Postdoctoral Fellowship in Cybersecurity

The Department of Systems and Computer Engineering at Carleton University is accepting applications for a postdoctoral fellowship in a project entitled "Realistic and Generalizable Training of Autonomous Cyber Agents". The anticipated start date will be July 1, 2024 (or as soon as possible) with a duration of initially two years (subject to the availability of funds), renewable for up to a total of three years. The postdoctoral fellow will be involved in research that uses Machine Learning, specifically Reinforcement Learning, to train autonomous blue (i.e., defensive) agents. The cyber environment is not static, with the network topology changing, new vulnerabilities occurring, new exploits being discovered, red agents deploying different attack strategies and/or different goals, etc. Therefore, the project aims to develop a training environment and training algorithms that result in blue agents capable of dealing with this changing landscape without extensive retraining.

Department Background Information

The Department of Systems and Computer Engineering at Carleton University (located in Ottawa, Canada) is a recognized world-class institution in computer systems engineering, electrical engineering, software engineering, communications engineering, and biomedical engineering. In January 2024, the university announced that 11 current and former faculty members in the department are among the globe's top 2% most cited scientists in their field.

Research Project Overview

The modern world relies heavily on the correct operation of communication networks such as the Internet. Involving human cyber experts in typical penetration tests is expensive and cumbersome. Machine Learning in general, and Reinforcement Learning in particular, hold great promise here. Trained autonomous agents may exhibit human-level or even superior intelligence in the choice of their actions.

Training such autonomous agents requires a suitable training environment. Simulation-based environments typically are abstract and high-level, making it difficult to transfer a trained agent into real networks. Emulation-based training environments usually suffer from very slow learning rates, limiting their use to small-scale networks. We are working with a unique training and evaluation environment for cyber agents that unifies both real (emulated) and simulated cyber networks with a complete cross-training loop.

Typically, the learning process is not general but trains agents to solve a specific task for a given network. We require training approaches that allow agents to generalize and perform well when the environment changes. Also, by carefully designing the training scenarios, we can learn complex scenarios incrementally and faster. Applying results from continual learning and decision transformer models as foundational models, we can train agents that will demonstrate generalizability. Ultimately, advances on both fronts will result in a training environment that allows us to train realistic agents for non-trivial scenarios that perform well across diverse scenarios.

Research Project Supervisor and Principal Investigator

The project is led by Professor Thomas Kunz, who will be the primary supervisor. The postdoctoral fellow will also interact closely with the two co-PIs on the project, Professor Lung and Professor Gao.

Salary
The postdoctoral fellow will be offered a salary of around $63K per annum, with the additional ability to opt into an extended health and dental benefit plan. The postdoc will be considered unionized and will be a member of PSAC Local 77000. Information on this bargaining unit can be found here: https://psac77000.ca/.

Position Duties and Responsibilities
The incumbent of this position will, under the direction of Professor Kunz, be responsible for leading the research activities of the project, including but not limited to the following core responsibilities:

- Primary contact for external partners (one company, one government research lab)
- Central resource person for graduate and undergraduate students working in this project
- In collaboration with PhD students, design and implement solution to the research problems, run experiments and collect data
- Document the results in internal reports and academic publications (conferences and journals)
- Present the work to external audiences (external partners, at conferences, etc.)

Job Requirements

- PhD in Computer Science or Computer Engineering or related disciplines within the past two years
- Expertise in Computer Networks and Cyber Operations
- Expertise in Machine Learning, particularly Reinforcement Learning
- Strong Programming Skills

Accommodations and Accessibility
Should you require a copy of this posting in an alternate format, please contact us as soon as possible and we would be happy to get one to you in a timely manner. We believe in the importance of supporting on the-job success for the incumbent and are pleased to discuss and/or provide specific tools, resources or other requirements for day-to-day work requirements, as needed.

About Carleton University:
Carleton University is a dynamic and innovative research and teaching institution with a national and international reputation as a leader in collaborative teaching and learning, research and governance. To learn more about our university and the City of Ottawa, please visit www.carleton.ca/provost.

Carleton University is committed to fostering diversity within its community as a source of excellence, cultural enrichment, and social strength. We welcome those who would contribute to the further diversification of our university including, but not limited to: women; visible minorities; First Nations, Inuit and Métis peoples; persons with disabilities; and persons of any sexual orientation, gender identity and/or expression. Carleton understands that career paths vary. Legitimate career interruptions will in no way prejudice the assessment process and their impact will be taken into careful consideration.

We thank all applicants for their interest, however, only those selected for a follow-up will be contacted. If contacted for an interview, please inform us should accommodation be required, and arrangements will be made in a timely manner. All qualified candidates are encouraged to apply.

How to Apply

Candidates that would like to apply for this fellowship opportunity are invited to submit their cover letter along with a resume/CV to Professor Kunz at tkunz@sce.carleton.ca by March 31, 2024, or until the position is filled. Please also include **one single** academic publication, preferably one that demonstrates the skills listed in the Job Requirements section. In your cover letter, describe how that paper relates, in your opinion, to the project as described, and detail your role in the submitted publication.