

Yash Sharma

✉ ysharma1126@gmail.com
🌐 <http://www.yash-sharma.com>
🔗 <https://scholar.google.com/citations?user=AlGCn8wAAAAJ&hl=en>
🐙 <http://www.github.com/ysharma1126>
📄 <http://www.kaggle.com/ysharma1126>
🌐 <http://www.linkedin.com/in/yashjsharma>

EDUCATION

Sep. 2014 - May. 2018 **Bachelor & Master in Electrical Engineering** - COOPER UNION
New York, NY, USA
Thesis: “Gradient-based Adversarial Attacks in Limited Access Settings”
Masters GPA: 3.8/4.0

RESEARCH EXPERIENCE

Sep. 2018 - Present **BOREALIS AI** - *ML Researcher*, Toronto, ON, Canada

- Working on developing more robust deep learning training methods, understanding adversarial examples, and improving generalization in reinforcement learning.

Jun. 2017 - Aug. 2017 **IBM RESEARCH** - *Research Intern*, Yorktown Heights, NY, USA

- Worked with the AI Foundations Learning Group on adversarial examples.
- Improved the state-of-the-art in black-box attacks (can query target model) and transfer attacks (cannot access target model) with [ZCS+17] and [SCZ+18].

TECHNICAL SKILLS

Programming Python, C++, Java
Machine Learning TensorFlow, PyTorch, Keras, Scikit-Learn

HONORS

2018 | **CAAD ATTACK COMPETITIONS WINNER**
2018 | **DEFCON 26 PRESENTER**
2017 | **KAGGLE COMPETITIONS MASTER**
2016 | **IBM BLOCKCHAIN HACKATHON WINNER**
2016 | **CODESUISSE WINNER**
2015 | **HACKRU PRIZE**
2014 | **HALF-TUITION SCHOLARSHIP**

Conference Proceedings

- [SAE+18] Y. Sharma, M. Alzantot, A. Elgohary, B.-J. Ho, M. Srivastava, and K.-W. Chang. “Generating Natural Language Adversarial Examples”. In *Conference on Empirical Methods in Natural Language Processing (EMNLP)*. <https://arxiv.org/abs/1804.07998>. 2018.
- [SCZ+18] Y. Sharma, P.-Y. Chen, H. Zhang, J. Yi, and C.-J. Hsieh. “EAD: Elastic-Net Attacks to Deep Neural Networks via Adversarial Examples”. In *AAAI Conference on Artificial Intelligence*. <https://arxiv.org/abs/1709.04114>. 2018.
- [ZCS+17] H. Zhang, P.-Y. Chen, Y. Sharma, J. Yi, and C.-J. Hsieh. “ZOO: Zeroth Order Optimization based Black-box Attacks to Deep Neural Networks without Training Substitute Models”. In *ACM Workshop on Artificial Intelligence and Security (AISeC)*. <https://arxiv.org/abs/1708.03999>. 2017.

Workshops

- [LBS18] Y. Li, J. Bradshaw, and Y. Sharma. “Are Generative Classifiers More Robust to Adversarial Attacks?” In *International Conference on Machine Learning (ICML) Workshops*. <https://arxiv.org/abs/1802.06552>. 2018.
- [SC18a] Y. Sharma and P.-Y. Chen. “Attacking the Madry Defense Model with L1-based Adversarial Examples”. In *International Conference on Learning Representations (ICLR) Workshops*. <https://arxiv.org/abs/1710.10733>. 2018.

Manuscripts

- [ASC+18] M. Alzantot, Y. Sharma, S. Chakraborty, and M. Srivastava. “GenAttack: Practical Black-box Attacks with Gradient-Free Optimization”. *arXiv preprint arXiv:1805.11090* (2018). <https://arxiv.org/abs/1805.11090>.
- [PFC+18] N. Papernot, F. Faghri, N. Carlini, I. Goodfellow, R. Feinman, A. Kurakin, C. Xie, Y. Sharma, T. Brown, A. Roy, A. Matyasko, V. Behzadan, K. Hambardzumyan, Z. Zhang, Y.-L. Juang, Z. Li, R. Sheatsley, A. Garg, J. Uesato, W. Gierke, Y. Dong, D. Berthelot, P. Hendricks, J. Rauber, and R. Long. “Technical Report on the CleverHans v2.1.0 Adversarial Examples Library”. *arXiv preprint arXiv:1610.00768* (2018). <https://arxiv.org/abs/1610.00768v6>.
- [SLA18] Y. Sharma, T.-D. Le, and M. Alzantot. “CAAD 2018: Generating Transferable Adversarial Examples”. *arXiv preprint arXiv:1810.01268* (2018). <https://arxiv.org/abs/1810.01268>.
- [SC18b] Y. Sharma and P.-Y. Chen. “Bypassing Feature Squeezing by Increasing Adversary Strength”. *arXiv preprint arXiv:1803.09868* (2018). <https://arxiv.org/abs/1803.09868>.

PROJECTS

- June. 2018 - Aug. 2018 **COMPETITION ON ADVERSARIAL ATTACKS AND DEFENSES (2018)**
Won Attacks Competitions + Placed 3rd in Defense
Participated in competition pitting submitted adversarial attacks against submitted defenses. Achieved **1st**, **1st**, and **3rd** in the Targeted Attack, Non-Targeted Attack and Defense competitions, respectively. Prize: \$38,000.
- Sep. 2017 - May. 2018 **LANE KEEPING AND NAVIGATION ASSIST SYSTEM**
IEEE Student Paper + Senior Project, 2018
Built a miniature autonomous vehicle which can navigate through maps consisting of various road topologies. System is comprised of a perception module, for detecting lanes and intersections, and a control module, for lane keeping and turn making.
- Aug. 2017 - Oct. 2017 **NIPS 2017 COMPETITION: ADVERSARIAL ATTACKS AND DEFENSES**
Achieved 1 Gold and 2 Silver Medals
Participated in competition pitting submitted adversarial attacks against submitted defenses. Achieved 6th, 11th, and 14th in the Targeted Attack, Defense, and Non-Targeted Attack competitions, respectively.
- Mar. 2017 - May. 2017 **LEARNING TO PLAY SUPER SMASH BROS. MELEE WITH DELAYED ACTIONS**
Used recurrent neural networks to teach a computer to play Super Smash Bros. Melee in a more humanlike way. Solution stabilized the training of competitive agents with reinforcement learning under human-level delay, as evidenced by qualitative and quantitative results against both the built-in AI and other trained agents.
- Jan. 2017 - May. 2017 **USING MACROECONOMIC FORECASTS TO IMPROVE MEAN REVERTING TRADING STRATEGIES**
Improved a multiple pairs trading strategy on major currency pairs using machine learning forecasts of a series of pertinent macroeconomic variables. This addition resulted in a clear improvement in the APR over the evaluation period.
- Mar. 2017 - May. 2017 **THE GAME OF SET**
Completed a client-server application which allows users to play the game of SET against each other over the internet. Used JavaFX8 for the UI and MySQL for the database. On the server-side, pipes were used to communicate between threads. Used the publish-subscribe messaging pattern for server-client communication.