Self-Robust 3D Point Recognition via Gather-vector Guidance

Xiaoyi Dong[1], Dongdong Chen[2]*, Hang Zhou[1] , Gang Hua[3], Weiming Zhang[1], Nenghai Yu[1],
[1]University of Science and Technology of China [2]Microsoft Cloud AI, [3]Wormpex AI Research
{dlight@mail., zh2991@mail., zhangwm@, ynh@ }.ustc.edu.cn {ganghua@,cddlyf@}gmail.com

1. Compare GvG-P with adversarial training and other defense methods.

Here we compare our method with two common adversarial defense methods: adversarial training and input preprocessing. The attack method used here is I-FGM with $\delta = 0.32$. For adversarial training, we follow the strategy in [1], the MSG-P with adversarial training shows better robustness that the attack success rate decrease from 93.88% to 76.12%, similar to the performance of our GvG-P which is 74.47%. For the input preprocessing, results of random point dropping are reported in Fig.5 in our paper. We can find that with the increase of dropped point number, the attack success rate decrease. When dropping 500 points(the original input point clouds contains 2048 points), the attack success rate of MSG-P is similar to our GvG-P that without dropping. When we add the same defense method on our GvG-P, we find the adversarial training decrease the success rate from 74.47% to 61.67%, while from Fig.5 in main paper, we find dropping 500 points decrease the success rate to 52.63%.

2. Robustness evaluation for GvG-P

Our method is not sensitive to non-adversarial perturbations. For example, Fig.5 shows the recognition accuracy of random dropped point clouds. We can observe that even if 900 points (2048 points in total) are randomly dropped, the recognition accuracy decrease of our method is very negligible (less than 1%). We also tried noisy perturbation and further demonstrate the insensitivity of our method to it. For small perturbations, we add random uniform distribution noise on the clean point clouds and keep the size of the perturbation equals to adversarial samples generated by I-FGM($\delta = 0.16$). The accuracy of our GvG-P decrease from 88.65% to 88.21%, less than 0.5%.

The robustness of our method toward non-adversarial perturbations are benefited from the robustness of PointNet++ structure. As we stated in Sec 3.3, the 'Local Feature Generation Network' part, we use the PointNet++ as the backbone for feature generation and calculate gather-vector from the generated features. So the sensitivity of gather-vector toward non-adversarial perturbations equals to the sensitivity of local features toward these non-adversarial perturbations. As illustrated in [2, 3], PointNet and PointNet++ is very robust to such perturbations.

*Dongdong Chen is the corresponding author.

References

[1] Daniel Liu, Ronald Yu, and Hao Su. Extending adversarial attacks and defenses to deep 3d point cloud classifiers. *arXiv preprint arXiv:1901.03006*, 2019.

[2] Charles R Qi, Hao Su, Kaichun Mo, and Leonidas J Guibas. Pointnet: Deep learning on point sets for 3d classification and segmentation. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 652–660, 2017.

[3] Charles Ruizhongtai Qi, Li Yi, Hao Su, and Leonidas J Guibas. Pointnet++: Deep hierarchical feature learning on point sets in a metric space. In *Advances in neural information processing systems*, pages 5099–5108, 2017.