به نام ایزد یکتا

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

تمرین هفتم درس روش پژوهش و ارائه

استاد: دکتر رضا صفابخش

تهیه کننده: بردیا اردکانیان

برسی و مهار مثال‌های خصمانه در یادگیری ماشین

Bibliography

Elsevier - Harvard

Adversarial Examples Are Not Easily Detected | Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security [WWW Document], n.d. URL https://dl.acm.org/doi/abs/10.1145/3128572.3140444 (accessed 5.28.22).

Adversarial Machine Learning Attacks and Defense Methods in the Cyber Security Domain | ACM Computing Surveys [WWW Document], n.d. URL https://dl.acm.org/doi/10.1145/3453158 (accessed 5.27.22).

Adversarial machine learning for cybersecurity and computer vision: : Current developments and challenges: WIREs Computational Statistics: Vol 12, No 5, n.d. . Wiley Interdisciplinary Reviews: Computational Statistics.

Biggio, B., Roli, F., 2018. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition 84, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

Brachman, R.J., Stone, P., n.d. Synthesis Lectures on Artificial Intelligence and Machine Learning 169.

Goodfellow, I.J., Shlens, J., Szegedy, C., 2015. Explaining and Harnessing Adversarial Examples.

Huang, L., Joseph, A.D., Nelson, B., Rubinstein, B.I.P., Tygar, J.D., 2011. Adversarial machine learning, in: Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence, AISec '11. Association for Computing Machinery, New York, NY, USA, pp. 43–58. https://doi.org/10.1145/2046684.2046692

Laskov, P., Lippmann, R., 2010. Machine learning in adversarial environments. Mach Learn 81, 115–119. https://doi.org/10.1007/s10994-010-5207-6

Machine learning uncertainties with adversarial neural networks | SpringerLink [WWW Document], n.d. URL https://link.springer.com/article/10.1140/epjc/s10052-018-6511-8 (accessed 5.27.22).

McDaniel, P., Papernot, N., Celik, Z.B., 2016. Machine Learning in Adversarial Settings. IEEE Security Privacy 14, 68–72. https://doi.org/10.1109/MSP.2016.51

Tabassi, E., Burns, K.J., Hadjimichael, M., Molina-Markham, A.D., Sexton, J.T., 2019. A taxonomy and terminology of adversarial machine learning (preprint). https://doi.org/10.6028/NIST.IR.8269-draft

Wiyatno, R.R., Xu, A., Dia, O., de Berker, A., 2019. Adversarial Examples in Modern Machine Learning: A Review.

Yuan, X., He, P., Zhu, Q., Li, X., 2019. Adversarial Examples: Attacks and Defenses for Deep Learning. IEEE Transactions on Neural Networks and Learning Systems 30, 2805–2824. https://doi.org/10.1109/TNNLS.2018.2886017

Zhang, C., Benz, P., Imtiaz, T., Kweon, I.S., 2020. Understanding Adversarial Examples From the Mutual Influence of Images and Perturbations, in: 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Presented at the 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 14509–14518. https://doi.org/10.1109/CVPR42600.2020.01453

Zhao, Z., Dua, D., Singh, S., 2018. Generating Natural Adversarial Examples.

Zheng, H., Zhang, Z., Gu, J., Lee, H., Prakash, A., 2020. Efficient Adversarial Training With Transferable Adversarial Examples, in: 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Presented at the 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), IEEE, Seattle, WA, USA, pp. 1178–1187. https://doi.org/10.1109/CVPR42600.2020.00126

Zizzo, G., Hankin, C., Maffeis, S., Jones, K., 2019. INVITED: Adversarial Machine Learning Beyond the Image Domain, in: 2019 56th ACM/IEEE Design Automation Conference (DAC). Presented at the 2019 56th ACM/IEEE Design Automation Conference (DAC), pp. 1–4.