Generating 3D Adversarial Point Clouds
Supplementary Material

Chong Xiang
Shanghai Jiao Tong University
Shanghai, China
xiangchong97@gmail.com

Charles R. Qi
Facebook AI Research
California, USA
charlesq34@gmail.com

Bo Li
University of Illinois at Urbana-Champaign
Illinois, USA
lxbosky@gmail.com

A. Additional Quantitative Results

In this section, we provide additional quantitative results for point clouds attacks from adversarial clusters, adversarial objects, adversarial point perturbation, and independent points adding.

Adversarial Clusters and Adversarial Object under Three Attack Cases. Table 1 and Table 2 report our attacks under three cases: best case, average case and worst case for adversarial cluster attack and adversarial object attack respectively. We report (victim,target) pairs with the least distance losses among all 100% successfully attacked pairs as the best cases. We report the (victim, target) pairs with the smallest success rates as the worst cases. It is obvious that constraining the attack to only one cluster significantly increases the attack difficulty.

Adversarial Point Perturbation. To better understand the attack performance of point shifting in adversarial point perturbation, we plot the distribution of perturbation magnitude (L_2 norm) for each point in Figure 1. It is obvious that for all three cases, most points (80%) are barely shifted (less than 0.005 compared to the object scale of 1.0), and the shifting distances for most shifted point are within 0.03, which is negligible comparing with the size of a unit ball.

Adversarial Independent Points. To help further understand the characteristics of Hausdorff and Chamfer constraints and explain why we include Hausdorff distance despite of its "poor" quantitative performance, we plot the distribution of distances from each point to the object surface in Figure 2. As expected, the number or percentage of points with non-trivial distance under Hausdorff optimization is larger than that under Chamfer optimization. However, it should be noticed that the largest distance of the Hausdorff case (0.18) is much smaller than that of Chamfer (0.42). This difference suggests that added points with Hausdorff constraint are likely to have fewer outliers, and thus less noticeable compared with those added based on Chamfer constraint. This result justifies our proposal to include Hausdorff distance as a perturbation metric $\mathcal{D}$.

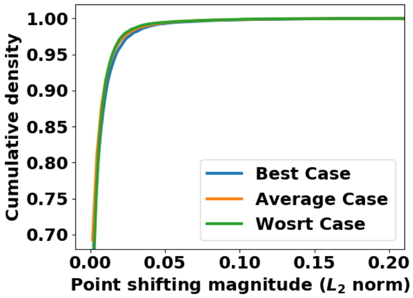

Figure 1: CDF of point shifting distance for adversarial point perturbation.

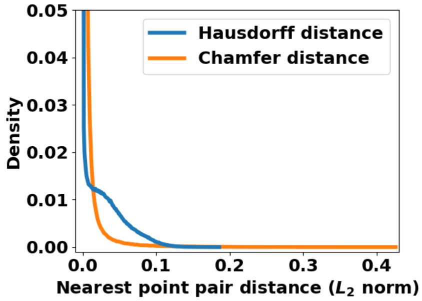

Figure 2: Distributions for distance of nearest point pairs in independent point adding attack.

B. Additional Visualization Results

Besides bottles, here we provide visualizations of victim objects in more categories. The visualization results for adversarial clusters and adversarial objects are in Figure 3 and Figure 4, respectively.

C. Acknowledgement

This work is supported by Zhiyuan Scholar Program (Grant No. ZIRC2018-04).

Case	1 cluster			2 clusters			3 clusters		
	$\mathcal{D}_{far}$	$\mathcal{D}_C$	success rate	$\mathcal{D}_{far}$	$\mathcal{D}_C$	success rate	$\mathcal{D}_{far}$	$\mathcal{D}_C$	success rate
Best	0.0207	0.0300	100%	0.0184	0.0331	100%	0.0191	0.0349	100%
Average	0.5401	0.1372	78.8%	0.3118	0.1839	98.2%	0.1818	0.1744	99.3%
Worst	0.0265	0.0051	4.0%	0.4452	0.0286	64.0%	0.4797	0.1410	80.0%

Table 1: Attack performance evaluation for adversarial clusters (three cases).

Case	1 cluster			2 clusters			3 clusters		
	$\mathcal{D}_{L_2}$	$\mathcal{D}_C$	success rate	$\mathcal{D}_{L_2}$	$\mathcal{D}_C$	success rate	$\mathcal{D}_{L_2}$	$\mathcal{D}_C$	success rate
Best	0.0071	0.0176	100%	0.0019	0.0072	100%	0.0021	0.0073	100%
Average	0.5539	0.1776	54.6%	0.0838	0.1332	93.8%	0.0212	0.0850	97.3%
Worst	0.1256	0.0223	8.0%	0.0883	0.0205	20.0%	0.0485	0.0832	56.0%

Table 2: Attack performance evaluation for adversarial objects (three cases).

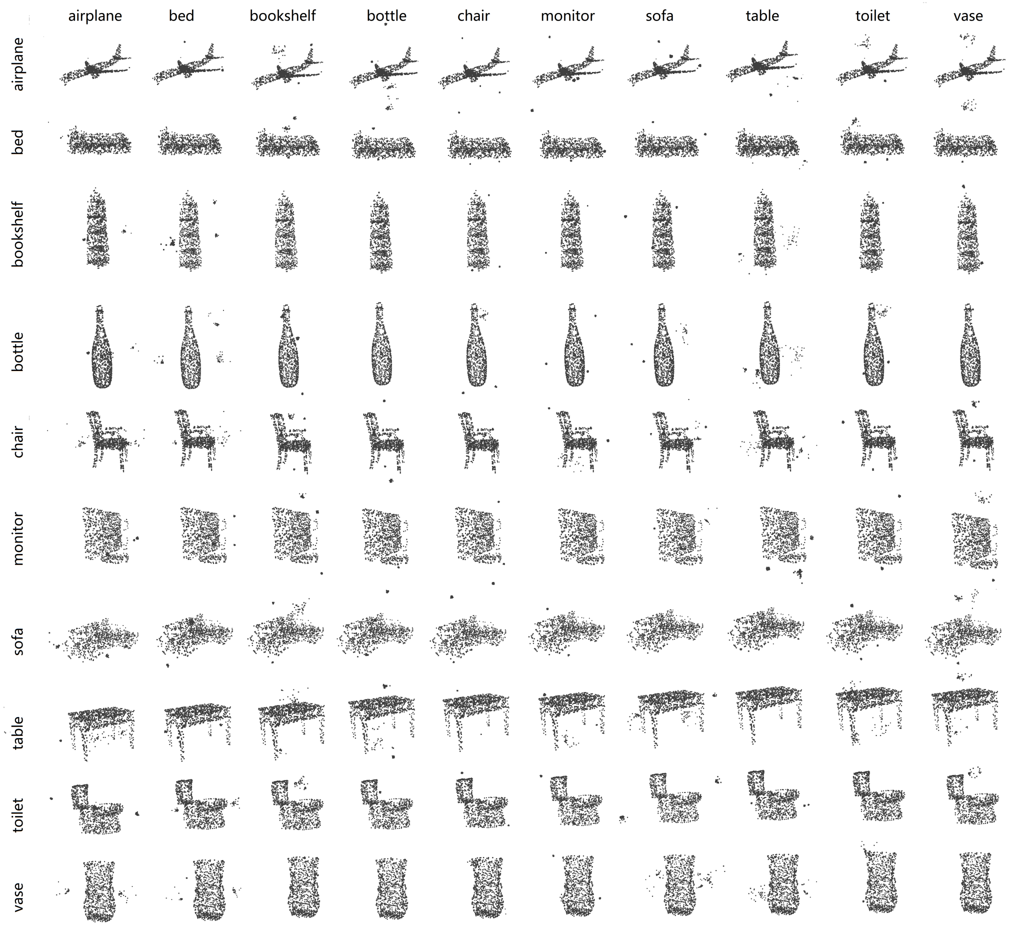

Figure 3: Visualization for adding 3 adversarial clusters (all attack pairs).

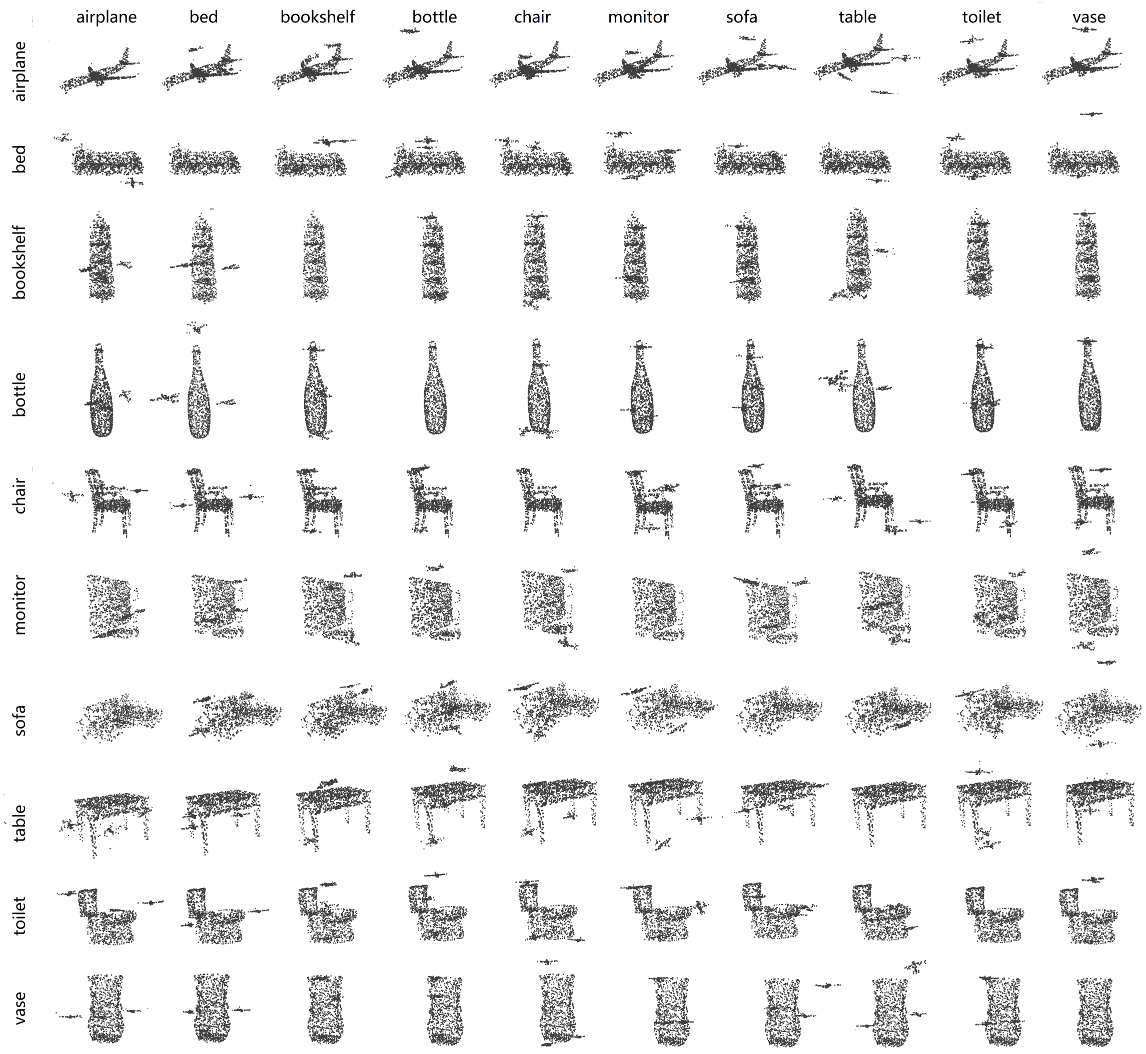

Figure 4: Visualization for adding 3 adversarial objects (all attack pairs).