# BEYOND5G – Thesis proposal #2 on 5G Slice Security (WP3T3)

Hervé Debar Christophe Kiennert Gregory Blanc
Télécom SudParis
Institut Polytechnique de Paris
{firstname.familyname}@telecom-sudparis.eu

## Context

5G slices will enable network users to finely specify and operate network resources to fulfil services in diverse settings, simultaneously and over heterogeneous infrastructure networks. In such a complex environment, the multiplicity of actors and the opacity induced by using virtualization technologies may render security measures harder to enforce. Security orchestration needs therefore to adapt to the changes brought by 5G-and-beyond network slices. In particular, technologies such as IoT, SDN and ML are expected to transform networks and the way to manage them [6]. They also offer opportunities to build improved security functions.

## Objectives

The objective of the proposed work is to secure slices through continuous and adaptive monitoring as well as automated countermeasure selection and deployment. The proposal aims at offering a slice network state and security monitoring that is i) distributed [4], ii) federated [5], and iii) self-adaptive [3]. Additionally, leveraging language models that express security policies, the proposal will develop a countermeasure selection mechanism that is i) knowledge-based [1], ii) intent-based [8], and iii) able to mitigate collateral damages [7]. The whole autonomic loop will require explanations [2] to better act upon the detected events and selected security functions.

## Proposal

The proposed work aims at securing 5G slices by implementing an autonomic cybersecurity loop including monitoring, analysis, planning and execution of selected security policies, and relying on knowledge obtained from analyzing the collected data on the state of the slices, both in terms of network and security.

The approach is two-fold. First, the work will focus on developing a continuous monitoring system that detects anomalies in and out of 5G slices thanks to behaviors learned during nominal phases of the network. Such knowledge is completed by distributing probes both at the edge and the core of the networks. Challenges lie in the ability to aggregate different levels and granularities of information, while still retaining the legitimate behavior of the network traffic. Explainability is another key aspect that will improve the ability to update the security policy both in terms of monitoring and response.

Another aspect of the work deals with the design of a countermeasure selection and deployment mechanism that leverages automation from network virtualization technologies and adaptation from machine/deep learning approaches. Challenges lie in the ability to find optimal policies in a dynamic setting, where even monitoring functions are moving, while reducing collateral damages as much as possible.

## Application

We are open to applications to be reviewed as soon as possible, and followed by an (remote) interview, if accepted. Potential candidates MUST hold a Master-level degree or equivalent (e.g., a French *diplôme d'ingénieur*) and have experience in domains related to this thesis offer (machine learning, network virtualization, intrusion detection, automation) as well as a strong motivation for research. The candidate SHOULD provide the following items as an application package by email to all the thesis supervisors:

- up-to-date resume (CV);
- a copy of the latest degree (or ongoing if completion date is September 2021);
- letters of recommendation, or a list of references (people that would recommend the candidate).

Incomplete packages will not be reviewed.

The thesis work will take place at Télécom SudParis (Palaiseau or Evry), within a restricted access area, for which the candidate will need to get clearance. The thesis work will contribute to a national project funded by Bpifrance, the French public investment bank.

## References


[1] E. Aguas, A. Lambert, G. Blanc, and H. Debar. Automated Saturation Mitigation Controlled by Deep Reinforcement Learning. In *Proc. of ICNP'20*.

[2] D. L. Marino, C. S. Wickramasinghe, and M. Manic. An Adversarial Approach for Explainable AI in Intrusion Detection Systems. In *IECON'18*, pages 3237–3243. IEEE, 2018.

[3] M. V. Ngo, H. Chaouchi, T. Luo, and T. Quek. Adaptive Anomaly Detection for IoT Data in Hierarchical Edge Computing. In *AIoT'20*, 2020.

[4] M. V. Ngo, T. Luo, H. Chaouchi, and T. Quek. Contextual-bandit anomaly detection for IoT data in distributed hierarchical edge computing. In *ICDCS'20*, 2020.

[5] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A. Sadeghi. DÏoT: A Federated Self-Learning Anomaly Detection System for IoT. In *ICDCS'19*, pages 756–767. IEEE, 2019.

[6] F. Restuccia, S. D'Oro, and T. Melodia. Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. *IEEE Internet of Things Journal*, 5(6):4829–4842, 2018.

[7] R. Sahay, G. Blanc, Z. Zhang, and H. Debar. Adaptive policy-driven attack mitigation in SDN. In *Proc. of XDOM0'17*. ACM, 2017.

[8] E. J. Scheid, C. C. Machado, M. F. Franco, R. dos Santos, R. Pfitscher, A. Schaeffer-Filho, and L. Granville. INSpIRE: Integrated NFV-based intent refinement environment. In *IM'17*, 2017.