



**Offer #2024-08357**

## **STAGE MASTER 2 - Sécurisation des échanges dans les protocoles pour véhicules connectés**

*The offer description below is in French*

**Contract type :** Internship agreement

**Level of qualifications required :** Graduate degree or equivalent

**Fonction :** Internship Research

### **Context**

*Ce sujet s'inscrit dans le dispositif PhD tracks du centre Inria de l'Université de Lorraine et antenne de Strasbourg. Ce dispositif vise à attirer et accompagner des éléments prometteurs et motivés, inscrits actuellement en Master 2, vers le doctorat en proposant un financement couplé de quatre ans couvrant stage de Master2 + thèse. Le stage de Master 2, d'une durée de 5 à 6 mois, sera gratifié à 4.35 €/heure (plus ou moins 670 €/mois). Les candidats admis dans le dispositif présenteront en mai 2025 l'avancement de leurs travaux devant un jury qui validera l'entrée en thèse (l'arrêt du PhD track devrait être exceptionnel).*

*Ce dispositif, le mode de candidature et le calendrier sont décrits dans l'onglet PhD track du site <https://www.inria.fr/fr/centre-inria-universite-lorraine>*

### **Dans le cadre d'un partenariat**

- collaboration entre 2 équipes Inria : RESIST et CARAMBA,

Contexte :

Les véhicules connectés utilisent des protocoles de communication basés sur Ethernet pour les échanges de données entre les composants intra-véhiculaire (moteur, capteurs, divertissement, affichage, etc). Traditionnellement, ces communications utilisent des protocoles comme CAN ou LIN. En revanche, des passerelles sont nécessaires entre ces composants pour garantir l'interopérabilité entre leurs échanges. Un modèle de communication basé sur Ethernet simplifie ces architectures de communication et réduit également les besoins en câblage. Cette communication basée sur Ethernet opère sur des fonctions critiques et sensibles d'un véhicule (freinage, gestion moteur, fonctions d'assistance à la conduite, etc.). Pour cette raison, il est besoin d'utiliser un protocole déterministe capable de garantir une base latence et une bande passante suffisante. Cette communication basée sur Ethernet, doit également garantir la sécurité de ces véhicules connectés qui un enjeu majeur pour leur adoption et garantir un usage de confiance [KE21, EBN+21]. On s'intéressera donc dans ce stage d'une part au protocole de communication dédié à la voiture connectée, notamment le protocole Time-sensitive networking (TSN) [ALD+21] et à assurer un minimum de confidentialité dans les échanges en chiffrant et/ou authentifiant le contenu des messages échangés. Il s'agira donc d'intégrer des solutions à bas coût de cryptographie pour faire du chiffrement authentifié sur la pile TSN et à comparer les résultats de performance obtenus.

Références

[ALD+21] Mohammad Ashjaei, Lucia Lo Bello, Masoud Daneshtalab, Gaetano Patti, Sergio Saponara, and Saad Mubeen. Time-sensitive networking in automotive embedded systems : State of the art and research opportunities. *Journal of Systems Architecture*, 117 :102137, 2021.

[EBN+21] Doğanalp Ergenç, Cornelia Brühlhart, Jens Neumann, Leo Krüger, and Mathias Fischer. On the security of IEEE 802.1 time-sensitive networking. In *2021 IEEE International Conference on Communications*

## Assignment

TSN est décrit dans un standard 1 pour offrir des fonctions et d'extensions de sûreté au protocole Ethernet (IEEE 802.1) pour l'industrie de l'automobile. Les piles de communication sont disponible pour Linux 2, FreeRTOS et Zephyr et également sur du matériel embarqué à l'image des plateformes NXP3 (plateforme i.MX RT1170 EVK board : 4) ou Texas Instrument 5 . L'objectif de ce stage est d'étudier comment intégrer à cette pile protocolaire quelques finalistes d'algorithmes cryptographiques de la compétition "lightweight" du NIST (voir : <https://csrc.nist.gov/Projects/lightweight-cryptography/finalists>). Ensuite, il s'agira de produire une proof-of-concept entre deux entités afin d'étudier les métriques classiques réseaux (débit, latence, énergie, etc.) pour savoir quels est le chiffrement le plus adapté. Ce stage pourra être suivi d'une thèse sur le même sujet : la sécurité des véhicules connectés et le protocole TSN.

1. <https://1.ieee802.org/tsn/>
2. <https://tsn.readthedocs.io>
3. [https://github.com/NXP/GenAVB\\_TSN](https://github.com/NXP/GenAVB_TSN)
4. [https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/imx-processors/178770/1/NXP\\_GenAVB\\_TSN\\_Stack\\_FreeRTOS\\_5](https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/imx-processors/178770/1/NXP_GenAVB_TSN_Stack_FreeRTOS_5). <https://github.com/TexasInstruments/enet-tsn-stack>

## Main activities

L'objectif de ce stage est d'étudier comment intégrer à cette pile protocolaire quelques finalistes d'algorithmes cryptographiques de la compétition "lightweight" du NIST (voir : <https://csrc.nist.gov/Projects/lightweight-cryptography/finalists>). Ensuite, il s'agira de produire une proof-of-concept entre deux entités afin d'étudier les métriques classiques réseaux (débit, latence, énergie, etc.) pour savoir quels est le chiffrement le plus adapté. Ce stage pourra être suivi d'une thèse sur le même sujet : la sécurité des véhicules connectés et le protocole TSN.

## Skills

Etudiant en M2 Informatique.

## Benefits package

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail (après 6 mois d'ancienneté) et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)
- Accès à la formation professionnelle
- Sécurité sociale

## Remuneration

Gratification de stage : 4,35 €/heure (plus ou moins 670 €/mois)

Rémunération de la thèse : 2100 € brut/mois la 1ère année

## General Information

- **Theme/Domain** : Security and Confidentiality System & Networks (BAP E)
- **Town/city** : Villers lès Nancy
- **Inria Center** : [Centre Inria de l'Université de Lorraine](#)
- **Starting date** : 2024-03-01
- **Duration of contract** : 6 months
- **Deadline to apply** : 2024-12-01

## Contacts

- **Inria Team** : [CARAMBA](#)
- **Recruiter** :  
Minier Marine / [marine.minier@loria.fr](mailto:marine.minier@loria.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

Conditions du Stage. Le stage se déroulera au sein du Laboratoire d'Informatique Lorrain (le LORIA) à Nancy et sera gratifié à hauteur d'environ 473 euros par mois.

Contact. Pour candidater, contactez Abdelkader Lahmadi et Marine Minier (voir ci-dessus) en joignant :  
— un CV,  
— les relevés de notes des deux dernières années,  
— une liste des cours suivis lors de l'année universitaire, ainsi que les noms des responsables de ces cours.

**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.