The offered position is proposed by the RESIST team of the Inria Nancy Grand Est research lab, the French national public institute dedicated to research in digital Science and technology. The team is one of the European research group in network management and is particularly focused on empowering scalability and security of networked systems through a strong coupling between monitoring, analytics and network orchestration.

https://team.inria.fr/resist/

This work is in the context of the HiSec project. The HiSec project is part of the 5G PEPR founded by the ANR, which focuses on cyber-security issues in future networks. These networks have played a key role in service delivery for digital infrastructures. These new networking technologies have also penetrated essential and critical services for our daily lives, such as energy, transportation or healthcare. The pervasive use of digital services and networks to control these critical infrastructures significantly increases the attack surface and the opportunities for attackers. We regularly observe attacks against these infrastructures, leading to successful compromise and very significant impacts. The objective of the HiSec project is thus to handle cybersecurity issues in these environments, and propose new mechanisms to protect these networks and detect attacks, attacks against the networking infrastructure itself, or against the services hosted or the users of the network.

**Mission confiée**

Smart objects of 5G/6G networks are exposed to a large variety of attacks. Their protection is challenged by their resource constraints in terms of CPU, memory and energy. Security chains, composed of network functions, such as firewalls, intrusion detection systems and data leakage prevention mechanisms, offer new perspectives to protect these devices using software-defined networking and network function virtualization. However, the complexity and dynamics of these chains require new automation techniques to orchestrate them, more specifically when the security functions are offloaded at the network edge.

The objective of this PhD thesis is to automate and verify the building and off-loading of chains of security functions at the edge level, in the context of 5G/6G networks. Depending on contextual changes, such as new security threats, resource degradations and network failures, the security chains may be subject to different off-loading strategies including the transfer, merging and splitting of network functions and their rules. The approach aims at enabling a high level of automation by formally verifying these strategies to make sure that they do not impact on the performance and the security properties of the orchestrated chains and should take into account the knowledge and experience from the different network edges. Moreover, it is well known that formal methods themselves have an exponential complexity both in terms of running time and in terms of resource consumption, which strongly hinder their actual deployment for runtime verification in the network.

**Principales activités**

Several axes are envisioned to cover this issue, first of all we can exploit our knowledge of networking and programmability technologies to design domain specific decision procedures specially optimized for considered use cases. A second axis of research would be the parallelization and distribution of the tasks of verification. Indeed, it is often possible to identify independent parts of the model that can be verified in parallel, leading to a more efficient verification in terms of response time. It would then become possible to design the integration of solvers at different levels into the network architecture to verify the correct properties, while preserving network performances, in particular it could be interesting to consider verification methods relying on partially specified systems in order to work with the highly dynamic nature of most 5G and 6G devices.

The expected results include a state-of-the-art with respect to the topic, the identification of one or several specific use case(s), the specification of the decision problem related to this/these use case(s), the proof of it/them class(es) of computational complexity and some related results, the specification and implementation of dedicated decision procedures for solving this problem and some reproducibility packages showing their practical efficiency against baseline approaches, as well as a network architecture integrating these solvers and some reproducibility package showing its practical feasibility.

**References**


Compétences
- Required qualification: Master in Computer Science / Engineering Degree in Computer Science
- Required knowledge: solid knowledge in computer science and networking, Interest for (or experience in) network security, formalization/verification methods
- Languages: programming languages (python, c)
- Fluent in english (writing and oral communication)

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 (after 6 months of employment) 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

Rémunération
2051 gross/month for the 1st and 2nd years. 2158€ gross/month for the 3rd year.