CHRISTOPHER SERRANO

MACHINE LEARNING RESEARCHER

cserrano@gmail.com
(626) 388-8342

LinkedIn | Google Scholar | arXiv | GitHub

Machine Learning Researcher focused on Perception, Reinforcement Learning, and Trusted Autonomy for mission-critical autonomous platforms. Applied R&D Scientist, experienced in leading and supporting projects and proposals, developing innovative algorithms, communicating effectively with stakeholders, and integration of perception and control systems into customer platforms.

Experience

HRL Laboratories, LLC September 2019 - Present
Scientist V
Machine Learning Researcher focused on Perception, Reinforcement Learning, and Safe Autonomy.

- Led and supported multiple CRAD proposals, including as PI on a DARPA BAA.
- Led and supported multiple IRAD proposals annually with a 67% win rate.
- As PI planned requirements and deliverables, identified risks, led cross-functional teams, and communicated regularly with project stakeholders at all leadership levels.
- Developed novel effecient Transformer architectures for processing of formal logics in IRAD.
- Developed a real time Deep RL adversarial AI attack algorithm *(RTA3)* and demonstrated it on RNNs for audio transcription and CNNs for object identification with a 91% attack success rate.
- Developed a formal verification methodology *(Generate & Verify)* to guarantee performance of neural network visual perception systems in lane line estimation and cross track error scenarios.
- Developed neural network LiDAR perception systems for ground plane segmentation with formally verified performance guarantees and integrated it into customer platforms.
- Developed and integrated formally verified neural network perception systems and deep reinforcement learning based neural network controllers into an autonomous US Army GVSC Polaris MRZR as part of the DARPA Assued Autonomy program. youtu.be/bE2UpKHxsLg?t=102
- Developed an augmented reality adversarial AI attack algorithm against 9DoF autonomous vision and control systems operating in the real world.
- Developed Machine Learning methods to accelerate Formal Methods.
- Developed custom GPU accelerated RL training environments in NVIDIA's IsaacGym that scaled simulation 10,000x.
- 5 patent applications, 7 invention disclosures, 5 paper submissions

Deep Reinforcement Learning Research Intern May 2018 - August 2019
Graduate Research Intern focused on verifying the safety of Reinforcement Learning agents.

- Developed a formally verified Deep RL agent for continuous control of a ground vehicle in an A to B scenario.
- Developed an algorithm to incorporate formal verification artifacts into Deel RL agent training *(Introspection Learning)* resulting in a 99.6% reduction in failures during training.
- Developed custom RL training environments in Python and C++ with PyBullet, Unreal Engine, and AirSim.
- 1 patent application, 1 invention disclosure, 1 paper submission

Georgia Institute of Technology May 2019 - Present
Remote Instructional Associate, CS7642 Reinforcement Learning
Graduate course TA focused on course development and student mentorship.

Publications

Generate and Verify: Semantically Meaningful Formal Analysis of Neural Network Perception Systems
Serrano, C.R., Sylla, P., Warren, M.A. (2020)
In this work, we propose a notion of global correctness for neural network perception models performing regression with respect to a generative neural network with a semantically meaningful latent space.
arXiv preprint arxiv.org/abs/2012.09313

RTA3: A real time adversarial attack on recurrent neural networks
Serrano, C.R., Sylla, P., Gao, S., Warren, M.A. (2020)
In this paper, we demonstrate a general application of deep reinforcement learning to the generation of periodic adversarial perturbations in a black-box approach to attack recurrent neural networks processing sequential data.
Presented at the 2020 IEEE Deep Learning and Security Workshop ieee-security.org/TC/SPW2020/DLS/

Introspection Learning
Serrano, C.R., Warren, M.A. (2019)
Our approach synthesizes experience, without requiring an agent to interact with their environment, by asking the policy directly “Are there situations X, Y , and Z, such that in these situations you would select actions A, B, and C?”
Presented at the 2019 AAAI Spring Symposium on Verification of Neural Networks arxiv.org/abs/1902.10754

Patents

Neural network architecture for small lidar processing networks for slope estimation and ground plane segmentation
Serrano, C.R., Warren, M.A., Nogin, A. (2021) *US Patent App. 16/950,803*

Automated system for generating approximate safety conditions for monitoring and verification
Heersink, B.N., Warren, M.A., **Serrano, C.R.** (2021) *US Patent App. 17/115,770*

Deep reinforcement learning method for generation of environmental features for vulnerability analysis and improved performance of computer vision systems
Warren, M.A., **Serrano, C.R.** (2021) *US Patent App. 17/115,646*

Method for proving or identifying counter-examples in neural network systems that process point cloud data
Warren, M.A., **Serrano, C.R.**, Nogin, A. (2021) *US Patent App. 17/078,079*

Deep reinforcement learning based method for surreptitiously generating signals to fool a recurrent neural network
Warren, M.A., **Serrano, C.R.**, Sylla, P. (2021) *US Patent App. 16/937,503*

Solving based introspection to augment the training of reinforcement learning agents for control and planning on robots and autonomous vehicles
Warren, M.A., **Serrano, C.R.** (2020) *US Patent App. 16/691,446*

Education

Georgia Institute of Technology 2019
MS, Computer Science specializing in Machine Learning

University of California at Santa Barbara 2004
BA, Political Science with minors in History and Art History

Leadership	PyTorch	OpenCV	Computer Vision	Robotics	Docker
Mentoring	TensorFlow	Unreal	NLP	ROS	git
Project Manager	PyTorch Lightning	Ray	Object Detection	Sensor Fusion	Python
Force Multiplier	Jax	Simulation	Segmentation	Autonomous	C++
R&D	CUDA	OpenAI Gym	Prediction	Vehicles	C