*Titre :* Sécurisation de l’envoie de données sans fils

*Résumé de 1500 caractères, espaces compris :*

La question de sécurisation des données est au cœur du débat sociétal actuel dans un monde où de plus en plus d’appareils sont connectés. Vous n’aimeriez en effet pas apprendre que vos conversations téléphoniques sont mises sur écoute ou que les données de santé transmises par votre montre intelligente soient interceptées.

Dans le cadre de mes travaux de recherche, j’ai mis au point une technique permettant de sécuriser l’envoi de données sans fils. Il faut savoir que lorsqu’on envoie de l’information via une antenne, les ondes vont se propager partout et peuvent donc être **interceptées**. Elles ne sont donc pas sécurisées.

Grâce à ma technique, l’information envoyée depuis un émetteur (une antenne dans la rue par exemple) ne sera compréhensible qu’au récepteur légitime (un téléphone portable, une montre connectée par exemple) et restera brouillée partout ailleurs.

L’idée est de tirer profit des **propriétés physiques de l’environnement**. Lorsqu’on émet des signaux via une antenne, ils arriveront à notre téléphone de manière aléatoire et à des instants différents, en raison des obstacles qu’ils rencontrent sur leurs trajectoires (les immeubles, les véhicules,…). J’utilise ensuite cet aléa pour générer, uniquement entre l’antenne et mon téléphone, une signature spécifique sécurisant la communication. Si un appareil malveillant est présent à un autre endroit, il réceptionnera l’information provenant de l’antenne, mais ne disposera pas de la signature pour pouvoir l’interpréter.

*Contenu : 1495 caractères espaces compris.*