2021-04281 - Post-Doctoral Research Visit
F/M Detection and Localisation of attacks in outdoor wireless networks (M/F)

Type de contrat : CDD
Contrat renouvelable : Oui
Niveau de diplôme exigé : Thèse ou équivalent
Fonction : Post-Doctorant
Niveau d’expérience souhaité : Jeune diplômé

A propos du centre ou de la direction fonctionnelle

The Inria Lille - Nord Europe research centre, created in 2008, employs 360 people including 305 scientists in 15 research teams. Recognised for its strong involvement in the socio-economic development of the Hauts-De-France region, the Inria Lille - Nord Europe research centre pursues a close relationship with large companies and SMEs. By promoting synergies between researchers and industrialists, Inria participates in the transfer of skills and expertise in digital technologies 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 centre 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 in Lille, on the EurA Technologies site of economic excellence dedicated to information and communication technologies (ICT).

Contexte et atouts du poste

In the context of DEPOSIA, an ASTRID/ANR project: Specific Support for Defense research and innovation work - Thematic call for projects on artificial intelligence (https://anr.fr/en/call-for-proposals-details/call/specific-support-for-defense-research-and-innovation-work-thematic-call-for-projects-on-artificial), DEPOSIA focuses on the detection and geolocation of various radio frequency signal sources in order to thwart attacks on connected systems and infrastructures. The sources considered are elements which by their characteristics or their position, present an illicit character and which threaten the people security or the infrastructures. For outdoor cases, we consider drones flying over forbidden areas, telecommunication 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 use cases 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 algorithms. These algorithms will deal with the problems of detecting attacks and locating illicit sources. These algorithms will have to take into account: the evolutionary aspect brought by the non-fixed character in time 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.

Mission confiée

In this DEPOSIA context, the FUN team is in charge of developing detection and localization 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

Informations générales

- Thème/Domaine : Réseaux et télécommunications
- Instrumentation et expérimentation (BAP C)
- Ville : Villeneuve d’Ascq
- Centre Inria : CRI Lille - Nord Europe
- Date de prise de fonction souhaitée : 2022-03-01
- Durée de contrat : 2 ans
- Date limite pour postuler : 2022-01-07

Contacts

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

A propos d’Inria

Inria est l’institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3500 scientifiques pour relever les défis du numérique, souvent à l’interface d’autres disciplines. L’Institut fait appel à de nombreux talents dans plus d’une quarantaine de métiers différents. 900 personnels d’appui à la recherche et à l’innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 180 start-up. L’institut s’efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l’économie.

L’essentiel pour réussir

We are looking for a candidate that owns a PhD in computer science, who is creative in proposing solutions, capable of critical analysis of results and leading research activities. We demand the candidate:

1) to be curious and interested in new technologies
2) to have excellent skills in scripting and programming (e.g., python, C/C++, java, ROS) as well as previous experience with simulation and experimentation tools;
3) to have a strong background in mobile networks and forwarding protocols;
4) to be fluent in spoken and written English with strong communication and presentation skills;
5) to be autonomous, open minded, team working, sense of organization and rigor;
6) experience with mobility modeling, localisation algorithms and resource management for wireless networks are considered a plus.

Consignes pour postuler

CV + covering letter + letter(s) of recommendation

Sécurité défense :
- 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
- Integration of the developed approaches in real devices
- Participate to the DEPOSIJA project (meeting, deliverables, etc.)

**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, hackAthec, 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)

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 recrutement.

**Politique de recrutement :**

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.

**Attention**: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d’autres canaux n’est pas garanti.