Application - Canada Graduate Scholarships-Master's Program

Identification

Applicant

Family Name: Lanctot **First Name:** Jordan

Middle Names:

Application

Application Title Deep Learning for Network Attack and Defense

Language in which the proposal is written (•) English ( ) French

Field of Research natural sciences and/or engineering

Start date or proposed start date of program of study 2022-09-01 **Proposed end date of program of study** 2024-09-01

Number of months of graduate studies completed as of December 31 of year of application

Months of full-time study 8 **Months of part-time study** 0

If you are successful in obtaining a Canada Graduate Scholarship will you consider applying for a Michael Smith Foreign Study Supplement? ( ) Yes (•) No

Supplements/Joint Initiatives

To be considered for one or more Supplements or Joint Initiatives, select all that apply

Proposed Host Organization

Proposed Host Organization #1

Organization Toronto Metropolitan University

Faculty Science

Department/Division Physics

Proposed Host Organization #2

Organization

Faculty

Department/Division

Proposed Host Organization #3

Organization

Faculty

Department/Division

Summary of Proposal

Summary

Novel research has been conducted to transform the structure of networks into tensors suitable for Deep Learning (DL) – motivating whether DL can be used to discover network weaknesses and exploit them. Should DL agents gain the ability to exploit and attack networks, the security and robustness of infrastructure and information networks comes in question. Are there any limits on the capacity for DL to discover network weaknesses and selectively attack them? If not, can this capacity be mitigated through efficient strategies which conceal some of the information about the network, allowing for a defensive response?

We will create a framework which maps this targeted network attack to a two-player game, allowing us to leverage the field of Deep Reinforcement Learning. Through this novel framework, the first DL player will be presented a network and will be rewarded for choosing nodes which quickly break apart the network – simulating network attack. The second DL agent will receive the network before the first agent and will hide a fraction of the network links before it is shown to the first agent. The second agent will be rewarded if the partially concealed network requires more moves to be broken by the first DL agent – simulating network defense. To this end, we will determine the limits to malicious DL attackers and develop defensive strategies to reduce their effectiveness.

Activity Details

Certification Requirements

Does the proposed research involve humans as research participants? ○ Yes ◉ No

Does the proposed research involve animals? ○ Yes ◉ No

Does the proposed research involve human pluripotent stem cells? ○ Yes ◉ No

Does the proposed research involve controlled drugs and/or substances?

○ Yes ◉ No

Does the proposed research involve human totipotent stem cells?

○ Yes ◉ No

For statistical purposes only

Does this application propose research involving Indigenous people?

○ Yes ◉ No

Sex- and Gender-Based Analysis

Are sex (biological) considerations taken into account in this research proposal?

○ Yes ◉ No

Are gender (socio-cultural) considerations taken into account in this research proposal?

○ Yes ◉ No

Keywords

List up to 10 keywords that best describe the proposal.

Deep Learning, Artificial Intelligence, Networks, Adversarial Learning, Defense, Information Theory, Percolation, NP-Hard, Infrastructure Security, Network Security

Field of Study

Indicate and rank up to three primary fields of study relevant to your proposal, with #1 the most relevant and #3 the least relevant.

1. PHYSICS
2. INFORMATION TECHNOLOGY
3. COMPUTER HARDWARE

Special circumstances

Do you have any special circumstances to take into consideration that may have affected your research, professional career, record of academic or research achievement or completion of degrees?

○ Yes ○ No

Introduction: With the spectacular advances in Deep Learning over the past decade, humanity has gained new tools to solve previously intractable problems. These include superhuman machine performance in strategy games such as Go and StarCraft, and simplifying large, macroscopic problems in math and physics like discovering new algorithms for matrix multiplication. At the intersection physics and deep learning there has been cutting edge research to learn how to embed *network* (graph) data into a deep learning framework [1] [2] – potentially allowing deep learning to explore network data and discover network weaknesses. Indeed, real-world networks such as power grids are fundamentally vulnerable to attacks on a small number of key components (nodes), whose removal can cause the system as a whole to collapse. Though identifying these "Achilles Heels" of a given network is a computationally intractable (NP-Hard) problem [3], deep learning might effectively surmount this obstacle, providing new destabilizing tools that malicious agents could use to attack real-world infrastructure networks. To our knowledge, little research has sought to understand the limits to deep learning's capacity to efficiently destroy networks, and counterstrategies that might mitigate this capacity.

Objectives: To understand the limits of deep learning's ability to dismantle networks by removing key nodes. And should no such limits exist, to develop AI-based counterstrategies to in a "fight fire with fire" approach.

Hypothesis: I hypothesize that deep learning will have the capacity to discover key network features at decreasing rates as more information about the structure of the network is hidden from the deep learning agent (an attacker). Further, I hypothesize this trend will hold for networks of varying sizes and degrees of interconnection. I suggest that the most efficient concealment strategy can be discovered by a *second* deep learning agent (an opposing defender), tasked with learning to undermine the first agent through tandem learning strategies – allowing for the creation of strategies to defend real world networks and infrastructure.

Methods: I will create a framework which maps the real-world problem of network attack and defense to a two-player strategy game that can be solved with Deep Graph Learning. Specifically, my framework will replicate network attack through the network dismantling effects of node destruction – a deterministic process with sequential outcomes resembling percolation [3] [4]. For the attacker, the game will be defined by taking actions on a set of nodes which will break down the network, ending the process when a specified portion of the network is fragmented from the rest of the network. For the defender, the network learning problem will be defined by taking actions on a set of links until a certain fraction of the network is concealed. As such, the attacker will attempt to make its decision based only the information left after the defender has obscured part of the network.

The game will be played on networks of varying size and degrees of interconnection. To this end, I will use network embedding to capture important network features, transforming the structure of the data into a fixed dimensional tensor suitable for deep reinforcement learning [1]. Through expanding this approach to allow for link selection, not only node selection, I enable a deep learning agent (the defender) to learn to conceal network links, reducing the effectiveness of the node selecting deep learning (the attacker). I will reward each player based effectively they shorten or lengthen the number of moves taken by the attacker – incentivize each of their defined objectives.

Anticipated Results: Using this approach, I will determine whether the deep learning of weak points of a network can be thwarted by strategic concealment of key network information, and what the optimal such defensive strategy might be. If an attacker's ability to quickly dismantle networks cannot be reduced in a meaningful way, this might reveal a fundamental weakness of infrastructure and other-real world networks to malicious attacks by a deep-learning equipped adversary [5] [6] [7].

Conclusion and Significance: The deliverable from this research will be defensive strategies which thwart malicious deep learnings seeking to destroy networks.

Personal information will be stored in the Personal Information Bank for the appropriate program.
PROTECTED B WHEN COMPLETED

References

[1] H. Dai, E. B. Khalil, Y. Zhang, B. Dilkina and L. Song, "Learning Combinatorial Optimization Algorithms over Graphs," in *31st Conference on Neural Information Processing Systems (NIPS 2017)*, Long Beach, CA, USA, 2017.

[2] C. Fan, L. Zeng, Y. Sun and Y.-Y. Liu, "Finding key players in complex networks through deep reinforcement learning," *Nature Machine Intelligence,* vol. 2, pp. 317-324, 2020.

[3] H. Bennett, D. Reichman and I. Shinkar, "On Percolation and N P-Hardness," *Random structures & algorithms,* vol. 54, no. 2, pp. 228-257, 2019.

[4] F. Morone and H. A. Makse, "Influence maximization in complex networks through optimal percolation," *Nature,* vol. 514, pp. 65-68, 2015.

[5] X.-L. Ren, N. Gleinig, D. Helbing and N. Antulov-Fantulin, "Generalized network dismantling," *PNAS,* vol. 116, no. 14, pp. 6554-6559, 2018.

[6] M. Grassia, M. De Domenico and G. Mangioni, "Machine learning dismantling and early-warning," *Nature Communications,* vol. 12, no. 1, 2021.

[7] R. Albert, H. Jeong and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature,* vol. 406, p. 378–382, 2000.

[8] V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves and I. Antonoglou, "Playing Atari with Deep Reinforcement Learning," *ArXiv,* vol. abs/1312.5602, 2013.

Personal information will be stored in the Personal Information Bank for the appropriate program.
PROTECTED B WHEN COMPLETED

RYERSON UNIVERSITY

Graduate

Name: **Mr Jordan Lanctot**
Student ID: **500910358**
OEN: **664268737**

Print Date: 10/16/2022
Birthdate: 01/01/1993

Academic Program History

Program: MSc Physics
05/02/2022: Active in Program
05/02/2022: PHYSICS Major

Program: MSc Physics
08/26/2022: Active in Program
08/26/2022: PHYSICS - COMPLEX SYSTEMS Major

Degrees Awarded

Degree: Bachelor of Science (Honours) with Distinction
Confer Date: 06/01/2022
Plan: MEDICAL PHYSICS

Beginning of Graduate Record

Spring/Summer 2022

Session:Regular

Course		Description	Attempted	Earned	Grade	Points
GD	1000	Continuing Graduate Studies	0.000	0.000		0.000

			Attempted	Earned	GPA Units	Points
Term GPA	0.000	Term Totals	0.000	0.000	0.000	0.000
Transfer Term GPA		Transfer Totals	0.000	0.000	0.000	0.000
Combined GPA	0.000	Comb Totals	0.000	0.000	0.000	0.000

Fall 2022

Session:Regular

Course		Description	Attempted	Earned	Grade	Points
BP	8116	Many-body Theory				
BP	8201	Master's Seminar 1				
GD	1000	Continuing Graduate Studies				

Graduate Career Totals

Cum GPA:	0.000	Cum Totals	1.000	0.000	0.000	0.000
Transfer Cum GPA		Transfer Totals	0.000	0.000	0.000	0.000
Combined Cum GPA	0.000	Comb Totals	1.000	0.000	0.000	0.000

End of Graduate

RYERSON

RYERSON UNIVERSITY

Undergraduate

Name: **Mr Jordan Lanctot**
Student ID: **500910358**
OEN: **664268737**

Print Date: 10/16/2022
Birthdate: 01/01/1993

Academic Program History

Program: Bachelor of Science
07/21/2018: Active in Program
07/21/2018: MEDICAL PHYSICS Major

Program: Bachelor of Science
06/01/2022: Completed Program
06/01/2022: MEDICAL PHYSICS Major

Degrees Awarded

Degree: Bachelor of Science (Honours) with Distinction
Confer Date: 06/01/2022
Plan: MEDICAL PHYSICS

Transfer Credits

Transfer Credit from University Of Ottawa
Applied Toward Bachelor of Science Program

Fall 2018

Course		Description	Attempted	Earned	Grade	Points
CPS	109	Computer Science I	1.000	1.000	CRT	0.000
ECN	104	Introductory Microeconomics	1.000	1.000	CRT	0.000
ECN	204	Introductory Macroeconomics	1.000	1.000	CRT	0.000
ENG	LLS	1 Lower Level Liberal Studies	1.000	1.000	CRT	0.000
MTH	540	Geometry	1.000	1.000	CRT	0.000
MTH	207	Calc and Computatnl Methods I	1.000	1.000	CRT	0.000
MTH	108	Linear Algebra	1.000	1.000	CRT	0.000

Course Trans GPA: 0.000 Transfer Totals: 7.000 7.000 0.000

Beginning of Undergraduate Record

Fall 2018

Session:Undergraduate Regular

Course		Description	Attempted	Earned	Grade	Points
BLG	143	Biology I	1.000	1.000	B	3.000
CHY	103	General Chemistry I	1.000	1.000	C+	2.330
MTH	131	Modern Mathematics I	1.000	1.000	A-	3.670
PCS	120	Physics I	1.000	1.000	A+	4.330
SCI	180	Orientation	1.000	1.000	PSD	0.000

			Attempted	Earned	GPA Units	Points
Term GPA	3.330	Term Totals	5.000	5.000	4.000	13.330
Transfer Term GPA		Transfer Totals	7.000	7.000	0.000	0.000
Combined GPA	3.330	Comb Totals	12.000	12.000	4.000	13.330

Academic Standing Effective 12/21/2018: Academic Standing: Clear

Winter 2019

Session:Undergraduate Regular

Course		Description	Attempted	Earned	Grade	Points
BLG	144	Biology II	1.000	1.000	A-	3.670
CHY	113	General Chemistry II	1.000	1.000	C+	2.330
MTH	231	Modern Mathematics II	1.000	1.000	B+	3.330
PCS	130	Physics II	1.000	1.000	A-	3.670

			Attempted	Earned	GPA Units	Points
Term GPA	3.250	Term Totals	4.000	4.000	4.000	13.000
Transfer Term GPA		Transfer Totals	0.000	0.000	0.000	0.000
Combined GPA	3.250	Comb Totals	4.000	4.000	4.000	13.000

Academic Standing Effective 05/06/2019: Academic Standing: Clear

Fall 2019

Session:Undergraduate Regular

Course		Description	Attempted	Earned	Grade	Points
MTH	330	Calculus and Geometry	1.000	1.000	A	4.000
PCS	182	Life in the Milky Way Galaxy	1.000	1.000	A-	3.670
PCS	229	Intro to Medical Physics	1.000	1.000	A-	3.670
PCS	300	Modern Physics	1.000	1.000	A+	4.330

			Attempted	Earned	GPA Units	Points
Term GPA	3.920	Term Totals	4.000	4.000	4.000	15.670
Transfer Term GPA		Transfer Totals	0.000	0.000	0.000	0.000
Combined GPA	3.920	Comb Totals	4.000	4.000	4.000	15.670

Academic Standing Effective 12/19/2019: Academic Standing: Clear

Personal information will be stored in the Personal Information Bank for the appropriate program.
PROTECTED B WHEN COMPLETED

RYERSON UNIVERSITY

Undergraduate

Name: Mr Jordan Lanctot
Student ID: 500910358
OEN: 664268737

Winter 2020

Session:Undergraduate Regular

Course		Description	Attempted	Earned	Grade	Points
MTH	430	Dynamic Sys Diff Equations	1.000	1.000	A+	4.330
PCS	227	Biophysics	1.000	1.000	A+	4.330
PCS	228	Electricity and Magnetism	1.000	1.000	A	4.000
PCS	401	Quantum Mechanics I	1.000	1.000	A-	3.670
PCS	521	Mathematical Physics	1.000	1.000	A+	4.330

			Attempted	Earned	GPA Units	Points
Term GPA	4.130	Term Totals	5.000	5.000	5.000	20.660
Transfer Term GPA		Transfer Totals	0.000	0.000	0.000	0.000
Combined GPA	4.130	Comb Totals	5.000	5.000	5.000	20.660

Term Honor: Dean's List

Academic Standing Effective 05/13/2020: Academic Standing: Clear

Fall 2020

Session:Undergraduate Regular

Course		Description	Attempted	Earned	Grade	Points
BLG	311	Cell Biology	1.000	1.000	A+	4.330
PCS	230	Photonics and Optical Devices	1.000	1.000	A	4.000
PCS	358	Mechanics	1.000	1.000	A	4.000
PCS	622	Math Methods in MedPhys	1.000	1.000	A-	3.670
PCS	623	Biostatistics	1.000	1.000	A+	4.330

			Attempted	Earned	GPA Units	Points
Term GPA	4.070	Term Totals	5.000	5.000	5.000	20.330
Transfer Term GPA		Transfer Totals	0.000	0.000	0.000	0.000
Combined GPA	4.070	Comb Totals	5.000	5.000	5.000	20.330

Academic Standing Effective 01/11/2021: Academic Standing: Clear

Winter 2021

Session:Undergraduate Regular

Course		Description	Attempted	Earned	Grade	Points
PCS	335	Thermodynamics Stat. Physics	1.000	1.000	A-	3.670
PCS	350	Computatnl Methds/Med Physics	1.000	1.000	B	3.000
PCS	352	Nuclear Physics	1.000	1.000	A	4.000
PCS	405	Medical Imaging	1.000	1.000	A+	4.330
PHL	201	Problems in Philosophy	1.000	1.000	A+	4.330

			Attempted	Earned	GPA Units	Points
Term GPA	3.870	Term Totals	5.000	5.000	5.000	19.330
Transfer Term GPA		Transfer Totals	0.000	0.000	0.000	0.000
Combined GPA	3.870	Comb Totals	5.000	5.000	5.000	19.330

Term Honor: Dean's List

Academic Standing Effective 05/10/2021: Academic Standing: Clear

Fall 2021

Session:Undergraduate Regular

Course		Description	Attempted	Earned	Grade	Points
CPS	501	Bioinformatics	1.000	1.000	A+	4.330
PCS	354	Radiation Biology	1.000	1.000	A+	4.330
PCS	810	Complex Networks and Appl	1.000	1.000	A+	4.330
PHL	611	Philosophy of Mind	1.000	1.000	A	4.000

			Attempted	Earned	GPA Units	Points
Term GPA	4.250	Term Totals	4.000	4.000	4.000	16.990
Transfer Term GPA		Transfer Totals	0.000	0.000	0.000	0.000
Combined GPA	4.250	Comb Totals	4.000	4.000	4.000	16.990

Academic Standing Effective 01/13/2022: Academic Standing: Clear

Winter 2022

Session:Undergraduate Regular

Course		Description	Attempted	Earned	Grade	Points
CPS	616	Algorithms	1.000	1.000	B+	3.330
CPS	650	Computational Thinking	1.000	1.000	A+	4.330
PCS	40B	Medical Physics - Thesis-B	2.000	2.000	A+	8.660
PCS	407	Radiation Therapy	1.000	1.000	A+	4.330
PHL	612	Philosophy of Law	1.000	1.000	A-	3.670

Personal information will be stored in the Personal Information Bank for the appropriate program.
PROTECTED B WHEN COMPLETED

RYERSON UNIVERSITY

Undergraduate

Name: **Mr Jordan Lanctot**
Student ID: **500910358**
OEN: **664268737**

			Attempted	Earned	GPA Units	Points
Term GPA	4.050	Term Totals	6.000	6.000	6.000	24.320
Transfer Term GPA		Transfer Totals	0.000	0.000	0.000	0.000
Combined GPA	4.050	Comb Totals	6.000	6.000	6.000	24.320

Term Honor: Dean's List

Academic Standing Effective 05/04/2022: Academic Standing: Clear

Undergraduate Career Totals

Cum GPA:	3.880	Cum Totals	38.000	38.000	37.000	143.630
Transfer Cum GPA		Transfer Totals	7.000	7.000	0.000	0.000
Combined Cum GPA	3.880	Comb Totals	45.000	45.000	37.000	143.630

End of Undergraduate

RYERSON