Open Ph.D Position at Ca' Foscari University of Venice

July 23, 2026

This document provides details on the open position at the university of Venice, financed by the Italian National Cybersecurity Agency[1]. This Ph.D. proposal ranked among the top-20 among hundreds of other proposals submitted by Italian universities, the advisor of the student will be Prof. Leonardo Maccari[2] (feel free to contact me for further information), the official open call is on the university website[3].

Project Overview

This fully funded PhD position aims to resolve one of the most critical vulnerabilities of the global Internet infrastructure: **Border Gateway Protocol (BGP) path hijacking** as described by Tao et al. [1]. While origin hijacking is progressively mitigated by the global adoption of the RPKI standard [2], path hijacking remains highly evasive because it manipulates the `AS-PATH` attribute without generating direct IP prefix conflicts. While solutions like ASPA exist, their adoption is low[3]. The primary objective of this doctoral project is to conceive, design, and standardize an innovative, high-accuracy framework capable of detecting and actively mitigating diverse variants of BGP path hijacking.

Core Research Objectives

The project is structured around three specific, highly-interconnected research objectives:

- **Detection via Topological Dynamics:** Develop an anomaly detection engine based on routing graph analysis. The core innovation lies in dynamically measuring and monitoring the graph centrality of Autonomous System (AS) nodes to observe sudden, temporary, or periodic deviations in topological importance [4]. This approach will significantly reduce background noise and false positives. Anomaly detection will compare classical statistical methods and machine learning algorithms, leveraging both offline datasets (e.g., CAIDA) and real-time feeds.
- **Architectural Integration and Active Reaction:** Design native reaction mechanisms directly within BGP. Drawing inspiration from successful DDoS mitigation standards (such as BGP Flowspec), the project will adapt these logics to filter or

[1] `https://www.acn.gov.it/portale/en/home`
[2] `https://www.dais.unive.it/~maccari`
[3] `https://www.unive.it/web/en/2161/calls-for-application`

"de-prefer" compromised routes. This reactive layer will be tightly integrated to complement Autonomous System Provider Authorization (ASPA), merging deterministic cryptographic validation with adaptive topological anomaly detection.

- **Standardization and Operational Adoption:** Translate academic research into real-world operational standards. Through proactive participation in the Internet Engineering Task Force (IETF), the candidate will propose Internet-Drafts to ensure that the newly developed reaction mechanisms are computationally lightweight, backward-compatible, and seamlessly deployable on commercial routers.

Key Distinctive Innovations

The project bridges the current dichotomy between passive academic monitoring and operational routing protocols by embedding intelligence directly into routing mechanics:

- **Algorithmic Breakthrough:** The systematic use of time-varying graph centrality overcomes the limitations of simple heuristic-based systems that trigger excessive false positives. Restricting calculations to specific sub-graphs (such as an AS's BGP "customer cone") ensures computational scalability.
- **Active Mitigation:** Translating successful automated DDoS mitigation frameworks into pure routing security allows routers to propagate real-time alarms, empowering individual ASes with dynamic, local policy options.
- **Architectural Synergy:** While ASPA provides a rigorous deterministic cryptographic filter for customer-provider relations, this framework complements it by intercepting complex manipulations (e.g., sophisticated MITM attacks or malicious peer leaks) through a dynamic, secure-by-design response mechanism.

Multi-Stakeholder Collaboration Ecosystem

Modifying global routing foundations requires extensive empirical validation and operational consensus across multiple levels:

- **International (IETF):** Active contribution to the Internet Engineering Task Force (specifically IDR and SIDROPS working groups) to transform research into core "Internet Standards".
- **European (RIPE NCC):** Collaboration to access real-time and historical routing datasets (RIPE RIS) and leverage the RIPE Academic Cooperation Initiative (RACI) to engage with the continental network operators' community.
- **National (Italy):** Alignment with operational best practices via direct interaction with strategic entities such as the Italian Research and Education Network (GARR) and major national Internet Exchange Points (IXPs) including MIX (Milan) and Namex (Rome).

References

[1] Y. Tao, C. Zhang, C. An, S. Zhuang, J. Wang, and C. Miao, "Ares: Comprehensive path hijacking detection via routing tree," in *Proceedings of the 34th USENIX Security Symposium*. USENIX Association, 2025.

[2] D. Mirdita, H. Schulmann, and M. Waidner, "Sok: An introspective analysis of rpki security," in *Proceedings of the 34th USENIX Security Symposium*. USENIX Association, 2025.

[3] J. Furuness, C. Morris, B. Wang, R. Morillo, A. Herzberg, and A. Kasiliya, "Securing bgp asap: Aspa and other post-rov defenses," in *Proceedings of the Network and Distributed System Security Symposium*. Internet Society, 2025.

[4] M. Milani, M. Segata, L. Baldesi, M. Nesler, R. Lo Cigno, and L. Maccari, "Optimizing MRAI on large scale BGP networks: An emulation-based approach," *Computer Communications*, 2024.