Offer #2024-07773

PhD Position F/M Anomaly and attack detection in the IoT paradigm

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

About the research centre or Inria department

The Inria University of Lille 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 University of Lille 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 University of Lille 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 EuraTechnologies site of economic excellence dedicated to information and communication technologies (ICT)

Context

The PhD student will be co-supervised by Valeria Loscri (FUN Team) and Kevin Jiokeng (École Polytechnique).

The Inria FUN research group investigates solutions to enhance programmability, adaptability and reachability of FUN (Future Ubiquitous Networks) composed of RFID, wireless sensor and robot networks. Limited resources, and high mobility evolving in distrusted environments characterize the objects that compose FUN. They communicate in a wireless way. To be operational and efficient, such networks have to follow some self-organizing rules. Indeed, components of FUN have to be able in a distributed and energy-efficient way to discover the network, self-deploy, communicate, self- structure in spite of their hardware constraints while adapting the environment in which adapting the environment in which they evolve. For additional information on the FUN research group, please see http://team.inria.fr/fun/

Assignment

The ubiquitous deployment of Internet of Things (IoT) devices, make this technology a key actor of our daily activities, by enabling advanced services and applications that could not be imagined few years ago. This PhD will be in the context of a National project, NEMIoT (NEtwork Methods for IoT). This project aims at developing new methods to increase trust in IoT devices before and after their deployment on existing network infrastructures. Although many efforts have been made in securing IoT devices with regards to hardware, software, trustworthiness, data leaking, interoperability, or privacy, relatively little has been made on the issue of the availability of existing and expected services following the introduction of a (fleet of) new IoT device(s) (e.g., massive access problem) [1, 2]. After deployment, IoT devices may remain vulnerable and prone to abnormal behavior that needs to be quickly identified and mitigated. The characterization of the IoT devices and their traffic, to identify if it is normal/anomalous or under attack, will revolve on Machine Learning approaches [3].

The primary objective is developing original cross-layer solutions to finely and quickly detect and/or mitigate potential anomalies resulting from the introduction of IoT devices.

Expected outcomes

The specific outcomes will be new methods and tools resorting to a cross-layer approach, to finely characterize the activity of IoT nodes, to detect eventual anomaly behaviors, and ultimately to identify the root cause of these anomalies.

Main Activities

- Study of the State of Art of anomaly/attack detection in IoT systems
- Characterization of IoT devices behavior through Machine Learning approaches
- Design of new cross-layer detection approaches in IoT architectures
- Validation of the solutions via simulation and experiments

Additional activities :

- Writing reports
- Participation to the deliverables writing

References:

[1] Emilie Bout, Valentin Bout, Alessandro Brighente, Mauro Conti, Valeria Loscri. Evaluation of Channel Hopping Strategies Against Smart Jamming Attacks. IEEE ICC 2023 - IEEE International Conference on Communications, IEEE, May 2023, Rome, Italy.

[2] E. Bout, V. Loscri and A. Gallais, "HARPAGON: An Energy Management Framework for Attacks in IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 20, pp. 19959-19970, 15 Oct.15, 2022, doi: 10.1109/JIOT.2022.3172849.

[3] E. Bout, V. Loscri and A. Gallais, "How Machine Learning Changes the Nature of Cyberattacks on IoT Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 248-279, Firstquarter 2022, doi: 10.1109/COMST.2021.3127267.

Skills

Skills

Technical skills and level required :Programming skills on C++, Python and Matlab

Languages : English or French

Relational skills :Capacity to work in team

Benefits package

- 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 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

Remuneration

1st and 2nd year : 2100 € (gross monthly salarye)

3rd year : 2190 € (gross monthly salary)

General Information

- **Theme/Domain :** Networks and Telecommunications
  System & Networks (BAP E)
- **Town/city :** Villeneuve d'Ascq
- **Inria Center :** Centre Inria de l'Université de Lille
- **Starting date :** 2024-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2024-07-14

Contacts

- **Inria Team :** FUN
- **PhD Supervisor :**
  Loscri Valeria / Valeria.Loscri@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.