TITLE AND ABSTRACT OF THE RESEARCH TOPIC OF PHD STUDENTS IN THE PHD'S NATIONAL PROGRAM UNDER SUPERVISION ONE OF DIEE PROFESSOR

XL CYCLE

Emmanuel Ayora

PhD: *Sustainable Development and Climate Change*. **(IUSS PAVIA)**

Tema di Ricerca:

Artificial intelligence for energy management systems in public transport electrification.

Abstract:

Recent international energy transition policies set increasingly challenging targets for reducing pollutant emissions for the transportation sector. However, electric private cars are not a sustainable solution because of their high consumption per person and km, and the inherent poor public space utilization and congestion issues. Consequently, improving local public transport is the best solution in the urban context especially when clean vehicles are considered. Particularly, multi-source electric propulsion system architectures with multiple energy sources are very promising for public transport vehicles. They rely on a combination of technologies among batteries, supercapacitors, hydrogen fuel-cells, diesel engines and catenary/wireless power supply which require managing the power flows among the energy sources properly. In this context, the research activity will regard the development of advanced energy management and control strategies for multi-source electric propulsion systems for public transport vehicles, with particular reference to artificial intelligence techniques. More in detail, these will be based on infomobility data collectable during the repetitive scheduled duties that characterize public transportation fleets, thus enabling a suitable data forecast and the employment of real-time optimisation-based energy management and control systems.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Muzamil Hussain Wadho

PhD: *Sustainable Development and Climate Change*. **(IUSS PAVIA)**

Tema di Ricerca:

Highly integrated hybrid energy storage systems for marine electric propulsion systems.

Abstract:

Recent international energy transition policies have established increasingly challenging emission reduction targets for the transport sector, including ships and boats. In particular, the International Maritime Organisation (IMO) has set ambitious emission reductions, such as 40% in 2030 and 70% in 2050 for international shipping, to be achieved through improvements in energy efficiency and the adoption of near-zero greenhouse gas emission technologies and energy sources. In this context, multi-source electric propulsion architectures for vessels based on a combination of technologies such as batteries, supercapacitors, hydrogen fuel cells and diesel engines are very promising. The research activity focuses on the study, development and prototyping of innovative and highly integrated configurations of hybrid energy storage systems for marine electric propulsion systems. As these systems require proper management of the power flows between the energy sources, i.e. multi-mode, the research activity also deals with the development and implementation of advanced energy management and control strategies by combining conventional and novel approaches, with particular reference to artificial intelligence techniques.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Hicham Eddoubi

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Robust Machine Learning against Adversarial and Out-of-Distribution Drift.

Abstract:

The recent advancement in machine learning has prompted the widespread adoption of its various techniques to solve numerous problems and tasks in many fields; however, while showcasing exceedingly high degrees of accuracy in their tasks, most machine learning models rely on their training data and as such suffer from a lack of robustness to the natural progression of data and samples that exists outside the training data distribution. Furthermore, the rise of the field of adversarial machine learning highlighted the many weaknesses of machine learning models, as malicious actors can manipulate the output of models relatively easily by adding perturbations that may go unnoticed by the human eye. Therefore, this project focuses on bridging the gap between the in-lab results and in-the-wild performance, as an urgent need exists for fortifying machine learning models against adversarial and data drift. For instance, deepfake images have become exceedingly realistic, and while detection methods exist, their robustness to adversarial attacks remains largely unverified. The existing literature fails to address this issue rigorously. Thus, standardized benchmark tools are developed to ensure more effective and robust detection methods.

Daniele Ghiani

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Machine Learning for Adaptive Malware Detection in Continually Evolving Threat Scenarios

Abstract:

Malicious software (i.e., malware) is a pervasive and highly impactful cyber threat, capable of compromising sensitive data, disrupting critical services, and causing severe economic damage. Over the last decade, machine learning (ML) has emerged as a key technology for enhancing malware detection, thanks to its ability to learn complex patterns from large volumes of data and automate the identification process. However, malware evolves rapidly over time, frequently altering its structure and behavior to evade detection methods. Consequently, maintaining high detection performance requires frequent updates of ML-based detectors. At the same time, retraining models on large historical datasets is often infeasible due to high computational costs and growing concerns over data privacy and retention. A practical alternative is to update models using only the most recent data. While this approach addresses privacy and efficiency constraints, it introduces the challenge of catastrophic forgetting, where the model loses the ability to recall previously learned knowledge. To address this challenge, this research explores the use of continual learning (CL) techniques, which allow ML models to learn from new data while preserving performance on previously learned tasks. Beyond catastrophic forgetting, which refers to global performance metrics, this study also investigates the issue of regression, a related phenomenon in which specific examples once correctly classified may be misclassified in future model states—highlighting the complexity of maintaining consistent performance over time. The impact of this problem and the applicable mitigation strategies have not yet been addressed in continual learning settings. At the core of this research project lies the need for malware detection systems that can effectively adapt to new threats while retaining the ability to detect previously observed malicious behaviors.

Aurora Arrus

PhD: *Cybersecurity*. **(IMT Alti studi Lucca)**

Tema di Ricerca:

Advanced Malware Detection Framework for Linux-Based IoT Systems Using Binary Emulation.

Abstract:

The proliferation of Internet of Things (IoT) devices, particularly those based on Linux, has introduced major cybersecurity challenges due to their architectural diversity and limited security features. Existing malware detection techniques, often optimized for standard computing environments, are ill-suited for the highly heterogeneous and resource-constrained IoT ecosystem. This research project proposes the development of an advanced malware detection framework that leverages full binary emulation to replicate real-world operational conditions across various IoT architectures. By integrating CPU and operating system emulation with containerization technologies, the framework aims to efficiently analyze malware behavior while maintaining scalability, security, and isolation. Data collected from static analysis and binary execution will feed into machine learning algorithms to identify malicious patterns and behaviors. The project aspires to bridge the limitations of traditional static and dynamic analysis by creating a flexible, real-time capable detection system, ultimately improving the security posture of Linux-based IoT infrastructures.

Nicola Deidda

PhD: *Cybersecurity*. **(IMT Alti studi Lucca)**

Tema di Ricerca:

Advanced Machine Learning Approaches for Cyber Threat Management.

Abstract:

Machine learning models are widely used in cyber threat analysis and detection, supporting tasks such as network traffic analysis, anomaly detection, and malware classification. The emergence of large language models (LLMs) introduces new opportunities at multiple levels of granularity, ranging from vulnerability analysis in source and machine code to the management, enrichment, and contextualization of cyber threat intelligence (CTI) feeds. As cyber threats grow increasingly sophisticated, characterized by advanced obfuscation techniques, covert communication channels, and rapidly evolving tactics, traditional CTI processes often struggle with the overwhelming volume of unstructured and heterogeneous data, as well as the high demands placed on human analysts. LLMs offer promising solutions by automating critical tasks such as data extraction from diverse sources, threat summarization, correlation of threat indicators, and generation of analytical insights. This project explores the integration of LLMs and other advanced machine learning techniques into cyber threat intelligence and management workflows, focusing on their potential to enhance prevention, early detection, analysis, and incident response. Furthermore, it examines the challenges of applying LLMs in cybersecurity, including concerns over model accuracy and data protection. By evaluating both the opportunities and limitations, this work aims to provide a forward-looking perspective on the evolving role of LLMs in strengthening cyber threat intelligence capabilities.

Christian Scano

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Robust Machine Learning for Web Application Vulnerability Detection.

Abstract:

Web applications constitute a critical backbone of modern digital ecosystems. However, they remain highly exposed to an expanding spectrum of sophisticated attacks, including SQL Injection (SQLi), Cross-Site Scripting (XSS), and emerging classes of vulnerabilities. To mitigate these risks, Web Application Firewalls (WAFs) are widely deployed, traditionally adopting rule-based approaches that rely on static signatures and handcrafted heuristics. However, these methods often exhibit limited adaptability and resilience against obfuscated or novel attack techniques. The advent of machine learning-based WAFs offers a promising alternative, enabling the dynamic identification of complex threat patterns and improving the responsiveness of security systems. This research project focuses on developing comprehensive methodologies for attacking and defending web applications in this evolving landscape. On the offensive side, it investigates black-box approaches to systematically evaluate web defences' robustness, including rule-based and machine learning-enhanced WAFs. By generating adversarial payloads capable of bypassing security measures, the project aims to assess the resilience of these systems under realistic attack scenarios. Particular attention is placed on generating adversarial examples within the discrete and structured nature of web inputs, ensuring semantic preservation and maintaining malicious functionality. Additionally, a further research direction focuses on the large-scale black-box testing of web applications to discover known vulnerabilities. This line of work aims to develop efficient, scalable methodologies for vulnerability detection, simulating external attacker behaviour without requiring access to source code. On the defensive side, the project aims to design robust machine-learning models capable of detecting anomalous and malicious web traffic in real time. These models intend to improve resilience against adversarial manipulations and ensure high performance even as threats evolve. Strategies

such as adversarial training, ensemble modelling, and robust optimization guide the development of defences that minimize false positives while maintaining reliable threat detection capabilities. By integrating offensive and defensive research directions, this project wants to advance the development of proactive, adaptive, and resilient security solutions for web applications, thereby contributing to the protection and reliability of critical digital infrastructures.

Claudio Frongia

PhD: *Micro and Nano-Electronics*. **(Università degli Studi di Pavia)**

Tema di Ricerca:

Development of an integrated circuit based on the RISC-V ultra-low power platform for the optimization of biosignal acquisition and processing.

Abstract:

The research project focuses on two fundamental objectives:

1. The development of a custom RISC-V-based integrated circuit for the acceleration of biosignal processing and other Digital Signal Processing (DSP) advanced applications.
2. The design of adaptive analog front-end systems for efficient multi-signal acquisition and biosignal-to-spike conversion.

The analog front-end is tailored to acquire heterogeneous signals such as EEG, EMG, ENG, and ECoG. Efficient spike-encoding mixed-signals techniques are being exploring, including delta modulation, sigma-delta modulation, and multi-level crossing, aimed at reducing energy consumed and data dimensionality while preserving biosignal crucial information. The custom RISC-V core is being designed to serve as an interface between the analog front-end and a potential spiking neural network (SNN), performing signal preprocessing and managing spike routing through an Address-Event Representation (AER) mechanism. Various innovative integration strategies will be explored to interface the analog front end with the custom RISC-V core. The final goal of the project is to achieve an effective trade-off between low power consumption and high information reliability in the acquisition, processing and

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

analysis of biosignals. In collaboration with Insyde srls, we are designing a custom RISC-V microcontroller for advanced DSP application featuring instruction and data RAM (Harvard architecture), Timer (with PWM modulation and others advanced features), SPI master, I3C, APB and AXI bus interfaces, and a core_top module that includes the processor core, debug interface (DM+DTM, alias JTAG interface), and FPU. RISC-V non-standard instruction extensions such as fast_mult, fast_mac, fast_mult_fp, and fast_matmul are integrated to support key DSP applications including Fourier transforms, FIR and IIR filtering. For the optimization of DSP operations, the Karatsuba algorithm, the Booth algorithm, Vedic mathematics (for fast multiplication and MAC), and vectorized execution strategies (for fast matrix multiplication) are exploited.

Mahdi Yektai

PhD: *Micro and Nano-Electronics*. **(Università degli Studi di Pavia)**

Tema di Ricerca:

Development of a high-voltage compliance CMOS current stimulator for sensory feedback restoring.

Abstract:

Advancements in neuroscience and robotics have opened up new possibilities for developing innovative neural prostheses for limb replacement. To ensure the success of such prostheses, it is crucial to establish a stable and reliable connection between the artificial limb, residual muscles, and the nervous system. Communication with the nervous system can be established using invasive or non-invasive techniques. However, to restore the natural sense of touch, prosthetic devices and stimulating strategies must be capable of imitating the natural pattern activation of skin receptors. The use of invasive interfaces with the Peripheral Nervous System has shown promising results thanks to their selectivity in the elicitation of somatotopic tactile sensations, but they present disadvantages related to invasiveness due to surgery, fibrotic reaction, and weak long-term stability. Transcutaneous Electrical Nerve Stimulation (TENS) is an emerging technology in the field of upper and lower

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

limb prosthetics to restore sensory feedback without the need for a surgery. The development of electrical stimulators suitable for TENS requires several technological challenges. Electrical stimulation must be performed in current-controlled mode (CCM) to prevent any damage to tissues, and voltage compliance should be high to ensure the capability to deliver the proper charge to the nervous fibers. Furthermore, the stimulator must have multiple stimulation channels in order to imitate the natural activation of peripheral nervous tissues and also it is required to work in various situations with regard to power consumption, area and temperature. This thesis aims to realize a high-voltage CMOS Integrated Circuit capable of properly stimulating peripheral nerves through the skin.

Ejaz Zohaib

PhD: *Photovoltaics*. **(Università degli Studi di Salerno)**

Tema di Ricerca:

Development of conversion systems for DC management of photovoltaic plants oriented to green hydrogen production.

Abstract:

The activity involves the development of innovative conversion system configurations for the DC management of photovoltaic systems devoted to green hydrogen production. Specifically, the activity involves the development of a power conditioning system from photovoltaic plants aimed at optimizing the alkaline electrolyser usage for minimizing hydrogen production cost. For this purpose and with the aim of maximizing conversion efficiency, the photovoltaic plants will be interconnected to the electrolyser with multi-port DC/DC converters. The latter will be characterized by four bidirectional ports for managing DC power flows from the PV plant to the electrolyzer, the electrochemical storage system, and the grid. The management of the power flows as well as the sizing of the equipment will be the PhD target. The PhD activities will be developed for 12 months at the Renewable Energy Platform of Sardegna Ricerche where part of the mentioned equipment is already located.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

XXIX CYCLE

Alì Arshad

PhD: *Photovoltaics*. **(Università degli Studi di Salerno)**

Tema di Ricerca:

Systematic Development, Modeling, and Experimental Validation of a Multiactive Bridge (MAB) Converter for EV Charging Stations Supplied by PV.

Abstract:

This research focuses on the development of a Multi-Active Bridge (MAB) DC-DC converter specifically designed for electric vehicle (EV) charging stations powered by photovoltaic (PV) systems. The converter is developed with an emphasis on efficient power transfer to the EV battery using a multi-active bridge topology. The proposed model is further validated through experimental testing to ensure reliable performance under realistic operating conditions. The outcomes of this research aim to contribute to the design of efficient, scalable, and renewable-powered EV charging infrastructure.

Moein Taghavikoutenaei

PhD: *Photovoltaics*. **(Università degli Studi di Salerno)**

Tema di Ricerca:

Development of energy storage systems for improving power quality and decoupling the electric vehicles ultra-fast charging systems powered by PV power plant from power system.

Abstract:

The activity involves the analysis, development and implementation of integrated management systems of PV power systems to provide tailored energy services for electric mobility. The goal is to identify the integrated configurations of PV power plants and storage to manage the energy services electric vehicles require. The activity will investigate

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

developing a PV / storage system integrated with bi-directional charging station configuration and optimization algorithms for distributed management devoted to optimizing self-consumption levels for electric mobility.

Sodessa Soma Shonkora

PhD: *Sustainable Development and Climate Change*. **(IUSS PAVIA)**

Tema di ricerca:

Novel Energy Conversion System Topologies: Design and Control Approaches.

Abstract:

The primary goal of this research is to explore and analyze innovative energy conversion system configurations in modular multi-source systems to optimize electrification applications across diverse sectors, but especially focusing on marine applications. Specifically, the study aims to identify and evaluate novel energy conversion technologies that can seamlessly integrate with various energy sources, including renewable and conventional options, to enhance system efficiency. The research will involve modeling and designing of novel power electronic converter topologies that can adapt to different electrification needs, ensuring scalability and flexibility. The research will extend to develop and optimize control strategies for energy conversion systems by exploring suitable control techniques to improve system performance, stability, and response under varying loads and environmental conditions. These will be followed by assessing the efficiency and operating stability of the proposed configurations through simulations and experimental setups. Additionally, the research will identify specific application areas to demonstrate the practical implications of the findings.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Dell'Aquila Salvatore Dario

PhD: *Space Science and Technology*. **(Università degli Studi di Trento)**

Tema di Ricerca:

Application of Optimization Techniques to Satellite Layout Design (Satellite Layout Optimization Design, SLOD).

Abstract:

The satellite design process involves several critical phases, from the preliminary concept of the layout to the detailed integration of subsystems and final testing. In the initial stages, engineers define the mechanical structure, perform orbital simulations, and size the essential subsystems such as power, thermal control, and communication systems. The detailed design stages employ advanced computational tools, such as Finite Element Analysis (FEA) and Computational Fluid Dynamics (CFD), to ensure structural integrity and thermal performance. However, this process is time-consuming and costly, relying heavily on specialized expertise that is difficult to maintain over time. Automating and optimizing the satellite design process, with particular focus on the layout, offers a significant competitive advantage. The focus of this research is the application of optimization techniques to satellite layout design (Satellite Layout Optimization Design, SLOD), through an innovative approach combining the optimization of levels and positions, extending the problem to a multi-objective formulation aimed at minimizing both the satellite's moment of inertia and thermal non-uniformities. Another innovative aspect will be the introduction of surrogate modeling: based on models of varying fidelity, with the goal of ensuring adequate accuracy while reducing computational costs, thus accelerating the optimization process. Specifically, the use of Geometric Deep Learning (GDL), and more precisely Graph Convolutional Networks (GCN), will be explored as surrogates for the satellite's thermal models derived from CFD simulations. GDL allows for the analysis of 3D CAD geometries in non-Euclidean domains, preserving complex topological information without requiring extensive parameterization. It is believed that the application of these models could have a significant impact on the rapid prototyping of satellites.

Luca Scionis

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Methodologies for Evaluating Adversarial Robustness in Computer Vision Models: From Attack Optimization to Analysis.

Abstract:

This research falls within the field of Adversarial Machine Learning and focuses on evaluating the robustness of computer vision models when subjected to targeted attacks. The work unfolds across several complementary phases. The first phase involves optimizing hyperparameters for a specific category of attacks known as *minimal norm attacks*. A framework has been developed to enhance their effectiveness,and through this tool, robustness evaluation curves have been introduced. These graphs demonstrate how a model's ability to resist attacks varies with the intensity of perturbations applied to images. Subsequently, the research concentrates on evaluating black-box attacks, where the attacker lacks direct access to model details. Practical guidelines have been defined to ensure these attacks are analyzed more correctly and realistically, helping to highlight and resolve critical issues in existing literature. Current work explores combining multiple minimal norm attacks into an ensemble, with the goal of achieving a more comprehensive and reliable assessment of model robustness. This approach enables more precise measurement of the effectiveness of defensive techniques,offering a more concrete view of vulnerabilities still present in computer vision systems.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Affan Younas

PhD: *Cybersecurity*. **(IMT Alti studi Lucca)**

Tema di Ricerca:

Machine learning models for the analysis and detection of stealth threats and latent vulnerabilities in source code.

Abstract:

Modern software systems serve as the foundation of today's digital infrastructure, enabling a wide range of applications across diverse domains. As these systems increase in complexity, the likelihood of hidden security vulnerabilities within their source code also rises. Such vulnerabilities, often latent and context-dependent, are inherently difficult to detect and may pose significant security risks if not identified and addressed early in the development lifecycle. This research project explores the use of machine learning and deep learning models to automatically analyze source code and identify potential vulnerabilities. Leveraging Transformerbased architectures such as CodeBERT, along with structural information from Abstract Syntax Trees (ASTs), the approach enables the model to understand both the logic and context of code more effectively. The method also includes domain-specific processing steps to accurately represent the unique structural and semantic properties of programming languages. In addition to improving detection accuracy, the proposed framework can identify the specific lines of code most likely to contain vulnerabilities. The objective is to develop automated, highprecision ML models that support developers in detecting and addressing security weaknesses throughout the software development lifecycle, ultimately contributing to the development of more secure and resilient software systems.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Zohreh Shahrouei

PhD: *Autonomous Systems (Dausy)*. **(Politecnico di Bari)**

Tema di Ricerca:

Management and automation systems for energy management in buildings and industrial processes

Abstract:

The framework for the proposed thesis is part of ongoing projects at the industrial partner, funded either by private companies or public agencies, as well as at the Department of Electrical and Electronic Engineering, funded by the PNRR. The aim of the project is the study and development of tools for the energy management of the use of energy either in a civil contest or in industrial settlements. The full exploitation of renewable energy sources should be achieved by distributed control and optimization algorithms, possibly considering the specific characteristics of the users and producers connected in the network. The role of explicit or implicit energy storage systems, e.g., batteries and building structures respectively, will be considered in the optimization procedures as well as the knowledge of behavioural and meteorological forecasts. To this aim, models of the single user or producer will be analysed and developed by means of both physical modelling and data-based approaches. The design of the energy management and optimization system should be versatile enough to adapt to the monitoring, security, and automation level of the building or of the industrial activity, depending on the specific application.

The main goals of the program are detailed below:

- Define a flexible approach for the energy management in civil and industrial applications.

Taking int account the variability of the context, a theoretic approach that can be properly suited for different energy management situation will be studied and developed, specifying its validity conditions.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

- Identify a set of performance indexes that can be used for the optimisation of the use of energy.

The management of a complex system can require the use of proper performance indexes suited for economic and technical purposes that depend on the application. This implies the development of different tools.

- Application of optimisation approaches in specific cases.

Considering the applicative cases handled by STAM during the PhD course period, the studied and developed approaches will be suited for the use case and tested in a real applicative context.

XXXVIII CYCLE

Silvia Lucia Sanna

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Applying Artificial Intelligence Algorithms to Digital Forensics Techniques for Android Threat Detection.

Abstract:

In the last decades mobile devices are widely used by common people and companies, between them, Android is the most used mobile Operating System (OS) worldwide. Additionally, in the last years the number of attacks and threats to mobile devices is increasing rapidly, both to companies and personal devices. For these reasons, it is important to develop efficient detection mechanisms. The current literature methodologies are almost based on static and dynamic techniques, that is the analysis of the Android application (apk)

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

based on its code (static) or during execution (dynamic). Most of the current state-of-the-art works use the output of such techniques as features for Machine Learning (ML) or Deep Learning (DL) algorithms to classify and detect Android malware. Such techniques do not consider the effects of the malware execution in the whole OS and moreover some algorithms are not efficient due to the adversarial attacks, i.e., changing the malware behavior or structure to bypass the detection of the Artificial Intelligence (AI) algorithms. Most of the works using dynamic analysis are based on the execution of the malware in emulators but some malware can detect the use of the emulator and change the behavior so that the maliciousness is not detected. Additionally, there are some malware families where traditional techniques cannot be used to detect the threat and the suspicious behavior, such as fileless malware (i.e., malware executing in RAM and not leaving traces in disk) or stegomalware (i.e., malware using steganographic techniques to hide the malicious payload). Such malware executes malicious behavior directly in RAM and are detectable only in that specific timeframe (i.e., only during execution). Digital Forensics analysis could be used to overcome these presented problems. In fact, specific features can be extracted from the RAM or specific directories in disk can be monitored to check the effects of the malware execution in the whole OS. In order to apply such techniques to real Android devices, a root (i.e., acquiring the super user privileges) is required, otherwise the OS blocks the access to specific memory areas, both in disk and in RAM. The acquisition of the root privileges strictly depends on the used OS version, vendor, Google security patches, kernel version and currently there is no universal methodology. AI algorithms can be applied also to general Digital Forensics investigations, for example automatically detecting the presence of specific multimedia files objects of the prosecution or to generate automatic reports.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Gupta Srishti

PhD: *Artificial Intelligence*. **(Università la Sapienza Roma)**

Tema di Ricerca:

Towards Robust Machine Learning Systems Incrementally Trained in the Open World.

Abstract:

The recent tide in Artificial Intelligence (AI) is specifically attributed to high-performance computing and availability of the large amounts of data. Recently, since the performance of large models has stabilised, researchers face different problems: trying to keep up with changing trends of data, inability to deal with wild samples, prevent adversarial attacks on fundamental models, and so on. In this work, we mainly focus on first two problems. To solve the first issue, retraining the model from scratch is a default solution. However, there's a problem. First, training large models from scratch is: a) computationally expensive, b) environmentally unfriendly, and c) resource-intensive. Whereas for the second issue, models are implicitly trained with an iid (independent and identically distributed) assumption, meaning, the data used at the time of training is sampled from an underlying distribution, that the test data will be sampled. However, having an oracle distribution is not possible, therefore, for real-world setting this is an overarched assumption. In this work, we tackle these problems by exploring dynamic-ness of the model by continual training – continually training on new data without training from the scratch -- with out-of-distribution detection, making the model suitable for real-world application. This research also focuses on robustness of these realistic AI systems.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Yike Li

PhD: *Autonomous Systems (Dausy)*. **(Politecnico di Bari)**

Tema di Ricerca:

Optimal safety control for next-generation train control systems.

Abstract:

Compared to constructing new lines, the development of a railway signaling system is a more cost-efficient and eco-friendly way to accommodate the growing capacity demand. Leveraging the development of Train-to-Train communication, Virtual Coupling (VC) has gained increasing attention as a next-generation railway signaling system. Rather than using the traditional physical coupler made of steering axles, trains operated in VC are connected with each other by means of a Wi-Fi connection or 5G network, and run together at similar speed and shorter distance to form a convoy. Its implementation, however, poses critical control challenges, as following trains must maintain small inter-train spacing under dynamic operating conditions, as well as uncertainties such as communication losses and measurement errors. This project aims to apply optimal control methodologies to VC train control. We build upon and extend the rigorous safety control tool, Control Barrier Functions (CBFs), combing Quadratic Programming (QP), to develop a real-time capable controller that guarantees safety and stability for trains in VC convoys, without requiring centralized coordination or full trajectory prediction of the preceding trains, while preserving short inter-train spacing enabled by VC. Besides being robust to uncertainties, we also investigate VC convoys consisting of heterogeneous train fleets during different operational phases, in order to enhance the controller's applicability in real-world scenarios.

Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it