Politecnico di Torino

COMPUTER AND CONTROL ENGINEERING

CNR/IEIIT - Secure and Green Digital Networks

Funded By	C.N.R. - CONSIGLIO NAZIONALE DELLE RICERCHE [P.iva/CF:02118311006]
Supervisor	VALENZA FULVIO - fulvio.valenza@polito.it
Contact	DURANTE LUCA - luca.durante@polito.it SISTO RICCARDO - riccardo.sisto@polito.it
Context of the research activity	Digital networks such as cloud, edge, and virtualized infrastructures must guarantee strong cybersecurity and resilience while operating under increasing energy and efficiency constraints. This PhD project aims to design adaptive and automated approaches for secure and energy-aware network optimization, enabling resilient reactions to cyber attacks and failures through continuous monitoring, formal modeling, and security-driven reconfiguration.
	Modern digital networks, including cloud, edge, and software-defined infrastructures, are increasingly complex, dynamic, and exposed to cyber threats. At the same time, they are required to operate under strict efficiency and sustainability constraints. In this context, cybersecurity and network resilience cannot be treated as static properties, but must be continuously enforced through adaptive, automated, and optimized configuration mechanisms. The main objective of this PhD research is to advance the state of the art in secure and green digital networks by developing optimization models and automated approaches for the configuration of network security devices. The proposed approaches will combine cybersecurity protection, resilience to attacks and failures in dynamic digital networks, and energy-aware optimization for efficient security configurations. Current network security management solutions still rely heavily on manual configuration and human-driven decision processes. This limits scalability, slows reaction to attacks or failures, and increases the risk of misconfigurations, especially in highly dynamic cloud and virtualized environments. The proposed research aims to reduce human intervention by introducing model-driven and optimization-based approaches that enable automated, correct-by-construction security configurations and adaptive reconfiguration at runtime. The research will build upon consolidated expertise in network security automation and formal methods, and will be conducted in synergy with ongoing scientific activities in collaboration with CNR-IEIIT. Energy awareness will be treated as a constraint and optimization dimension influencing security

Objectives	decisions, rather than as an independent objective, enabling the joint management of security, resilience, and efficiency. The research activity will be structured in three main phases. Year 1: analysis of the state of the art in cybersecurity automation, network resilience, and energy-aware network optimization, with particular attention to formal and optimization-based modeling approaches. Initial problem formulations and models for the secure and green configuration of network security devices will be defined. Year 2: development and implementation of the proposed models and automated mechanisms, including security-aware and energy-aware optimization strategies. Experimental evaluation will assess correctness, scalability, performance, and resilience under representative attack and failure scenarios. The results of this phase are expected to lead to publications in international conferences and journals. Year 3: refinement and extension of the proposed approaches to improve scalability, generality, and applicability to different network architectures, security devices, and threat models. Data-driven and AI-based techniques may be investigated to support adaptive decision-making under changing network and threat conditions. Dissemination of the research results will be completed. The outcomes of this research are expected to contribute to high-impact scientific venues in the areas of cybersecurity, networking, and dependable systems, such as IEEE S&P, ACM CCS, NDSS, ESORICS, IFIP SEC, IEEE Transactions on Secure and Dependable Computing, and ACM Transactions on Privacy and Security.

Skills and competencies for the development of the activity	The candidate should have a solid background in computer networks and cybersecurity, along with good programming skills. Knowledge of network security mechanisms and distributed systems is required. Familiarity with formal methods, optimization, or automation techniques is a plus but not mandatory and can be acquired during the PhD program.