COMPUTER AND CONTROL ENGINEERING

PNRR/CNMS/To Move - Generative and Adversarial AI for Testing and Optimization of Connected and Automated Vehicles

Funded By	MINISTERO DELL'UNIVERSITA' E DELLA RICERCA [P.iva/CF:97429780584] Politecnico di TORINO [P.iva/CF:00518460019]
Supervisor	CASETTI CLAUDIO ETTORE - claudio.casetti@polito.it
Contact	
Context of the research activity	The research aims to explore the integration of generative and adversarial AI techniques to enhance the robustness, safety, and efficiency of Connected and Automated Vehicles (CAVs). By creating realistic and complex driving scenarios on demand, and using adversarial methods to identify and address potential vulnerabilities, the goal will be to develop a comprehensive framework for the rigorous testing and optimization of CAVs. Progetto finanziato nell'ambito del * PNRR M4C2, Investimento 1.4 - Avviso n. 3138 del 16/12/2021 - CN00000023 Sustainable Mobility Center (Centro Nazionale per la Mobilità Sostenibile) – CNMS - CUP E13C22000980001 + * PNRR PNC-A.1-N1 Living Lab “To Move” CUP: C15C22007220001
	Digital twin (DT) and Mixed Reality (MR) systems and technologies can assist Connected and Automated Vehicles (CAVs) in using advanced sensors, like ultrasonic radars, cameras, and LiDAR, to gather data from their surroundings and create virtual representations. Artificial intelligence (AI) methods then use these virtual models to inform driving decisions, enhancing CAVs' responses to dynamic road conditions. However, CAVs still face limitations in environmental perception due to occlusions and other sensor limitations, even with high-class LiDAR and panoramic cameras. Leveraging inter-vehicle connectivity and Road Side Units (RSU) communicating with vehicles can alleviate these problems. To overcome these challenges, there is a need for a system where CAVs, roadside units (RSUs), and virtual simulators collaboratively share and fuse

Objectives	sensing data to achieve comprehensive environmental perception. Realizing this large-scale data collection and processing for real-time driving simulation and training of CAVs usually means developing virtual traffic and driving simulation platforms. These platforms leverage DT and MR technologies to create virtual representations of AVs, facilitating efficient traffic and training data collection and allowing for simulation and testing of rare scenarios, like virtual traffic accidents and car collisions, under realistic conditions. However, traditional testing methods may not cover all possible scenarios, especially unusual, or extreme, conditions. Generative AI offers a solution by creating synthetic data and scenarios, while adversarial AI can help identify weaknesses. Combining these approaches has the potential to provide a powerful framework for comprehensive testing and optimization. Research Objectives (1) Development of Generative Models:Design and train generative models (e.g., GANs, VAEs) to create diverse driving scenarios.Generate synthetic datasets (or integration of existing datasets using synthetic data) including varying weather conditions, traffic/movement patterns, and unexpected obstacles. (2) Adversarial AI Implementation:Develop methods to create adversarial examples that challenge the vehicle's perception and decision-making processes, identifying the types of scenarios that are most likely to cause failures or suboptimal performance in CAVs.Investigate the use of Adversarial AI for the setting and optimization of system parameters. (3) Integration and Adaptive Testing:Combine generative and adversarial methods to create a dynamic testing environment, based on simulation or hardware-in-the-loop emulationImplement adaptive testing where generative models produce scenarios based on adversarial findings.Continuously refine and improve CAV systems based on testing outcomes. (4) Evaluation:Conduct extensive simulations to evaluate the effectiveness of the proposed framework.Analyze the impact on safety, reliability, and performance of CAVs.Compare results with traditional testing methods to highlight improvements. Research Work Plan - Year 1: Literature review, development of generative models, evaluation of suitable adversarial AI techniques, initial scenario generation.- Year 2: Implementation of adversarial AI techniques, integration with generative models.- Year 3: Adaptive testing, extensive simulations and evaluation, system refinement.

Skills and competencies for the development of the activity	The ideal candidate should: - possess a strong foundation in machine learning concepts, algorithms, and frameworks - be proficient in programming languages such as Python and C++ - have strong development skills, including code versioning (e.g., Git), debugging, and optimization - have experience in using ML libraries and tools such as TensorFlow, PyTorch, and Keras Past experience in the application of AI/ML techniques in the analysis of wireless and/or mobile networks is a plus.