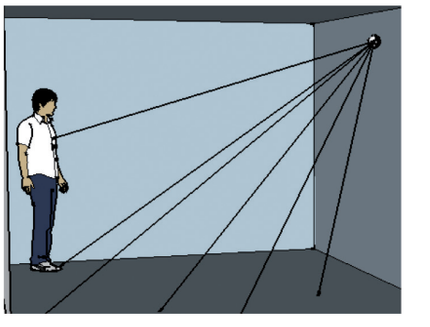
La sécurité grâce au « Li-Fi » Communiquer via la lumière de led

L'institut Fraunhofer, qui a son siège en Allemagne, est l'une des plus grandes organisations d'Europe en matière de recherche appliquée. Les efforts de recherche de Fraunhofer sont totalement orientés vers les besoins des gens : santé, sécurité, communication, énergie et environnement. Le professeur Harald Haas est l'une des chevilles ouvrières de l'Institut Fraunhofer. Sous sa direction, les chercheurs ont développé une technologie permettant de transmettre des données grâce à une source lumineuse à leds. Cette technique est connue sous diverses appellations telles que Li-Fi (Light Fidelity), D-light ou encore VLC (Visible Light Communications). Au plan mondial, outre Fraunhofer, d'autres instituts de recherche et d'universités font des recherches au sujet de la communication de données via des sources lumineuses à leds. Ces intervenants sont réunis dans le Consortium Li-Fi, au sein duquel ils œuvrent à une norme concernant le Li-Fi. Outre les propriétés de communication de données, cette norme décrit aussi un certain nombre de fonctionnalités intéressantes relatives aux applications de sécurité, et sur lesquelles nous reviendrons plus tard.

Le Li-Fi est une technique grâce à laquelle des sources lumineuses à leds peuvent être utilisées pour la transmission de données. Ceci est réalisé à l'aide d'impulsions lumineuses ultra courtes, invisibles à l'œil nu. Il suffit d'adapter quelques composantes de luminaires à leds existants pour les faire fonctionner comme transmetteurs de données. En principe, toute lampe à leds conventionnelle peut être transformée en transmetteur Li-Fi au moyen d'un microcontrôleur spécifique. La lumière émise est ensuite captée par un récepteur optique et convertie en signal numérique, en engendrant ainsi un flux de communications de données. La technique du Li-Fi peut être utilisée pour une transmission bidirectionnelle. Les liaisons montante et descendante peuvent être dissociées de différentes manières. On peut penser ici à une séparation basée sur la longueur d'onde, un intervalle de temps et/ou un codage type. Autre possibilité, une séparation spatiale et/ou optique. En cas de transmission de données bidirectionnelle, le microcontrôleur Li-Fi doit être équipé d'une source lumineuse en tant qu'émetteur et d'un récepteur optique, installés de préférence dans l'enveloppe d'un luminaire. Des chercheurs des universités britanniques d'Oxford et d'Édinbourg ont imaginé une technique permettant d'envoyer les données parallèlement à l'aide d'une série de leds dont chaque lampe émet un flux de données différent. Ceci est réalisé à l'aide d'une association de leds rouges, vertes et bleues. La couleur modifie la fréquence de la lumière. Chacune de ces fréquences émet un flux de données différent. Une équipe de scientifiques de l'université chinoise de Fudan, sous la direction du professeur Chi Nan, a affirmé avoir obtenu à l'aide d'une lampe à leds d'1 watt, une vitesse de Li-Fi de 150 Mbits/sec dans des situations pratiques. Ces dernières étaient obtenues à l'aide d'équipements normaux, disponibles dans le commerce.

Le Li-Fi du point de vue de la sécurité des informations

L'utilisation du Li-Fi présente du point de vue de la sécurité des informations de nombreux avantages par rapport au Wifi. Les murs constituant un obstacle pour la lumière, le Li-Fi reste dans le local où il est émis. Si le local est équipé de fenêtres, il est possible de créer, de façon simple, une barrière à l'aide de film transparent. Le Li-Fi n'est pas influencé par des émissions radio non désirées, extérieures au bâtiment. Et ceci, contrairement au Wifi. Le Li-Fi ne peut donc pas être piraté. Les interférences entre différents réseaux, souvent présentes avec le Wifi, sont pratiquement absentes car les murs arrêtent la lumière. Il est relativement simple d'éliminer la grande majorité des interférences produites par les sources naturelles telles que la lumière du soleil et les sources artificielles (on peut penser ici au faisceau d'une lampe de poche éclairant le récepteur optique), au moyen de filtres optiques (qui empêchent la saturation du récepteur). Les filtres analogiques et numériques en aval des filtres optiques rendent le reliquat d'interférences négligeable. Le risque de sabotage de la liaison sans fil est dès lors minime. Ceci, contrairement au Wifi, avec lequel il est assez facile, à l'aide d'un brouilleur radio, de perturber la liaison. Il est évident qu'une vue directe entre l'émetteur et le récepteur est préférable. Toutefois, ceci n'est pas indispensable ; tant que le récepteur optique peut récolter des photons, la transmission de données est possible, bien que la vitesse de transmission soit alors réduite. Le signal n'est que peu impacté par la réflexion de la lumière sur des obstacles. L'occultation complète de la source lumineuse entraîne la suppression du signal. L'utilisateur du local se retrouve alors dans le noir et remarquera donc immédiatement cette forme de sabotage. En outre, le Consortium Li-Fi met au point un certain nombre de caractéris-



tiques de sécurité pour le Li-Fi. Le consortium impose ainsi que les sources à leds créent des zones de 'nuage Li-Fi' (ou en anglais Li-Fi cloud areas) surveillées par des récepteurs optiques. Ces derniers sont équipés d'un circuit intégré comportant une fonctionnalité de détection de mouvement. Bien que le but de cette dernière soit de favoriser la mobilité de l'utilisateur entre les zones de nuage Li-Fi, cette fonctionnalité peut également être utilisée pour la détection intrusion, ou encore comme l'indique le consortium lui-même, pour la « Home or office security » (Sécurité du logement ou du bureau). Comme mentionné plus haut, les récepteurs optiques seront installés dans les luminaires. Ceci entraîne, par rapport à une détection de mouvement traditionnelle, une densité par projection exceptionnelle de la détection, que l'on ne rencontre normalement que dans des environnements haute sécurité. L'apparition de la fonctionnalité de détection de mouvement dans les infrastructures informatiques peut être considérée comme une étape supplémentaire dans la convergence entre sécurité physique et sécurité informatique.

Autres sons de cloche

L'Association néerlandaise de recherche expérimentale en radio (Vereniging voor Experimenteel Radio Onderzoek ou VERON) a fait part récemment d'un certain nombre de préoccupations concernant le Li-Fi. Ainsi, pour amener le flux de données vers la source à leds il faut un câblage véhiculant des signaux à impulsions rapides. Cette combinaison de câble et d'impulsions se comportera comme une antenne radio. Ceci peut engendrer des perturbations du spectre de radiofréquences. La VERON s'attend à ce que ses membres en soient gênés. Un autre risque survenant lorsqu'un câble et des impulsions fonctionnent en antenne émettrice, est que des personnes mal intentionnées puissent capter le signal radio. Il y a donc un risque pour la sécurité. Il importe donc que le câble soit équipé d'un écran, et que ce dernier soit relié à une terre appropriée. Tout ceci pour se protéger d'un effet TEMPEST.

Conclusion

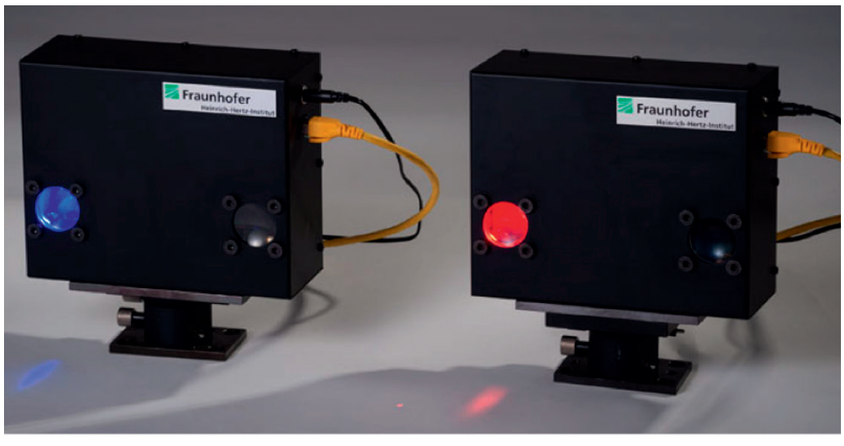
Le bureau d'études de marché MarketsandMarkets s'attend à ce que l'industrie du Li-Fi-représente dans moins de cinq ans 5 milliards d'euros. Le Li-Fi est une technologie qui se développe rapidement et fait apparaître de nouvelles infrastructures informatiques qui sont sur le point d'être commercialisées. Au Consumer Electronics Show 2014 de Las Vegas, SunPartner Technologies et Oledcomm ont présenté le premier smartphone équipé de Li-Fi. Le géant de l'énergie français EDF a lancé

La situation pratique de l'Université de Fudan.

également les premiers pilotes à base de réseaux Li-Fi. La montée en puissance du Li-Fi fait jeter un autre regard sur la sécurité des infrastructures informatiques sans fil.

(Par Ronald Eygendaal, principal security consultant chez eygendaals services et qui s'occupe depuis 1990 de protection des informations, de sécurité électronique et technique, de détection des fraudes ainsi que de lutte, de surveillance et de sécurité en particulier. Il est membre du comité de direction de l'Association néerlandaise des professionnels de la sécurité (Vereniging Beveiligingsprofessionals Nederland ou VBN).)

- **www.eygendaals.nl**



Bronnen

http://visiblelightcomm.com/top-10-li-fi-myths/
http://www.lificonsortium.org/
http://alexwiddowson.co.uk/2014/01/08/lifi-wireless-communication/
http://purelifi.co.uk/news/
http://www.het-bar.net/modules.php?name=News&file=article&sid=3093
http://www.engineersonline.nl/nieuws/id21799-lifi-wifi-met-licht.html
http://www.international.to/index.php?option=com_content&view=article&id=13048:visible-light-communication-(vlc)-li-fi-technology-market-worth-$6-138-02-million-2018&catid=309:pitchengine&Itemid=446
http://www.digitalversus.com/mobile-phone/li-fi-smartphone-presented-at-ces-n32333.html