<u>Progetto di ricerca</u> correlato all'assegno "Reliability and Anomaly Detection on random networks."

Funded by the European Union - NextGenerationEU under the National Recovery and Resilience Plan (PNRR) - Mission 4 Education and research - Component 2 From research to business - Investment Investimento 1.3 , Notice D.D. 341 del 15/03/2022, from title: SEcurity and RIghts in the CyberSpace, proposal code PE0000014 - CUP J33C22002810001 (PE – PE7 – SERICS) for € 35.000,00 and on University Funding allocated within the first round BIR 2024 for € 7.675,00.

The research activity related to this call concerns the theoretical work-package of the project PE7 Serics-Ecocyber, in particular the WP1, Continuous risk management indicators and models.

The activity will be focused on finding heterogeneous indicators for real-time cyber-risk recognition and analysis of networked systems, from the perspective of complex systems and by using techniques from statistical mechanics. The goal will be the introduction of global indicators of systemic vulnerabilities and measures of collective instabilities.

The activity of the candidate will be

1) the introduction of probabilistic mathematical models for static and dynamic complex networks;

2) the development of statistical inference methods for network reliability and for anomaly detection at both local and global scale;

The structure of the network of interconnections between the units of a system affects the system's dynamics and conveys information about the functional needs of the system, its evolution, and the role of individual units. For these reasons, complex network theory has become a cornerstone mathematical framework for a wide variety of disciplines ranging from systems biology and sociology to finance and cybersecurity.

The organization of real networks and their dynamics usually embodies both regularities and irregularities. In principle, the former can be easily modelled, while the latter can be detected accordingly. The extent to which regularities can be explained affects the ability to correctly identify possible anomalies. Conversely, the presence of irregularities, anomalies, or data unreliability, can affect the possibility to understand and extract regularities efficiently. The aim of this project is to study the dual relationship between regularity vs anomaly detection in networked systems.

Network regularities can be investigated by introducing random generative models for static and dynamics networks, as for example the well-known Stochastic Block model and its generalizations [White1976, ...]. These models can be estimated on the base of some observed network and the possibility to extract regularities is known to have some efficiency limits due to the amount of anomalies. The problem can be studied by setting up a statistical inference problem that can be investigated in the theoretical framework of Statistical Mechanics of phase transitions [Decelle 2011]. Moreover, this approach suggests numerical algorithms that turn out to be both efficient and scalable [BP...].

Network anomalies likewise can be defined and detected statistically on the base of a null model for regularities that has been previously estimated on real data [Guimera2009]. Different approaches are nonparametric and are typically based on spectral perturbation theory and the hypothesis that network regularity is reflected in the consistency of structural features before and after a random removal of a small set of links [Lu2015].

We aim at studying regularity and anomaly detection both separately, by extending the existing models in literature to the specific case of cyber-physical networked systems, and simultaneously, i.e. under the same mathematical framework and as they can mutually improve their performance. This analysis can be

extended to network dynamics, with further applications in real time monitoring of sudden changes in evolving network mechanisms due for example to cyber threats.

REFERENCES

[Decelle 2011] Decelle, Aurelien, et al. "Inference and phase transitions in the detection of modules in sparse networks." *Physical Review Letters* 107.6 (2011): 065701.

[Guimera 2009] Guimerà, Roger, and Marta Sales-Pardo. "Missing and spurious interactions and the reconstruction of complex networks." *Proceedings of the National Academy of Sciences* 106.52 (2009): 22073-22078.

[Lu 2015] Lu, Linyuan, et al. Toward link predictability of complex networks. *Proceedings of the National Academy of Sciences*, 2015, 112.8: 2325-2330.

[White 1976] White, Harrison C., Scott A. Boorman, and Ronald L. Breiger. "Social structure from multiple networks. I. Blockmodels of roles and positions." *American journal of sociology* 81.4 (1976): 730-780