



Ingénieurs 2000
*Nouvelles Technologies
des Réseaux*



CPL

Courants Porteurs en Ligne



Membres du groupe :

Yaël HACCOUN
Maxime BAUDET
Fabrice PODEVIN



Sommaire

I. Introduction.....	4
II. Historique.....	5
III. Principe de fonctionnement.....	6
IV. Le CPL Indoor.....	7
V. Le CPL Outdoor.....	9
VI. Canal de transmission.....	10
VII. Techniques de modulation de données.....	11
VII.1. OFDM : Orthogonal Frequency Division Multiplexing.....	11
VII.2. Spread Spectrum : Modulation à étalement de spectre.....	12
VIII. Liaison de données.....	13
VIII.1. CSMA/CD.....	13
1.1 Format des trames.....	15
IX. Normes et réglementations.....	18
IX.1. Un seul standard reconnu.....	18
IX.2. Cadre juridique.....	19
X. Sécurité.....	20
X.1. Rôle du compteur.....	20
X.2. Sécurité offerte par le standard HomePlug.....	20
X.3. Le cryptage D.E.S.....	21
XI. Les utilisations du CPL.....	23
XI.1. Accès Internet dans tout un bâtiment.....	23
XI.2. Etendre le réseau local.....	24
XI.3. Module CPL pour la télévision.....	24
XI.4. Multimédia.....	25



XII. Avantages et inconvénients de la technologie.....	26
XII.1. Avantages.....	26
XII.2. Inconvénients.....	26
XIII. Comparaison CPL – Wi-Fi.....	27
XIII.1. Rappels sur le Wi-Fi.....	27
XIII.2. Etude comparative.....	27
2.1 Les câbles.....	27
2.2 La sécurité.....	28
2.3 Les débits.....	28
2.4 La distance.....	28
2.5 Les normes.....	29
2.6 Le prix.....	29
XIII.3. Bilan de cette comparaison.....	29
XIV. Perspectives d'évolution.....	30
XIV.1. HomePlug AV.....	30
XIV.2. Domotique.....	30
XIV.3. Fracture numérique.....	30
XV. Conclusion.....	31
XVI. Sources.....	32



I. Introduction

Le CPL (Courants Porteurs en Ligne) est une technologie qui permet de transmettre des informations numériques sur le réseau électrique existant. Son utilisation pour le haut débit est très récente car elle date de la fin des années 90.

Après un petit historique, nous étudierons le fonctionnement du CPL ainsi que ses deux architectures possibles à savoir le CPL Indoor et le CPL Outdoor. Nous verrons ensuite le niveau de sécurité puis des utilisations possibles du CPL. Enfin, après un listage des avantages et inconvénients du CPL ainsi qu'une comparaison avec le Wi-Fi, nous verrons les différentes possibilités d'évolution du CPL.

II. Historique

L'utilisation du courant électrique pour commander du matériel remonte aux années **1950**. Il était, par exemple, utilisé sur une fréquence de 10Hz à une puissance de 10kW pour commander l'éclairage public.

Dans le **milieu des années 1980**, nous avons pu voir apparaître le début des recherches pour utiliser l'électricité comme support de données. A cette époque, la transmission était unidirectionnelle.

Il faut attendre la **fin des années 1990** pour voir le haut débit sur CPL se développer. En particulier en **1997** où les premiers tests de transmission de signaux de données sur un réseau électrique sont apparus. Ces transmissions étaient en bidirectionnelles.

Mais ce n'est qu'en **2000** que les premières expérimentations ont été effectuées en France. A cette même date, on peut noter la création de la HomePlug Powerline Alliance. Cette alliance est un regroupement de grandes sociétés qui souhaitent définir une norme pour le CPL.

En **2001**, la HomePlug Powerline Alliance sort le standard HomePlug 1.0 dans un premier temps, puis le standard HomePlug 1.0.1 quelques mois plus tard.

En janvier **2005**, les débits théoriques annoncés approchent des 200 Mbits/s sur une distance de 300 mètres.

III. Principe de fonctionnement

En effectuant la technologie CPL à haut débit, il est possible de faire passer des données informatiques sur le réseau électrique, et ainsi étendre un réseau local existant ou partager un accès Internet existant via les prises électriques grâce à la mise en place de boîtiers spécifiques.

Le principe des CPL consiste à superposer au signal électrique de 50 Hz un autre signal à plus haute fréquence (bande 1,6 à 30 MHz) et de faible énergie (2 Volts environ). Ce deuxième signal se propage sur l'installation électrique et peut être reçu et décodé à distance. Ainsi le signal CPL est reçu par tout récepteur CPL qui se trouve sur le même réseau électrique.

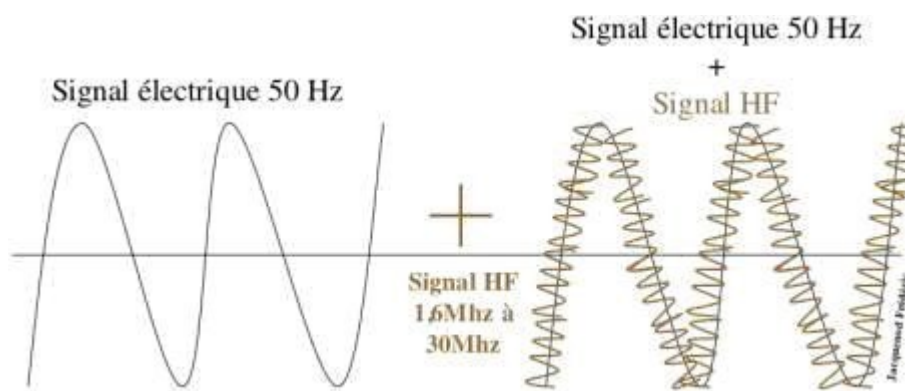


Illustration 1: Le signal électrique

Un coupleur intégré en entrée des récepteurs CPL élimine les composantes basse fréquence avant le traitement du signal.

Il existe deux architectures du réseaux CPL : l'indoor et l'outdoor. Nous allons détailler chacun de ces réseaux.

IV. Le CPL Indoor

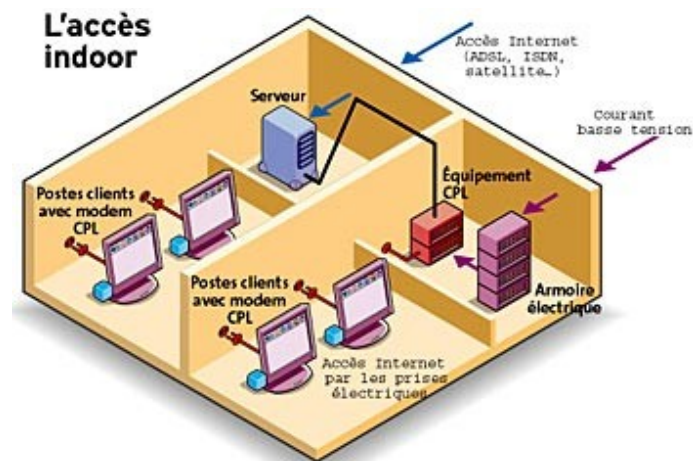


Illustration 2: Réseau Indoor

Les solutions CPL commercialisées à ce jour, de type *Homeplug* pour l'indoor, sont des solutions parfaites pour étendre le réseau local et partager l'accès Internet haut débit existant, notamment à la maison ou en petite entreprise, avec une mise en œuvre simple. Les boîtiers CPL se présentent en général avec un port Ethernet ou USB suivant le modèle choisi, et une connexion vers la prise électrique.

La mise en œuvre d'une solution CPL en intérieur demande au niveau informatique comme configuration minimum un PC avec carte Ethernet ou une prise USB selon le choix du boîtier. Attention tout de même à la disponibilité des drivers (pour les modèles en USB) selon le système d'exploitation.

- Pour la mise en place d'un boîtier Ethernet, l'installation est équivalente à celle d'un réseau local Ethernet filaire.
- Pour la mise en place d'un boîtier USB, la configuration se fait via le pilote fourni, une carte réseau virtuelle est alors à configurer comme la carte Ethernet en réseau local.

Au niveau électrique, l'installation ne pose aucun souci à l'intérieur d'un logement derrière un compteur monophasé dans la mesure où les adaptateurs se branchent directement sur les prises électriques. En revanche l'intégration est plus complexe dans les immeubles, que ce soit en



résidentiel avec une arrivée triphasée et différents compteurs, ou bien dans les bâtiments de grande taille, tels que des collèges, des hôpitaux ou immeubles administratifs. La mise en œuvre d'une solution CPL « étendue » nécessite alors une double compétence : expertise en réseau électrique et en réseau informatique, ainsi que l'utilisation de matériel différent des boîtiers Homeplug vendus pour l'indoor.

La solution grand public actuellement vendue, Homeplug, possède un débit théorique de 14 Mbps. D'autres solutions existent toutefois avec des débits allant de 2 Mbps à 45 Mbps. Une solution à 200 Mbps a été testée en laboratoire.

Les débits réels se voient amputés de la partie du trafic réservé à la gestion du système. Pour autant les débits obtenus restent suffisants pour la majorité des applications domestiques si on part des 14 Mbps de Homeplug par exemple.

V. Le CPL Outdoor

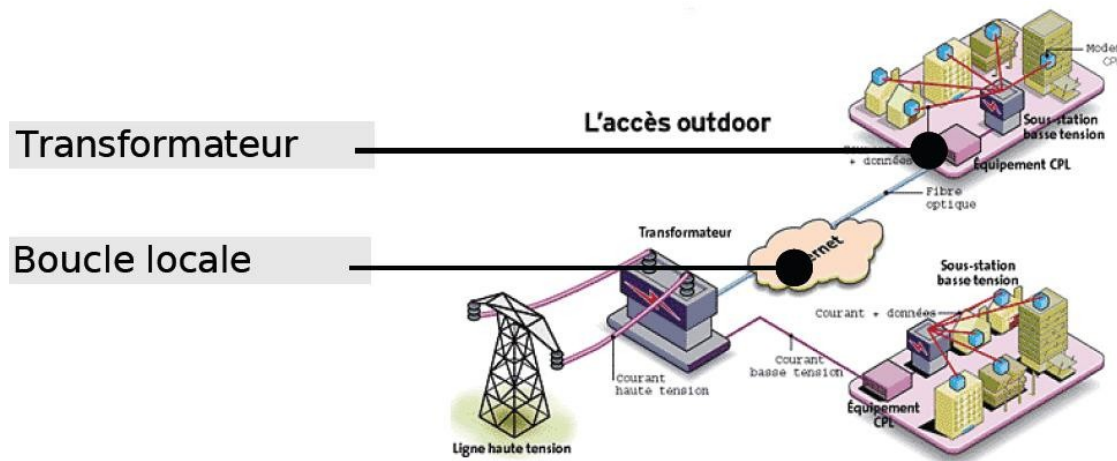


Illustration 3: Réseau Outdoor

Des expérimentations sont en cours pour des installations extérieures, avec un couplage entre l'arrivée Internet haut débit et le réseau électrique via un transformateur HTA/BT pour la création d'une boucle locale électrique.

En effet, pour des raisons juridiques, en France, le CPL outdoor est encore au stade de l'expérimentation. L'activité de transport de données relève des télécommunications et nécessite une licence d'opérateur de réseaux et télécoms ce qui n'est pas le cas d'EDF.

La France contrairement à l'Allemagne qui commercialise déjà des offres haut débit via CPL devra attendre la privatisation d'EDF.

L'accès Outdoor peut-il constituer une solution pour les collectivités locales ?

Dans de nombreuses parties du territoire, les opérateurs télécoms ont jugé non rentable l'ADSL et la mise en place de câblages classiques représente un investissement trop lourd. Le réseau haut débit semble réservé aux habitants de zones urbaines relativement densément peuplées, ainsi des zones d'activité économique importantes ne peuvent accéder à cette technologie pourtant essentielle à leur développement. Une possibilité pour les collectivités locales et les entreprises concernées est d'utiliser la technologie CPL afin d'acheminer un flux haut débit depuis un point d'accès préexistant. La capillarité extrêmement fine du réseau électrique permet en effet d'atteindre virtuellement l'ensemble du territoire, et en particulier les zones rurales qui semblaient jusqu'à présent exclues de la « révolution » haut débit.

Concrètement, les CPL sont complémentaires d'une technologie haut débit déjà installée et viennent remplacer la boucle locale qui n'a pas été mise en place pour cause de non rentabilité économique. Les CPL sont une plate-forme particulièrement flexible, qui peut se déployer suivant les cibles visées, par grappes au niveau d'un transformateur, et en complément avec d'autres infrastructures.

VI. Canal de transmission

Le support du réseau électrique n'a pas été étudié pour transporter des signaux haute fréquence (HF). Il faut donc prendre en compte les contraintes de ce support pour assurer une bonne transmission de ces signaux HF sans pour autant perturber les appareils environnants, ni les fréquences de la bande 1-30 MHz par rayonnement, certaines fréquences de cette bande étant réservées à l'armée ou bien aux radioamateurs.

Tout ceci doit enfin être étudié pour donner un débit suffisant à l'utilisateur en bout de ligne. Tout le problème consiste ainsi à limiter la puissance de fonctionnement des courants porteurs tout en assurant un débit suffisant, et limiter les effets du bruit et de la distorsion sur la ligne. La solution : allier un traitement du signal le plus performant possible et effectuer un couplage optimal du réseau CPL au réseau électrique.

Il existe deux méthodes de couplage : couplage capacitif en parallèle sur le réseau électrique ou couplage inductif via un tore de ferrite. En ce qui concerne les installations en intérieur (indoor), le couplage capacitif est fait par défaut lorsqu'on branche l'équipement CPL sur la prise électrique, le problème ne se pose donc que pour les installations en extérieur (outdoor), beaucoup plus complexes à réaliser.

VII. Techniques de modulation de données

Tout l'enjeu des CPL est de « tenir » un débit avec un niveau d'émission faible, d'où une limitation de la puissance de fonctionnement des courants porteurs, ou bien un traitement du signal le plus performant possible pour contourner cette contrainte de niveau d'émission. Sur les solutions actuelles, deux types de modulation ressortent particulièrement : **OFDM** (*Orthogonal Frequency Division Multiplexing*) et **Spread Spectrum** (ou *modulation à étalement de spectre*).

VII.1. OFDM : Orthogonal Frequency Division Multiplexing

La technique de transmission OFDM est basée sur l'émission simultanée sur n bandes de fréquence (situées entre 2 et 30 MHz) de N porteuses sur chaque bande. Le signal est réparti sur les porteuses. Les fréquences de travail sont choisies en fonction des réglementations, les autres sont « éteintes » de manière logicielle. Le signal est émis à un niveau assez élevé pour pouvoir monter en débit, et injecté sur plusieurs fréquences à la fois. Si l'une d'elles est atténuée le signal passera quand même grâce à l'émission simultanée. Le spectre du signal OFDM présente une occupation optimale de la bande allouée grâce à l'orthogonalité des sous-porteuses.

N.B. : Cette modulation a été choisie par le comité HomePlug, donc tous les équipements qui respectent la norme HomePlug sont en modulation OFDM. C'est notamment cette modulation qui est utilisée pour les transmissions sans fil Wi-Fi (802.11a).

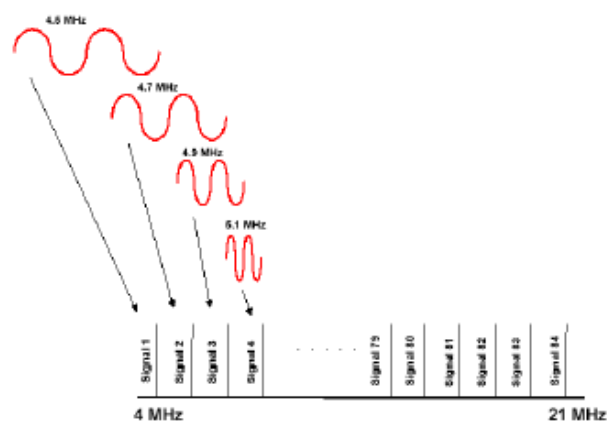


Illustration 4: Principe de l'OFDM

VII.2. Spread Spectrum : Modulation à étalement de spectre

Le principe de la modulation à étalement de spectre (*Spread Spectrum*) consiste à « étaler » l'information sur une bande de fréquences beaucoup plus large que la bande nécessaire, dans le but de combattre les signaux interférents et les distorsions liées à la propagation : le signal se confond avec le bruit. Le signal est codé au départ, un code est assigné à chacun des usagers afin de permettre le décodage à l'arrivée. L'étalement est assuré par un signal pseudo aléatoire appelé code d'étalement. A la réception le signal est perçu comme du bruit si le récepteur n'a pas le code. Le signal étant émis à un niveau plus faible que celui du bruit, le débit reste faible. La modulation avec étalement de spectre est ainsi optimisée pour lutter contre le bruit, dont elle limite mieux les effets.

La modulation CDMA (*Code Division Multiple Access*) est une modulation à étalement de spectre utilisée pour certaines solutions CPL. Lorsqu'on fait le point des différentes solutions existantes à ce jour on note que les solutions qui utilisent l'étalement de spectre restent à bas débit, seules les solutions qui utilisent OFDM peuvent monter en débit à ce jour.

VIII. Liaison de données

Toute solution CPL doit inclure une couche physique robuste mais également un protocole d'accès à la couche réseau efficace. Ce protocole contrôle le partage du média de transmission entre de nombreux clients, pendant que la couche physique spécifie la modulation, le codage et le format des paquets.

La méthode d'accès utilisée par les machines utilisant les courants porteurs en ligne est le CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), c'est-à-dire la même méthode utilisée pour les réseaux sans fils Wi-Fi.

VIII.1. CSMA/CD

Dans un réseau local Ethernet classique, la méthode d'accès utilisée par les machines est le CSMA/CD (*Carrier Sense Multiple Access with Collision Detect*), pour lequel chaque machine est libre de communiquer à n'importe quel moment. Chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine. Si c'est le cas, les deux machines patientent pendant un temps aléatoire avant de recommencer à émettre.

Dans un environnement sans fil ce procédé n'est pas possible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée. Ainsi la norme 802.11 propose un protocole similaire appelé CSMA/CA. Le protocole CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réceptions réciproques entre l'émetteur et le récepteur,

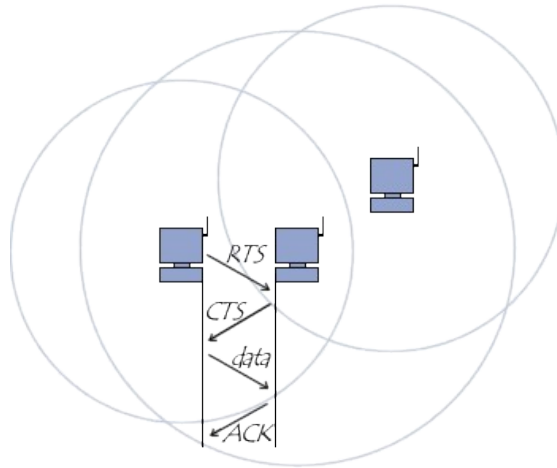


Illustration 5: mécanisme du CSMA/CA

La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé *DIFS* pour *Distributed Inter Frame Space*), alors la station peut émettre. La station transmet un message appelé *Ready To Send* (noté *RTS* signifiant *prêt à émettre*) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un *Clear To Send* (*CTS*, signifiant *Le champ est libre pour émettre*), puis la station commence l'émission des données.

A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (*ACK*). Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

1.1 Format des trames

Le standard 802.11 définit le format des trames échangées. Chaque trame est constituée d'un en-tête (appelé *MAC header*, d'une longueur de 30 octets), d'un corps et d'un *FCS* (*Frame Sequence Check*) permettant la correction d'erreur.

FC (2)	D/ID (2)	Adresse 1 (4 octets)	Adresse 2 (4 octets)	Adresse 3 (4 octets)	SC (2)	Adresse 4 (4 octets)
Corps de la trame (0 à 2313 octets)						
						FCS (2)

Voici la description de ces champs :

- **FC** (*Frame Control*, en français *contrôle de trame*) : ce champ de deux octets est constitué des informations suivantes :

Version de protocole (2 bits)		Type (2 bits)		Sous-Type (4 bits)			
To DS (1 bit)	From DS (1 bit)	More Frag (1 bit)	Retry (1 bit)	Power Mgt (1 bit)	More Data (1 bit)	WEP (1 bit)	Order (1 bit)

- **Version de protocole** : ce champs de 2 bits permettra de prendre en compte les évolutions de version du standard 802.11. La valeur est égale à zéro pour la première version
- **Type** et **Sous-type** : ces champs, respectivement de 2 et 4 bits, définissent le type et le sous-type des trames explicités dans le tableau ci-dessous. Le type *gestion* correspond aux demandes d'association ainsi qu'aux messages d'annonce du point d'accès. Le type *contrôle* est utilisé pour l'accès au média afin de demander des autorisations pour émettre. Enfin le type *données* concerne les envois de données (la plus grande partie du trafic).

- **To DS** : ce bit vaut 1 lorsque la trame est destinée au système de distribution (DS), il vaut zéro dans les autres cas. Toute trame envoyée par une station à destination d'un point d'accès possède ainsi un champ *To DS* positionné à 1.
 - **From DS** : ce bit vaut 1 lorsque la trame provient du système de distribution (DS), il vaut zéro dans les autres cas. Ainsi, lorsque les deux champs *To* et *From* sont positionnés à zéro il s'agit d'une communication directe entre deux stations (mode *ad hoc*).
 - **More Fragments** (*fragments supplémentaires*) : permet d'indiquer (lorsqu'il vaut 1) qu'il reste des fragments à transmettre
 - **Retry** : ce bit spécifie que le fragment en cours est une retransmission d'un fragment précédemment envoyé (et sûrement perdu)
 - **Power Management** (*gestion d'énergie*) : indique, lorsqu'il est à 1, que la station ayant envoyé ce fragment entre en mode de gestion d'énergie
 - **More Data** (*gestion d'énergie*) : ce bit, utilisé pour le mode de gestion d'énergie, est utilisé par le point d'accès pour spécifier à une station que des trames supplémentaires sont stockées en attente.
 - **WEP** : ce bit indique que l'algorithme de chiffrement WEP a été utilisé pour chiffrer le corps de la trame.
 - **Order** (*ordre*) : indique que la trame a été envoyée en utilisant la classe de service strictement ordonnée (*Strictly-Ordered service class*)
-
- **Durée / ID** : Ce champ indique la durée d'utilisation du canal de transmission.
 - **Champs adresses** : une trame peut contenir jusqu'à 3 adresses en plus de l'adresse de 48 bits
 - **Contrôle de séquence** : ce champ permet de distinguer les divers fragments d'une même trame. Il est composé de deux sous-champs permettant de réordonner les fragments :
 - Le *numéro de fragment*
 - Le *numéro de séquence*
 - **CRC** : une somme de contrôle servant à vérifier l'intégrité de la trame.

Le tableau ci-dessous récapitule les types et sous-type de trame encapsulés dans le champ de contrôle de trame de l'en-tête MAC :

Type	Description du type	Sous-type	Description du sous-type
00	Management (gestion)	0000	Association request (requête d'association)
00	Management (gestion)	0001	Association response (réponse d'association)
00	Management (gestion)	0010	Reassociation request (requête ré-association)
00	Management (gestion)	0011	Reassociation response (réponse de ré-association)
00	Management (gestion)	0100	Probe request (requête d'enquête)
00	Management (gestion)	0101	Probe response (réponse d'enquête)
00	Management (gestion)	0110-0111	Reserved (réservé)
00	Management (gestion)	1000	Beacon (balise)
00	Management (gestion)	1001	Annoucement traffic indication message (ATIM)
00	Management (gestion)	1010	Disassociation (désassociation)
00	Management (gestion)	1011	Authentication (authentification)
00	Management (gestion)	1100	Deauthentication (désauthentification)
00	Management (gestion)	1101-1111	Reserved (réservé)
01	Control (contrôle)	0000-1001	Reserved (réservé)
01	Control (contrôle)	1010	Power Save (PS)-Poll (économie d'énergie)
01	Control (contrôle)	1011	Request To Send (RTS)
01	Control (contrôle)	1100	Clear To Send (CTS)
01	Control (contrôle)	1101	ACK
01	Control (contrôle)	1110	Contention Free (CF)-end
01	Control (contrôle)	1111	CF-end + CF-ACK
10	Data (données)	0000	Data (données)
10	Data (données)	0001	Data (données) + CF-Ack
10	Data (données)	0010	Data (données) + CF-Poll
10	Data (données)	0011	Data (données) + CF-Ack+CF-Poll
10	Data (données)	0100	Null function (no Data (données))
10	Data (données)	0101	CF-Ack
10	Data (données)	0110	CF-Poll
10	Data (données)	0111	CF-Ack + CF-Poll
10	Data (données)	1000-1111	Reserved (réservé)
11	Data (données)	0000-1111	Reserved (réservé)

IX. Normes et réglementations

IX.1. Un seul standard reconnu

Pendant de nombreuses années, les industriels n'ont pas beaucoup investi en faveur du CPL étant donné qu'aucun réel standard n'existait. Certains ont alors essayé d'imposer leurs produits mais sans réel succès auprès du grand public. En effet, les différents produits commercialisés ne pouvaient communiquer entre eux d'un constructeur à un autre.

Partant de ce constat, plusieurs entreprises du monde des télécommunications et de l'informatique ont décidé de s'unir pour développer ensemble un standard pour le CPL. La *HomePlug Powerline Alliance* a donc été créée en Mars 2000 afin de normaliser l'essentiel de cette technologie. L'organisation compte aujourd'hui de très grands noms comme 3Com, AMD, Cisco, Intel, Intellon, Panasonic ou encore Texas Instrument.

Ils ont mis au point un standard en Juin 2001 appelé HomePlug 1.0, mais celui-ci a rapidement évolué pour passer en Novembre 2001 à **HomePlug 1.0.1**. Ce standard permet à des périphériques de communiquer entre eux via le réseau électrique. Les produits certifiés HomePlug connectent des ordinateurs et autres matériels qui utilisent une connexion Ethernet, USB ou Wi-Fi au réseau électrique en passant par des ponts ou adaptateurs HomePlug.



Niveau débit, HomePlug 1.0.1 annonce 14 Mbps sur une portée de 300 mètres. Réellement, le débit varie entre 2 et 10 Mbps selon l'installation électrique et la distance séparant les équipements. Le débit commence à réellement s'affaiblir au-delà des 200 mètres. De plus, un maximum de 16 adaptateurs CPL par installation électrique est préconisé par la HomePlug Powerline Alliance.

Cette spécification, qui est donc américaine, ne concerne cependant que les installations « indoor » et n'est pas interopérable avec les solutions « outdoor » existantes à ce jour. L'Europe travaille quant à elle avec le PLC Forum sur un standard généralisé qui permettrait la coexistence des solutions « indoor » et « outdoor » dans la bande de fréquence allouée.

Le PLC Forum est une autre organisation qui regroupe des entreprises telles que Ascom, EDF, DS2, LEA... Elle travaille en étroite collaboration avec le Cenelec et l'ETSI. Dans l'attente de cette standardisation européenne, les industriels qui ont leurs propres solutions ne développent pas encore leurs produits en masse.

N.B. : tous les équipements commercialisés à ce jour pour le grand public sont des produits *HomePlug*.

IX.2. Cadre juridique

La mise en place de réseaux CPL personnels est libre tant que les installations se situent derrière un compteur privé, sous réserve de ne pas créer de nuisances. Pour ce qui est des installations extérieures, l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes -anciennement Autorité de Régulation des Télécommunications-) a levé le 20 avril 2005 le caractère expérimental qui encadrait le déploiement du CPL.

En effet, L'ARCEP considère que les contraintes qui avaient justifié le statut expérimental de la mise en place de réseau CPL n'étaient plus pertinentes. Il est désormais possible aux personnes souhaitant déployer un réseau filaire CPL de s'inscrire dans le cadre réglementaire et de se déclarer comme opérateur conformément à l'article L.33-1 du Code des Postes et des Communications Electroniques.

X. Sécurité

La technologie CPL utilise donc le réseau électrique afin de faire circuler des informations. Les données sont envoyées sur tout le réseau électrique du lieu et l'on peut se demander si le compteur électrique constitue une sécurité ou non.

X.1. Rôle du compteur

Formellement, le compteur représente la frontière entre le réseau « indoor » et le réseau « outdoor ». Mais il ne faut pas compter sur le compteur comme sécurisation du réseau CPL car cette frontière est franchie par le signal CPL sans problème, avec tout au plus une dégradation, plus ou moins importante, du signal. Il est donc tout à fait possible qu'un voisin de palier se connecte sur votre réseau tout en restant chez lui. Cependant, il est possible de connecter un filtre au niveau du compteur afin d'affaiblir sensiblement le signal du CPL.

X.2. Sécurité offerte par le standard HomePlug

La spécification HomePlug 1.0.1 inclut une solution de cryptage D.E.S. (chiffrement à clé secrète) par clé de 56 ou 128 bits. Celle-ci permet donc de crypter les données transitant sur le réseau, et il faut configurer cette clé sur chaque poste afin qu'il puisse envoyer et recevoir les données sur le réseau. Il est conseillé de mettre en place cette sécurité avec une clé de 128 bits afin de réduire très considérablement les risques d'intrusion.

Le fait de crypter les données d'un réseau va également permettre au CPL d'offrir deux réseaux différents sur une même installation. En effet, il suffit de modifier la clé de cryptage, une différente par réseau. La configuration de la clé dans un adaptateur CPL permettra au périphérique relié d'être connecté sur l'un ou l'autre des réseaux.

X.3. Le cryptage D.E.S.

Le D.E.S. (Data Encryption Standard, c'est-à-dire Standard de Chiffrement de Données) est un standard mondial depuis plus de 15 ans. Bien qu'il soit un peu vieillissant, il résiste toujours très bien à la cryptanalyse et reste un algorithme sûr.

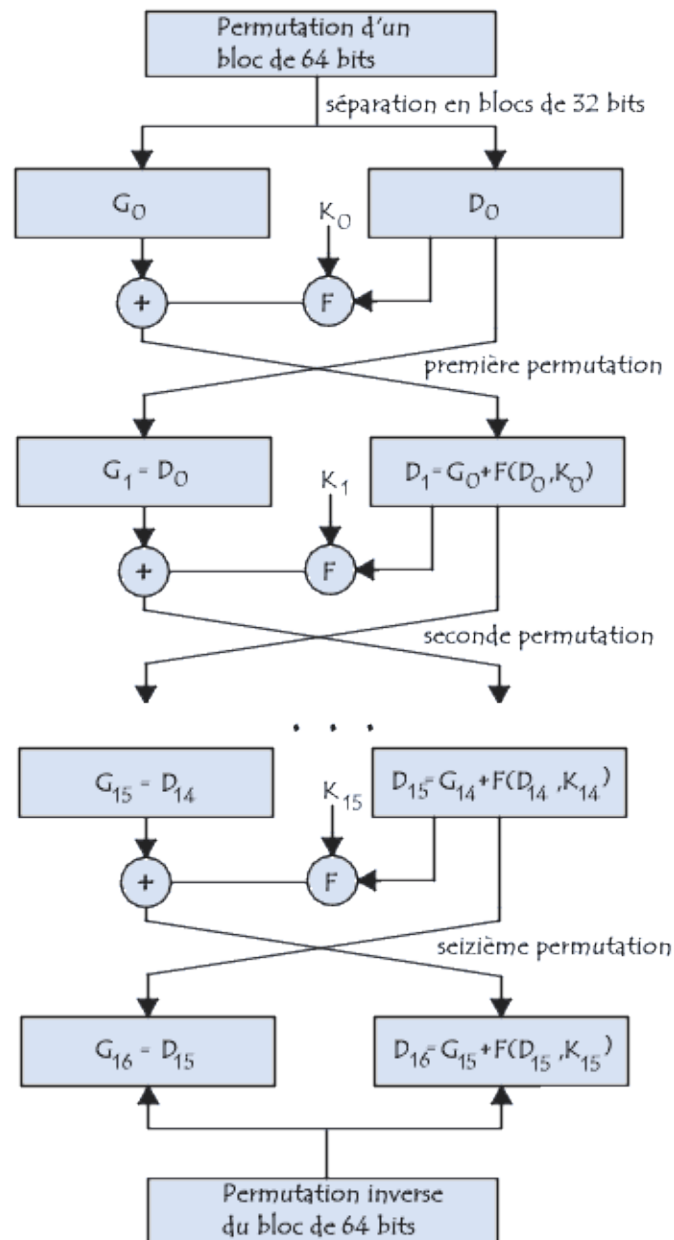
Le D.E.S. est un système de chiffrement par blocs. Cela signifie que D.E.S. ne chiffre pas les données à la volée quand les caractères arrivent, mais il découpe virtuellement le texte clair en blocs de 64 bits qu'il code séparément, puis qu'il concatène. Un bloc de 64 bits du texte clair entre par un côté de l'algorithme et un bloc de 64 bits de texte chiffré sort de l'autre côté. L'algorithme est assez simple puisqu'il ne combine en fait que des permutations et des substitutions en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). On parle en cryptologie de techniques de confusion et de diffusion. La combinaison entre substitutions et permutations est appelée « code produit ».

Le chiffrement est symétrique, par blocs de 64 bits donc, dont 8 bits (un octet) servent de test de parité pour vérifier l'intégrité de la clé. Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient.

La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k_1 à k_{16} . Cependant, la clé possède une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme. Il peut donc exister 2^{56} (soit plus de $7.2 \cdot 10^{16}$) clés différentes.

Les grandes lignes de l'algorithme sont :

- Fractionnement du texte en blocs de 64 bits (8 octets)
- Permutation initiale des blocs
- Découpage des blocs en deux parties : gauche et droite, nommées G et D
- Etapes de permutation et de substitution répétées 16 fois (appelées « rondes »)
- Recollement des parties gauche et droite puis permutation initiale inverse



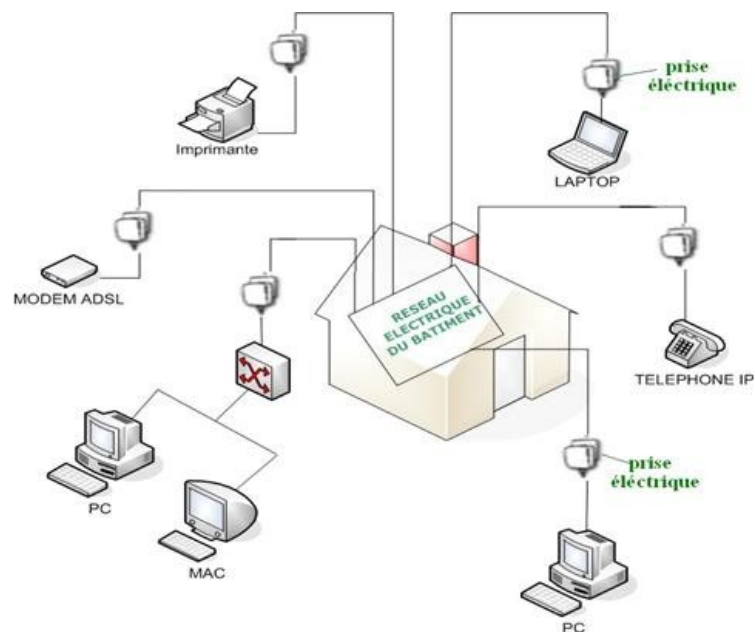
source : <http://www.commentcamarche.net>

Le chiffrement D.E.S. permet donc de sécuriser un réseau CPL mais le code peut vite être « casser » avec les machines actuelles qui sont beaucoup plus puissantes qu'aux origines du D.E.S. C'est pourquoi cette technique de chiffrement laisse dorénavant sa place à une autre solution, beaucoup plus sûre, nommée A.E.S. (Advanced Encryption Standard).

XI. Les utilisations du CPL

XI.1. Accès Internet dans tout un bâtiment

Le courant porteur est très avantageux dans les bâtiments parce que l'infrastructure permet d'obtenir une grande mobilité au niveau de la connexion Internet. En effet, il suffit de se brancher sur de simples prises électriques.



Un exemple concret de ce type d'installation et d'utilisation de la technologie est celui de l'institut Gustave Roussy (94). Un réseau haut débit par CPL y a été installé dans l'espace Vie dédié aux enfants et adolescents. Il permet aux enfants hospitalisés d'avoir un accès Internet à haut débit sur n'importe quelle prise électrique de l'unité, y compris dans les chambres stériles. Plusieurs tests ont été réalisés près de matériels hospitaliers et ont démontré que ces matériels n'ont pas été perturbés par la présence du réseau CPL.

XI.2. Etendre le réseau local

Un autre cas a été relevé dans un collège de Saint-Lô (50) où des chariots mobiles comprenant PC, imprimantes, vidéo-projecteurs et adaptateurs CPL permettent à chaque classe d'être tout à tour reliée au réseau local (et à Internet via un accès haut débit) en connectant le boîtier CPL sur une prise électrique de la classe.

L'intérêt de cette installation est surtout dans son coût : 3 à 5 moins cher que pour câbler tout le collège étant donné que le réseau électrique, déjà existant, est utilisé.

XI.3. Module CPL pour la télévision

Depuis le mois de Décembre 2006 des F.A.I. (Fournisseurs d'Accès à Internet) français ont proposé à leurs clients des modules CPL pour relier leur modem au décodeur placé à côté de la télévision pour recevoir la télévision par ADSL.

Neuf Cegetel a lancé le pack CPL Netplug Turbo 85 Mbps du nom des adaptateurs CPL du fabricant français LEA. Ce pack comprend deux adaptateurs qui se branchent directement sur des prises électriques : le premier est connecté au modem Neuf Box (par un câble Ethernet fourni), tandis que le second, branché aussi sur le courant, est connecté au décodeur TV près du poste de télévision.

L'intérêt ? Supprimer le câble nécessaire jusqu'ici pour relier le modem au décodeur, une vraie contrainte pour ceux dont l'ordinateur et le téléviseur ne sont pas à proximité. Même le Wi-Fi ne leur était d'aucune aide, les flux vidéo numériques étant très sensibles aux contraintes des transmissions sans-fil et à certains murs.

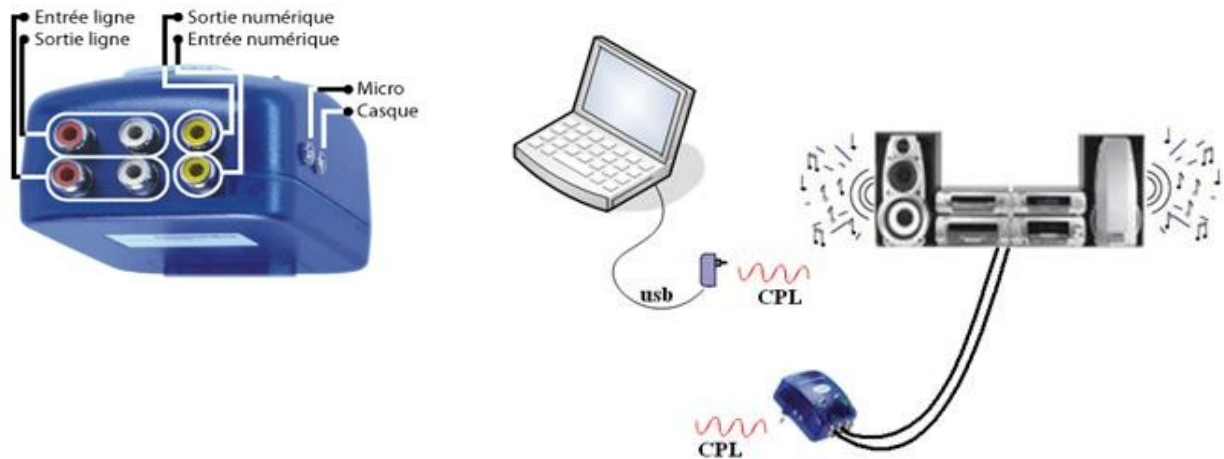
Wanadoo a été le premier sur cette utilisation, avec des adaptateurs fabriqués par Denovo, le grand concurrent germanique de LEA. Les deux F.A.I. proposent cette technologie pour moins de 100 euros, et la concurrence va les suivre dans les mois à venir.

XI.4. Multimédia

La technologie CPL permet de bénéficier de toutes les nouvelles applications multimédia. En effet, la « maison du futur » est réalisable : contrôler, surveiller mais aussi améliorer son cadre de vie c'est possible !

Sur le même principe que le module CPL pour la télévision, on peut relier son téléviseur directement à son ordinateur (situé dans une autre pièce) pour y visionner aisément un film, des photos...

Devolo (entreprise allemande) propose de son côté un émetteur / récepteur offrant la possibilité d'écouter de la musique où que l'on soit à l'intérieur d'un bâtiment. Il offre une connectique complète permettant d'élaborer plusieurs configurations audio :



Ici, l'ordinateur envoie la musique sur le réseau électrique via l'adaptateur CPL. Cette musique, qui a été convertie en signaux numériques, est réceptionnée par l'adaptateur relié à la chaîne Hi-Fi qui restitue les signaux numériques en musique.

XII. Avantages et inconvénients de la technologie

XII.1. Avantages

Le CPL présente de nombreux avantages qui peuvent pousser les particuliers comme les entreprises à se connecter via cette technologie. En effet, il n'est pas nécessaire de réaliser une opération de câblage souvent coûteuse : le CPL utilise le réseau électrique existant. L'installation est assez aisée puisqu'elle se résume en « indoor » à brancher un adaptateur sur le périphérique que l'on souhaite connecter, et d'appliquer la clé de chiffrement utilisée.

Le gros atout réside dans le fait que le courant porteur permet une mobilité importante. Il suffit simplement d'une prise électrique (souvent une ou plusieurs dans chaque pièce d'un bâtiment) pour être connecté au réseau. C'est une solution qui est complémentaire aux autres, on peut donc faire coexister un réseau CPL avec du Wi-Fi et du câblage Ethernet.

Enfin, le CPL a de grandes chances s'imposer et de perdurer pour connecter de nombreux équipements électriques comme un réfrigérateur, un four, ou encore un portail électrique.

XII.2. Inconvénients

La technologie a cependant quelques points faibles comme le manque de standardisation et de normes (un seul standard reconnu actuellement). Cela mène donc à un problème d'interopérabilité, que ce soit entre un réseau « indoor » et un réseau « outdoor », mais aussi entre différents équipements. Les débits ne sont plus suffisants pour répondre à la forte utilisation de bande passante que requièrent les nombreux services qui se lancent, comme notamment la vidéo à la demande.

De plus, le débit « indoor » est partagé, c'est-à-dire que si cinq utilisateurs sont connectés, le débit est divisé par cinq pour chacun des utilisateurs. La sécurité n'est pas non plus le point fort du CPL car le cryptage D.E.S. est dépassé. Il faut donc encore attendre pour bénéficier d'un cryptage plus avancé.

XIII. Comparaison CPL – Wi-Fi

XIII.1. Rappels sur le Wi-Fi

Le Wi-Fi est une technologie de réseau sans fil. C'est aussi le nom commercial pour la norme Ethernet sans fil IEEE 802.11. Le Wi-Fi utilise la fréquence radio entre deux matériels pour échanger les données.

A partir d'un accès Wi-Fi (modem, routeur, etc...) un utilisateur ayant un ordinateur possédant une carte Wi-Fi peut se connecter au réseau en étant situé dans un certain périmètre. Ce périmètre peut varier selon les perturbations et obstacles (murs par exemple).

XIII.2. Etude comparative

Nous allons voir dans cette partie les différents points entre le Wi-Fi et le CPL. En effet, ces deux technologies ont pour but de permettre la création d'un réseau local. Il est donc assez logique de les comparer. Nous verrons leurs différences point par point.

2.1 Les câbles

En ce qui concerne le Wi-Fi, celui-ci fonctionne sans fil c'est-à-dire que de n'importe quel endroit d'une pièce il est possible d'accéder au réseau. Il est aussi possible d'y accéder depuis n'importe quelle pièce de la maison (sous réserve d'être à une distance suffisante pour capter le signal).

Le CPL, quant à lui, utilise les câbles électriques. Il est donc nécessaire de se trouver à proximité d'une prise de courant pour pouvoir utiliser le réseau. Là aussi, il est nécessaire d'être à une certaine distance pour pouvoir y accéder. Nous verrons les distances par la suite.

2.2 La sécurité

Le CPL possède, comme quasiment toutes les technologies liées au réseau, un système de cryptage des données. Il a aussi l'avantage de devoir se brancher sur une prise électrique. Bien que le compteur électrique ne bloque pas obligatoirement les informations émises, il est possible de mettre un filtre pour empêcher les données de sortir du réseau électrique de la maison. Il sera donc nécessaire à un pirate de se brancher à l'intérieur du réseau électrique, autrement dit, il devra être dans l'habitation.

Tandis que pour le Wi-Fi, bien que celui-ci utilise aussi un système de cryptage des données, il est tout à fait possible d'accéder au réseau sans être dans la maison. En effet, les ondes radios utilisées par le Wi-Fi ne s'arrêtent pas aux murs de l'habitation. Un pirate pourra donc, en étant à l'extérieur des locaux, utiliser le réseau en piratant le système de sécurité du réseau Wi-Fi.

2.3 Les débits

Les débits théoriques du CPL sont de 14 Mbps bien qu'un débit de 200 Mbps est annoncé pour l'avenir. En pratique, les débits approchent plus de 10 Mbps. Il est à noter que le CPL partage la bande passante entre les différents matériels connectés au réseau.

Le Wifi, selon les normes 802.11a et 802.11g, peut atteindre un débit de 54 Mbps. Là encore, le débit peut rapidement diminuer selon l'environnement d'utilisation du réseau.

2.4 La distance

Les distances d'utilisation du Wi-Fi sont très variées car elles dépendent de l'environnement. En effet, les ondes radios sont atténuées par les murs. D'après les normes il serait possible d'avoir une distance théorique d'environ 100 mètres (norme 802.11b).

Quant au CPL, il est théoriquement possible d'atteindre des distances de 200 voire 300 mètres. Bien sûr, cette distance peut être diminuée par la qualité du réseau électrique.

2.5 Les normes

Les normes assurent un fonctionnement identique pour tous les produits fabriqués selon elles. Ce qui permet d'avoir une compatibilité entre les différents matériels.

Le CPL ne possède pas de norme a proprement parlé. Bien qu'il existe la spécification HomePlug, celle-ci n'est pas une norme.

Contrairement au Wi-Fi qui possède quelques normes comme la IEEE 802.11a ou encore la IEEE 802.11b et IEEE 802.11g qui sont les plus utilisées à l'heure actuelle.

2.6 Le prix

Le prix du CPL reste encore assez élevé puisqu'il faut compter entre 50 et 100€ pour un adaptateur. Alors qu'une carte Wi-Fi ne coûte qu'environ 40€.

XIII.3. Bilan de cette comparaison

Le CPL et le Wi-Fi ont chacun leurs avantages et inconvénients mais ces technologies sont complémentaires. En effet, les points faibles d'un sont les points forts de l'autre. Il est donc imaginable, à l'avenir, d'avoir un réseau possédant un mixte de ces deux technologies.

XIV. Perspectives d'évolution

XIV.1. HomePlug AV

La principale évolution concerne la nouvelle norme HomePlug AV qui devrait voir le jour courant 2006. Compatible avec la spécification HomePlug 1.0.1, elle aura pour principale innovation une meilleure sécurité (cryptage AES au lieu de DES) ainsi que la possibilité de streaming audio et vidéo dont la HDTV (Télévision Haute Définition).

XIV.2. Domotique

Le CPL est aussi très présent dans la Domotique (ensemble des techniques et technologies permettant de gérer les différents matériels d'une habitation). On peut, par exemple, l'utiliser pour gérer à distance les caméras de surveillance d'une maison. Mais il est tout à fait envisageable de voir le CPL se développer pour gérer à distance le chauffage d'une maison ou bien encore le réfrigérateur. Celui-ci pourrait par exemple transmettre directement par mail les courses à faire à son propriétaire.

XIV.3. Fracture numérique

Enfin, le CPL pourrait permettre aux collectivités rurales d'apporter le haut débit à leurs habitants à moindre frais. En effet, si amener l'ADSL peut coûter assez cher, utiliser le CPL est avantageux. Utilisant les câbles électriques (déjà existants) il sera alors possible à n'importe quelle personne possédant l'électricité d'avoir le haut débit. Le gouvernement s'étant engagé à réduire la « fracture numérique », le CPL pourrait bien arriver en force dans les campagnes durant les prochaines années.

XV. Conclusion

Le Courant Porteur en Ligne est une technologie assez simple basée sur le transport de données en utilisant les câbles électriques. La mise en place d'un réseau est facile et rapide et permet d'obtenir un accès à Internet (dans le cas où le réseau est connecté à Internet) depuis n'importe quelle pièce de la maison grâce à des distances pouvant aller jusqu'à 200 mètres.

Le débit reste encore peu élevé (14 Mbps) et surtout la bande passante est partagée par tous les matériels connectés. Mais en complément d'un réseau Wi-Fi, le CPL peut être très intéressant. Grâce à la nouvelle spécification HomePlug AV qui devrait arriver très prochainement, le CPL risque de prendre une plus grande envergure dans les moyens de télécommunications en particulier dans la domotique ainsi que la réduction de la « fracture numérique ».

Le CPL est pour le moment une technologie « branchée » mais pourrait donc devenir très prisée par la suite...

XVI. Sources

Voici les différentes sources que nous avons utilisées pour réaliser ce dossier :

- <http://www.zdnet.fr>
- <http://www.01net.com>
- <http://www.alterlane.fr>
- <http://www.cpl-france.org>
- <http://www.supinfo-projects.com>
- <http://www.commentcamarche.net>
- http://fr.wikipedia.org/wiki/Courants_porteurs_en_ligne

