**Offre de stage en laboratoire entre mars et août 2023 :**

**Expérimentation d'attaques sur des flux de type Metavers sur un réseau 4G/5G**

## Contexte du stage

Une faible latence et un débit élevé sont deux exigences des applications Metavers sur les réseaux 5G (et au-delà). Le terme « Mobile Broadband Reliable Low Latency Communication » (MBRLLC) résume ces exigences pour ces futures applications. Dans ce contexte, il est proposé, dans ce stage, d'étudier le trafic MBRLLC synthétique entre les équipements utilisateurs (UE) et une station de base (BS) 5G dans le cadre d'un comportement adverse dont le but est de perturber la qualité de service (QoS)/qualité d'expérience (QoE) du flux MBRLLC, nuisant ainsi à la disponibilité du service offert.

## Objectif du stage

L'objectif de ce stage de mettre en œuvre une première plateforme expérimentale qui permette de reproduire des attaques de déni de service et/ou réduction de qualité de flux de type Metavers entre un terminal 5G et une station de base.

## Travail attendu

Les différentes étapes du travail à réaliser sont les suivantes :

1. Une étude en profondeur de la littérature scientifique qui permette de comprendre les profils de trafic existants qui peuvent circuler entre les UE et un cœur de réseau 5G et qui correspondent à notre cas d'usage de type flux Metavers ou équivalent.
2. Après une phase de montée en compétences, il s'agira de déployer une plate-forme expérimentale élémentaire qui se compose d'un 5G BS et de plusieurs UE s'appuyant sur les technologies Software-Defined-Radio (SDR) (par exemple, ETTUS B210/N310) et le logiciel OpenAir Interface.
3. Enfin, la dernière partie du stage consistera à explorer les attaques adverses potentielles qui perturbent le comportement « attendu » des communications sur cette plateforme et pour le cas d'usage Metavers que l'on considère ici.

## Compétences nécessaires

Des compétences informatiques pratiques sont indispensables pour la mise en œuvre de la plateforme (au niveau réseau, système et programmation/scripting) ainsi que des compétences en réseau (architecture en couches, réseaux locaux, TCP/IP). Une connaissance du fonctionnement global d'un réseau cellulaire 4G ou 5G est souhaitée. Celle-ci peut être acquise par les Moocs https://www.coursera.org/learn/4g-principes-des-reseaux-mobiles? et https://www.coursera.org/learn/5g-principes-de-fonctionnement. Des connaissances en sécurité et détection d'intrusion en particulier seront appréciées.

## Conditions du stage

Le stage se déroule à IMT Atlantique (site de Rennes) au sein l'équipe ADOPNET de l'IRISA. Le stagiaire aura accès à la plateforme du laboratoire et aux ressources nécessaires pour le travail (poste de travail, ressources bibliographiques, etc.).
La rémunération de stage se situe autour de 530€ par mois.

**Contacts**

Renzo Navas : renzo.navas@imt-atlantique.fr
Georgios Papadopoulos : georgios.papadopoulos@imt-atlantique.fr
Guillaume Doyen : guillaume.doyen@imt-atlantique.fr
Xavier Lagrange : xavier.lagrange@imt-atlantique.fr

**Références**

[1] Park, J. H., Rathore, S., Singh, S. K., Salim, M. M., Azzaoui, A. E., Kim, T. W., ... & Park, J. H. (2021). A comprehensive survey on core technologies and services for 5G security: taxonomies, issues, and solutions. Hum-Centric Comput. Inf. Sci, 11(3).
[2] Lanoue, M., Bollmann, C. A., Michael, J. B., Roth, J., & Wijesekera, D. (2021). An attack vector taxonomy for mobile telephony security vulnerabilities. Computer, 54(04), 76-84.
[3] Chen, C. Y., Hung, G. L., & Hsieh, H. Y. (2020, June). A study on a new type of DDoS attack against 5G ultra-reliable and low-latency communications. In 2020 European Conference on Networks and Communications (EuCNC) (pp. 188-193). IEEE.