

Projet d'Initiation à la Recherche ou Projet d'Innovation-Recherche (barrer)

Nom du laboratoire ou de l'entreprise/établissement :

TUTEUR(S)

NOM-Prénom	Tel	Mel
- Hoger Thomas	06 76 68 63 58	thomas.hoger@laas.fr
-		

Tuteurs INSA si projet industriel:

Prénom NOM
Mel:

TITRE DU PROJET

Mise en place d'attaques dans un réseau 5G

MOT-CLES

Réseaux mobiles, cybersécurité, 5G

DESCRIPTIF (RESUME), indiquer l'enjeu sociétal de l'INSA de Toulouse s'il y a lieu

Les réseaux 5G sont en plein essor et suscitent un intérêt croissant dans le domaine de la recherche, tant pour leur optimisation que pour leur sécurisation. Contrairement aux générations précédentes, la 5G se distingue par une architecture profondément transformée et un fonctionnement beaucoup plus dynamique. Elle repose sur une séparation nette entre deux grandes composantes : le réseau d'accès (notamment les antennes) auquel se connectent les équipements utilisateurs (tels que les téléphones mobiles), et le cœur de réseau, composé de fonctions réseau virtualisées (Network Functions) dédiées à des tâches précises (authentification, gestion de session, routage des paquets, etc.).

Cette nouvelle architecture, pensée pour être modulaire, flexible et personnalisable, ouvre de nombreuses surfaces d'attaque potentielles. Ces attaques peuvent agir aussi bien au niveau de la gestion des fonctions réseau, du plan de contrôle, du plan utilisateur, que du lien physique. Plusieurs travaux ont déjà mis en lumière certaines vulnérabilités mais beaucoup de ces attaques restent pour l'instant à l'état théorique ou ont été explorées de manière superficielle. Par ailleurs, certaines vulnérabilités identifiées ne sont pas entièrement réalistes car elles reposent sur des implémentations non conformes aux standards de la 5G.

Dans ce contexte, les pistes de ce projet d'initiation à la recherche pourront être multiples :

- Réaliser un état de l'art des attaques existantes sur les réseaux 5G, en identifiant les surfaces d'attaque déjà explorées et celles encore peu étudiées.

- Étudier leur faisabilité théorique en regard de la norme 5G.
- Concevoir de nouveaux scénarios d'attaque ciblant des points faibles peu documentés.
- Expérimenter certains de ces scénarios dans un environnement de test.
- Analyser leur impact potentiel sur les infrastructures, et d'explorer des pistes de remédiation ou de renforcement de la sécurité.

PROFIL DES ETUDIANTS SOUHAITE (1 seul choix par projet)

☐ AE-SE : spécialité Automatique-Electronique parcours Systèmes Embarqués

☐ IR-SI : spécialité Informatique parcours Systèmes Informatiques

☐ IR-SC : spécialité Informatique parcours Systèmes Communicants

☐ (optionnel) ce projet peut être proposé à un ou des étudiants d'échange sur la partie réalisation seule (semestre 1 et/ou semestre 2)

PRIORITE : si vous posez plusieurs sujets, indiquer ici la priorité de ce sujet (1= plus prioritaire)