# 2021-03264 - PhD Position F/M Automation of attack mitigations in 5G environments

**Type de contrat :** CDD
**Niveau de diplôme exigé :** Bac + 5 ou équivalent
**Fonction :** Doctorant

## Contexte et atouts du poste

The PhD position is proposed by the RESIST team of the Inria Nancy Grand Est research lab, the French national public institute dedicated to research in digital Science and technology. The team is one of the European research group in network management and is particularly focused on empowering scalability and security of networked systems through a strong coupling between monitoring, analytics and network orchestration. https://team.inria.fr/resist/

This work is in the context of the H2020 AI@EDGE project (A Secure and Reusable Artificial Intelligence Platform for Edge Computing in Beyond 5G Networks starts in January, 2020) involving partners all around Europe. This project will bring different use cases for testing solutions. The student will actively contribute to the project and will have the opportunity to work with the different partners. It also includes traveling in Europe.

## Mission confiée

**Scientific context:**

Nowadays, cybersecurity is a major concern everywhere with the growth of connected devices that are beyond common computers. People are connected using their smartphones but also with Internet-of-Things (IoT) devices. Everything tends to be connected in buildings, cars, factories, cities, airplanes... with all the risks that induces. To circumvent these problems, decades of research and development have led to build new techniques and tools to fight back to the attacks over Internet. Nonetheless, the number of attacks and their magnitude still grow. The attack surface continues to increase along with number of connected devices but also due to the number of application, services or software that make the IT ecosystem far from its origin today. Indeed, in the early 2000, most of services over Internet were static webpages while today services are of various kind: video streaming, online gaming, IoT traffic, messaging, voice over IP, webconferencing, blockchain... New type of attacks and threats will continuously occur.

Techniques used by both the attackers and defenders evolve to complex mechanisms [4]. It leads to massive use of encryption to avoid data leaks but simultaneously attackers can benefit from massive encryption to hide their own activities. From simple regular expression machines in firewalls, anomaly detection method relying on artificial intelligence is a vast topic both in research and in industry [1,2]. Attackers also can leverage machine learning [3].

As a result, guaranteeing a high level of security is very challenging. New methods to counteract against new threats and attacks will be proposed. However, a practical problem is to properly use the arsenal of all these techniques: What to use? For which purposes? When? How to configure it? What should be given as inputs... Hence, a large set of questions remain even if you assume that you have all possible techniques at your disposal. Unfortunately security is still mostly manual or only assisted. Developing an autopilot for managing the security of connected systems is an ultimate goal but highly challenging.

## Principales activités

**Objectives**

This thesis aims at proposing a framework and techniques to empower the automation of network security assuming a highly dynamic environment, in particular Mobile-Edge Computing infrastructure and 5G. In such an environment, resources are virtualized and shared among users with an underlying high volatility and changes in resource allocations and needs. Globally, the context of where the security must be enforced is continuously evolving. Unfortunately, developed techniques using artificial intelligence for network security assumes quite homogeneous environment. They may require extensive datasets and long learning time to produce accurate models. So, they are not tailored fog highly changing and volatile environments. More generally, the security configuration using AI techniques but also more standard techniques must be dynamically reconfigured.

In this thesis, the student will thus consider a very volatile environment in terms of topology, services, applications and traffic. Even the attacker has various strategies they can switch between. Regular optimization techniques to find best arrangements between configurations are not anymore possible. To address the proposed challenge, (Deep) Reinforcement Learning will be considered as a first direction. Several propositions already exist [5] but they are still used in restricted environments (for example focused on a particular scenario or protocol). So, the student will have to research on (1) defining a model to describe the potential action in terms of security assuming an heterogeneous set, (2) leverage (deep) reinforcement learning to deduce automatically the proper counter-measures to tackle a single attack and (3) extend this solution to a very volatile environment and so adapt the DRL technique to have a good-tradeoff between security and resources. The PhD student will evaluate his or her solution on different scenarios.

This work is in the context of the H2020 AI@EDGE project (A Secure and Reusable Artificial Intelligence Platform for Edge Computing in Beyond 5G Networks starts in January, 2020) involving partners all around Europe. This project will bring different use cases for testing solutions. The student will actively contribute to the project and will have the opportunity to work with the different partners. It also include traveling in Europe.

[1] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016, doi: 10.1109/COMST.2015.2494502.

[2] R. Boutaba, M. A. Salahuddin, N. Limam, S. Ayoubi, N. Shahriar, F. Estrada-Solano, and O. M. Caicedo. A comprehensive survey on machine learning for networking: evolution,

## Informations générales

- **Thème/Domaine :** Réseaux et télécommunications
  Système & réseaux (BAP E)
- **Ville :** Villers lès Nancy
- **Centre Inria :** CRI Nancy - Grand Est
- **Date de prise de fonction souhaitée :** 2021-05-01
- **Durée de contrat :** 3 ans
- **Date limite pour postuler :** 2021-02-14

## Contacts

- **Equipe Inria :** RESIST
- **Directeur de thèse :**
  François Jérôme / jerome.francois@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

Applications are to be sent as soon as possible.

Starting date: February 2021 or later

**How to apply**

Upload your file on jobs.inria.fr in a single pdf or zip file, and send it as well by email to jerome.francois@inria.fr and abdelkader.lahmadi@loria.fr. Your file should contain the following documents:

- Your CV
- A cover/motivation letter describing your interest in this topic
- A short (max one page) description of your Master thesis (or equivalent) or of the work in progress if not yet completed.
- Your degree certificates and transcripts for Bachelor and Master (or the last 5 years).
- Master thesis (or equivalent) if it is already completed and publications if any (it is not expected that you have any). Only the web links to these documents are preferable, if possible.
- In addition, one recommendation letter from the person who supervises(d) your Master thesis (or research project or internship) should be sent directly by his/her author to jerome.francois@inria.fr and abdelkader.lahmadi@loria.fr

## Consignes pour postuler

**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

applications and research opportunities. Journal of Internet Services and Applications, 9(1):16, Jun 2018.

[3] Z. Abaid, M. A. Kaafar, and S. Jha. Quantifying the impact of adversarial evasion attacks on machine learning based android malware classifiers. In International Symposium on Network Computing and Applications (NCA). IEEE, 2017.

[4] I. Friedberg, F. Skopik, G. Settanni, and R. Fiedler. Combating advanced persistent threats: From network event correlation to incident detection. Computers & Security, 48:35 – 57, 2015.

[5] N. C. Luong et al., "Applications of Deep Reinforcement Learning in Communications and Networking: A Survey," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3133-3174, Fourthquarter 2019, doi: 10.1109/COMST.2019.2916583.

## Compétences

· Required qualification: Master in computer science
· Required knowledge: networking (protocols, architecture), network security (common attack and defense mechanisms), programming (python, java or others...)
· Knowledge and skills in the following fields will be appreciated: machine learning, artificial intelligence, big data, Linux (command line use, shells)

## Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

## Rémunération

Salary: 1982€ gross/month for 1st and 2nd year. 2085€ gross/month for 3rd year.

Monthly salary after taxes : around 1596,05€ for 1st and 2nd year. 1678,99€ for 3rd year. (medical insurance included).

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.