Type de porteuse : ASK, FSK ou PSK
- Type de protocole : maître – esclave
- Norme : CENELEC – EN50065 (1991)

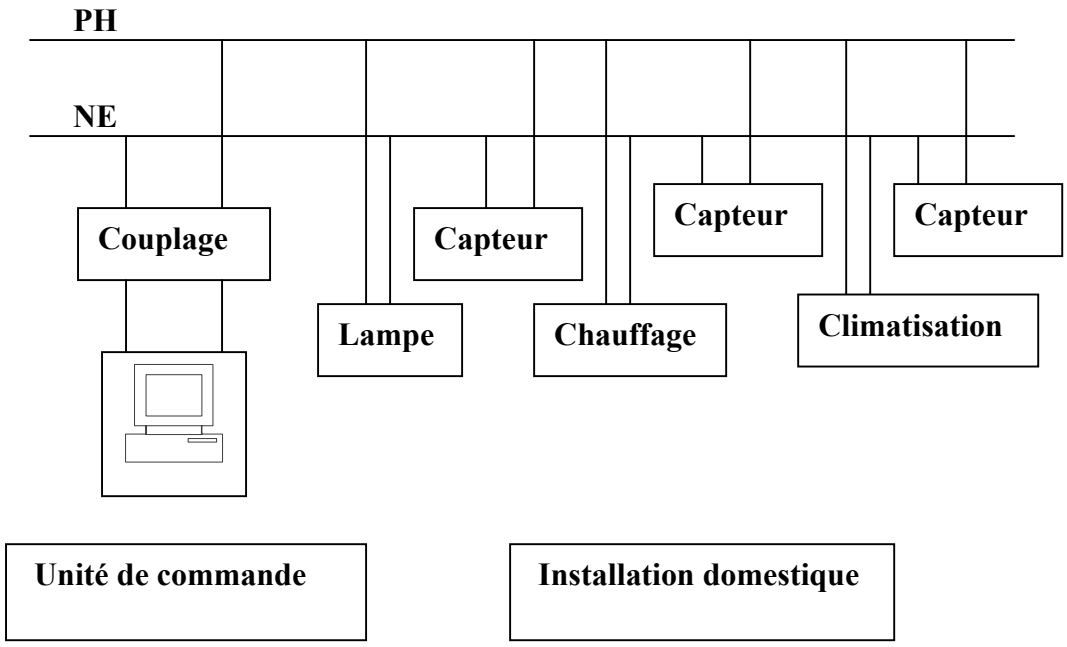


Figure II–2 : Schéma synoptique d'un réseau télédomotique

L'unité de commande est généralement un ordinateur qui gère toutes les actions souhaitées (éclairage, conditionnement..) suivant le programme et les paramètres mesurés .

De point de vue principe, l'ordinateur fait correspondre à chaque installation domestique une adresse spécifique sous forme de séquence binaire. Chaque adresse est envoyée

évidemment après codage et modulation sur la ligne BT pour commander l'installation concernée.

Le signal émis sera modulé à une haute fréquence connue par l'équipement désigné. A la réception, chaque équipement possède un filtre passe bande accordé sur la fréquence concernée. Une simple démodulation permet l'identification du signal émis par l'ordinateur.

Les applications possibles de cette technologie sont nombreuses est peuvent s'orienter vers divers domaines de la domotique.

II-2-2 Structure du protocole

La définition d'un protocole de transmission de données selon la technique CPL nécessite l'intervention uniquement au niveau des couches physique et liaison de données. Le reste des couches du modèle OSI seront définies suivant les exigences de l'application considérée. La couche liaison de données est elle même subdivisée en deux sous-couches:

- Logical Link Control (LLC) : définit les techniques de contrôle d'erreurs et de flux de données.
- Media Access control (MAC): définit la technique de partage adéquat du canal de transmission.

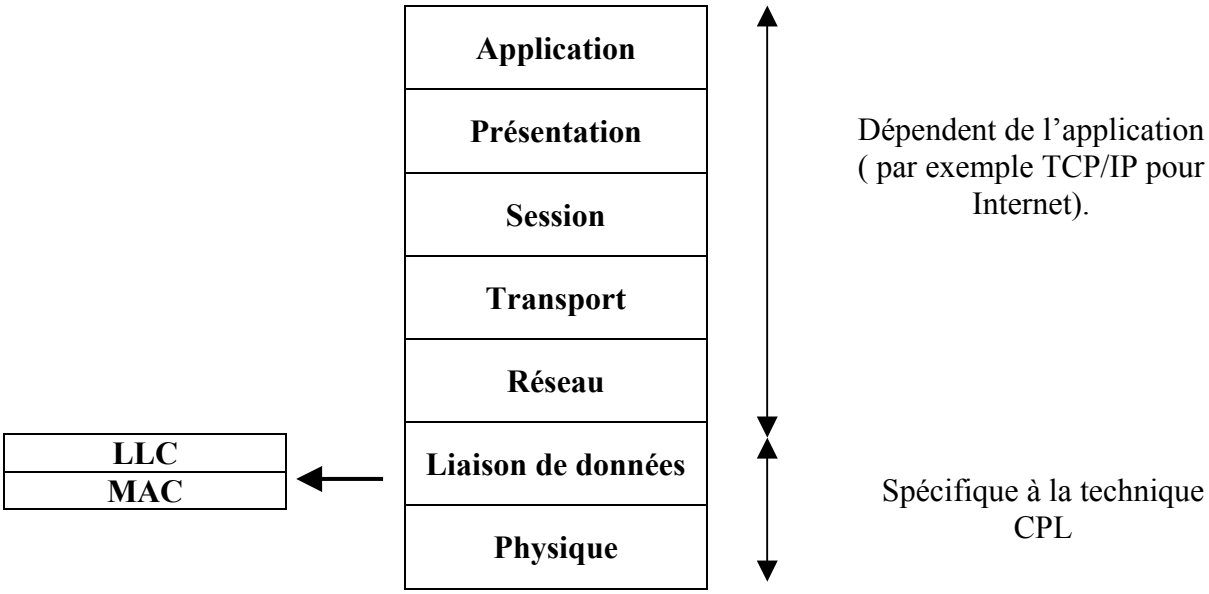


Figure II-3 : Répartition du choix des couches du protocole pour la technique CPL

II-2-3 Contraintes de l'accès en technique CPL

La transmission en technique CPL présente la complexité du partage du même support physique par tous les utilisateurs connectés à la ligne de distribution électrique alimentée par le même transformateur. Ce partage est d'autant plus complexe que celui du canal radio vu la caractéristique de son modèle d'atténuation (variation rapide en fonction de la distance). De même la limitation de la bande de transmission (≤ 30 MHz) associé avec le débit élevé requis par les nouveaux services de télécommunications rend les techniques classiques de multiplexage temporel et fréquentiel insuffisantes. D'où la nécessité d'un effort supplémentaire au niveau de la couche MAC.

Plus particulièrement l'atténuation du canal qui a un comportement d'une ligne de transmission (eq-1) fait accentuer le problème de nœud caché "hidden node".

$$\text{Atténuation} = \gamma \cdot \delta^{d} \quad \begin{cases} \delta \text{ et } \gamma \text{ : constantes de propagation} \\ d \text{ : distance} \end{cases} \qquad \text{(eq-1)}$$

Le problème "hidden node" est du à la grande variation de l'atténuation avec la distance entre les nœuds.

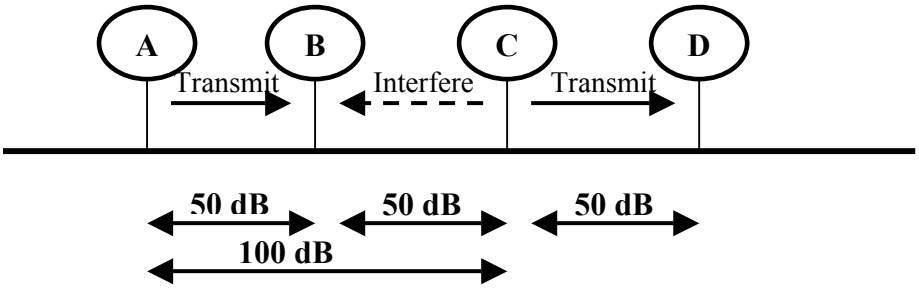


Figure II-4: Le problème "hidden node"

Pour l'exemple de la figure II-4, l'atténuation entre les nœuds A et B, B et C et C et D est de 50dB alors qu'entre A et C, B et D est de 100 dB. Cette variation a pour conséquence que A et C ne peuvent pas s'entendre (la même chose pour A et D). En effet lorsque A transmet vers B, il arrive que C puisse s'interférer en transmettant vers D, provoquant le problème "hidden node" [10].

II-3 Etude de la couche MAC pour la technique CPL

II-3-1 Définition des caractéristiques de la couche MAC

La couche MAC est responsable du contrôle d'accès au réseau. Pour accomplir cette tâche elle doit s'assurer que deux stations ne transmettent jamais des trames simultanément sur le réseau. Outre le contrôle de l'accès au réseau, la couche MAC est aussi responsable de l'ordonnancement du mouvement des données sur le réseau. Pour ce faire, elle s'occupe de l'adressage, de la définition et du contrôle des trames.

La tâche essentielle du protocole MAC est de gérer l'allocation et la réallocation du canal entre les abonnés CPL et la transmission des différents types de service.

On propose un traitement séparé des différents services transmis en CPL ce qui permet une garantie de la qualité de service QoS pour chacun.

A cause des perturbations qui influencent le réseau CPL, on propose une segmentation de l'information utilisateur en de petites unités de données de longueur fixe appelée "segments CPL".

Le protocole MAC doit préciser la stratégie de partage de ressources puisqu'on a un accès multiple. La stratégie d'accès statique est souhaitable pour le trafic continu et non pour le trafic variable. L'accès dynamique est adéquat pour la transmission de données et dans certains cas il est possible d'assurer la satisfaction de la qualité de transmission pour le délai critique de trafic [2].

Ainsi tout mécanisme MAC pour CPL haut débit doit respecter les exigences suivantes:

- Coexistence de systèmes communicants voisins.
- Utilisation efficace du spectre alloué.
- Solution robuste pour le problème "hidden node".

II-3-2 Analyse des modes d'accès

Le mode de transmission par diffusion engendre de la compétition pour l'accès au support. Il faut alors des stratégies pour l'allocation des canaux:

Allocation statique : multiplexage (fréquentiel / temporel / statistique).

Allocation dynamique : on distingue trois principales stratégies:

- Round Robin: chaque station peut transmettre une trame selon :
  - Un temps fixe pour chaque station.
  - Une permission donnée par un contrôleur central.
  - Une permission donnée à chaque station en alternance.
- Réservation : chaque station doit réserver un temps de transmission auprès d'un contrôleur central.
- Contention : il n'y a pas de contrôle central. Chaque station transmet quand elle veut (accès multiple). S'il y a des conflits, les stations retransmettent la trame.

Les protocoles existants pour la transmission des données à haut débit peuvent être utilisés avec succès uniquement dans le cas des canaux très faiblement bruités. Dans le cas de la transmission sur les lignes d'énergie, l'environnement de perturbation très sévère nécessite des modifications des protocoles existants ou la définition de nouveaux protocoles.

II-3-3 Principaux protocoles d'accès

II-3-3-1 Le protocole ALOHA

Il s'agit d'une technique simple à accès multiple en étoile. Le cœur de l'étoile est chargé de distribuer les messages émis par les machines et en cas de collision, les paquets perdus sont réémis. Cependant ce système est rapidement inefficace en cas de forte charge du réseau.

a) ALOHA Pur

L'idée principale est de permettre à toute station de transmettre dès qu'elle a des données à envoyer. Il n'y a pas d'écoute du support avant la transmission. Des collisions vont éventuellement se produire. Les expéditeurs sont capables de détecter les collisions en écoutant les paquets en retour. En cas de collision l'expéditeur attend un temps aléatoire avant de retransmettre le même paquet. Deux paquets chevauchant même d'un seul bit seront tous deux détruits [8].

b) ALOHA en tranches ou discrétisé

L'idée de cette méthode est de découper le temps en tranches correspondant chacune au temps de transmission d'un paquet, les émissions sont alors synchronisées en début de tranches. Grâce à cette méthode, s'il y a détection de collisions, c'est sur l'ensemble de la tranche de temps, et non plus sur une partie d'un paquet. Cette méthode de découpage du temps en tranches, tout en gardant le système de l'ALHOA, améliore le taux d'utilisation du canal et le ramène à 36 %. La transmission d'un paquet n'est permise qu'au début d'une tranche d'où le débit est deux fois meilleur que celui d'ALOHA pur (débit faible max. 18%).

Remarque: Quand la charge est très élevée les paquets sont retardées pour de longues période. L'ALOHA par tranche n'est pas stable. A la suite de charge de pointe, L'ALOHA par tranche ne peut pas se réajuster lui-même. Il y a plusieurs méthodes pour contrôler la distribution de génération des messages et stabiliser l'ALOHA par tranches. (Par exemple augmenter le délai de retransmission de paquets après chaque transmission ratée)[8].

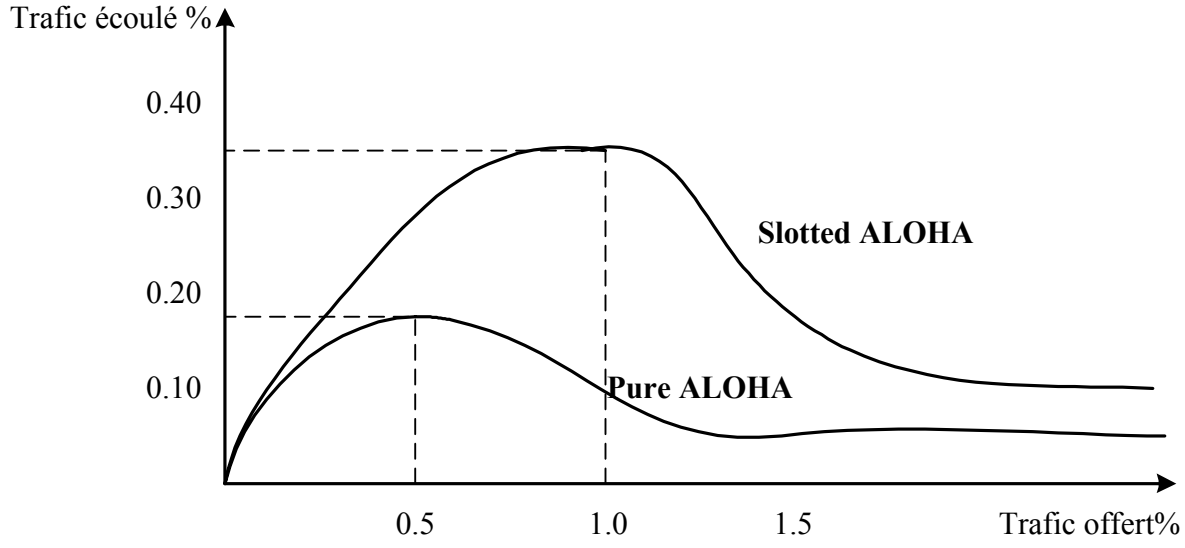


Figure II-5 : Diagramme du trafic du système ALOHA

c) ALOHA avec réservation

Cette méthode est basée sur la notion de probabilité. Si une station commence à émettre un paquet, il y a de fortes chances qu'elle en émette un autre immédiatement. Ce raisonnement va mener à l'idée de réserver plusieurs tranches de temps à une station qui commence à émettre. De plus s'il y a collision, celle-ci s'effectue sur un intervalle complet et non sur une partie. Plus de détails sur ce protocole sont présentés en Annexe A.

II-3-3-2 Le protocole Polling

La station de base envoie un message appelé "Polling-message" pour chaque station utilisateur suivant la procédure Round Robin. Lorsqu'une station désire émettre, elle fait une requête auprès du hub qui lui alloue ou non le support (Demand Priority Access Method ou **DPAM**). Les collisions sont donc impossibles et le délai d'attente dû aux jetons est supprimé.

Les stations informent le hub de leurs disponibilités en lui transmettant le "signal Idle". La station désirant émettre formule une requête avec un niveau de priorité. Les autres machines raccordées sont averties par le hub que quelqu'un va émettre et se mettent en état de recevoir (signal INComming (INC)). Lorsque toutes les stations ont cessé l'émission du Idle, cela signifie qu'elles sont prêtes à recevoir et la station émettrice transmet sa trame. Le hub l'analyse et la transmet à la station intéressée et reprend l'émission du Idle.

Les signaux de signalisation sont émis en basse fréquence (30 Mhz), ils se composent de deux tonalités. La première tonalité correspond à la transmission de 16 bits à 1 suivis de 16 bits à 0, ce qui donne un signal de 0.9375 Mhz, la seconde tonalité alterne la transmission de 8 bits à 0 et 8 bits à 1, ce qui donne un signal de 1.875 MHz[8].

Les différents signaux de signalisation sont reproduits dans le tableau suivant :

Tonalité	**Hub vers station**	**Station vers Hub**
Silence	Prêt à émettre ou à recevoir	

1 et 1	**IDLE** : rien à envoyer ou à transmettre	
1 et 2	**INC** : demande de passage en état de réception	**NPR** : Requête de priorité normale
2 et 1		**HPR** : requête de priorité haute
2 et 2	Initialisation **INIT** : déclenché pour connaître les adresses MAC des stations	

Tableau II-1 : Signaux de signalisation dans le protocole Polling

Cette méthode d'accès garantit que chaque station aura accès au support. Afin d'éviter un usage abusif des données prioritaires, le hub surveille les files d'attente de requêtes de données normales et les transforment en priorité haute à l'échéance d'une temporisation (TTT : Target Transmission Time). Les stations sont donc sûre d'émettre après *n* TTT secondes où *n* est le nombre de stations.

En Polling, le poste Master invite les autres postes à émettre chacun leur tour. Le poste consulté répond par un message s'il a quelque chose à émettre, sinon il répond négativement.

Le format type d'un message est indiqué ci-après. On donne parfois la notion de bloc. Ce bloc peut être de taille quelconque.

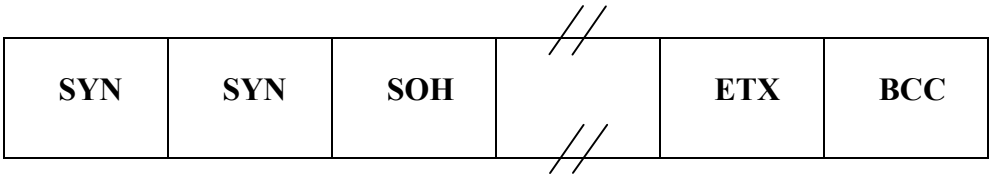


Figure II-6 : Format de la trame pour le protocole Polling

Deux caractères de synchronisation (SYN) précèdent une entête facultative annoncée par SOH. Le texte commence par STX et se termine par ETX ou par ETB et BCC.

II-3-3-3 Mode d'accès CSMA

Le principe de bas du mécanisme CSMA(Carrier Sense Multiple Acess) repose sur le fait qu'un nœud qui souhaite transmettre retient le canal pendant un certain temps en envoyant un signal ou un message approprié. Ainsi pendant ce temps aucun autre nœud n'est autorisé à transmettre. Le mécanisme CSMA possède deux avantages pour son utilisation en CPL. Premièrement, il permet un partage dynamique du canal (plus efficace que le partage statique). Deuxièmement, la retenue du canal est effectuée localement.

Selon le mode de retenue du canal (capture) le mécanisme CSMA peut être classé en trois types: "Physical Carrier Sense", "Virtual Carrier Sense" et "Virtual Carrier Sense with CTS". Le mécanisme CSMA peut ainsi être classé selon la technique de "contention" du canal.

- CA (Collision Avoidance).
- CD (Collision Detection).
- CR (Collision Resolution).

II-4 Configuration de la couche MAC pour le standard Home Plug

Le standard Home Plug définit pour la couche MAC l'utilisation du mécanisme d'accès CSMA/CA avec VCS.

II-4-1 Principe de l'accès CSMA/CA

Le mécanisme d'accès de base, appelé Distributed Coordination Function est typiquement le mécanisme Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Les protocoles CSMA sont bien connus de l'industrie, où le plus célèbre est Ethernet, qui est un protocole CSMA/CD.

Ces types de protocoles sont très efficaces quand le support n'est pas surchargé, puisqu'il autorise les stations à émettre avec un minimum de délai, mais il y a toujours une chance que des stations émettent en même temps (collision). Ceci est dû au fait que les stations écoutent

le support, le repèrent libre, et finalement décident de transmettre, parfois en même temps qu'une autre exécutant cette même suite d'opérations.

Ces collisions doivent être détectées, pour que la couche MAC puisse retransmettre le paquet repasser par les couches supérieures, ce qui engendrerait des délais significatifs. Dans le cas d'Ethernet, cette collision est repérée par les stations qui transmettent, celles-ci allant à la phase de retransmission basée sur un algorithme de retour aléatoire exponentiel (exponential random backoff). Le backoff exponentiel signifie qu'à chaque fois qu'une station choisit un slot et provoque une collision, le nombre maximum pour la sélection aléatoire est augmenté exponentiellement.

Si ces mécanismes de détection de collision sont bons sur certains réseaux, ils ne peuvent pas être utilisés dans un LAN CPL, pour les raisons définies précédemment.

Pour dépasser ces problèmes, 802.11 utilise le mécanisme d'esquive de collision (Collision Avoidance), ainsi que le principe d'accusé de réception (Positif Acknowledge) comme suit: Une station voulant transmettre écoute le support, et s'il est occupé, la transmission est différée. Si le support est libre pour un temps spécifique (appelé DIFS, Distributed Inter Frame Space, dans le standard), alors la station est autorisée à transmettre. La station réceptrice va vérifier le CRC du paquet reçu et renvoie un accusé de réception (ACK). La réception de l'ACK indiquera à l'émetteur qu'aucune collision n'a eu lieu. Si l'émetteur ne reçoit pas l'accusé de réception, alors il retransmet le fragment jusqu'à ce qu'il l'obtienne ou abandonne au bout d'un certain nombre de retransmissions [10].

II-4-2 Mécanisme Virtual Carrier Sense (VCS) avec CTS

Dans le mécanisme VCS pur, un message de contrôle est envoyé avant la transmission des données. Ce message contient des informations sur la durée de la transmission, il est détecté par tous les nœuds. Cette technique permet de dépasser les problèmes de non-fiabilité dans "Carrier Sense" mais elle ne résout pas le problème de "hidden node". Par conséquent, on ne peut pas l'appliquer pour les réseaux CPL [11].

Pour réduire la probabilité d'avoir deux stations entrant en collision car ne pouvant pas s'entendre l'une l'autre, le standard définit le mécanisme de Virtual Carrier Sense with CTS (sensation virtuelle de porteuse).

Une station voulant émettre transmet d'abord un petit paquet de contrôle appelé RTS (Request To Send), qui donnera la source, la destination, et la durée de la transaction. La station destination répond (si le support est libre) avec un paquet de contrôle de réponse appelé CTS (Clear To Send), qui incluera les mêmes informations sur la durée.

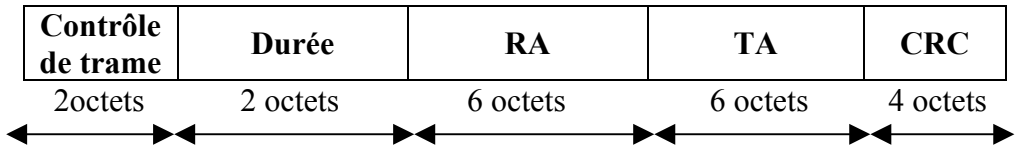


Figure II-7: Trame RTS

RA est l'adresse du récepteur de la prochaine trame de données ou de gestion. TA est l'adresse de la station qui transmet la trame RTS. La valeur de la durée est le temps, en microsecondes, nécessaire à la transmission de la trame de gestion ou de données suivantes, plus une trame CTS, plus une trame ACK, plus 3 intervalles SIFS.

Figure II-8 : Trame CTS

RA est l'adresse du récepteur de la trame CTS, directement copiée du champ TA de la trame RTS. La valeur de la durée est la valeur obtenue dans la trame RTS, moins le temps de transmission, en microsecondes, de la trame CTS et d'un intervalle SIFS.

Toutes les stations recevant soit le RTS, soit le CTS, déclencheront leur indicateur de "Virtual Carrier Sense" (appelé NAV pour Network Allocation Vector), pour une certaine durée, et utiliseront cette information avec le"Physical Carrier Sense" pour écouter le support.

II-4-3 Analyse des performances pour le canal CPL

Ce mécanisme réduit la probabilité de collision par une station "cachée" de l'émetteur dans la zone du récepteur à la courte durée de transmission du RTS, parce que la station entendra le CTS et considèrera le support comme occupé jusqu'à la fin de la transaction. L'information "durée" dans le RTS protège la zone de l'émetteur des collisions pendant la transmission de l'accusé de réception (par les stations étant hors de portée de la station accusant la réception).

Il est également à noter que grâce au fait que le RTS et le CTS sont des trames courtes, le nombre de collisions est réduit, puisque ces trames sont reconnues plus rapidement que si tout le paquet devait être transmis (ceci est vrai si le paquet est beaucoup plus important que le RTS, donc le standard autorise les paquets courts à être transmis sans l'échange de RTS/CTS, ceci étant contrôlé pour chaque station grâce au paramètre appelé RTS Threshold).

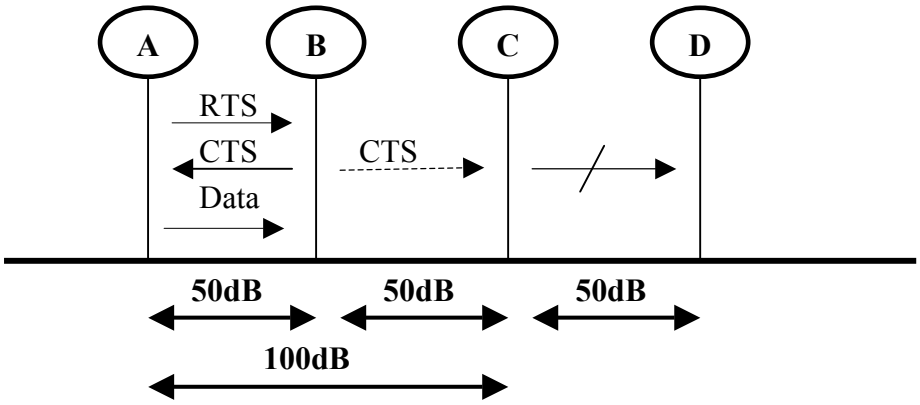


Figure II-9 : RTS/CTS La solution pour le problème "Hidden Node"

Le CTS est transmis par le nœud B vers le nœud C pour l'empêcher de transmettre vers le nœud D.

Malgré cette amélioration, il existe des situations ou les problèmes persistent encore. En effet, si le nœud B envoie un CTS au nœud A, D transmet un message à un autre nœud (non représenté dans la figure) et C est inconsciente de l'état du canal alors on confronte un nouveau problème de "hidden node" appelé "masked node problem". Le standard Home Plug néglige ce cas pour ne pas avoir un protocole complexe. Néanmoins des travaux de recherche

récents ont permis l'apparition d'une nouvelle technique appelée "Distributed Synchronised Media Acess Control Mechanism"[11].Cette technique est détaille en Annexe D.

II-5 Conclusion

Ce chapitre a été consacré à la mise en œuvre du protocole de la couche MAC selon le standard Home Plug. En effet, la technique CPL présente beaucoup de contraintes de transmission telle que le partage d'un seul support physique et le comportement très bruité de ce canal avec une forte atténuation.

Afin de compenser les effets néfastes de ces contraintes, il est nécessaire d'apporter un soin particulier à la définition de la couche MAC. La définition d'un mécanisme CSMA/CA avec VCS–CTS a été justifiée et ses performances pour la technique CPL ont été montrées.

Chapitre III :

IMPLANTATION ET TEST DU PROTOCOLE

III-1 Introduction

Pour compléter l'étude de conception d'un protocole de communication selon les recommandations de la norme Home Plug, on se propose dans ce chapitre de faire une étude pratique. Compte tenu de la complexité du protocole défini pour le Home Plug, le cahier des charges de notre projet nous a imposé pour l'implantation l'utilisation du protocole SNAP qui est une version plus simple adaptée pour la communication CPL.

Après la présentation du protocole SNAP, nous allons décrire les techniques de validation de protocoles. La dernière partie du chapitre est consacrée à la description et les tests expérimentaux de l'application pratique.

III-2 Présentation du protocole SNAP

III-2-1 Description du protocole

III-2-1-1 Définition

SNAP (Scaleable Node Address Protocol) est un protocole de réseau libre et ouvert qui peut être mis en application dans n'importe quel microcontrôleur MCU, disponible aujourd'hui. Il a été principalement développé pour les systèmes d'automation à la maison mais il est aussi employé comme un réseau générique qui peut être utilisé dans n'importe quel type d'application. Il est facile à apprendre: C'est un protocole flexible.

SNAP tient compte de la longueur variable de paquet et de la complexité du protocole. Il peut être employé comme un protocole très simple sans aucune adresse, drapeau ou détection d'erreur ou employé avec la pleine plage d'adresse, de drapeau et une variété de méthode de détection d'erreur. Cette scalabilité rend SNAP unique[12].

III-2-1-2 Caractéristiques du protocole SNAP

Ce protocole présente les caractéristiques suivantes :

- Facile à implémenter, à employer et à mettre en œuvre.
- Protocole de réseau libre et ouvert.
- Exige des ressources minimales de MCU(Micro Controller Unit) à implanter.
- Supporte jusqu'à 16.7 millions d'adresses de nœud et jusqu'à 24 drapeaux spécifiques de protocole
- Demande optionnelle de ACK/NACK.
- Mode de commande optionnel.
- 8 méthodes de détection d'erreur (Checksun, CRC…).
- Peut être utilisé en mode Master / Slave et point à point.
- Supporte les messages diffusés.
- Utilise des supports différents (CPL, RF..).
- Travaille avec des liaisons simplex, half duplex, full duplex.
- Taille de l'entête varie entre 3 et 12 octets.
- L'utilisateur spécifie le nombre d'octets dans le préambule(0-*n*).
- Fonctionne en mode de communication synchrone et asynchrone.

III-2-1-3 Description fonctionnelle

SNAP est un protocole qui utilise le mode paquet c'est à dire l'information échangée entre deux nœuds du réseau est sous forme de bloc de bits (octets). Ce paquet peut avoir des longueurs différentes qui dépendent du nombre d'octets qui définissent l'adresse (0-6 octets), le drapeau (0-3 octets), la taille des données à transmettre (0-512 octets) et la méthode de détection d'erreur utilisée.

a) Format de trame

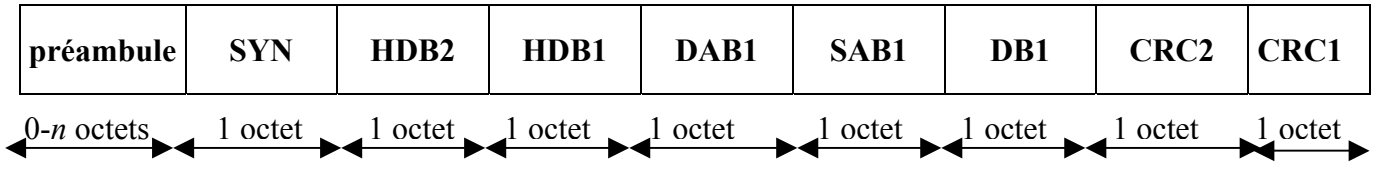


Figure III-1 : Format de la trame SNAP

- **Préambule :** C'est une séquence d'octets qui peut avoir une taille variable (0-*n* octets) fixée par l'utilisateur. Ce champ est optionnel et il est utilisé pour la calibration.

- **Synchronisation :** C'est un champ prédéfinit qui a une séquence fixe (01010100). Le but de la synchronisation est d'indiquer le début de paquet. Cette séquence de synchronisation n'est pas incluse dans le calcul de la détection d'erreur. Elle est aussi spécifique pour la synchronisation et ne peut pas être utilisée comme préambule.

- **L'entête de définition d'octet** (HDB1 et HDB2) : Ces champs permettent de définir le nombre d'octets utilisés pour l'adresse, le drapeau ainsi que la taille des données à envoyer. On spécifie aussi la méthode de détection d'erreur. Ils définissent la structure complète du paquet.
- **DAB1** (Destination Address Byte) : Ce champ contient l'adresse destination.
- **SAB1** (Source Address Byte) : Ce champ contient l'adresse source.
- **DB** (Data Byte) : Ce champ contient les données à transmettre.
- **CRC** (Cyclic Redundancy Check) : Ce champ permet la détection d'erreur, il dépend de la méthode utilisée.

b) Structure du champ HDB2

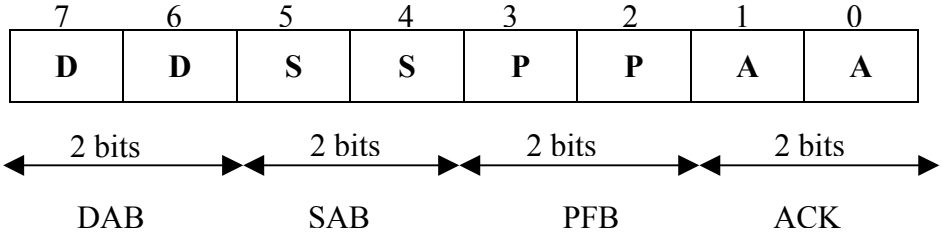


Figure III-2 : Structure du champ HDB2

- **DAB** (Number of Destination Address Bytes) est représenté par les deux bits 7 et 6. Avec une taille maximale de 3 octets, on peut avoir jusqu'à 16777215 destinations différentes.

0	**0**	: 0 octet pour l'adresse destination
0	**1**	: 1 octet pour l'adresse destination
1	**0**	: 2 octets pour l'adresse destination
1	**1**	: 3 octets pour l'adresse destination

Tableau III-1 : Nombre d'octets de l'adresse de destination

- **SAB (**Number of Source Address Bytes) définit le nombre d'octets de l'adresse source dans le paquet. On peut avoir jusqu'à 16777215 adresses source différentes.

Remarque : SAB et DAB sont égaux à 0 lorsque la liaison est du type point à point.

- **PFB** (Number of Protocol specific Flag bytes) il définit le nombre d'octets pour le drapeau spécifique au protocole. On peut avoir un maximum de 24 drapeaux.
- **ACK/NACK** (Acknowledge/ No acknowledge) : Ce champ spécifie s'il y a une demande d'un accusé de réception ou non.

0	**0**	: Il n'y a pas de demande d'accusé de réception.
0	**1**	: Demande d'accusé de réception.
1	**0**	: Réponse par un accusé de réception ACK.
1	**1**	: Réponse par un NACK.

Tableau III-2 : Valeurs de l'ACK/NACK

c) Structure du champ HDB1

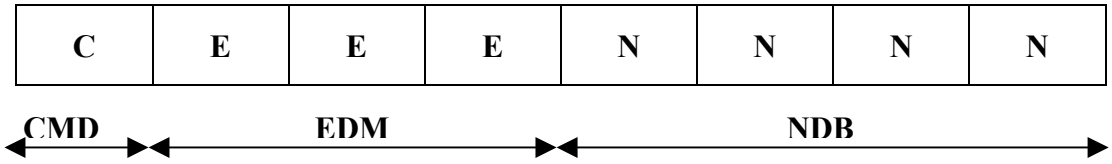


Figure III-3 : Structure du champ HDB1

- **CMD** (Command Mode Bit) C'est une caractéristique optionnelle. Il est à zéro si le nœud ne l'utilise pas. Un nœud qui utilise cette caractéristique sera capable de répondre aux questions des autres nœuds ainsi qu'envoyer des réponses si par exemple le nœud récepteur ne peut pas distinguer la structure de paquet. Il peut être utilisé pour parcourir les réseaux étendus pour répondre aux nœuds avec leur capacité ou pour deux nœuds qui discutent la structure réelle du paquet parmi d'autres choses. Si CMD=1 ceci signifie que les données dans DB1 contiennent une commande(demande ou réponse). On peut avoir jusqu'à 256 commandes (les demandes de 1 à 127 et les réponses de 128 à 256).

- **EDM** (Error Detection Mode) définissent la méthode utilisée pour la détection d'erreur pour valider le paquet. Le nœud peut ne pas adapter une méthode de détection d'erreur alors EDM = 0

0	**0**	**0**	: Pas de détection d'erreur
0	**0**	**1**	: Retransmettre trois fois
0	**1**	**0**	: 8 bits checksum
0	**1**	**1**	: 8 bits CRC
1	**0**	**0**	: 16 bits CRC
1	**0**	**1**	: 32 bits CRC
1	**1**	**0**	: FEC
1	**1**	**1**	: usage spécifié

Tableau II-3 : Sélection des méthodes de détection d'erreurs

Le but d'utilisation de plusieurs méthodes de détection d'erreurs est d'avoir un protocole générique qui peut s'adapter aux contraintes de chaque ligne d'énergie.

La sélection de la méthode de détection d'erreur prend en considération les caractéristiques de la ligne, la taille de paquet de données et le type de la liaison. Parmi les méthodes de détection d'erreur on cite:

- No Error Detection : le paquet est envoyé sans aucune information de détection d'erreur.
- 3 time re-transmission : c'est une méthode facile pour la détection d'erreur. Le nœud envoie trois fois le même paquet. La transmission est jugée correcte si le nœud récepteur détecte le même paquet à chaque fois.
- 8 bits checksum : Elle consiste à ajouter un octet contenant un checksum à la fin du paquet. Le principe consiste à additionner tous les octets à l'exception de l'octet de synchronisation et le résultat représente le paquet checksum.
- 8 bits CRC : Le calcul du CRC checksum est plus sophistiqué que "8-bit checksum" et plus fiable.
- 16-bits CRC : Cette méthode consiste à ajouter 2 octets contenant un checksum à la fin du paquet. Le calcul de CRC checksum est similaire à "8-bit CRC" mais plus fiable à cause de la taille plus grande de checksum.
- 32-bit CRC : Cette méthode consiste à ajouter 4 octets contenant un checksum à la fin du paquet. Le calcul de CRC checksum est similaire aux deux autres techniques mais plus fiable.
- FEC (Forward Error Correction) : Cette méthode permet la détection d'erreur et la correction des données

III-2-2 Algorithme d'implantation

III-2-2-1 Formatage de la trame d'émission

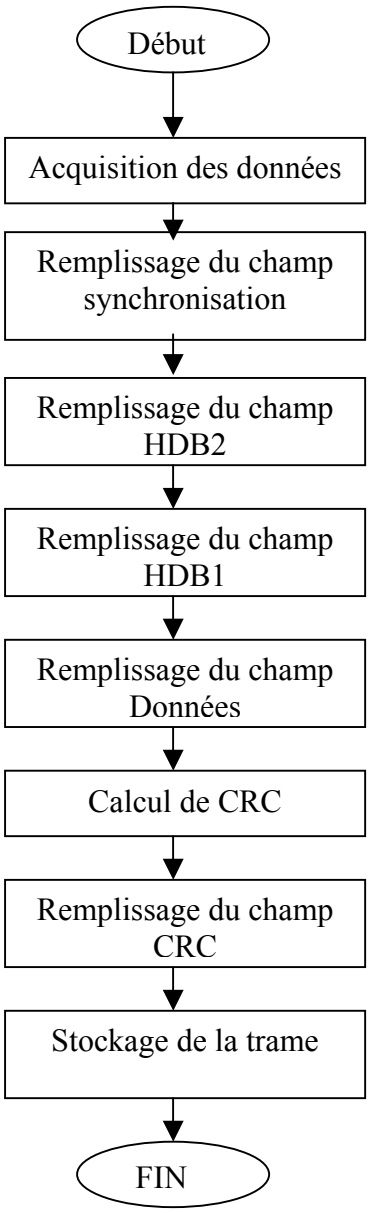


Figure III-4 : Organigramme de formatage de la trame d'émission

III-2-2-2 Algorithme d'analyse de la trame reçue et récupération des données

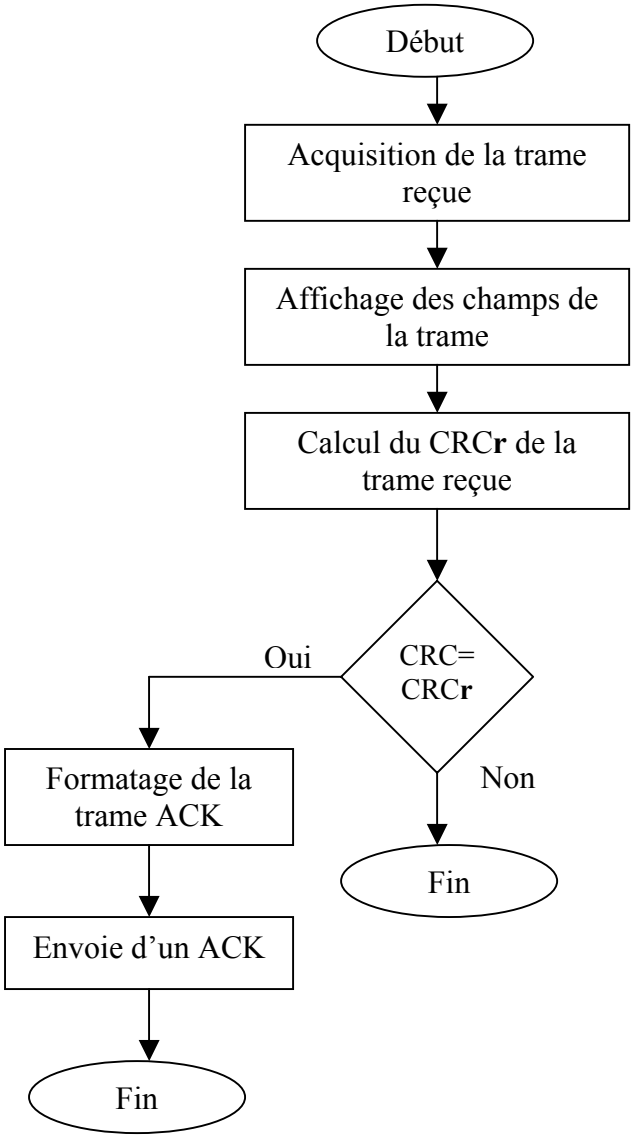


Figure III-5 : Organigramme d'analyse de la trame reçue et récupération des données

III-3 Techniques de validation des protocoles

III-3-1 Technique de description

Aujourd'hui pour spécifier les protocoles, plusieurs techniques sont utilisées. Le plus souvent, la spécification est faite à l'aide des langages naturels parfois accompagnés d'une spécification formelle utilisant une FDT (Formal Description Technique). Les FDT sont

basées sur des modèles abstraits tel que les systèmes de transitions, les algèbres de processus, les automates, les réseaux de Pétri.

Par exemple la description du comportement dynamique du protocole est généralement faite à l'aide des tables appelées les tables d'états. D'autres techniques possibles sont parfois utilisées comme par exemple les MSC (Message Sequence Charts) et les langages de description formelle normalisés tels que SDL, LOTOS,ou ESTELLE[13].

III-3-1-1 Description formelle

Dans cette technique de description, on peut distinguer trois composantes :

- Le langage de description.
- Un modèle mathématique (généralement de transition étiquetée).
- Une relation qui associe à chaque programme écrit dans le langage de description son expression dans le modèle mathématique.

On distingue deux types de techniques de description :

- Des techniques de type opérationnelles qui permettent de construire le système de transition étiqueté.
- Des techniques de type logique qui permettent d'énoncer des propriétés qui devront être satisfaite par le système de transition étiqueté.

III-3-1-2 Langage de description formelle

Ils sont accompagnés d'un environnement permettant d'assister l'utilisateur dans les tâches de spécification, de conception, de validation ou de simulation.

Il existe un certain nombre de langage qui sont normalisés par:

- ISO.
- recommandation du CCITT.

III-3-2 Techniques de simulation

La validation permet d'être exhaustif sur un modèle simplifié mais souvent incomplet tandis que la simulation est non exhaustif mais permet de travailler sur un modèle complexe. Le principal avantage de la simulation est qu'elle met en œuvre une spécification complète d'un protocole sur un modèle très proche de l'implantation

III-3-2-1 Les outils de validation des protocoles

Ils offrent tous ou une partie des fonctionnalités suivantes:

- Edition de la spécification (éditeur syntaxique, graphique).
- Validation de la description par génération exhaustive des graphes d'état ou par simulation aléatoire.
- Génération automatique d'un programme réalisant le protocole
- Génération de test.

III -3-3 Test de conformité

C'est une procédure technique visant à déterminer si un système ou un sous système possède les caractéristiques et répond aux besoins définis par une norme. Il est sanctionné par une opération administrative appelée certification à l'issu de laquelle un certificat de conformité est attribué au système.

III-3-3-1 Méthodologie de test et conformité de norme

Le test de conformité consiste à s'assurer qu'un système de données respecte un certain nombre de clauses imposées par les normes.

a) Exigences de conformité statique

Ils définissent les fonctions minimales requises pour autoriser l'interfonctionnement du système.

b) Exigences de conformité dynamique

Ils définissent un ensemble limité de comportements autorisés pour l'implantation d'un protocole.

Remarque

Plusieurs documents sont définis contenant toutes les informations nécessaires à la préparation et au déroulement de test de conformité d'un système (exemple système conformance statement, Protocol Implémentation Conformance Statement : PICS, Protocol Implémentation eXtre Information for Testing: PIXIT.).

c) Notion de système conforme

Un système est déclaré conforme lorsqu'il satisfait à la fois aux exigences de conformité statique et dynamique en accord avec les clauses spécifiées dans PICS et PIXIT pour chacun des protocoles qui le compose.

d) Classification des tests

- Test de base : Il a pour but de montrer que l'équipement ne présente pas de problèmes ou d'anomalies majeures de fonctionnement.
- Test d'aptitude : Il propose de contrôler l'équipement pour toutes les fonctions caractéristiques décrites dans le PICS.
- Test de comportement: Il vérifie le comportement de l'équipement sur l'occurrence d'évènement important, de message invalide. Il regroupe tous les tests de contrôle du système testé face aux divers évènements et situations possibles pouvant survenir lors du fonctionnement réel.
- Test de décision de conformité : Il vise la conformité des exigences particulières de conformité afin, après examen approfondi des résultats, de statuer ou non.

e) Méthodes de test

- Méthode de test local : Elle consiste à l'activation par le testeur supérieur et le testeur inférieur de l'implantation sous test grâce au moyen de primitives de service abstrait.
- Méthode de test distribué : Cette méthode présuppose qu'il est possible de contrôler l'interface haute de l'implantation sous test grâce à un testeur supérieur localisé dans l'équipement à tester.

- Méthode de test coordonné : L'application de cette méthode nécessite que le testeur supérieur implémente le protocole normalisé de gestion de test.
- Méthode de test à distance : Cette méthode se révèle utile lorsque l'implantation sous test n'offre aucune possibilité d'accéder aux primitives de service abstrait.

Remarque

A l'issu de chaque test élémentaire est attribué un Veldict pouvant être pass(succès), fall (échec) ou inconclusive (non concluent)

f) Outils de test

Un outil de test regroupe tous les moyens tant matériels que logiciels permettant le contrôle de la conformité d'une implantation à une norme en se basant sur plusieurs suites de test abstrait. Il permet de:

- Passer du test abstrait à un test exécutable sur un testeur.
- Isoler un sous ensemble de test à effectuer à partir des informations précisées dans le PICS et le PIXIT.
- Paramétrer la suite de test selon les valeurs consignes dans le PICS.
- Exécuter les tests sur le testeur en conservant la trace du dialogue entre le testeur et l'implantation sous test.

Chaque méthode de test abstrait peut être réalisée par différents testeurs et inversement, un même testeur peut supporter plusieurs méthodes de test abstrait.

Il existe deux types d'outil de test:

- Testeur inférieur : Il doit générer et contrôler les primitives de services abstraits PSA et les unités de données de protocole UDP ainsi qu'observer et stoker les échanges intervenant entre l'implantation sous test et son environnement.
- Testeur supérieur : la réalisation d'un testeur supérieur peut prendre différentes formes:

- Couches supérieures de l'implantation sous test (méthode de test à distance).
- Opérateur humain.
- Interpréteur de scénarios préenregistrés dans des fichiers.
- Implantation rebouclée retournant les données au testeur inférieur via un canal de transmission spécifique.

Remarque:

A l'outil de test est jointe une documentation permettant de mener le test en accord avec la suite de test abstrait et la norme de conformité.

g) Déroulement de test

- Préparation de test : La méthode de test appropriée ou le type de l'implantation est choisi à ce stade en vérifiant que l'implantation supporte cette méthode en terme de procédure de coordination de test et de point de contrôle. Lors de cette phase le client et le centre de test s'assurent que tout document est disponible.

- Opération de test : Cette opération débute par un revu de conformité statique consistant à un contrôle d'occurrence de PICS en lui même comme par rapport au clause de conformité de la norme. Il se poursuit par la sélection de la suite de test ensuite la paramétrisation de la suite de test.

- Compagne de test : La suite de test sélectionnée et paramétrée est exécutée. Une trace de l'exécution de test élémentaire est conservée en vue de l'analyse des Verdicts.

- Production du rapport de test : Il existe deux types de rapport afin d'établir les diagnostiques de conformité que le centre de test consigne.

h) Génération de test de conformité

La technique sur laquelle se basent les méthodes de génération est dérivée des tests matériels. On teste l'implémentation correcte des entrées et des sorties des transitions aussi bien que les états de départ et d'arrivée. La majorité des méthodes de génération sont fondées sur un nombre de séquences de base qui permettent de :

- Faire évoluer l'implémentation du protocole vers un état bien déterminé (séquence de synchronisation ou préambule).

- Faire évoluer l'implémentation du protocole d'un état donné vers un autre état (séquence de transfert).
- Tester l'entrée et la sortie d'une transition d'état.
- Vérifier l'état dans lequel l'implémentation du protocole réside(séquence d'entrée/sortie unique).

En combinant ces séquences suivant des méthodes différentes, on peut dériver des tests ayant des objectifs différents. En tous cas les tests examineront l'implémentation correcte du comportement dynamique du protocole.

III-4 Description du prototype de test

III-4-1 Environnement hardware

Notre application consiste à transmettre des données entre deux ordinateurs à travers une ligne d'énergie en utilisant un modem CPL piloté par un protocole SNAP. (voir figure III-6).

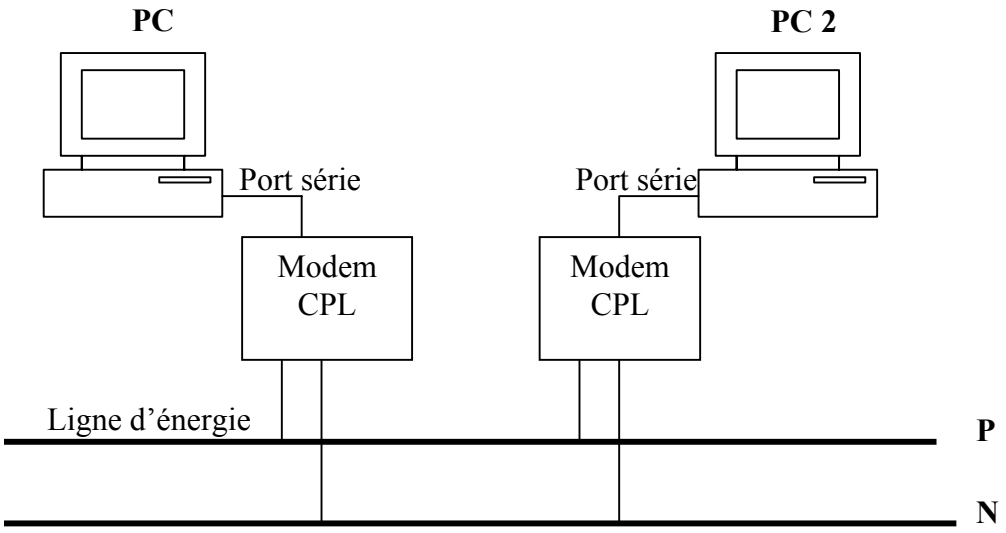


Figure III-6 : Environnement hardware de test de l'application

La plate-forme de test de cette application est composée du matériel suivant :

- Un ordinateur Pentium IV caractérisé par une fréquence de 1 GHz.
- Un modem CPL : c'est une carte DSP 2186 de fréquence d'horloge 15,36 MHZ. La carte contient de plus une interface EZICE qui permet de charger les programmes.
- Une interface série.

III-4-2 Environnement logiciel

Pour la réalisation de notre application nous avons tout d'abord choisi de programmer avec le langage Turbo C. Ce langage est caractérisé par une efficacité d'exécution des programmes, un compilateur simple et efficace et un accès à de nombreuses bibliothèques.

Néanmoins, on a eu des problèmes lors de la programmation des ports. Pour cela, nous avons eu recours à la programmation en Visual Basic qui comprend tous les outils de programmation nécessaires à la construction rapide et efficace des programmes puissants.

III-4-3 Structure du programme

Pour dialoguer avec l'utilisateur en langage compréhensible, nous avons développé le code source d'une interface graphique. Cette interface gère des fenêtres d'affichage pour l'acquisition et la visualisation des données. Elle contient par exemple des boutons, des zones de liste que nous avons personnalisés.

Côté émission, notre interface est composée d'un champ réservé à la saisie des données à transmettre, d'un autre réservé pour l'affichage de l'accusé de réception sous forme d'un message "OK". L'interface contient aussi un bouton de commande " Envoyer" permettant la commande du programme. Côté réception, on a conçu l'interface utilisateur qui permet l'affichage des données reçues.

Notre programme doit assurer la communication entre deux ordinateurs selon le protocole à implanter. Pour cela, au niveau de notre code, nous devons utiliser certaines fonctions afin d'assurer le formatage des données et leur transmission sur le port dont :

- **Asc** qui assure la conversion en ASCII

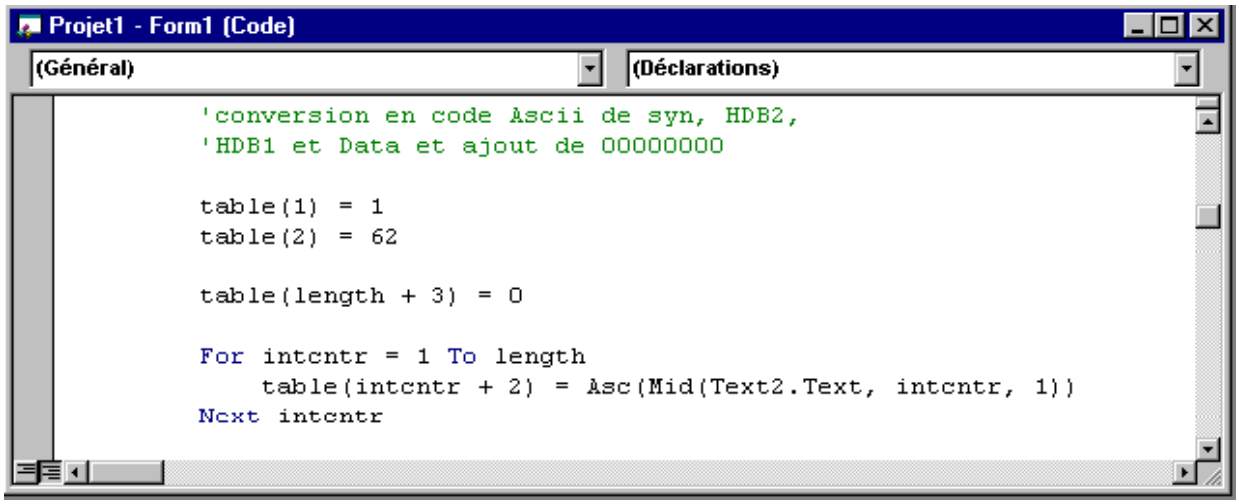


Figure III-7 : Fonction de la conversion en ASCII

- **Chr** qui permet la conversion de l'ASCII en caractère.

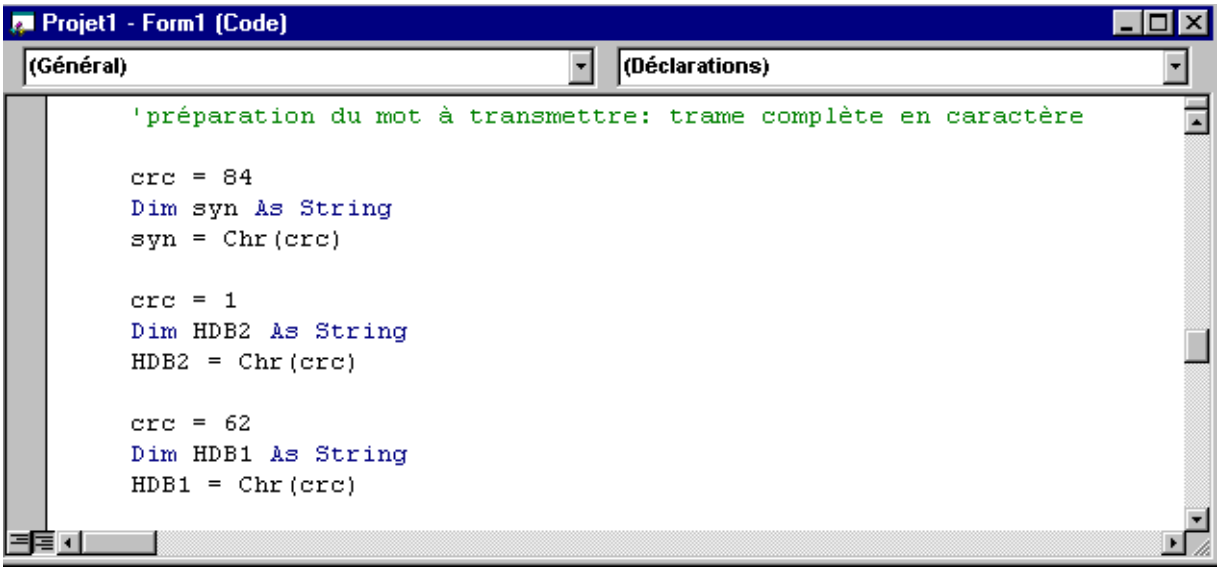


Figure III-8 : Fonction de la conversion en caractère

- **MSComm** offre à une application les fonctionnalités de communication série en autorisant la transmission et la réception des données par l'intermédiaire d'un port série.

- **PortOpen** définit et renvoie l'état d'un port de communication. Il permet également d'ouvrir et de fermer un port.

- **Input** renvoie des caractères du tampon de réception.
- **Output** écrit une chaîne de caractère dans le tampon de transmission.

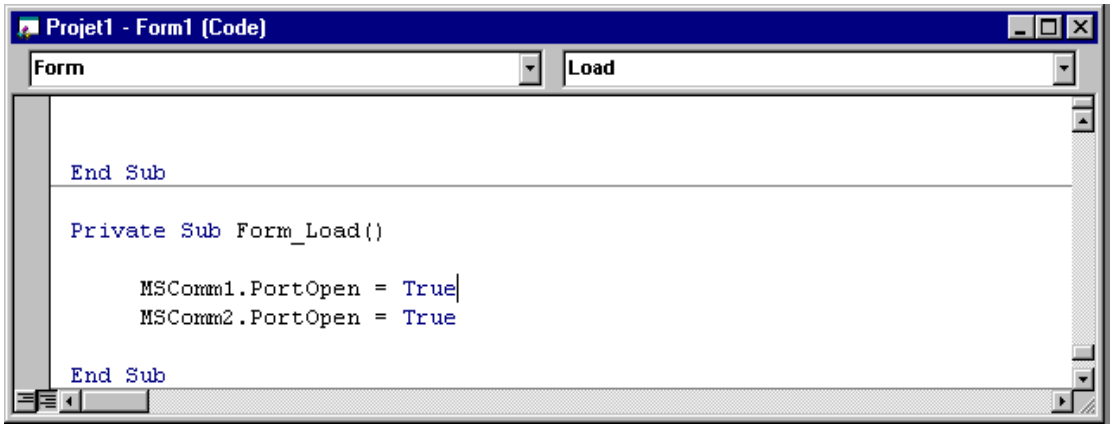


Figure III-9 : Programmation des ports

III-5 Résultats des tests expérimentaux

III-5-1 Interface graphique

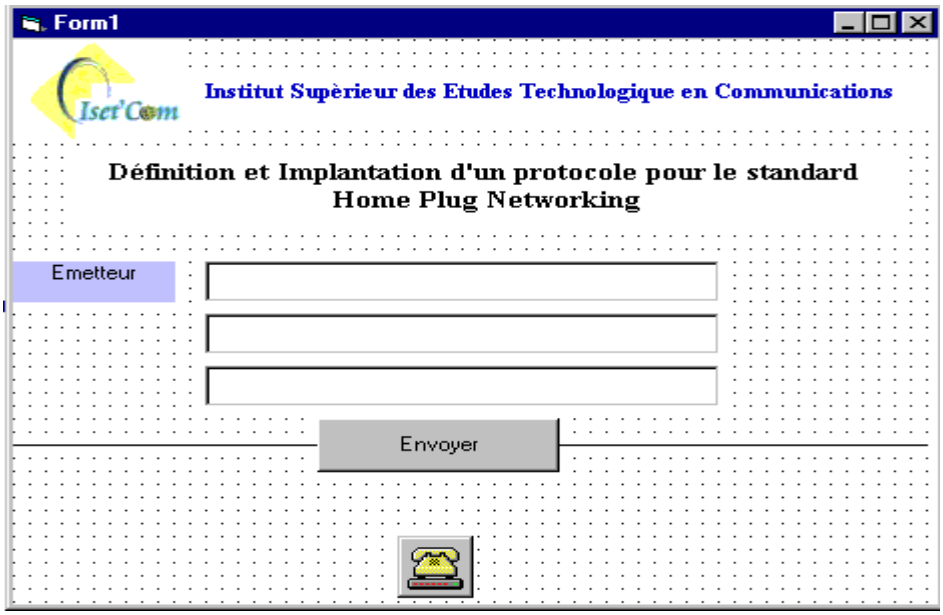


Figure III-7 : Interface utilisateur côté émission

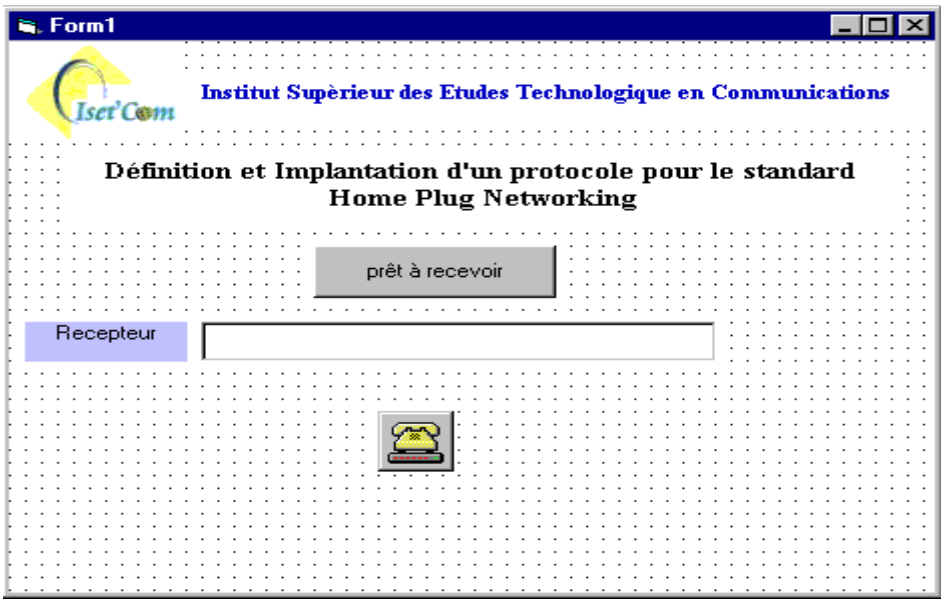


Figure III-8 : Interface utilisateur côté réception

III-5-2 Résultats de l'exécution

Lors de l'émission, le texte saisi par l'émetteur sera affiché chez le récepteur dans un champ réservé. Ce dernier envoie un accusé de réception à l'émetteur sous forme d'un message "OK".

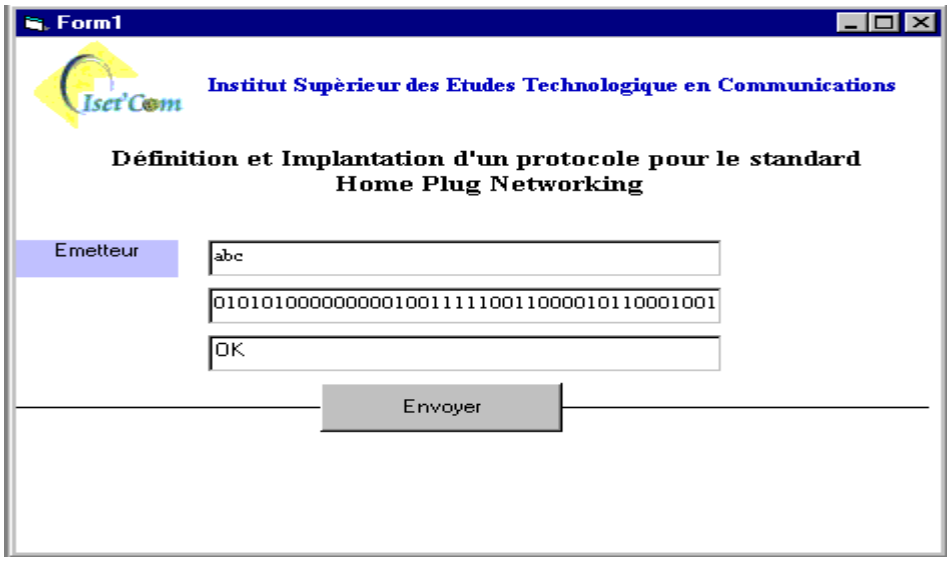


Figure III-9 : Résultat de l'émission

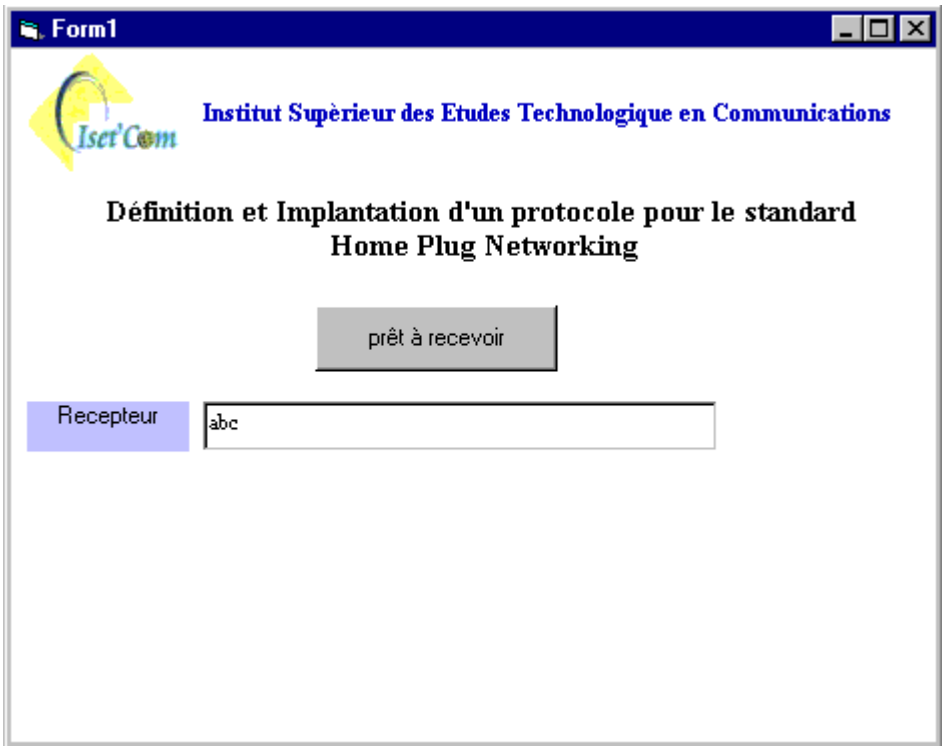


Figure III-10 : Résultat de la réception

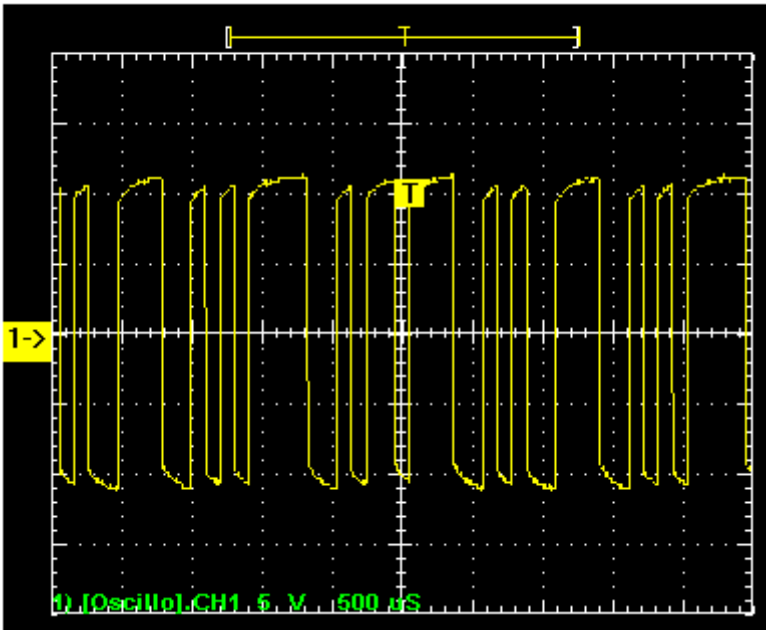


Figure III-11 : Visualisation des signaux à l'entrée de la carte DSP

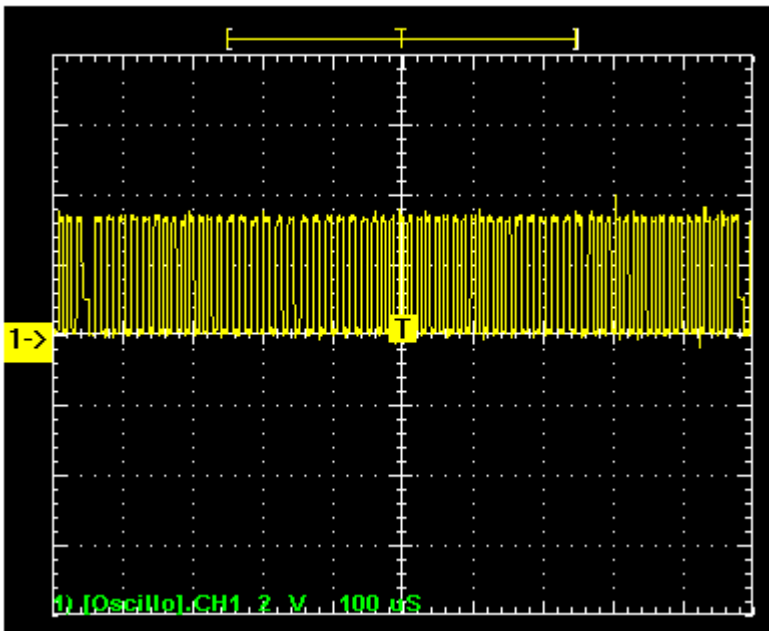


Figure III-12 : Visualisation des signaux à la sortie de la carte DSP

III-6 Conclusion

Dans ce chapitre nous avons présenté le protocole SNAP ainsi que ses caractéristiques dont nous devons tenir compte lors de formatage des données et l'implantation en visual basic. Les résultats expérimentaux présentés dans la dernière partie du chapitre ont montré l'efficacité de ce protocole puisqu'on a pu communiquer entre deux PC.

SOMMAIRE

TABLE DES FIGURES

LISTE DES TABLEAUX

CONCLUSION GENERALE

La technique des courants porteurs de lignes se présente comme une des techniques du futur. Pourtant, il existe des applications réelles et suffisamment fiables pour considérer sérieusement la question. En effet, depuis quelques années, les recherches portant sur ces techniques se sont multipliées. Cet intérêt s'est vu s'accroître avec la mise sur le marché de compteurs électroniques. Pourcela, il a fallu définir des normes pour l'utilisation efficace du canal CPLqui représente un environnement très sévère .D'où la norme Home Plug Networking.

Dans ce projet de fin d'étude, nous avons essayé d'implanter un protocole de communication sur les lignes d'énergie appelé Scaleable Node Address Protocol. Pour ce faire, nous avons tout d'abord accordé un intérêt à l'étude de la configuration du réseau courant porteur de ligne afin de mettre en évidence les différentes difficultés auxquelles nous devons faire face pour mettre à jour la communication via le réseau d'énergie et définir notre protocole.

Ensuite, nous avons étudié quelques modes d'accès au support de transmission qui s'avère insuffisants pour répondre aux exigences de canal CPL. Cette étude nous a amené à définir le protocole SNAP, l'implanter en Visual Basic et le tester.

Ce travail nous a permis d'acquérir et de consolider nos connaissances en des domaines tel que : la technique courant porteur de ligne, les modes d'accès, le langage de programmation en Visual Basic.

BIBLIOGRAPHIE

[1] http: // www. ibsuisse.ch/pages/archives/01.05/0105compowerline.html

[2] Hrasnica Halid ,Abdelfatteh Haidine , Ralf Lehnert "Reservation MAC Protocols for Powerline Communications". ISPLC 2001, Malmö-Suède, avril 2001.

[3] Adel GHAZEL, "technique CPL numérique" polycopie de cours DESS SUP'COM, Tunis, octobre 2001.

[4] Laurant Toutain, "Réseaux locaux et Internet" édition Hermes, Paris 1996.

[5] Steve Gardener, "The Home Plug Standard for Powerline Home Networking", ISPLC2001, Home Networking, Malmö-Suède, avril 2001.

[6] http: // www. Internaute .ch / se_connecter / powerline .asp

[7] Grira Sami, Ghorghar Soufien, "La transmission par CPL: Principe et Applications", projet de fin d'études de Technicien Supérieur en Télécommunication, ISET' COM, Tunis, février 2001.

[8] http: // www. perso.club-internet.fr/f bailly/satellite/services /htm

[9] Shinji Tsuzuki , Yoshio Yamada ,Utilisation and Delay Performance Analysis of Carrier Sense CDMA Protocol , ISPLC 2000, Irlande, mars 2000.

[10] http://www.guill.net/reseaux/80211.html

[11] DR. Mordechai Mushkin "A Novel Distributed Synchronized Media access Control Mechanism and its Applicability to In- House Power-line Networking" ISPLC2001, Malmö-Suède, avril 2001.

[12] http://www. hth .com

[13] Paul Angost, Benoit Gaillaut, Michel Delaure, Rémi Guestchel ,Bernard Jouga ,Dominique LeFoll, Jean–Jacque Maret, Pierre Rocher, Gilles Vaucher, Groupe Argoat, association Granit, "l'ingénierie des protocoles", édition interédition, Paris 1993.

ANNEXES

ANNEXE A :
LE PROTOCOLE ALOHA

A-1 Réservation par une file d'attente fictive

Cette méthode utilise des tranches de temps regroupées en trames de longueur supérieure au temps de propagation aller-retour. Chaque trame débute par une tranche elle-même décomposée en mini-tranches. Il y a autant de mini-tranches que de tranches restant disponibles dans la trame. Ces mini-tranches vont servir aux stations qui veulent émettre dans la trame suivante à réserver leur tranche de temps. L'accès aux mini-tranches se fait en mode aléatoire avec la méthode ALOHA, on obtient donc une file d'attente fictive qui va être vidée en servant les stations une par une (par ordre d'arrivée dans les mini-tranches) dans les tranches de temps. Cette méthode nécessite une gestion complexe des affectations des tranches aux stations, notamment la principale difficulté est de connaître à l'avance le nombre optimal de tranches et mini-tranches dans la trame[8].

A-2 Réservation ordonnée

La méthode de réservation ordonnée (per-burst reservation) utilise une trame avec autant de mini-tranches dans l'en-tête de réservation qu'il y a de tranches. Les minis tranches sont dédiées aux stations et leurs permettent de prévenir les autres stations de l'utilisation ou non de sa tranche de temps dans la prochaine trame. Dans le cas où une mini-tranche ne serait pas utilisée par la station correspondante, elle devient libre d'accès et les autres stations peuvent y accéder en mode aléatoire pour réserver une tranche de temps.

L'inconvénient de cette technique est la perte de la capacité du réseau, qui a du être utilisée par un autre utilisateur, lorsque la station a fini la transmission et la station de base n'a pas encore détecté la fin de la transmission.

Le "per-burst reservation" augmente la complexité du canal dans le cas du mécanisme de réallocation dues aux perturbations dans le réseau CPL. D'où, on propose la solution "per packet reservation".

Dans les techniques de réservation par paquet, on cherche une utilisation optimum du canal par les stations en accédant aux mini-tranches soit nominalement soit en mode aléatoire. Mais pour diminuer les problèmes de collision dus au nombre élevé de demande de transmission, on peut adapter la méthode de "piggy backing". Cette méthode utilise des segments qui contiennent les données de l'utilisateur et les demandes de transmission.

Par exemple, pour indiquer qu'il y a d'autres paquets à transmettre, la station peut transmettre une demande à la fin du segment de donnée, donc la signalisation n'est pas utilisé pour ce type de demande de transmission d'où la diminution de probabilité de collision [9].

Au niveau des performances des techniques d'accès, les temps de réponse les meilleurs sont obtenus par ALOHA pour de faibles débits puis par la méthode de réservation par paquet

ANNEXE B:

LE PROTOCOLE POLLING

B-1 Protocole d'accès hybride

On peut ajouter au protocole Polling un composant aléatoire qui le rend plus robuste contre les perturbations et diminue le temps d'accès. Dans le cas d'accès aléatoire au canal de transmission libre, la station envoie les segments de données sur le support et en même temps des demandes de transmission. S'il y a une collision alors la demande doit se faire dans un intervalle de temps dédié et la station doit attendre une permission de transmission.

Cette méthode est appliquée si on a des collisions qui se produisent rarement et si le canal est chargé. Autrement, on doit tenir compte des toutes les méthodes d'accès aléatoires dans le canal. L'accès aléatoire au canal de transmission libre n'est permis que pour les demandes de transmission. Donc les segments de données transmis n'entrent pas en collision et la station peut transmettre la demande sur un canal sans attendre les intervalles de temps dédiés dans le canal de signalisation. La signalisation du canal est divisée en deux parties qui sont aléatoire et dédié. Les stations essaient de faire des demandes dans la partie aléatoire de la signalisation et si on ne réussit pas on utilise les intervalles dédiés [9].

B-2 Protocole adaptatif

Les inconvénients des protocoles aléatoires, dédiés et combinés peuvent être améliorés en utilisant le Protocole adaptatif qui utilise des mécanismes d'accès variés selon la situation des réseaux.

Par suite, la station avec un débit élevé a une grande probabilité d'établir les demandes ce qui réduit le temps d'accès. Les stations sont divisées en deux groupes qui sont actif et inactif. La station active reçoit le droit de transmission d'après l'accès Polling dédié. Quand une station inactive devient active, elle utilise la partie aléatoire suivant le protocole ALOHA pour se déclarer comme une station active. Ensuite, la station reçoit un intervalle de temps dédié pour la transmission de sa demande.

Le protocole adaptatif peut faire varier ses paramètres selon la charge du trafic dans le réseau. Ce principe peut être appliqué dans le protocole hybride qui produit la demande avec les deux méthodes Aloha et Polling. Si le protocole hybride est inclut dans une méthode

d'accès adaptatif alors la relation entre le nombre des slots aléatoires et dédiés est calculée d'après la charge du réseau. La variation du nombre des intervalles aléatoires et dédiés peut améliorer les performances du protocol hybride [2].

ANNEXE C :

LE MODE D'ACCES CSMA/CD

Les trames émises par les différentes stations utilisent le même support physique: une station peut émettre à tout moment; l'occupation du câble doit se faire successivement dans le temps. Il faut définir une politique d'accès au support physique donc:

- Définir comment les utilisateurs accèdent au support
- Définir comment on règle les collisions

Ethernet utilise pour cela CSMA/CD pour accès multiple avec écoute de la porteuse et détection de la porteuse.

On définit la trame Ethernet comme suit:

Trame Ethernet originale:

7 octets	1 octet	6 octets	6 octets	2 octets	1-n octets	4 octets
préambule	**Délimiteur de début**	**Adresse source destination**	**Adresse destination source**	**protocole**	**information**	**FCS (frame) chek séquence**

Trame Ethernet

7 octets	1 octet	6 octets	6 octets	2 octets	3 octets	54-n octets	4 octets
préambule	**Délimiteur de début**	**Adresse destination**	**Adresse source**	**longueur**	**protocole**	**information**	**FCS**

Figure C-1 : Format de trame Ethernet

Préambule: 64 bits de synchronisation alternance de 0 et 1 et les deux derniers bits à1.

Adresse destination: **adresse de niveau MAC**

Adresse source: adresse de niveau MAC

FCS: contrôle de redondance cyclique portant sur tout ce qui précède sauf le préambule.

$G(x) = X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{2}+X+1$

Le temps d'espacement entre 2 trames est de $9.6 * 10^{-3}$ secondes.

C-1 Caractéristiques Fonctionnelles

La technique CSMA/CD est la base de protocole Ethernet donc elle obéit à ses critères dont :

- Topologie bus.
- Emission par trame = émission d'une suite de bit.
- Taille minimale = 64 octets.
- Taille maximale = 1518 octets.
- Transmission asynchrone de trames : on peut émettre une trame à tout moment (Si on en a le droit) pas de signal synchronisateur.
- Transmission série, tous les bits sont émis successivement sur le même support physique.
- Emission en diffusion: une trame émise par une station est reçue par toutes les stations.
- Propagation bidirectionnelle.
- Permet le multiplexage dans le temps.

C-2 Principe de fonctionnement

Tout appareil a le droit d'essayer d'accéder au support à tout moment (Accès Multiple). Avant d'émettre, l'appareil doit d'abord écouter pour voir s'il y a transmission en cours c'est à dire écouter la porteuse.

Si le support est libre, l'appareil peut envoyer une trame et continuer son écoute de la porteuse pour détecter d'éventuelles collisions (c'est un choc entre deux messages différents émis par deux machines en même temps et sur le même support).

Si le support est occupé, il n'émet pas et doit poursuivre son écoute et dès qu'il devient libre, il émet une trame.

Cette trame peut entrer en collision avec d'autre trame si deux ou plusieurs appareils commencent à émettre au même moment alors les deux stations détectent la collision. Dans ce cas, les deux hôtes arrêtent la transmission et tentent une nouvelle fois une retransmission après un délais de temps aléatoire (différent pour chaque station).[9]

Le processus Ethernet CSMA/CD

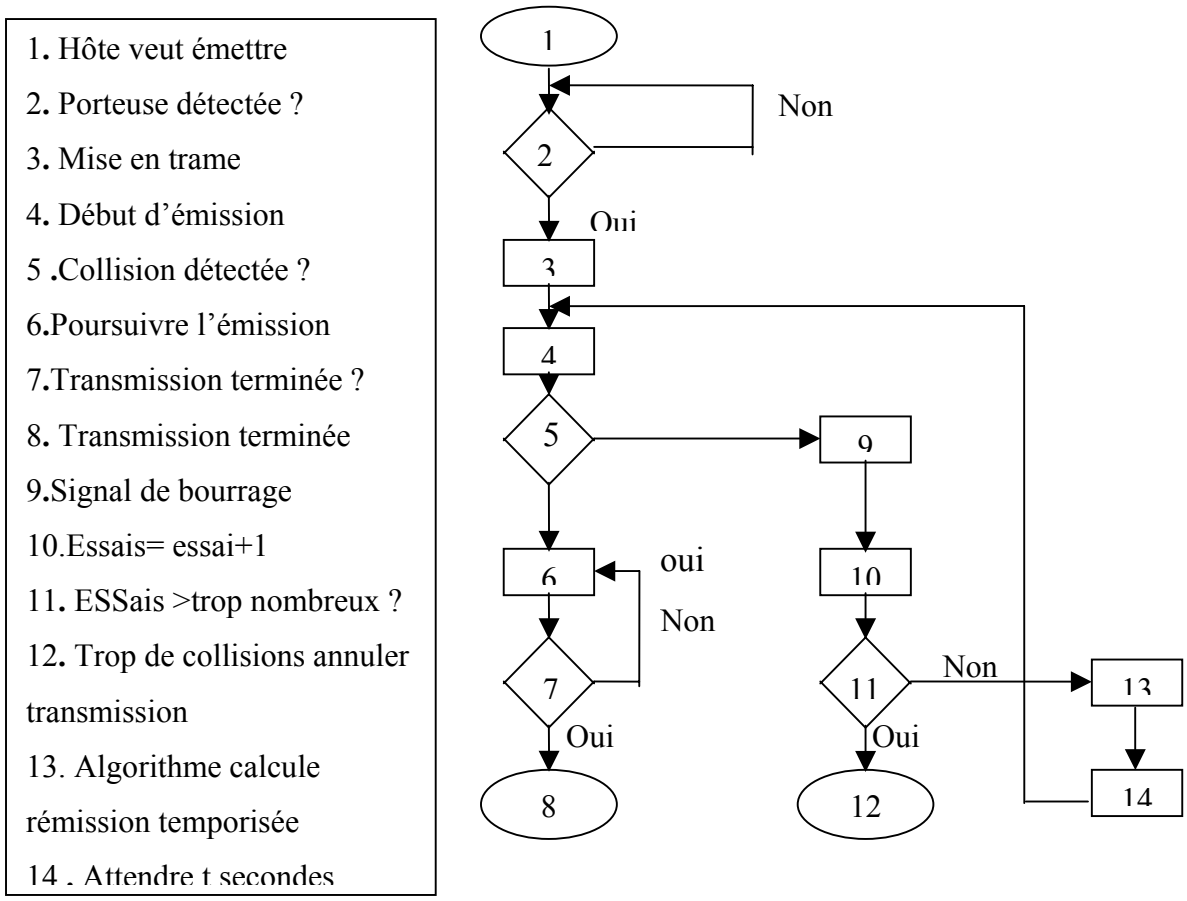


Figure C-2 : Processus Ethernet CSMA/CD

C-3 Physical Carrier Sense

Ce mécanisme permet de déterminer immédiatement et continuellement l'état du canal par une simple détection de porteuse (écoute de canal) ce qui favorise un mécanisme de contention simple et efficace.

Il est simple à implémenter, indépendant des couches physique et MAC qui sont déjà existantes, permet à tous les nœuds qui partagent le même média de s'entendre et assure une

grande fiabilité de détection. Cependant cette technique ne peut pas être appliquée pour in-house CPL car :

- La nature bruyante du support rend la détection non fiable.
- La variation de l'atténuation entre nœud provoque le problème de "hidden node".

ANNEXE D :

MECANISME DE CONTROLE D'ACCES DISTRIBUE

D-1 Principe de fonctionnement

Le mécanisme d'accès est défini et il doit être respecté par chaque nœud. La définition de ce mécanisme est obligatoire uniquement pour la coordination d'accès au support entre nœuds qui appartiennent à des réseaux différents. Tandis que la communication entre nœuds du même réseau reste non spécifiée. Aussi que l'efficacité et la robustesse du mécanisme proposé, il peut être utilisé pour le contrôle d'accès au média dans le même réseau. Cet accès qui se fait par le mécanisme CSMA pour lequel chaque nœud détecte l'état du canal et transmet lorsqu'il est libre.

L'identification de l'état du canal est assurée par la détection du signal d'occupation qui est transmis par les nœuds (la source et la destination) qui utilisent le canal afin de surmonter les problèmes de "hidden node".

Cette méthode permet la détection de l'état du canal et la diminution du bruit qui rend la détection non fiable, sur le réseau "in house CPL" [11].

Le signal d'occupation, comme les autres signaux utilisés pour l'accès au support, est basé sur le temps : à chaque signal est spécifié un intervalle de temps. Cette méthode est utilisée pour permettre une transmission et une réception simultanée, pour améliorer la diversité de fréquence et pour assurer une résistance aux collisions. L'utilisation et l'occupation du support sont exécutées en deux niveaux:

- Un niveau d'occupation périodique de trame basé sur une structure appelée "super frame structure" (16 ou 32 trames). Un groupe de nœud qui occupent une trame donnée dans le super trame en cours peut capturer la même trame dans le prochain super trame.
- Un niveau d'accès aléatoire. La capture et l'occupation dans le niveau d'accès aléatoire sont exécutées en plusieurs niveau de priorité. La transmission pour un "Lower Priority Level" est interrompue par le "Higher Priority Level".

L'efficacité d'accès au média est assurée par la résolution de collision et elle est déterminée non seulement par la source mais aussi par la destination. Ceci permet de diminuer

quelques aspect des problèmes de "hidden node". La résolution de collision par les sources qui est basé sur l'écho permet de résoudre les problèmes de "hidden node".

D-2 La structure de la trame

Chaque trame a une durée fixe de 1ms et est composée d'une entête "header" et d'un corps "body".

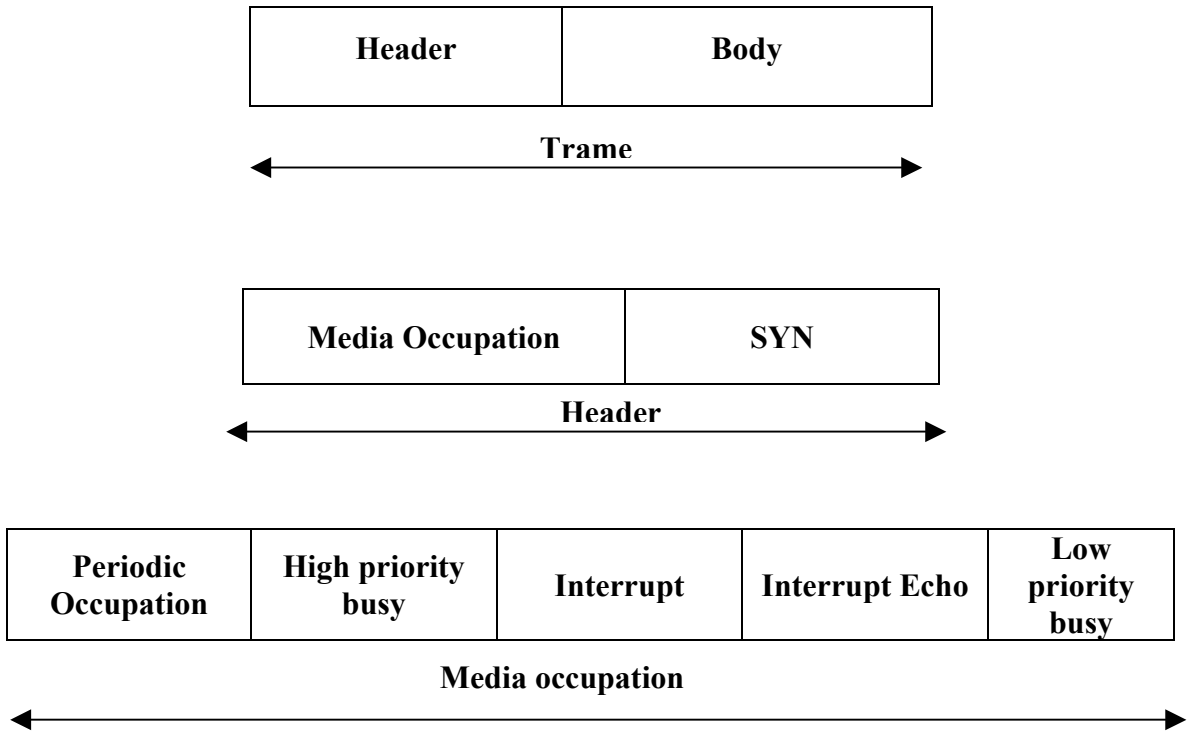
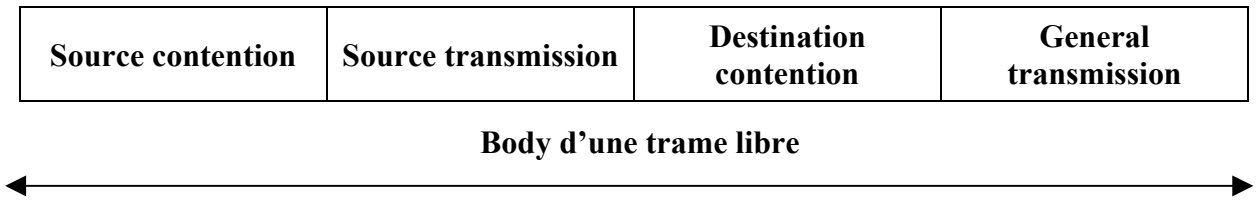


Figure D-1 : Structure de la trame

La structure d'une trame libre est comme suit :



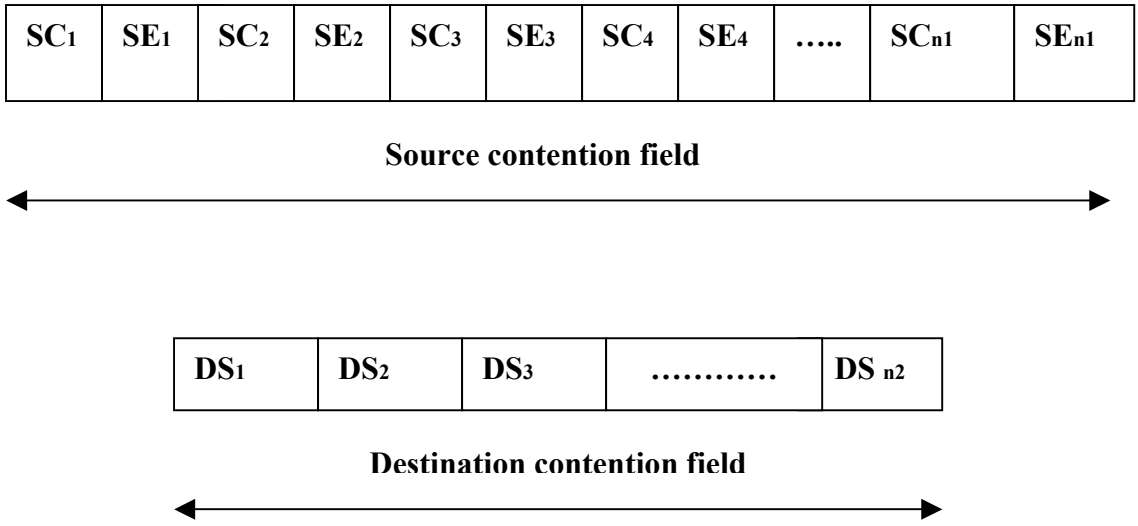


Figure D-2 : Structure d'une trame libre

- **SC :** Contention sequence.
- **SE :** Echo sequence.
- **DS :** Contention sequence.
- **Body :** La structure du corps de la trame dépend de son état (occupé ou libre). Une trame est considérée occupée lorsqu'elle contient un signal d'occupation sinon elle est libre. Le corps d'une trame occupée dépend de la technologie de transmission employée.
- **SC :** Contention séquence.
- **SE :** Echo sequence.
- **DS :** Contention séquence.
- **Général transmission :** Ce champ dépend de la technologie de transmission.
- **SYN :** Ce champ est utilisé pour compléter et maintenir la synchronisation entre les nœuds connectés sur le support. Chaque nœud a une horloge interne qui génère la période de la trame et transmet les impulsions de synchronisation au champ SYN dans un cycle ordonné "d" pour permettre la réception des

impulsions des autres nœuds. A chaque trame, le nœud décide aléatoirement en se basant sur la probabilité "d" s'il transmet les impulsions de synchronisation. Si un nœud ne transmet pas les impulsions de synchronisation pour la trame alors il contrôle le champ SYN et détecte un signal de combinaison des impulsions de synchronisation transmis par les autres nœuds. Le signal détecté est utilisé pour déduire le signal de référence de temps et règle son horloge interne avec cette référence. Pour se synchroniser avec le reste des nœuds, le nœud arrête la transmission du signal de synchronisation ou tout autre signal, Ce même principe est utilisé lorsque la synchronisation est perdue.

- **Periodic Occupation :** Ce champ est utilisé pour signaler l'occupation périodique du support. Si un groupe de nœud (source et destination) utilise le canal en occupant une trame dans une Super trame et ceci pour un ensemble de super trame successive alors il a tendance à occuper la même trame pour la Super trame en cours. L'occupation d'une trame est exécutée par la transmission d'un signal au champ "Periodic Occupation" de cette trame. Ce signal est transmis par la destination aussi. Chaque nœud qui n'a pas préoccupé le support contrôle la présence du signal de préoccupation. Si ce signal est détecté, la trame est considérée préoccupée et le nœud ne peut pas avoir accès au support ni de se concurrencer pendant la période de cette trame. Sinon, le nœud peut l'occuper.

- **High /Low Priority Busy :** Ces champs sont utilisés pour indiquer l'occupation du signal. Un groupe de nœud (source et destination) qui capture le canal selon une priorité dans les trames précédente peut continuer à l'occuper dans la trame en cours. L'occupation du support est réalisée par la transmission d'un signal d'occupation au champ "Priority Busy". Ce signal est aussi transmis par la destination. Chaque nœud qui n'occupe pas le support contrôle la présence des signaux d'occupation dans la trame. Si l'un d'eux est détecté alors la trame est considérée occupée et le nœud n'a pas le droit d'y accéder au support. Dans le cas contraire, cette dernière peut se concurrencer pour l'occuper.

- **Interrupt And Interrupt Echo :** Ces signaux sont utilisés dans le processus de capturation de canal dans le cas de la priorité élevée. Chaque nœud contrôle

le signal "High Priority Busy". Si ce signal n'est pas détecté, alors le nœud déduit que le support n'est pas occupé avec une priorité élevée et se considère comme prioritaire pour occuper cette trame. Lorsque le nœud détermine que la trame n'est pas occupée avec "High Priority", il commence à envoyer un signal d'interruption. Ce dernier et son écho empêchent l'occupation de la trame par un nœud de faible priorité. Chaque nœud qui a une priorité élevée et qui veut capturer le canal contrôle le champ "Interrupt". Si le signal est détecté, le nœud envoie un signal dans le champ "Interrupt Echo". Mais pour le nœud qui veut occuper la trame en cours avec "Low Priority", il contrôle les champ "Interrup" et "Interrupt echo". Si un signal est détecté dans l'un de ces champs, le nœud arrête l'occupation de trame en cours (il ne transmet pas le signal "Low Priority Busy"). Le nœud qui veut accéder au support avec une priorité élevée peut le faire pourvu que la trame n'est pas occupée (aucun signal d'occupation ou de priorité n'est détectée). Il peut aussi y accéder avec une priorité faible, mais on doit satisfaire la première condition et aussi il ne faut détecter aucun signal "Interrupt" ou "Interrupt Echo".

- **Source compétition :** ce champ est utilisé pour résoudre les compétitions entre les sources sur le support. Chaque nœud contrôle les deux champs d'occupation. Le nœud qui ne détecte aucun signal d'occupation sur ces champs, détermine la trame libre et se considère potentiel pour l'accès au support. La source doit se concurrencer à l'accès au canal suivant les règles de priorités et l'état du canal). La source concurrente choisit une "Contention Sequence" qui a une séquence binaire aléatoire de n_1 bits. Le nœud concurrent transmet le signal à chaque élément binaire qui correspond à "1" bit dans "contention Sequence". Le nœud qui se considère prioritaire pour la trame en cours, contrôle les éléments binaires dans SC de champ "Source Contention". A chaque fois que le signal est détecté dans la séquence binaire, le nœud transmet un signal à la séquence d'écho binaire. Ce nœud contrôle le support à chaque élément binaire qui correspond à "0" bit dans SC et SE. Si un signal est détecté dans les deux séquences alors le nœud détermine qu'il y a une concurrente pour la trame en cours qui a une "contention sequence" plus élevée alors le nœud cesse la transmission. La source qui a complété le SC sans détecter aucun un autre concurrent se considère comme une "surviving source"

qui peut transmettre n'importe quel message dans les champs "**Source transmission**" et "**General transmission**".

- **Destination competition :** Ce champ est utilisé pour résoudre les contestations entres les destinations sur le support. Tous les nœuds contrôlent les champs d'occupation. Le nœud qui ne détecte aucun signal d'occupation sur ces champs, détermine la trame libre et se considère potentiel pour l'accès au support. Le nœud qui reçoit un message de "surviving source" pendant la zone "Source transmission" peut se concurrencer pour l'accès au support. Cette destination choisit une "Contention Sequence" qui a une séquence binaire aléatoire de n_2 bits avec une valeur inférieure à n_1. Elle transmet le signal à chaque élément binaire égal à "1" et contrôle le support lorsqu'il est égal à "0". Si un signal est détecté alors le nœud détermine qu'il y a une concurrente pour la trame en cours qui a une DS plus élevée alors il cesse la transmission. La destination qui a complété le DS sans détecter aucune autre concurrente se considère comme une "surviving destination" qui peut transmettre n'importe quel message dans le champ "**General transmission**".

Dédicace

Je dédie ce travail

A ma très chère mère et à mon père pour leur affection et leur patience .

A mes sœurs Maha et Najoua et mon frère Slim en leur souhaitant le succès dans leur vie.

A tous mes amis .

RIM

Etude et Implantation d'un protocole pour le standard Home Plug Networking

Réalisé par

MANSOUR Hana & REZGUI Rim

Résumé

Ce travail concerne l'étude, la configuration et le test d'un protocole de communication sur les lignes d'énergie selon le standard Home Plug. Une première partie du travail a été consacrée à l'analyse de la technique CPL afin de dégager les particularités du canal de transmission qu'il faut en tenir compte dans la définition du protocole. En deuxième partie nous avons montré que les protocoles standards de transmission de données restent insuffisants pour compenser la sévérité du canal CPL. Ainsi un protocole amélioré a été configuré. Le travail est complété par une étude pratique de test de protocole.

Mots clés : technique CPL, protocole d'accès, couche MAC, CSMA.