Extrait du Spyworld Actu

http://www.spyworld-actu.com/spip.php?article2775

Une nouvelle technique d'encryptage sur fibre optique par le bruit

- Informatique - Sécurité Informatique -

Date de mise en ligne : dimanche 15 octobre 2006

Spyworld Actu

Coder un signal en le diluant dans les parasites : c'est l'idée développée par une équipe de l'université de Princeton et présentée au symposium annuel de l'Optical Society of America.

Prenez une fibre optique et envoyez à l'intérieur une jolie lumière laser parfaitement contrôlée en fréquence et en puissance. A l'autre bout, le faisceau aura subi de légères altérations de la fréquence et de l'intensité, fluctuant aléatoirement autour de leur valeur initiale. C'est l'inévitable phénomène du « bruit » que subit n'importe quel signal. Les parasites radio sont une forme de bruit. Même les photos numériques présentent un certain bruit, ensemble de points intempestifs ajoutés à l'image. Pour que le bruit ne soit pas gênant, il faut qu'il reste très faible par rapport au signal, c'est-à-dire que le rapport signal/bruit soit suffisamment élevé.

Bernard Wu et Evgenii Narimanov, deux spécialistes de l'optique à l'université de Princeton, ont eu cette idée, en apparence saugrenue : si, au contraire, on crée un signal aussi faible que le bruit, il sera très difficile de le récupérer à l'autre bout de la ligne. Ce sont alors les lois naturelles qui, au fil de son transport, recouvriront le signal de parasites, le rendant indéchiffrable. Voilà une méthode de cryptage originale : créer un message inaudible !

Le message était dans le bruit de fond...

Pourtant, ça marche... Les scientifiques ont trouvé une astuce pour coder le signal en utilisant les petites altérations de la lumière dans la fibre optique, en le noyant dans le bruit en quelque sorte. La belle lumière laser transmise par la fibre optique ne transporte aucune information. Le vrai signal, lui, est camouflé dans les parasites. L'astuce consiste à faire appel à un procédé connu, le CDMA, Code Division Multiple Access, une technique de multiplexage utilisée depuis longtemps en radio, notamment par les militaires, pour la téléphonie mobile Qualcomm aux Etats-Unis et dans le GPS. Dans ce système, le signal est étalé sur toute la bande de fréquence disponible, un peu comme si toutes les stations radio de la bande FM dispersaient des petits bouts de leur émission sur toute la bande. Cet éclatement des signaux n'est pas quelconque mais repose sur un code, propre à chaque émetteur. Le récepteur doit le connaître et s'en sert pour générer une clé, sorte de filtre appliqué sur le brouhaha résultant du mélange de tous les émetteurs. Il recueille alors un seul signal.

Dans le système de Wu et Narimanov, le signal initial est codé dans un dispositif optique comprenant un encodeur CDMA. Le réseau, par exemple Internet, peut ensuite le transmettre tout à fait normalement, le transport se chargeant d'ajouter les parasites qui dissimuleront l'information. Le récepteur n'aura qu'à appliquer son filtre au bruit de fond pour récupérer le signal.

Ce principe ne fait appel qu'à des outils techniques déjà existants. Pourtant, les deux auteurs ne semblent pas croire que leur trouvaille puisse déboucher rapidement sur une application réelle. Le codage optique en CDMA, disent-ils, fait encore l'objet de recherches. Mais ce codage très sûr pourrait être un jour, selon eux, utilisé pour des achats sur le Web à travers un réseau en fibres optiques.

Post-scriptum :

http://www.futura-sciences.com/news...