The Inria Lille - Nord Europe Research Centre was founded in 2008 and employs a staff of 320, including 280 scientists working in fourteen research teams. Recognised for its outstanding contribution to the socio-economic development of the Hauts-de-France region, the Inria Lille - Nord Europe Research Centre undertakes research in the field of computer science in collaboration with a wide range of academic, institutional and industrial partners.

The strategy of the Centre is to develop an internationally renowned centre of excellence with a significant impact on the City of Lille and its surrounding area. It works to achieve this by pursuing a range of ambitious research projects in such fields of computer science as the intelligence of data and adaptive software systems. Building on the synergies between research and industry, Inria is a major contributor to skills and technology transfer in the field of computer science.

Contexte et atouts du poste
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, high mobility and high security level 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 to improve efficiency and energy-efficient way to discover the network, to deploy, communicate, self-structure in spite of their hardware constraints while adapting the environment in which they evolve. For additional information on the FUN research group, please see http://team.inria.fr/FUN/

Context
Cooperation and coexistence of heterogeneous technologies and devices play a key role to realize ubiquitous and pervasive networks. Generally, the cooperation among heterogeneous devices is based on information acquired through the communication among the nodes. "Traditional" communication paradigms are based on link through electromagnetic fields waves (i.e. electromagnetic radiation), but alternative communication paradigms can be envisaged to improve efficiency, energy consumption and ubiquitous concept. For example, Visible Light Communication (VLC) has emerged as an alternative wireless communication paradigm, able to simultaneously exploit the illumination infrastructure and the light sources for transmission.

Among the different advantages of alternative communication paradigms are:

1) An environment where a "traditional" communication paradigm is difficult (e.g. environments too noisy with too many interferences);
2) Data rate could be higher than traditional communication (e.g. as in the case of the VLC paradigm);
3) The possibility to design and implement "smart" devices, that could adaptively select the best way to communicate based on their proper current status, the status of the neighbors and the surrounding conditions
4) The integration of mechanisms to make the communication system robust to attacks (e.g. Denial-of-Sleep attacks, eavesdropping).

Topic:
The objective of this thesis is to focus on both traditional wireless communication and alternative communication paradigm such as VLC and study the new security issues and new potentiality the co-existence and interaction of these different paradigms arise.

The first step will consist in the accurate revision of the state of the art in terms of advanced cyber-attacks against "traditional" wireless networks and VLC. The candidate will identify the specific new vulnerabilities related with the co-existing solutions of "traditional" and new wireless paradigm. He/She will investigate the potentiality to exploit the co-existence and the interaction as an effective solution for the most known attacks. The solutions will be evaluated from a theoretical/simulation point of view and will be also integrated in the testbeds developed in the FUN team.

He/She will benefit from the background and expertise of the team in this context, acquired in the last years and that dealt with the implementation of two testbeds [1], [2], [3], [4], [5].

The doctoral program will be devoted to the design and implementation co-existing communication protocols. The PhD candidate will analyse and identify some specific evaluation parameters, in order to define the goodness of the protocol and the critical issues in terms of security, by analyzing some specific types of attacks such as for instance Denial-of-Sleep attacks, eavesdropping [6]. Moreover, new types of smart attacks, able to exploit the specific vulnerabilities identified will be implemented ad-hoc and their impact on the system will be evaluated. Based on the results of this activity, new detection mechanisms and approaches for mitigate the identified vulnerabilities, will be designed and integrated in the whole wireless communication system.

• Listening and communicating with non-technical contacts;
• Teamwork taste
• Sense of organization, autonomy, rigor

Required qualities
• In-depth interest in scientific problems and the motivation for independent and goal-oriented research
• The willingness to contribute to interdisciplinary scientific projects
• Ability to implement code on real devices
• Very good programming skills in C/C++/Python, Experience using Linux systems

Skills
- Very good programming skills in C/C++/Python, Experience using Linux systems
- Ability to implement code on real devices
- The willingness to contribute to interdisciplinary scientific projects
- In-depth interest in scientific problems and the motivation for independent and goal-oriented research

Mission confiée
Under the direct responsibility of the supervisor, the candidate will be in charge to analyze and design coexistence and interaction between solutions with preexisting communication techniques (e.g. WiFi, Bluetooth, etc.) and Visible Light Communication paradigm. The candidate will analyze and study new potential threats deriving by the interaction of different wireless paradigms and will design specific attacks exploiting these vulnerabilities. Based on these attacks, new effective detection mechanisms and more robust protocols need to be designed and implemented. The candidate will validate theoretical solutions through simulation and proof-of-concept approaches based on implementation on real devices.

Principales activités

Time Schedule
Year 1
M0-M3: The PhD student will spend 2-3 months to survey the state of the art in terms of alternative communication paradigms also regarding the type of security attacks in the context of the IoT networks.
M4-M8: Based on the analysis and study of the literature, the student will focus on a specific alternative paradigm and will design a novel communication protocol, in order to make mobile devices able to communicate in the most efficient and secure way. The candidate will need to study and individuate the limitations and the criticism of the specific communication protocol also under specific networks attacks.
M9 – M12: The candidate will study the specific application scenarios that could put the communication system in crisis (e.g., by individuating specific types of interference or condition where the communication fails). At the end of the Year 1, the candidate should have acquired the theoretical background and knowledge to effectively design and develop communication techniques based on a different communication paradigm.

Year 2
M13 – M18: Based on the communication protocols developed, the candidate will design and implement cooperation techniques among the mobile nodes.
M19-M24: The candidate will evaluate the results of the cooperation techniques both theoretically and by the means of simulation tools. Based on the communication protocols developed, the candidate will design and implement cooperation/coexistent/interacting techniques among the mobile devices.
At the end of the Year 2 the candidate should have acquired the competencies to design and implement cooperation techniques based on a new communication paradigm and to individuate and recognize the limitations of a similar system.

Year 3
M25 - M27: The candidate will design and implement specific attacks exploiting the vulnerabilities identified in the coexistent and interacting wireless networks. The impact of the attacks will be analyzed both from a simulation point of view and on real devices. Moreover, new detection mechanisms and enhanced communication approaches for improving the robustness will be studied and integrate in the system.
M28-M36: The last six months will be devoted to the validation of the results achieved, both theoretically and via simulation, through the implementation of the techniques on the real robotic platform and to the evaluation of the performance in different scenarios and under different conditions.
At the end of the Year 3 the candidate should have acquired the competencies to propose adaptive real-time approaches, specifically addressing two different communication paradigms (the new selected and the “traditional” one based on electromagnetic fields waves) that coexist in a unique device. He/She is also supposed to have acquired the capabilities to test the effectiveness of the system in a real scenario. The candidate will be also asked to be able to create specific and critical scenarios in order to test the platform in “difficult” and critical situations.

Compétences
- Sense of organization, autonomy, rigor
- Teamwork taste
- Listening and communicating with non-technical contacts;
• Know write notes / reports
• Good knowledge of English

Required Diploma and experience: One among the following master or engineer degree is expected: Electrical, Electronic Engineer, Telecommunication Engineer, Computer Science, Informatics, or a related discipline.

**Avantages**

You will integrate a dynamic team of international scientific experts in the field of IoT ([http://team.inria.fr/fun/](http://team.inria.fr/fun/))

You will work on emerging research activities with recognized international cybersecurity actors in the context of European collaborations and projects of the FUN team.

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, hackAthon, etc.). [https://www.inria.fr/fr/inria-startup-studio](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**

1st and 2nd year: 1593.50€ Net monthly salary (after taxes)

3rd year: 1676.31€ Net monthly salary (after taxes)