The post-doctoral fellow will be in charge of real experiments to feed the simulator with real data. The solutions will be designed and implemented by the means of an open access simulator, through for outdoor wireless networks under different attacks.

In this DEPOSIA context, the FUN team is in charge of developing detection and localisation solutions that will constitute the Artificial Intelligence will be based on learning approaches that will correspond to Machine Learning and Deep Learning algorithms. These algorithms will deal with the problems of detecting attacks and locating illicit sources. Due to the multi-layered nature of the data, model aggregation algorithms will be deployed in order to homogenize the decision process.

**Mission confiée**

In this DEPOSIA context, the FUN team is in charge of developing detection and localisation solutions for outdoor wireless networks under different attacks.

The solutions will be designed and implemented by the means of an open access simulator, through a modular approach. Real experiments will be dealt in order to feed the simulator with real data.

**Principales activités**

The post-doctoral fellow will be in charge of:

- Characterization of the scenarios under attacks and definition of types of attacks
- Modeling and implementation of the network in a simulator
- Data collection in both normal working and under attacks
- Data verification
- Localisation algorithms for detected attacks
- Integrations of the developed approaches in real devices
- Participate to the DEPOSIA project (meeting, deliverables, etc.)

**Informations générales**

- **Thème/Domaine:** Réseaux et télécommunications
- **Instrumentation et expérimentation (BAP C)**
- **Ville:** Villeneuve d'Ascq
- **Centre Inria:** Lille - Nord Europe
- **Date de prise de fonction souhaitée:** 2022-03-01
- **Durée de contrat:** 12 mois
- **Date limite pour postuler:** 2022-02-07

**Contacts**

- **Equipe Inria:** FUN
- **Recruteur:** Loscri Valeria / Valeria.Loscri@inria.fr

**A propos d'Inria**

Inria is the French national research institute dedicated to sciences and technologies of the digital world. It employs 2600 people. Its 200 agencies, in general, work in collaboration with companies, laboratories, and academic institutions, which implies the use of 3500 scientific tools for the analysis, detection, and localization of attacks and illicit sources. These tools have a long-term impact on the society.

Inria has a strong relationship with large companies and SMEs. By promoting synergies between researchers and industrialists, Inria participates in the transfer of skills and expertise in digital and technological domains and provides access to the best European and international research for the benefit of innovation and companies, particularly in the region.

For more than 10 years, the Inria Lille - Nord Europe center has been located at the heart of Lille's university and scientific ecosystem, as well as at the heart of Frenchtech, with a technology showroom based on Avenue de Bretagne Lille, on the EuroTechnologies site of economic excellence dedicated to information and communication technologies (ICT).

**Contexte et atouts du poste**

In the context of the DEPOSIA project, the FUN team is in charge of developing detection and localisation solutions for outdoor wireless networks under different attacks. The solutions will be designed and implemented by the means of an open access simulator, through a modular approach. Real experiments will be dealt in order to feed the simulator with real data.

For outdoor cases, we consider drones flying over forbidden areas, communication jammers, spoofing signal transmitters or wireless connected sensors used to introduce false data in monitoring platforms. For indoor cases, we also consider jamming or spoofing sources that can cause denial of service within networks or infrastructures, or fake access points that aim to carry out man-in-the-middle attacks to intercept information. In this proposal, the indoor and outdoor case studies are considered separately in order to design monitoring infrastructures adapted to each case. For the outdoor case, we consider a surveillance architecture that could join the already existing cellular or WLAN communication infrastructures. In particular, with 5G technology and the higher employed frequencies, cellular networks are evolving towards finer meshes and have interfaces with the core network at each of their nodes. Thus, these interface points, equipped with receivers dedicated to monitoring, could enable the routing of monitoring data to centralized platforms, feeding an Artificial Intelligence for analysis, anomaly detection and source geolocation.

For the indoor case, we consider a distributed monitoring architecture deployed within a building based on SDR sensors and a data centralization and synchronization network.

In these two cases, we envisage an Artificial Intelligence working on data evolving in three dimensions: time, space, and direction, all for data of different natures, namely those from the physical layer and the data link layer. Whether for indoor or outdoor configurations, the algorithms that will constitute the Artificial Intelligence will be based on learning approaches that will correspond to Machine Learning and Deep Learning algorithms. These algorithms will deal with the problems of detecting attacks and locating illicit sources. These algorithms will have to take into account: the historical and present character of the attacks and the non-fixed location aspect of the localization of the source of the attack. A first Artificial Intelligence will be dedicated to data analysis and anomaly detection, i.e., highlighting the suspicious nature of the data, and a second Artificial Intelligence will be dedicated to extracting the location information of the attack source. Due to the multi-layered nature of the data, model aggregation algorithms will be deployed in order to homogenize the decision process.

**Consignes pour postuler**

CV + covering letter + letter(s) of recommendation

**Sécurité défense**

Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du...
Avantages
You will integrate a dynamic team of international scientific experts in the field of IoT (http://team.inria.fr/fun/)
You will work on emerging research activities with recognized international IoT and cybersecurity actors.
You will work in a stimulating and pleasant work environment (transport participation (50%), on-site catering, teleworking, leave and special leave of absence (45 days), video conference equipment, technical laboratory for experimentation...)
You can benefit from quality training adapted to your needs and skills, whether technical, methodological or linguistic.
In addition to improving your technical skills, Inria offers you the opportunity to develop your entrepreneurial skills by participating in awareness-raising events and training courses on the creation of start-ups (start-up horizon, intellectual property training, hackath, etc.).
https://www.inria.fr/fr/inria-startup-studio
For international candidates, our administrative services will help you with the various administrative procedures (visa, residence permit, social security, housing, bank, etc.)

Rémunération
2 653 € gross salary (before taxes)