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

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : CDD

Niveau de diplôme exigé : Thèse ou équivalent

Fonction : Post-Doctorant

Niveau d'expérience souhaité : De 3 à 5 ans

Contexte et atouts du poste

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-U). 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.

Mission confiée

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.


Principales activités
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.

Compétences

- 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

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 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

Informations générales

- Thème/Domaine : Réseaux et télécommunications
  Système & réseaux (BAP E)
- Ville : Villeneuve d'Ascq
- Centre Inria : Centre Inria de l'Université de Lille
- Date de prise de fonction souhaitée : 2024-02-01
- Durée de contrat : 1 an, 7 mois
- Date limite pour postuler : 2024-01-06

Contacts

- Équipe Inria : FUN
- Recruteur : Mitton Nathalie / Nathalie.Mitton@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 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 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 200 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 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)
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.

Consignes pour postuler

Please send us your CV and Cover letter.

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 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.