**MT 180s : Sélection du 02.02.2021**

Objectif: 90secondes pour présenter son sujet à un public profane ainsi que parler de ses motivations qui m’ont poussé à participer à ce concours.

En vert : pas indispensable

Bleu : reformuler ou dégager

**Description du sujet de thèse :**

Dans le cadre de mon doctorat, j’ai mis au point une technique novatrice permettant de sécuriser l’envoi de données sans fils à la couche physique.

Il y a deux termes à comprendre dans cet énoncé qui sont *sécurité*  et *couche physique*. Lorsque je parle de sécurité, il est entendu *rendre intelligible une communication d’un point A (dit émetteur) vers un point B (dit récepteur légitime) sans qu’il soit possible d’interpréter ce qui a été envoyé partout ailleurs*.

Lorsqu’on évoque *la couche physique* , on évoque le milieu chargé de la transmission et réception des ondes électromagnétiques (dans mon cas l’air) ainsi que tous les équipements nécessaires, à savoir les antennes, les téléphones portables, les ordinateurs, et autres..

Il faut savoir que lorsqu’on envoie de l’information via une antenne, les ondes vont se propager dans tout l’environnement. Il est par conséquent possible d’intercepter ces ondes à tout endroit de l’espace environnant, ce qui les rend intrinsèquement non sécurisées.

Le schéma que je développe dans mon travail de recherche va tirer profit des propriétés physiques de l’environnement pour sécuriser les communications. Lorsqu’on envoie des ondes à l’émetteur, celle-ci vont être réfléchies dans le milieu qui les entoure (à causes du sol des immeubles, des véhicules par exemple) et seront donc reçues au récepteur légitime en plusieurs répliques à des instants différents. Chaque réplique correspond à un trajet particulier de l’onde causé par les différentes réflexions qu’elle a subie, et l’ensemble de ces répliques peut être caractérisé de manière statistique. L’ensemble des répliques reçues a un comportement aléatoire et c’est ce comportement aléatoire qui permet de générer une clé d’encryption dite *physique* pour sécuriser la communication vers le récepteur légitime. rendant l’information intelligible à l’endroit où on désire communiquer et ininterprétable partout ailleurs. En effet, si un récepteur illégitime est présent pour intercepter l’information envoyée, vu qu’il se situe à un emplacement physique différent du récepteur légitime, il recevra des répliques totalement indépendantes de celle reçues par ce dernier et n’arrivera par conséquent pas à déchiffrer l’encryption physique qui a été utilisée.

La méthode que je développe permet donc de considérablement augmenter le degré de sécurité d’une communication sans fil d’un point à autre, et peut être implémentée en parallèle avec des techniques de sécurité informatiques classiques.

**Motivations :**

1. En tant que doctorant et jeune chercheur, nous avons l’habitude de parler en public mais pas devant un public profane avec un temps imparti si court. Je trouve qu’une qualité primordiale d’un chercheur est de pouvoir vulgariser ses travaux de recherches qui sont à l’état de l’art à un auditoire totalement extérieur au sujet je pars du principe que « *ce qui se conçoit bien s’énonce clairement ».*
2. Ce concours me permettra également de développer de nouvelles comme l’éloquence, la théâtralité, la prestance sur scène et devant une caméra, ou encore la vulgarisation scientifique. J’admire profondément les scientifiques qui parviennent à vulgariser leurs théories les plus compliquées soient-elles car je pars du principe que « *ce qui se conçoit bien s’énonce clairement ».*
3. Finalement, comme j’ai l’ambition de me lancer dans le monde de l’entreprenariat à la fin de mon doctorat, j’estime que savoir capter et attirer l’attention de son public, sur un sujet à la pointe du développement, dans un intervalle de temps aussi restreint est essentiel lorsque l’on veut convaincre des clients ou trouver des investisseurs.

Dans le cadre de mon doctorat, j’ai mis au point une technique novatrice permettant de **sécuriser** l’envoi de données sans fils en utilisant les propriétés physiques de l’environnement.

La sécurisation est entendu ici comme le fait de rendre intelligible une communication exclusivement entre un émetteur A et un récepteur B. Exclusivement, c’est-à-dire sans qu’il ne soit possible de lire l’information envoyée à un point C quelconque.

Il faut savoir que lorsqu’on envoie de l’information via une antenne, les ondes vont se propager dans tout l’environnement et peuvent donc être **interceptées** **partout**, ce qui pose la question de la sécurisation.

Ma technique de sécurisation des communications propose de tirer profit des **propriétés physiques de l’environnement**. Lorsqu’on émet des ondes d’un point A, chacune arrivera en B de manière aléatoire et à des instants différents, en raison des différents obstacles qu’elles rencontrent sur leurs trajectoires. Cet aléa est ensuite utilisé pour générer, uniquement entre A et B, une signature spécifique sécurisant la communication. Si un récepteur illégitime est présent à un endroit C quelconque, il réceptionnera l’information provenant de A, mais ne disposera pas de la signature pour pouvoir interpréter.

1. En tant que doctorant, nous avons l’habitude de parler en public, mais pas devant un public profane avec un temps alloué si court. Je trouve qu’une qualité primordiale d’un bon chercheur est de pouvoir **vulgariser** ses travaux qui sont à l’état de l’art.
2. Ce concours me permettra également de développer de nouvelles compétences : **l’éloquence, la théâtralité, la prestance sur scène et devant une caméra**.
3. J’aimerais me lancer dans l’entreprenariat à la fin de mon doctorat et j’estime que savoir rapidement capter et attirer l’attention de son public, sur un sujet à la pointe du développement, est essentiel lorsque l’on veut **convaincre**.