Supplementary Materials of On Isometry Robustness of Deep 3D Point Cloud Models Under Adversarial Attacks

Yue Zhao[1], Yuwei Wu[1], Caihua Chen[2]*, Andrew Lim[1]
[1]Department of Industrial Systems Engineering and Management, National University of Singapore
[2]School of Management and Engineering, Nanjing University
{yuezhao, ywwu}@u.nus.edu, chchen@nju.edu.cn, isealim@nus.edu.sg

Contents

*Corresponding author.

1. Isometry Formulas

1.1. Rotations

We use rotation matrices of the form [1]:

$$
\begin{aligned}
R_x(\theta_x) &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta_x & -\sin\theta_x \\ 0 & \sin\theta_x & \cos\theta_x \end{bmatrix} \\
R_y(\theta_y) &= \begin{bmatrix} \cos\theta_y & 0 & -\sin\theta_y \\ 0 & 1 & 0 \\ \sin\theta_y & 0 & \cos\theta_y \end{bmatrix} \\
R_z(\theta_z) &= \begin{bmatrix} \cos\theta_z & -\sin\theta_z & 0 \\ \sin\theta_z & \cos\theta_z & 0 \\ 0 & 0 & 1 \end{bmatrix}
\end{aligned} \tag{1}
$$

For a point cloud $P \in \mathbb{R}^{n\times 3}$, $PR(\theta_x)^T$ is to rotate P about x axis by θ_x clockwise using right-hand rule. Thus PR^T where $R = R_x(\theta_x)R_y(\theta_y)R_z(\theta_z)$ is to clockwise rotate P about axis z, y, x by $\theta_z, \theta_y, \theta_x$ sequentially.

1.2. Reflections

Reflection has many definitions, here we take the one defined by Householder matrix [2]

$$
P = I - vv^T, \tag{2}
$$

where v is a unit normal vector of hyper-plane $\{x \in \mathbb{R}^n : v^T x = 0\}$. Let $x' = Px, \forall x \in \mathbb{R}^n$. It is easy to prove that $(x - x')//v$ and the distances of x and x' to the hyper-plane are the same.

Since isometry in $\mathbb{R}^3$ can be represented by at most 3 reflections and the case of two reflections equals to a rotation, we can consider the following 3 situations

- One reflection, parameterized by formula 2
- Two reflections, considered as one rotation parameterized by fomula 1
- Three reflections, for efficiency we use one reflection and rotation about z axis in experiments

We already showed the experiments of case 2 in main body of the paper, in the following section we will show experiment results of case 1 and 3.

2. Experiment of Reflections

2.1. Case 1: One Reflection

In this subsection, we evaluate TSI and CTRI attacks based on initial isometry generated by reflections. There are only two parameters in this case.

	ModelNet40			ShapeNetPart		
	S=1	S=2	S=10	S=1	S=2	S=10
PointNet	75.52	91.23	98.72	58.15	79.79	97.13
PointNet++	58.24	78.14	93.51	49.75	69.13	90.81
DG-CNN	51.18	73.63	94.95	41.59	61.63	93.44
RS-CNN	58.85	79.31	96.25	47.62	70.13	95.50

Table 1. Attack success rates (%) of TSI initiated with case 1 (One reflection) for different S.

It is shown in Table 1 that when $S = 1$ attack success rates of TSI is not as high as those in rotation cases, but when we increase S, the attack performance becomes better.

	ModelNet40			ShapeNetPart		
	K=7	K=50	K=1000	K=7	K=50	K=1000
PointNet	99.39	99.61	100.00	99.02	99.39	100.00
PointNet++	97.31	97.60	98.61	96.10	96.45	99.34
DG-CNN	97.62	98.46	99.34	97.96	98.06	100.00
RS-CNN	97.65	97.82	99.39	97.93	98.13	100.00

Table 2. Attack success rates (%) of CTRI initiated with matrices in case 1. $\lambda = 0.001$ and learning step $\eta = 0.0005$. In order to get a good initial point here we use $S = 50$ for TSI.

	Max	Mean	Variance	Mean*	Variance*
PointNet	0.099	2E-4	2E-5	0.044	7E-4
PointNet++	0.044	2E-4	5E-6	0.006	1E-4
DG-CNN	0.095	2E-4	1E-5	0.023	6E-4
RS-CNN	0.068	9E-5	4E-6	0.021	4E-4

Table 3. Statistics of $\sigma(A^T A - I)$ for the second column (ModelNet40, $K = 50$) of table 2.

	Max	Mean	Variance	Mean*	Variance*
PointNet	1.251	0.001	0.001	0.184	0.093
PointNet++	0.803	0.002	0.001	0.062	0.026
DG-CNN	1.277	0.007	0.006	0.357	0.170
RS-CNN	0.937	0.008	0.006	0.482	0.123

Table 4. Statistics of $\sigma(A^T A - I)$ for the third column (ModelNet40, $K = 1000$) of table 2.

2.2. Case 3: One Reflection and one Rotation

In this subsection, we evaluate TSI and CTRI attacks based on inital isometry generated by one reflection and one rotation about z axis. There are only three parameters in this case.

	ModelNet40			ShapeNetPart		
	S=1	S=2	S=10	S=1	S=2	S=10
PointNet	89.76	96.50	99.05	78.85	90.21	97.90
PointNet++	82.38	90.94	95.29	74.23	86.29	92.80
DG-CNN	76.45	89.31	96.45	67.89	82.31	96.17
RS-CNN	82.07	92.98	97.00	73.03	88.24	96.96

Table 5. Attack success rates (%) of TSI initiated with case 3 (One reflection and one rotation) for different S.

	ModelNet40			ShapeNetPart		
	K=7	K=50	K=1000	K=7	K=50	K=1000
PointNet	99.16	99.55	100.00	99.23	99.54	100.00
PointNet++	97.88	98.10	98.66	96.35	97.15	99.29
DG-CNN	98.23	98.45	99.72	98.42	98.67	99.95
RS-CNN	97.88	98.27	99.10	98.27	98.73	99.90

Table 6. Attack success rates (%) of CTRI initiated with matrices in case 3. $\lambda = 0.001$ and learning step $\eta = 0.0005$. In order to get a good initial point here we use $S = 50$ for TSI.

	Max	Mean	Variance	Mean*	Variance*
PointNet	0.076	1E-4	7E-6	0.032	9E-4
PointNet++	0.072	2E-4	7E-6	0.007	2E-4
DG-CNN	0.048	9E-5	3E-6	0.017	2E-4
RS-CNN	0.050	8E-5	3E-6	0.026	3E-4

Table 7. Statistics of $\sigma(A^T A - I)$ for the second column (ModelNet40, $K = 50$) of table 6.

	Max	Mean	Variance	Mean*	Variance*
PointNet	0.634	0.001	4E-4	0.171	0.029
PointNet++	0.479	0.002	5E-4	0.057	0.013
DG-CNN	1.076	0.005	0.003	0.236	0.095
RS-CNN	0.924	0.004	0.003	0.413	0.115

Table 8. Statistics of $\sigma(A^TA - I)$ for the second column (ModelNet40, $K = 1000$) of table 6.

3. More Visualization

In this section we visualize adversarial samples generated by our algorithms. In the follow pictures, penalty refers to $\sigma(A^TA - I)$, A is an isometry when penalty is 0. The adversarial samples are generated from PointNet [3] model and two data sets: ModelNet40 [4] and part of ShapeNet [5].

Adversarial samples generated from ModelNet40 are shown in Figure 1 and 2, those from ShapeNetPart are illustrated in Figure 3 and 4. As we can see, even when penalty is relatively large (> 0.1), the global shape of objects is well preserved.

Examples of interactive 3D visualization are presented in the folder '/visual_html/', where the 3D objects can be zoomed in or out and rotated by the users for closer observations.

References

[1] Herbert Goldstein, Charles Poole, and John Safko. Classical mechanics, 2002. 2

[2] Alston S Householder. Unitary triangularization of a nonsymmetric matrix. *Journal of the ACM (JACM)*, 5(4):339–342, 1958. 2

[3] 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. 4

[4] Zhirong Wu, Shuran Song, Aditya Khosla, Fisher Yu, Linguang Zhang, Xiaoou Tang, and Jianxiong Xiao. 3d shapenets: A deep representation for volumetric shapes. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1912–1920, 2015. 4

[5] Li Yi, Vladimir G Kim, Duygu Ceylan, I Shen, Mengyan Yan, Hao Su, Cewu Lu, Qixing Huang, Alla Sheffer, Leonidas Guibas, et al. A scalable active framework for region annotation in 3d shape collections. *ACM Transactions on Graphics (TOG)*, 35(6):210, 2016. 4

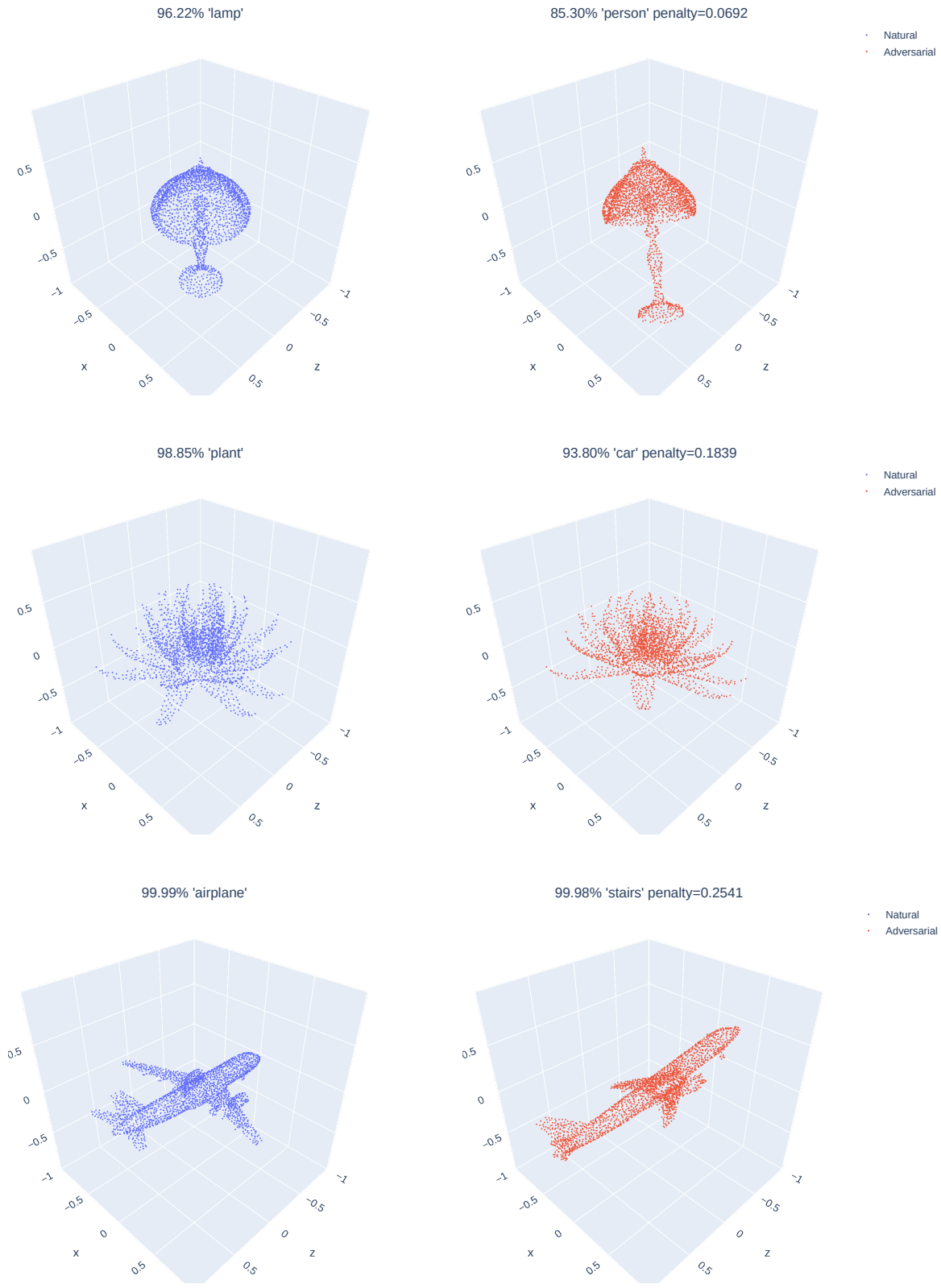

Figure 1. Generated from ModelNet40, rotation used in TSI

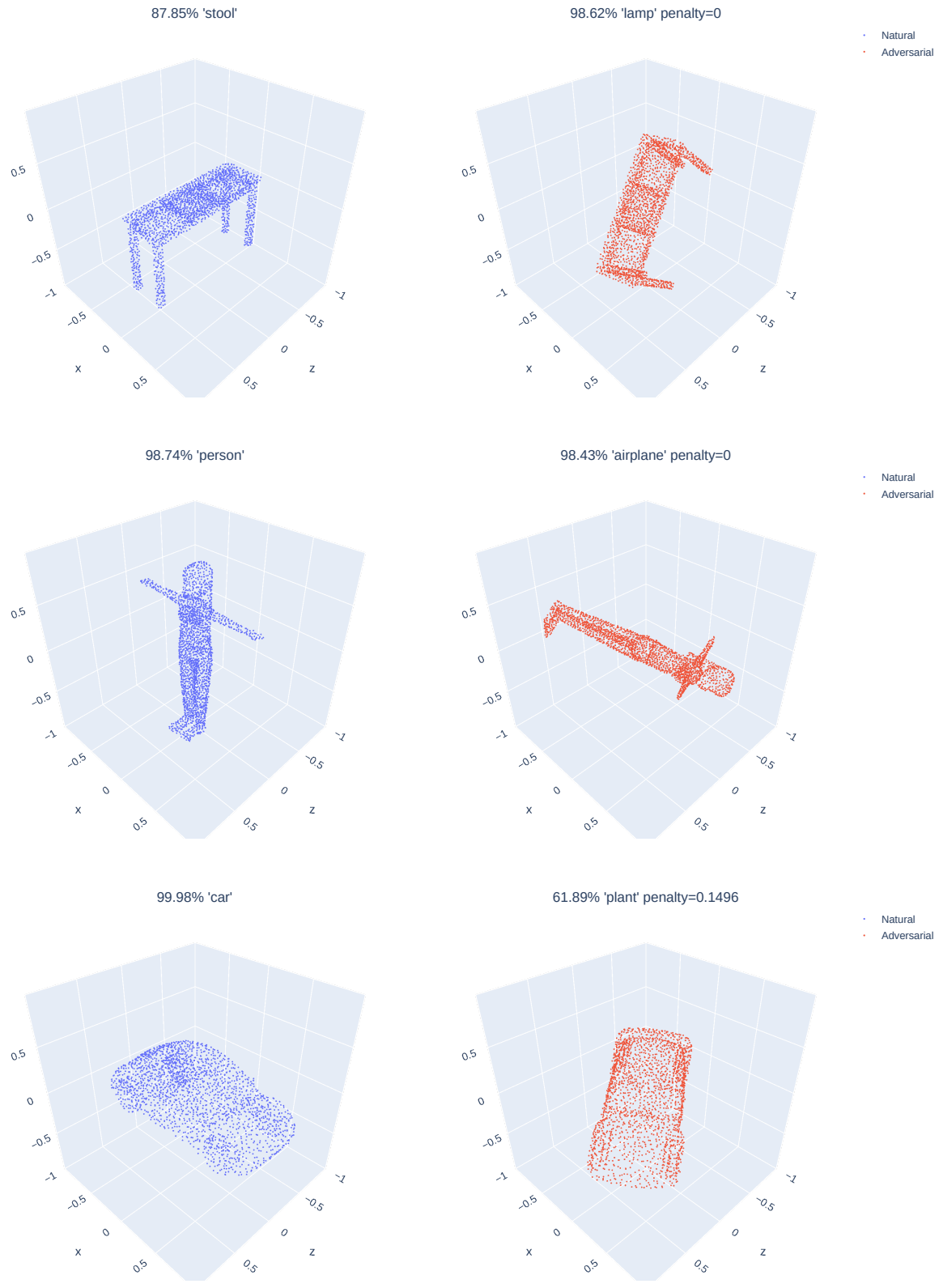

Figure 2. Generated from ModelNet40, reflection used in TSI

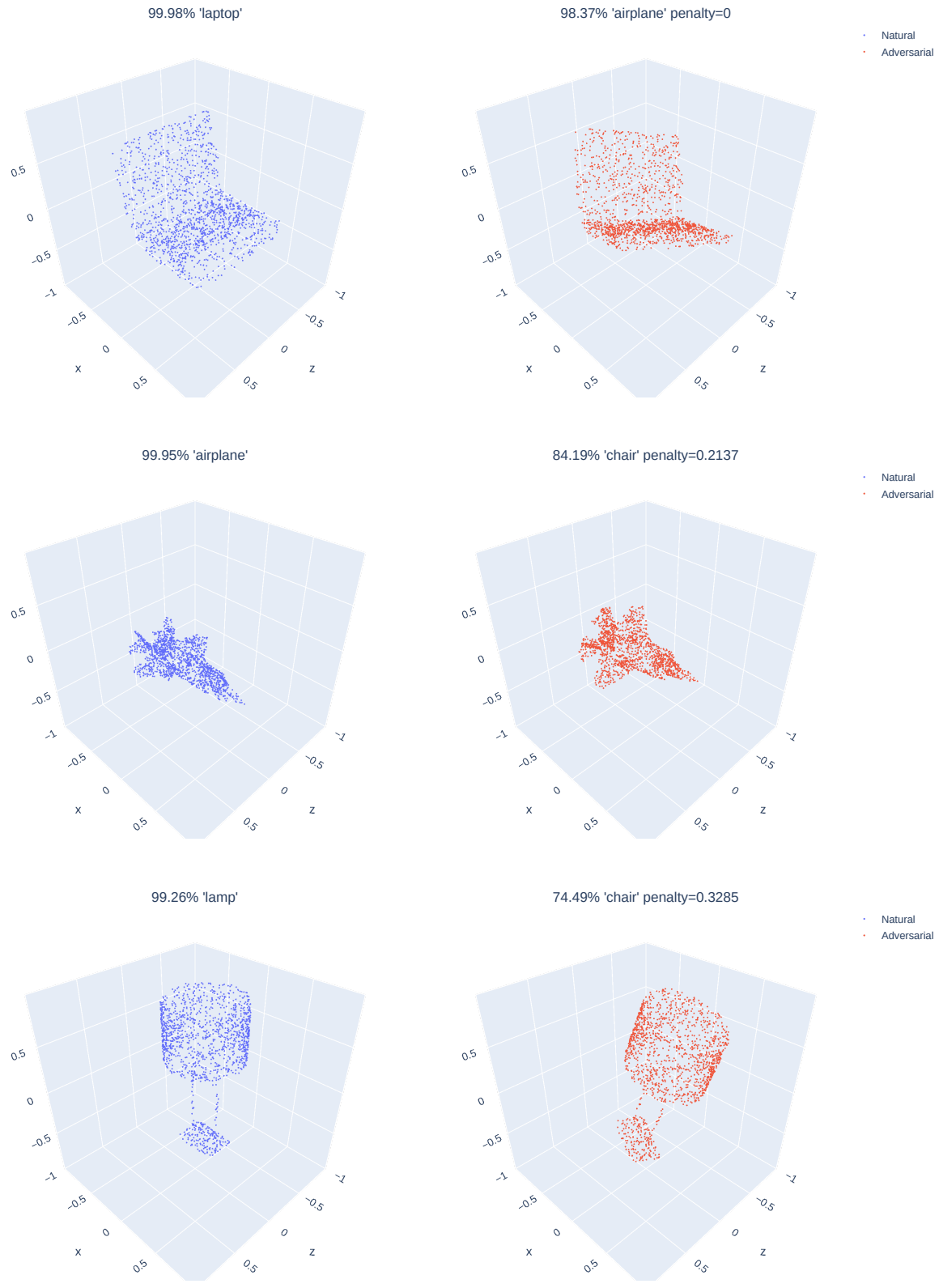

Figure 3. Generated from ShapeNetPart, rotation used in TSI

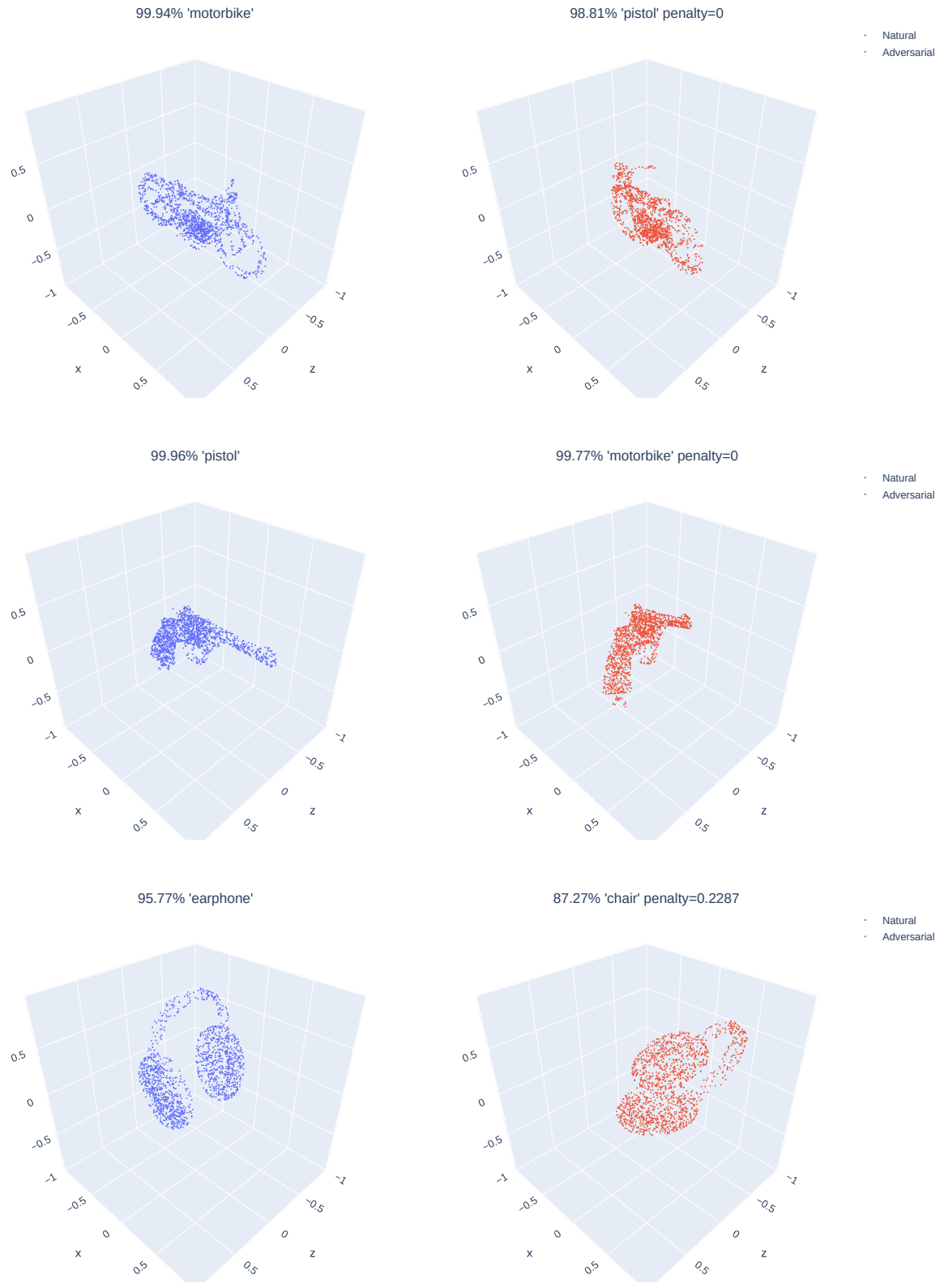

Figure 4. Generated from ShapeNetPart, reflection used in TSI