Offer #2023-06895

Post-Doctoral Research Visit F/M Post-Doctoral Research Visit F/M A tamper-proof distributed ledger for V2X communications audit

**Contract type:** Fixed-term contract

**Level of qualifications required:** PhD or equivalent

**Function:** Post-Doctoral Research Visit

**Level of experience:** From 3 to 5 years

**Context**

This postdoctoral position is part of the national PEPR (Programme et Equipement Prioritaire de Recherche) 5G NF-FITNESS project, coordinated by Daniel Koman, IMT. The PEPR involves several teams from various institutes (CEA, IMT, INRIA, Eurecom, CNRS, Centrale Supelec, INP Toulouse, Nantes Université, ESIEE Paris-UGE). The position is funded for 18 months, and will be conducted at Inria Lille - Nord Europe under the supervision of Nathalie Mitton (Inria) and Patrick Sondi (IMT Nord Europe). This is a postdoctoral position in Vehicle-to-Everything (V2X) communications, more specifically in security and audit of V2X communications.

The starting date is flexible with a potential start from Feb. 1st, 2024.

**Assignment**

Several technical means exist and are already used in communication networks and telecommunication infrastructures, including electronic certificates, to guarantee authentication, confidentiality, integrity and non-repudiation. The literature shows how identification mechanisms such as electronic certificates can be applied to ad hoc networks in general and to vehicle networks in particular [1]. They are usually accompanied by pseudonym assignment mechanisms in order to avoid the correlations that could be made from the identification if it were directly exposed in several contexts, and thus preserve the privacy of users participating in cooperative applications during their D2X or V2X electronic communications. However, cooperative applications rely on D2X and V2X communications that take place in the public domain. Indeed, in the physical domain, if we consider the example of road traffic, the privacy of road users does not call into question the fact that all vehicles on the road must have license plates visible to all. This offers a possibility for third parties, including insurance companies and judicial authorities, to trace the perpetrator of an offense on the basis of visual evidence from the victim or other persons who witnessed the scene. There is no reason for which this should not apply to the digital domain. For example, when a road user sends a message to the rest of the traffic via a V2I communication, the car manufacturer has the means to keep track of it if it goes through the on-board computer, the telecommunication operator has a public mandate to keep track of it in its network, and similar devices allow application publishers to keep track of it in their logs. Thus, as soon as V2V communications occur in the context of road traffic and may have consequences there, the technical means for identifying the vehicles involved (perpetrator, victim or witnesses) must exist, regardless of the procedures that will be established by the legislator to regulate their use. Recently, a broad survey of the scientific literature has pointed out the necessity of developing a new approach based on a distributed digital ledger in order to achieve a tamper-proof database capable of ensuring the audit of every V2X communications including those occurring in 5G D2D/V2V mode. The FUN team is currently developing this approach in collaboration with IMT Nord Europe in the context of every vehicular communication technologies, and they need to develop and evaluate these contributions specifically in the context of 5G technology.


**Main activities**

In the present post-doctoral project, a first objective will be to formalize and develop a distributed digital
ledger through every network components of a 5G/6G deployment in the context of Vehicle-to-everything communications. The second objective will be to design and develop a framework for evaluating the contributions of the team members in every identified scenarios and use cases that the candidate will contribute to define also. This post-doctoral project will take place in the FUN project-team at the Inria research center of Lille at Villeneuve d’Ascq. Moreover, it will be conducted in close collaboration with our cybersecurity partner at IMT Nord Europe.

Skills

- Knowledge in wireless networks and edge computing
- Skills in Simulation tools and development
- Skills in C and python
- English speaking
- Autonomy
- Open minded
- Team working

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

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: 2024-02-01
- Duration of contract: 1 year, 7 months
- Deadline to apply: 2024-01-06

Contacts

- Inria Team: FUN
- Recruiter: Mitton Nathalie / Nathalie.Mitton@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.

The keys to success

We are looking for a candidate that has a PhD in computer science who is creative in proposing solution solutions and capable of critical analysis of results. 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 tools (MatLab or NS3 or OMNET++, Multichain (is a plus).
- 3) to have a strong background in mobile networks, Computer security, Wireless and Mobile Networks. Knowledge in Blockchain is a plus
- 4) to be fluent in spoken and written English with strong communication and presentation skills.
- 5) to be a pleasant team worker (verbal communication, active listening, motivation and commitment)

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
**Instruction to apply**

Please send us your CV and Cover letter.

**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.