

ALLAYS Séverin
MAIRE Jean-Benoît

le 20/05/2009

MIF30 : Projet de Crypto

Sujet tiré d'un article de la revue MISC N°37 Mai/Juin 2008

Table des matières

1.	Présentation	3
2.	Historique	3
3.	Principe de fonctionnement	3
4.	Normes.....	5
5.	Sécurité	6
6.	Utilisations du CPL	6
7.	Avantages et Inconvénients	7
8.	Conclusion	8
9.	Bibliographie	9

1. Présentation

Notre projet porte sur la technologie CPL et détail le principe et la sécurité de cette technologie qui existe depuis 1980 et qui devient de plus en plus présente. Nous vous proposons donc d'en savoir un peu plus.

On utilise de plus en plus le CPL, plus stable que le Wifi et dont la portée n'est pas limitée par les murs.

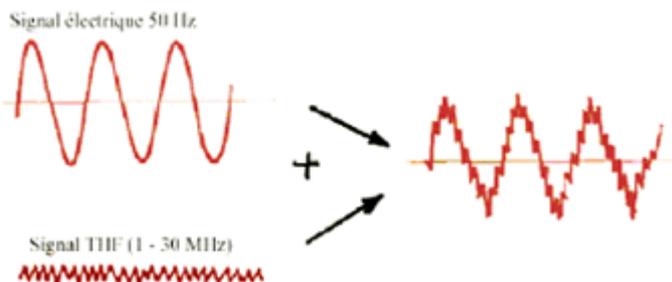
La technologie des courants porteurs en ligne permet de transmettre des informations numériques sur le réseau électrique existant. Son architecture s'apparente très fortement aux réseaux filaires RJ45 et sans-fil Wifi. Ici au lieu d'utiliser un câble réseau ou les ondes radio pour transmettre les informations, c'est le réseau électrique existant qui fait office de support de communication.

2. Historique

- **1950** : Fréquence 10Hz, puissance 10kW
- **Milieu des années 80** : début des recherches pour utiliser l'électricité comme support de transport de données
- **Fin des années 90** : début du haut débit sur CPL
- **1997** : Premiers tests de transmission de signaux de données sur réseau électrique
- **2000** : Premières expérimentations en France par EDF R&D et ASCOM, création de la Home Plug Powerline Alliance
- **Novembre 2001** : standard Home Plug 1.0.1
- **Janvier 2005** : débit de 200 Mbits/s sur une distance de 300 mètres annoncé
- **2007** : Arrivée sur le marché des produits à la norme HomePlug AV 200 Mbits Ajout de nouvelles fonctionnalités (QoS, VLAN...). L'IEEE prévoit la mise en œuvre d'une norme commune permettant l'interopérabilité des 3 grands systèmes CPL HPP,UPA,CEPCA



3. Principe de fonctionnement



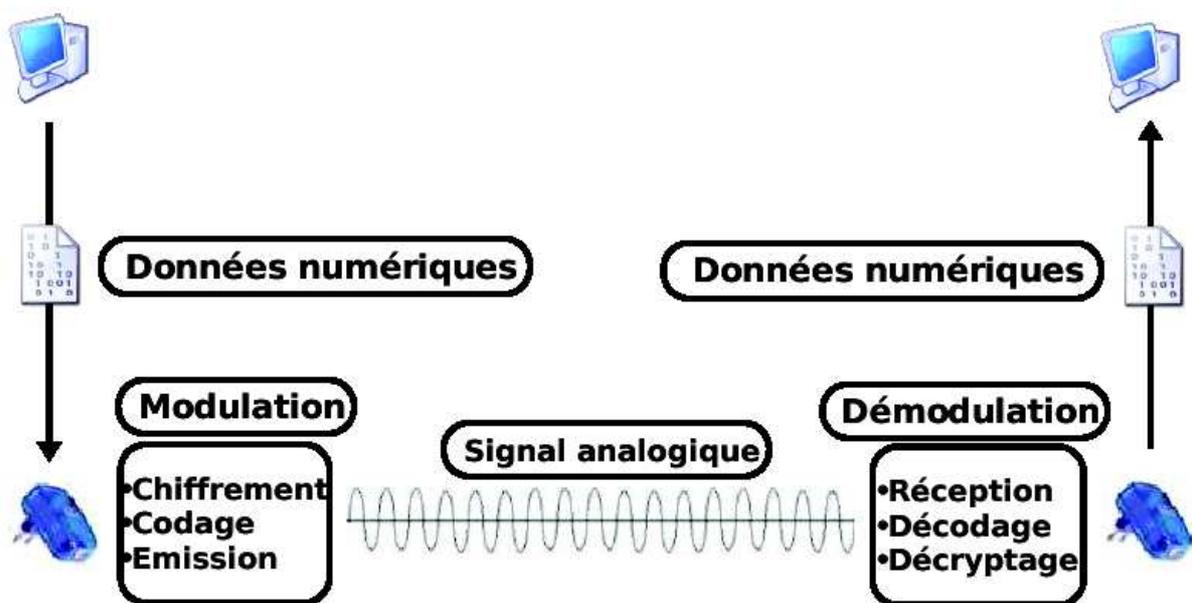
Le support du réseau électrique n'a pas été étudié pour transporter des signaux Haute Fréquence (HF). Il faut donc prendre en compte les contraintes de ce support pour assurer une bonne transmission de ces signaux HF sans pour autant perturber les appareils environnants, ni les fréquences de la bande 1-30 Mhz par rayonnement, certaines fréquences de cette bande étant

réservées à l'armée ou bien aux radios amateurs. 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
- ▶ Couplage inductif via un tors 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.



Technique de modulation des 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*).

a- Modulation de type 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. Il 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.

Nb : 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 Wifi (802.11a).

b- Modulation de type Spread Spectrum

Ce type de modulation consiste à « étaler » l'information sur une bande de fréquences beaucoup plus large que celle 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.

Lorsqu'on fait le point des différentes solutions existantes à ce jour nous remarquons que les solutions qui utilisent l'étalement de spectre restent à bas débit, seules les solutions qui utilisent OFDM peuvent monter en débit.



4. Normes

Un comité de normalisation HomePlug est en place pour faire standardiser cette technologie auprès de l'IEEE,

Voici les différents standards de CPL

HomePlug 1.1 : 14Mb (5Mb réel environ)

HomePlug Turbo : 85Mb (20Mb réel environ)

HomePlug AV : 200Mb (50Mb réel environ) (Audio Vidéo)

CPL HD : 200Mb (50Mb réel environ) (Haute Définition)

Il existe d'autres technologies qui présentent à un débit théorique de 400Mb, mais elles sont très peu connues en France, et une fois de plus incompatibles avec les Homeplugs.

Le FAI Free a attendu que la technologie des Homeplugs AV soit mature (stable et pas trop cher) pour faire ses Freeplugs.

En effet, les Homeplug Turbo sont suffisants pour faire passer votre connexion de 20Mb max ADSL dont l'internet et la TV, mais la moindre perturbation ou installation électrique de mauvaise qualité pourrait poser problème. Donc les Freeplugs sont à la norme Homeplug AV à 200 Mb.

Il n'est pas conseillé de faire cohabiter deux normes CPL sur la même installation pour des raisons évidentes de pertes de performances. Le plus faible ferait chuter le débit de transmission.

	HomePlug	Norme PLRP : PowerLine Routing Protocol de la compagnie Oxance	Norme DS2 (Schneider Electric Defidev)
Débit	14 Mb/s, 85 Mb/s (Turbo), 200 Mb/s (AV)	85 Mbps théorique	200 Mbps théorique
Sécurité	Chiffrement DES 56 bits	Chiffrement DES 56 bits avec gestion de la clé pour protéger le trafic des données sur le réseau électrique RVP AES 128 bits	
Nombre de clients possible	16 ou jusqu'à 255 mais des répéteurs sont nécessaires pour chaque grappe de 15 modems	16 ou jusqu'à 255 mais des répéteurs sont nécessaires pour chaque grappe de 15 modems	30 par injecteur
Portée	Environ 300 mètres	Environ 600 mètres	Environ 300 mètres

5. Sécurité

Le CPL est réputé pour une technologie fiable et sécurisée. Cependant, le compteur électrique du logement ne constitue pas une barrière étanche de sécurité au signal CPL. En effet on peut capter ce signal 200 mètres plus loin avec une légère dégradation.

On parle de frontière indoor / outdoor représentée par le compteur.

La norme « HomePlug 1.0.1 » inclut le cryptage DES (Data Encryption Standard) de 56 à 128 bits. Les DES est un algorithme de chiffrement par bloc, il transforme un bloc de 64 bits en un autre bloc de 64 bits.

Il est possible d'écouter un signal CPL, mais il est impossible de décrypter ce signal car cela prendrait quelques milliers d'années avec une méthode de brute force.

Malgré que les pirates puissent tester de plus en plus de clés à la seconde, le système HomePlug est suffisamment préparé pour résister à ces derniers. La seule manière de pirater un réseau CPL est de charger les clés une à une sur un adaptateur HomePlug afin de tester toutes les combinaisons, et ceci prendrait beaucoup trop de temps.

Le réseau CPL est donc pour le moment bien plus sûr qu'un réseau Wifi (normes actuelles).

6. Utilisations du CPL

Techniquement, la technologie CPL Outdoor ressemble à une "boucle locale". On fait circuler les informations numériques (voix, données IP, etc) entre le transformateur électrique du quartier et ses différents logements grâce aux réseaux EDF.

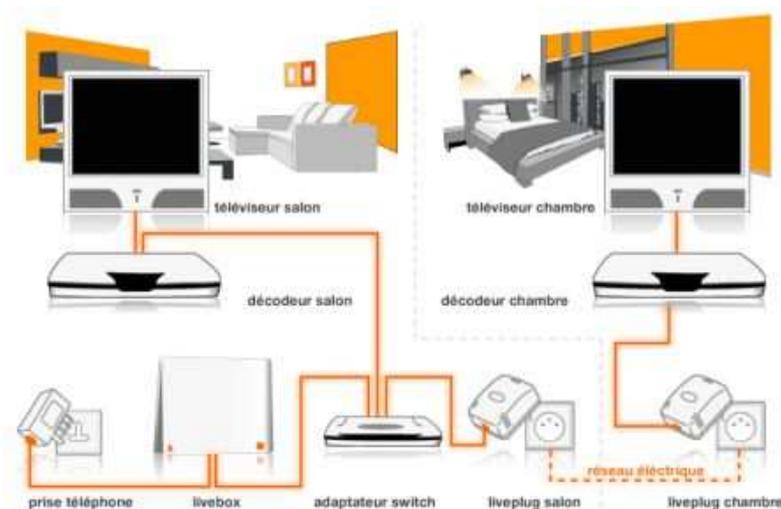
On a donc pas besoin de fibrer tout le monde. On peut, pour des zones un peu à l'écart se servir du réseau électrique bien présent et bien diffus pour les raccorder à l'Internet.

On trouve déjà du CPL dans des villes comme Nantes, Angers, qui propose aux habitants des logements sociaux l'Internet par le courant et la voix IP illimitée.

Les FAI internet comme Free, Orange, et Neuf(SFR) proposent maintenant, moyennant ou non le

CPL en sus, l'Internet dans toute la maison grâce à cette technologie.

Ils proposent aussi un service de Multi TV qui consiste à pouvoir brancher plusieurs télévisions dans différentes pièces de la maison et de capter les chaînes par le courant électrique diffusé par le boîtier CPL de la Box centrale.



7. Avantages et Inconvénients

Avantages

Le CPL a plusieurs avantages :

- Une portée d'environ 200 à 300 mètres.
- C'est une alternative intéressante aux câbles disgracieux et au Wifi pas toujours très sécurisé. Créer son réseau local et partager sa connexion ADSL devient alors aussi simple que de brancher n'importe quel appareil sur une prise électrique murale.
- On utilise un câblage existant, on a donc :
 - Une simplicité de mise en œuvre
 - Une bonne mobilité. Même tout au fond de son jardin on peut être connecté pourvu d'avoir une prise de courant.
 - Une solution complémentaire aux systèmes filaires (Ethernet) et sans fils (Wifi).
 - Application à d'autres domaines : domotique, audio, vidéo, surveillance,...

Inconvénients

La transmission des données est atténuée par différents critères comme la vétusté du réseau électrique, la longueur des câbles, l'utilisation de multiprises ou encore la qualité des adaptateurs CPL utilisés.

D'autres problèmes interviennent en ce qui concerne

- L'architecture présente du réseau électrique.

- Le débit partagé par tous les matériels connectés.
- La limite de 16 adaptateurs par réseau.
- la cohabitation entre les différents types d'équipements CPL.

De plus, les radios amateurs détestent cette technologie qui rayonne et perturbe leurs équipements. En effet les quelques dizaines de Milliwatts que produit un boîtier CPL s'entendent à des dizaines de kilomètres.

Ne pas oublier votre portail électrique ou votre interphone communicant peut être en CPL, ce qui est à prendre en compte si vous installez du CPL, ceci peut utiliser un signal différent et perturber celui que vous installez.

Enfin, le triphasé (380V sur 3 phases), les équipements branchés sur des phases différentes ne pourront pas communiquer, il faudra utiliser un coupleur afin de répartir le signal sur les trois phases.

Il y a un manque évident de normalisations et de standardisation, ce qui nuit à son développement, et freine son utilisation à travers le monde.

Les différents types existant de CPL n'étant pas associables, on a ici encore un autre inconvénient

8. Conclusion

Depuis quelques années, le système CPL connaît une réelle expansion de développement et d'utilisation. Avec la normalisation HomePlug, les débits ont pu être augmentés considérablement de sorte à avoir une portée plus étendue.

Son avenir est assuré grâce aux fournisseurs d'accès à Internet qui commencent à l'utiliser en abondance de par sa facilité d'utilisation ainsi que pour sa sécurité. Il permet aussi d'offrir un accès à Internet dans les zones non couvertes.

La technologie CPL n'est pas destinée à remplacer le Wifi, l'Ethernet et le WiMax mais à compléter l'offre.

9. Bibliographie

Livres

Réseau CPL par la pratique. Xavier Carcelle. EYROLLES éd

Sites Internet

http://www.exblog.fr/post/20080922_CPL-Freeplugs-norme-compatibilite
<http://www.generation-nt.com/cpl-norme-ieee-2007-actualite-11613.html>
<http://www.ariase.com/fr/news/article977cplcastresmazamet.html>
<http://fdigallo.online.fr/cours/cpl.pdf>
http://fr.wikipedia.org/wiki/Courants_porteurs_en_ligne
http://www.idate.fr/touraine_numerique/pdf/cpl.pdf
<http://www.commentcamarche.net/contents/cpl/cpl-intro.php3>
<http://www.linternaute.com/hightech/micro/cpl/06/test/060323-test/1.shtml>
<http://www.cpl-france.org/>
<http://www.cuc.fr/pagestatic/cpl.pdf>