5G-INSIGHT: Intelligent orchestrated security and privacy-aware slicing for 5G and beyond vehicular networks

Project Partners - Partenaires du projet

Country/Pays	Institution	Institution & Lab Logos
France	UGE	
France	UBFC	
France	ULR	
Luxembourg	UNILU	
Luxembourg	LIST	

Project objectives (EN)

The tremendous technological developments in the automotive industry today are mainly fueled by the development of vehicle-to-everything (V2X) communication capabilities and new automated driving features. Given their intrinsic requirements in terms of ultra-low latency and ultra-high reliable connectivity under high-mobility conditions, these features, as well as all the V2X communication services relaying on them, will only be unlocked over the long run with the large-scale adoption of 5G technologies along with the network-slicing paradigm.

Network slicing creates multiple logical instances of the physical network, the so-called network slices, ensuring strict traffic isolation among them, and tailoring the network resources of each slice to a specific (class of) application by leveraging the concepts of software-defined networking (SDN) and network functions virtualization (NFV). It has the potential to enable the coexistence of a wide range of mobile services in the same network infrastructure; however, enabling V2X slicing has brought new security requirements and challenges, which have not been addressed neither by 5G standards nor by automotive standards. Indeed, new slicing attack vectors will be added to traditional attacks on vehicular networks, which might jeopardize their adoption. Vehicular slicing attacks will exploit that weak point of the slicing chain, the vehicles to violate the slice isolation and deteriorate its performance. This might lead to dangerous road situations both for drivers and passengers.

The attacks on vehicular slicing can be more powerful, especially if they will be combined with internal attacks, which are themselves not easy to detect.
In this context, 5G-INSIGHT aims to fill this gap by building novel security mechanisms ranging from attack detection to attack mitigation leveraging novel tools and paradigms such as those based on Machine-Learning (ML), particularly federated and deep learning, to Blockchains and Deception Security, all while considering the specific but very sensitive (in terms of security) case of cross-border areas (i.e., the France-Luxembourg border-crossing case).

Objectives du projet (FR)

Les énormes progrès technologiques de l'industrie automobile actuelle sont principalement alimentés par le développement des capacités de communication véhiculaires (V2X) et par les nouvelles fonctions de conduite automatisée. Compte tenu de leurs exigences intrinsèques en termes de latence ultra-faible et de connectivité ultra-fiable dans des conditions de mobilité élevée, ces fonctionnalités, ainsi que tous les services de communication V2X qui en dépendent, ne seront débloqués à long terme qu'avec l'adoption à grande échelle des technologies 5G et du nouveau paradigme de *network-slicing*.
Le *network-slicing* crée de multiples instances logiques du réseau physique, appelées "tranches de réseau", en assurant une stricte isolation du trafic entre elles et en adaptant les ressources de chaque tranche à une application (ou classe d'applications) spécifique en exploitant les concepts de mise en réseau définie par logiciel (SDN, *software-defined networking*) et de virtualisation des fonctions de réseau (NFV, *network functions virtualization*). Il a le potentiel de permettre la coexistence d'un large éventail de services mobiles dans la même infrastructure réseau ; toutefois, le fait de permettre le découpage en tranches V2X entraîne de nouvelles exigences et de nouveaux défis en matière de sécurité, qui n'ont été abordés ni par les standards 5G ni par les standards automobiles. En effet, de nouveaux vecteurs d'attaque de *slicing* se rajoutent aux attaques traditionnelles sur les réseaux véhiculaires, ce qui pourrait compromettre leur adoption. Les attaques de slicing véhiculaire exploiteront ce point faible de la chaîne de slicing afin de violer l'isolation du slice et ainsi détériorer ses performances. Cela pourrait conduire à des situations dangereuses sur la route, tant pour les conducteurs que pour les passagers. Les attaques contre le slicing véhiculaire peuvent être plus puissantes, surtout si elles sont combinées à des attaques internes, qui ne sont déjà pas faciles à détecter.
Dans ce contexte, le projet 5G-INSIGHT vise à combler cette lacune en mettant en place des mécanismes de sécurité inédits allant de la détection des attaques à leur atténuation en s'appuyant sur des outils et des paradigmes nouveaux tels que ceux basés sur l'apprentissage machine, en particulier l'apprentissage fédéré et approfondi, les Blockchains et la *Deception Security*, tout en considérant le cas spécifique mais très sensible (en termes de sécurité) des zones transfrontalières (c'est-à-dire le cas du passage de la frontière France-Luxembourg).