REF-Union
32, rue de Suède
B.P. 7429
37074 Tours Cedex 2
ref@ref-union.org

Tours le 15 novembre 2004

REF-Union

IMPACT DES RESEAUX INFORMATIQUES DE TECHNOLOGIE CPL (COURANTS PORTEURS EN LIGNE) SUR LES RADIOCOMMUNICATIONS

RESUME

Technologie

La technologie des Courants Porteurs en Ligne (CPL) permet de constituer des réseaux informatiques.

Le principe est d'utiliser pour le transfert de données des signaux exploitant les ondes radio injectées sur les câbles de distribution d'électricité existants au moyen de modems émetteurs-récepteurs.

Applications

Les réseaux informatiques ainsi créés peuvent avoir des applications domestiques "indoor" et fournir un accès Internet à Moyen-Débit (application "outdoor").

Génération de Parasites

Certains des réseaux (câbles et modems) ainsi constitués génèrent des parasites radio intenses.

Les fils électriques font office de grandes antennes et les signaux sont audibles à des distances de plusieurs centaines de mètres.

Brouillages des radiocommunications

Les parasites générés par certains réseaux CPL perturbent les radiocommunications en brouillant la réception des fréquences radioélectriques concernées au voisinage du lieu d'utilisation.

Ces brouillages peuvent se produire 24 heures sur 24 sur une large plage du spectre radioélectrique, en empêchant toute utilisation normale, notamment dans des situations d'urgence.

Vérifications et mesures de bon sens

Lors de la mise au point de projets en technologie CPL, des vérifications et précautions de bon sens doivent permettre de limiter les brouillages en s'assurant que :

- les puissances des signaux radioélectriques injectées sont aussi basses que possibles et conformes aux prescriptions de l'Union Internationale des Télécommunications (UIT),
- l'installation des réseaux est limitée à des circuits de distribution électrique enterrés, à distance suffisante de stations de radiocommunication susceptibles d'être perturbées,
- les émissions des réseaux évitent les fréquences utilisées pour les radiocommunications en relation avec la sûreté de l'Etat et la sécurité des personnes et des biens,
- les solutions pour constater rapidement les interférences éventuelles et les moyens pour les éliminer sont prévus pour, en cas de perturbations résiduelles, interrompre sans délai le fonctionnement des réseaux.

Décryptage et intrusions

Les signaux émis par les réseaux CPL sont audibles à distance, et les risques de décryptage et d'intrusion par voie radioélectrique ne sont pas à exclure.

Des dispositifs de codage suffisants, garantissant aux utilisateurs la confidentialité des données échangées sur les réseaux et l'absence d'intrusions sont à prévoir.

Information aux utilisateurs

Les utilisateurs publics et privés de réseaux CPL doivent être informés des défauts inhérents à cette technologie et des risques encourus.

LES COURANTS PORTEURS EN LIGNE, PRINCIPE ET APPLICATIONS

Principe de base

Le **principe** des CPL est d'utiliser pour le transfert de données informatiques des signaux numériques exploitant des ondes radio haute fréquence injectées sur les fils de distribution électrique au moyen de modems émetteurs-récepteurs appropriés.

Il existe depuis de nombreuses années des applications industrielles et domestiques de ce principe, les technologies anciennes n'autorisant que de faibles débits, les solutions récentes permettant d'obtenir des débits plus importants.

Principales applications des CPL

Des modems CPL branchés sur les prises électriques permettent de constituer un réseau domestique ou de petite entreprise (CPL en intérieur, **application "indoor"**), sur des distances théoriques de quelques dizaines à quelques centaines de mètres.

A notre connaissance, en France, la mise en place de réseaux CPL "indoor", derrière un compteur électrique privé, est libre sous réserve de ne pas créer de nuisances, auquel cas le matériel doit être immédiatement retiré.

En utilisant le réseau de distribution électrique extérieur (**application "outdoor"**), il est possible de fournir l'accès Internet à des habitations, résidences ou groupes de maisons. Les signaux reçus par fibre optique ou satellite sont injectés sur le réseau au niveau du transformateur moyenne tension/basse tension au moyen d'un modem. Chez chaque utilisateur un modem dédié relié à l'ordinateur permet l'accès Internet. La distance maximale entre transformateur et utilisateur est de quelques centaines de mètres.

En France, les réseaux d'accès Internet par réseaux CPL "outdoor" sont soumis à autorisation temporaire, et à ce jour ouverts seulement à titre expérimental, en attente d'une réglementation claire particulièrement sur l'aspect de leur compatibilité avec certains services de radiocommunication.

Performances des réseaux CPL

En application "indoor", les **débits échangés** théoriques selon les données des constructeurs s'élèvent à quelques dizaines de mégabits par seconde sur des distances de quelques centaines de mètres. En pratique on réussit à transférer quelques mégabits par seconde à des distances de quelques dizaines de mètres, dans des conditions normales.

En application "outdoor", les CPL permettent des accès Internet de type Moyen-Débit, de l'ordre de quelques centaines de kilobits par seconde par utilisateur.

Dans les deux cas, on est loin évidemment, d'un facteur 10 environ, des performances des réseaux Ethernet filaires ou des solutions d'accès Internet Haut-Débit disponibles actuellement.

Les réseaux CPL sont très sensibles à des émissions radio situées à proximité, de puissance même faible, sur les bandes de fréquence utilisées, ainsi qu'aux divers parasites pouvant circuler sur les lignes. Cette **fragilité** se traduit par des baisses de débit ou des interruptions complètes des transferts de données pendant les émissions.

D'autres évènements anodins, comme par exemple l'allumage d'une lampe, la mise en service d'appareils domestiques électriques de forte puissance, perturbent le fonctionnement du réseau CPL et en dégradent les performances.

Confidentialité

Les fabricants de modems CPL ont mis au point des codages des signaux échangés, pour en protéger la confidentialité. Les risques de **décryptage mal intentionné** sont probablement limités, mais ils existent.

A noter que les ondes radio produites par les modems CPL et conduites par les fils électriques sont audibles dans leur voisinage, à plusieurs centaines de mètres, avec des moyens de réception très simples, sans liaison physique au réseau électrique et donc sans aucune intrusion dans les lieux.

Avec des systèmes plus sophistiqués (antennes directives à grand gain, récepteurs à grande sensibilité), c'est à des distances plus grandes que la réception des fréquences utilisées doit être possible, et donc le décryptage éventuel des données échangées.

Des **intrusions sur les réseaux CPL** sont, pour les mêmes raisons, théoriquement possibles à distance.

Aspects réglementaires et politiques

La présence du **sigle CE** librement apposé par le fabricant sur un modem CPL n'est qu'une présomption de conformité de l'appareil aux exigences essentielles des directives de Compatibilité Electro-Magnétique (CEM) en vigueur et non pas une garantie absolue de conformité du système complet (modems et câblage électrique). En cas de plainte, les autorités compétentes peuvent être amenées à contrôler cette conformité et, le cas échéant, à faire retirer le produit du marché.

Il n'existe pas encore à ce jour en Europe de **norme CEM spécifique** définissant les caractéristiques des réseaux CPL.

En 2001 la Commission Européenne a confié à un groupe de travail européen, le JWG ETSI-CENELEC, sous le mandat n°313, le soin de définir des standards appropriés.

Trois ans plus tard l'action est toujours en cours, les standards ne sont pas encore définis. La raison est simple : les utilisateurs des fréquences concernées par les réseaux CPL, soutenus par leurs administrations nationales, s'opposent à l'élaboration de limites de rayonnement parasites trop permissives.

Il y a donc un risque que les réseaux CPL ne soient jamais autorisés en Europe aux puissances qui seraient nécessaires pour en assurer un fonctionnement correct. Cela pourrait avoir pour conséquence la fermeture des réseaux existants et une perte financière importante sur les investissements réalisés.

Au niveau de la **Commission Européenne**, certains groupes de pression voient dans les réseaux CPL une alternative aux accès Internet traditionnels parmi les solutions au problème de "fracture numérique", permettant une bonne mise en concurrence des divers procédés. Ces groupes interviennent dans le débat normatif et cherchent à obtenir les standards les moins contraignants en favorisant ainsi les solutions CPL.

Aspects radioélectriques, services de radiocommunication

Les **fréquences des ondes radioélectriques utilisées** dans la technologie CPL sont comprises entre 2 et 30 MHz, soit des longueurs d'onde de 10 à 150 m (spectres hectométrique et décamétrique).

A ces fréquences, les ondes radio présentent la propriété exceptionnelle de permettre des radiocommunications à courte, moyenne et grande distances par réflexion sur les couches ionosphériques situées à plusieurs centaines de kilomètres d'altitude au-dessus de la terre (**propagation ionosphérique**).

Elles sont pour cette raison indispensables dans les zones où des infrastructures terrestres sont difficiles à installer (océans, grandes étendues, zones désertiques), et en cas de situations d'urgence où il faut installer rapidement des stations de radiocommunication simples et efficaces. Elles doivent rester une alternative en cas de dysfonctionnement des réseaux de communication par satellites ou de saturation des réseaux exploitant d'autres gammes de fréquences.

Ces fréquences sont protégées, leur utilisation est strictement régie au niveau de l'UIT à travers le Règlement des Radiocommunications. La révision récente de ce dernier confirme le besoin de garder ces ressources exploitables sans dégradation par rapport au niveau de pollution radioélectrique actuel.

Les attributions des fréquences entre 2 et 30 MHz sont organisées au niveau mondial par l'UIT. Cette partie du spectre radioélectrique est attribuée par bandes de fréquences aux services de radiocommunication suivants :

- services *fixes* et *fixe aéronautique*,
- services *mobiles*, mobile *maritime*, mobile *terrestre*, mobile *aéronautique*,
- service de *radiolocalisation*,
- service de *radiodiffusion*,
- service des *fréquences étalon* et *signaux horaires*,
- service de *radionavigation maritime*,
- services *amateur* et amateur par *satellite*,
- service de *radioastronomie*,
- service des auxiliaires de la *météorologie*.

En termes d'**utilisation des fréquences entre 2 et 30 MHz**, les stations classées dans ces services assurent notamment :

- la *radiodiffusion* en *ondes courtes*,
- des radiocommunications *terrestres*, *maritimes* et *aériennes*,
- des radiocommunications de *services officiels* (sécurité, police, organisations internationales, service des ambassades) notamment lors de catastrophes naturelles,
- des radiocommunications des *forces armées*,
- des mesures de type *scientifique* et *technique*, par exemple la radioastronomie, la radionavigation, la météorologie, l'identification à distance.

Les programmes de la *radiodiffusion en ondes courtes* sont écoutés par des centaines de millions de personnes sur l'ensemble du globe. Plus de 5 000 stations transmettent leurs émissions à partir de 120 Etats. La technologie Digital Radio Mondiale (DRM) est en cours de mise en place depuis 2003. Elle permet de recevoir des émissions de très haute qualité sonore, transmises par des émetteurs situés à des milliers de kilomètres.

Les *radiocommunications maritimes* sont régies par l'Organisation Maritime Internationale (OMI). Des fréquences entre 2 et 30 MHz sont utilisées pour notamment des communications de téléphonie, fax, transferts d'images météo.

Plus de 12 000 avions de ligne assurent le transport aérien au niveau mondial. Lors des trajets au-dessus des océans et des zones peu habitées, les *radiocommunications aéronautiques* sont effectuées notamment sur des fréquences comprises entre 2 et 30 MHz. La coordination de l'utilisation de ces fréquences est assurée par l'Organisation de l'Aviation Civile Internationale (OACI).

Les *services amateur et amateur par satellite* comprennent 3 000 000 d'opérateurs au niveau mondial, 400 000 en Europe, à qui sont attribuées de nombreuses plages de fréquences notamment entre 2 et 30 MHz. C'est le plus important réseau de personnes capables d'intervenir à la demande des autorités pour assurer des radiocommunications en situations d'urgence, lorsque les services publics sont débordés ou si des compétences particulières sont requises. En France par exemple des opérateurs de ces services réalisent chaque année des centaines de missions dans le cadre de la Sécurité Civile (radiocommunications, recherches de balises aéronautiques). La récente tragédie à l'usine AZF de Toulouse a mis en évidence la complémentarité de ces moyens avec ceux des services officiels. Aux USA des équipes équivalentes sont intervenues à New York le 11 septembre 2001.

Il existe d'autres utilisateurs des fréquences entre 2 et 30 MHz, pour des applications à *faible puissance* (télécommande, téléphonie sans fil, étiquettes radio-fréquence).

PARASITES ET BROUILLAGES GENERES PAR LES RESEAUX CPL

Les brouillages générés

La technologie des CPL utilise les fils électriques pour conduire les ondes radioélectriques injectées par un modem émetteur vers un modem récepteur.

Lors des transferts de données informatiques, les fils électriques peuvent se comporter comme des antennes qui rayonnent dans le voisinage. Ce processus peut être compris comme une source de fuites indésirables vers l'extérieur.

Les signaux émis ressemblent, dans certaines technologies, à des crachotements intenses, des **parasites radioélectriques** qui perturbent voire interdisent la réception des signaux radio utiles. Dans d'autres technologies, c'est un bruit blanc intense qui est généré sur une large bande de fréquences, saturant les récepteurs.

Dans le cas des applications "outdoor", ces parasites ou bruit à large bande couvrent tout ou partie de la plage de fréquences entre 2 et 30 MHz et parfois au-delà, 24h sur 24.

Les perturbations de la réception des fréquences radio se produisent en général à des distances comprises entre quelques dizaines de mètres et plusieurs kilomètres des réseaux CPL incriminés.

Dans certaines villes d'Europe où des réseaux commerciaux ont été déployés, les **zones parasitées** couvrent des quartiers entiers où la réception de ces fréquences est difficile (exemples en Allemagne, Autriche, Ecosse, Espagne et Finlande). Les grands objets métalliques (tubes de gouttière, lampadaires) peuvent accentuer le phénomène en entrant en résonance avec les ondes incidentes et en agissant comme des antennes qui ré-émettent aux alentours les parasites des réseaux CPL.

Aux Etats-Unis, où le déploiement de la technologie CPL est plus avancé qu'en Europe, certains réseaux ont dû être arrêtés sur plaintes d'exploitants des ondes courtes à proximité. L'administration fédérale des radiocommunications (FCC), a autorisé des limites de rayonnement trop permissives ; des mouvements se mettent en place pour les faire abaisser.

Les perturbations aux utilisateurs des fréquences radioélectriques

Dans les zones parasitées, on observe des **perturbations aux services de radiocommunication**. La réception des fréquences radio concernées peut être brouillée plus ou moins fortement : réception de la radiodiffusion en ondes courtes, radiocommunications terrestres, maritimes et aéronautiques, notamment depuis les préfectures, les ambassades, les sites militaires ainsi que depuis des installations mobiles.

Si des stations de services de radiocommunication concernés sont situées dans le voisinage, il y a lieu de craindre des **interruptions de leurs communications** en cours, partielles ou totales, lors des transferts de données informatiques utilisant des réseaux CPL.

Les radiocommunications des opérateurs de ces services peuvent être dégradées ou rendues impossibles dans un rayon de plusieurs kilomètres.

Des essais en radiodiffusion digitale DRM ont montré des **blocages complets des réceptions radio** lorsque le réseau CPL voisin se mettait en marche.

Les membres du groupe DRM chargé de promouvoir le déploiement de cette technologie de radiodiffusion internationale moderne s'inquiètent de cette situation. Ils invitent leurs représentants à demander à leurs autorités gouvernementales d'assurer la protection des ressources radioélectriques qui leur sont nécessaires.

Conséquences sur la vie de la société

Les communications établies par les stations des services ci-dessus, quelque soit l'année, le jour ou l'heure, peuvent revêtir un caractère *"d'utilité publique"* en *situations normale* ou *d'urgence*, et être en rapport avec la **sûreté de l'Etat** et la **sécurité des personnes et des biens**.

En cas de plaintes d'opérateurs ou d'utilisateurs de services de radiocommunication perturbés par les parasites de réseaux CPL, les autorités compétentes auront à en gérer les **aspects juridiques**, et à demander aux opérateurs de ces réseaux les modifications techniques nécessaires, voire les fermer, au détriment de leurs clients.

Les réseaux sans fil dits Wi-Fi, dont les portées sont pourtant très limitées (quelques dizaines de mètres), ont fait l'objet au niveau mondial d'un important travail normatif pour assurer la **sécurisation des échanges de données** et éviter les intrusions.

Les technologies CPL, dont les signaux sont audibles à des distances bien plus importantes, ne sont probablement pas aussi sûres. En effet, chaque fabricant de modems a mis au point ses propres solutions de codage, non encore normalisées.

En cas de **décryptage mal intentionné** ou d'**intrusion** sur les réseaux CPL, des utilisations délictueuses des données recueillies ou injectées ne sont pas à écarter, pouvant entraîner des suites judiciaires.

Les modems CPL peuvent être saturés par des émissions radio de puissance relativement faible à courte distance. Il en résulte des blocages partiel ou totaux du réseau. Les émissions radio peuvent provenir de services autorisés situés à proximité, et les blocages ne sont pas intentionnels. Il peut aussi s'agir de **blocages mal intentionnés de réseaux CPL**, réalisés avec du matériel grand-public.

Détails techniques radioélectriques

Dans un réseau CPL, la puissance radioélectrique est injectée sur les fils électriques ordinaires au moyen de modems. Une partie de cette puissance est conduite par les fils qui constituent des lignes de transmission très imparfaites, d'impédance non constante et à fortes pertes. L'autre partie de la puissance injectée est rayonnée dans le voisinage, de manière indésirable, car **les câblages font office de grandes antennes**.

Si les circuits de distribution électrique sont enterrés, la puissance rayonnée est moins forte et les parasites générés moins intenses.

En zones rurales, les fils électriques supportés par des poteaux constituent des antennes d'émission-réception bien dégagées pour ces ondes de longueurs comprises entre 10 et 150 m. Les dégâts en termes de pollution radioélectrique et de fragilité des réseaux sont maximum.

Pour fiabiliser le transfert des données, les **puissances radioélectriques injectées** sont parfois réglées à des niveaux très élevés, aggravant naturellement les perturbations.

SOLUTIONS POUR LIMITER LES PARASITES ET BROUILLAGES PAR LES RESEAUX CPL

Il n'y a pas de solution miracle

Utiliser les ondes radio sur des fils électriques ordinaires pour transporter des données numériques est par nature un **mauvais concept**. Les interférences sont inévitables. Il doit être cependant possible d'en limiter les conséquences.

Vérifications et mesures de bon sens

Abaisser les puissances injectées

La première mesure est d'**injecter des puissances radioélectriques très faibles** aussi basses que possibles, sur les fils électriques. En l'absence de norme spécifique aux réseaux CPL, il paraît raisonnable de s'appuyer sur le principal texte existant, le Règlement des Radiocommunications de l'UIT.

Lutter contre les rayonnements indésirables

Les câbles sous-terrains rayonnent beaucoup moins que les fils électriques aériens. Pour cette raison il faut **privilégier les circuits de distribution électrique enterrés** et éviter au maximum les lignes aériennes pour les réseaux CPL "outdoor".

On peut noter que les normes européennes en matière de CEM, appliquées au domaine des équipements informatiques, ont permis par l'installation de **blindages** et de dispositifs à **ferrites** sur les câbles d'abaisser de façon significative les niveaux de perturbation électromagnétique qu'ils génèrent ; il semble difficilement concevable de provoquer intentionnellement de nouvelles perturbations, à un niveau élevé, autour des équipements informatiques, par utilisation de certains modems CPL non conformes.

Protéger les services de radiocommunication

Il paraît raisonnable de **protéger les sites sensibles** (radioastronomie, police, ambassades, gendarmeries, administrations) et de façon générale les stations de services de radiocommunication utilisant les fréquences concernées ; des distances de protection suffisantes, au minimum plusieurs centaines de mètres, doivent permettre de limiter les brouillages par les parasites de réseaux CPL.

Certaines fréquences sont à protéger tout particulièrement, celles utilisées lorsque la sûreté de l'Etat, la sécurité des personnes et des biens est concernée, notamment dans les **situations d'urgence**.

Lutter contre la pollution radioélectrique

Il paraît indispensable de prévoir :

- les moyens de **constater rapidement des interférences** éventuelles,
- les solutions pour les diminuer à des niveaux acceptables ; dans le but de faciliter la recherche des brouilleurs, chaque source de signal pourrait émettre un signal d'identification,
- **les dispositifs d'interruption** sans délai des réseaux CPL par action locale et à distance, en cas de perturbations résiduelles, ainsi qu'en situations d'urgence (plans ORSEC) pour ne pas risquer de mettre en danger la vie humaine,
- la procédure à suivre pour l'application des solutions de protection de tous les services de radiocommunications perturbés.

Décryptages et intrusions

Les **cryptages des signaux** doivent être effectués à un niveau suffisant garantissant la confidentialité des échanges selon les règles juridiques en vigueur et évitant les intrusions.

Injecter sur les fils électriques des signaux radioélectriques à très faible puissance permet de diminuer l'étendue des zones où les signaux sont audibles et théoriquement décryptables.

Information aux utilisateurs

Dans les départements français, les modems CPL pour réseaux "indoor" sont en vente libre.

Il faudrait envisager une information suffisante incluant des **mises en garde aux utilisateurs des réseaux CPL**, publics et privés, contre les risques encourus à partager l'utilisation des fréquences radioélectriques avec des exploitants de services de radiocommunication, tout particulièrement lorsqu'ils relèvent de la *sûreté de l'Etat* ou de la *sécurité des personnes et des biens*.

En effet, les usagers de réseaux CPL ont l'**obligation de ne pas perturber les radiocommunications** des stations des services auxquels les fréquences qu'ils utilisent sont attribuées.

Ces mises en garde devraient être prévues au niveau des distributeurs qui commercialisent ce type d'équipements dans leurs établissements.

En cas de brouillages, les stations de radiocommunication ont droit à résolution des interférences, à charge des administrations nationales (en France l'Agence Nationale des FRéquences, l'ANFR). Dans de telles circonstances et du point de vue du droit, c'est le perturbateur et lui seul qui doit faire les efforts correctifs.

Les usagers de réseaux CPL ne sont pas des utilisateurs reconnus des fréquences radioélectriques et n'ont par conséquent pas droit à protection en cas d'interruption de leur réseau par des émissions proches.

Une telle information des utilisateurs relève de la législation en vigueur. La jurisprudence est claire sur le fait que le vendeur doit mettre ses clients en garde contre les dangers ou les inconvénients auxquels expose l'utilisation des biens qu'il fournit. Par ailleurs toute omission des problèmes liés à la CEM peut être considérée comme de la publicité mensongère.

Actuellement, ces problèmes ne sont généralement pas signalés dans les documents remis par les fabricants des produits.

Penser l'avenir

Si les réseaux CPL se développaient à grande échelle (villes entières, départements), il y aurait lieu de craindre une **pollution radioélectrique au niveau mondial** ; en effet, par propagation ionosphérique, les signaux CPL pourraient devenir gênants à grande ou très grande distance.

Les **responsables de l'aménagement des collectivités territoriales** ne peuvent rester étrangers à une analyse globale des conséquences de leurs choix. Ils ne peuvent s'exonérer d'une réflexion approfondie sur l'optimisation de l'utilisation des fonds publics, non dans des techniques déjà dépassées et sans visibilité future, mais plutôt dans des technologies modernes, performantes et respectueuses de l'environnement radioélectrique.