Supplement Material

Qiufan Ji[1], Lin Wang [2,3,*], Cong Shi[1], Shengshan Hu[4], Yingying Chen[5], Lichao Sun[6] *
[1]New Jersey Institute of Technology, [2]AI Thrust, HKUST(GZ), [3]Dept. of CSE, HKUST, [4]HUST,
[5]Rutgers University, [6]Lehigh University
qj39@njit.edu, linwang@ust.hk, cong.shi@njit.edu, hushengshan@hust.edu.cn,
yingche@scarletmail.rutgers.edu, james.lichao.sun@gmail.com

A. Implementation Details

In this section, we provide a comprehensive description of implementation details for adversarial attacks, defenses and point cloud DNNs. A visualization is shown in Figure 1

A.1. Adversarial Attacks

In our benchmark, we evaluate all attacks under the same untargeted settings. For targeted attacks, including GeoA3 [12], KNN [10], Perturb [14], Add Independent Points [14], and AdvPC [2], we assign the target class as the one with the highest logits value, excluding the ground truth label.

A.1.1 Adding Independent points

In this work, we adopt the methodology proposed by Xiang et al. [14], utilizing the C&W framework in conjunction with the Chamfer distance as the perturbation metric. To facilitate this process, we add 100 points in total and introduce perturbations throughout the optimization phase. Furthermore, we conduct a 10-step binary search, executing 500 iterations per step.

A.1.2 Removing Points

Following the approach proposed by Yang et al. [15], we utilized a greedy algorithm that iteratively computes the saliency map for all remaining points. In each iteration, the top five points with the highest saliency scores are removed.

A.1.3 PGD and IFGM

We adopt the default hyper-parameters as described in [5], setting the number of iterations to 50 and defining the step size λ as follows:

$$\lambda = \frac{\rho}{i}, \tag{1}$$

where ρ represents the perturbation budget and i denotes the number of iterations.

A.1.4 L3A

In accordance with the approach presented by Sun et al. [9], we utilize the Adam optimizer for the optimization of our objective loss function. The learning rate is set to 0.001, while the momentum parameters β_1 and β_2 are assigned values of 0.9 and 0.999, respectively.

*L. Wang and L. Sun are the corresponding authors.

A.1.5 KNN

In our implementation of the k-Nearest Neighbors (kNN) approach [10, 1], we employ the C&W optimization framework, utilizing the Chamfer distance as perturbation metrics. The algorithm is configured with a maximum of 2,500 iterations and a step size of 1e-4.

A.1.6 GeoA3

In the GeoA3 attack [12], we employ the C&W optimization framework, incorporating Chamfer distance, Hausdorff distance, and local curvatures as perturbation metrics [12]. Our benchmark comprises a 10-step binary search, executing 500 iterations.

A.1.7 AOF

In accordance with the methodology presented in Liu et al. [4], we set the number of low-frequency points to 100 and utilize the C&W optimization framework to compute the loss in time domain and frequency domain. The optimization process is carried out for 200 iterations, with a step size of 1e-3.

A.1.8 AdvPC

For AdvPC [2], we employ C&W attack framework with per-point L_2 norm as the perturbation metrics. The number of iterations is 200, binary search is 2, and step size is set to 1-e2.

A.1.9 Perturbation

Following [14], the perturbation metrics are same as AdvPC [2]. We perform a 10-step binary search with 500 iterations and the step size is set to 1e-2.

A.1.10 SIA

Based on the [3], we use a step size of 0.007 for 50 iterations to generate SIA adversarial examples.

A.2. Adversarial Defenses

A.2.1 Simple Random Sampling

Simple Random Sampling (SRS) is a technique for selecting a representative subset from a large-scale point cloud, wherein each point is assigned an equal probability of inclusion. In our benchmark, we randomly dropped 500 points from the input.

A.2.2 Statistic Outlier Removal

In the Statistic Outlier Removal (SOR) method, we leverage the k-Nearest Neighbors (kNN) algorithm [1] to compute the average pairwise distance for each point. Subsequently, points surpassing the threshold of $\mu + \alpha \cdot \sigma$ are removed, where μ and σ represent the mean and standard deviation, respectively, while k and α are hyperparameters. In our experiments, we set $k = 2$ and $\alpha = 1.1$.

A.2.3 DUP-Net

Regarding the implementation of DUP-Net [18], we adopt the PU-Net [16] and train it on the Visionair dataset [16]. To enhance the model's performance on point cloud data, we establish an upsampling rate of 4.

A.2.4 IF-Defense

In light of the experimental findings reported in IF-Defense [13], ConvONet [6] demonstrates superior performance in terms of accuracy across diverse adversarial scenarios. Consequently, we adopt ConvONet as the baseline model for our IF-Defense benchmark. The ConvONet model is trained to utilize two widely-established datasets: ModelNet40 and ShapeNet. A learning rate of 1e-4 is employed throughout the training process.

Figure 1. Visualization of different attacks and defense results. For the attacks, we choice Add, Drop, PGD, SIA, AOF, and KNN. For defenses, we shows the results of SOR, ConvONet, and SOR+ConvONet.

A.2.5 PointCutMix

In PointCutmix [17], the superior adversarial robustness of PointCutmix-R has led to its selection as the baseline method. During the training process, the probability of augmenting each point cloud is set at 0.5.

A.3. Point Cloud DNNs

For the surrogate models, we train them for 100 epochs using a batch size of 32, while for the victim models, we employ the same batch size but extend the training to 200 epochs. We utilize the Adam optimization algorithm and adopt a cosine annealing scheduler to progressively decay the learning rate from 1e-3 to 1e-5. For DGCNN, PointConv, Curvenet, GDANet, and RPC, we set the number of neighbors $k = 20$. Additionally, we set the number of points in each component to 256 in the frequency operation of GDANet.

B. Additional Discussion

B.1. Ablation Study of Our Defense Framework

As shown in Table 1, we perform an ablation study by removing one component at a time from our defense framework to evaluate the individual contributions of each component to the overall adversarial robustness. The complete defense framework consistently achieves the highest accuracy across all models, indicating that each key component positively contributes to the adversarial robustness. Furthermore, the variant without hybrid training exhibits the lowest accuracy for every model, suggesting that hybrid training is the most critical component for enhancing adversarial robustness in our defense framework.

Table 1. Ablation Study: Robustness of ensemble defense framework. Bold: the best on each point cloud DNNs.

Model	Defense	PGD	SIA	L3A	AOF	Drop	KNN	GEOA3	ADVPC	IFGM	ADD	Perturb	Acc
PointNet	w/o SOR	75.89	60.21	60.74	77.55	81.48	77.63	83.02	84.32	76.74	85.25	86.67	77.23
	w/o Hybrid Training	44.89	68.60	68.76	65.19	75.28	82.46	82.74	83.79	85.41	82.86	85.01	74.99
	w/o ConvONet	77.14	72.81	69.36	79.13	74.75	83.91	80.87	85.33	86.62	88.12	87.56	80.51
	Ours	76.70	76.26	75.04	80.79	81.60	85.53	84.04	86.22	87.28	86.26	86.35	**82.37**
PointNet++	w/o SOR	71.07	61.18	65.32	80.19	84.04	80.51	85.13	86.35	71.19	86.47	88.61	78.18
	w/o Hybrid Training	38.61	72.45	72.33	73.01	78.28	85.56	85.17	85.66	87.20	85.37	87.12	77.34
	w/o ConvONet	74.83	78.81	74.84	82.34	82.49	87.48	83.02	86.59	88.49	89.42	88.82	83.37
	Ours	71.56	78.61	76.70	83.14	84.12	86.87	85.78	87.40	88.45	88.17	88.70	**83.59**
DGCNN	w/o SOR	72.37	70.02	70.54	81.93	82.70	82.13	84.93	86.47	72.85	87.12	88.13	79.93
	w/o Hybrid Training	40.32	77.92	76.05	71.48	80.35	85.78	85.41	85.49	86.75	85.86	87.32	78.43
	w/o ConvONet	75.20	82.37	75.24	79.62	82.34	87.24	75.93	85.78	87.60	89.38	87.92	82.60
	Ours	72.93	81.81	77.96	82.94	84.08	86.39	84.81	86.71	88.17	87.76	87.32	**83.72**
PointConv	w/o SOR	69.53	66.00	69.17	78.44	83.91	81.81	85.09	86.02	71.03	87.24	87.40	78.69
	w/o Hybrid Training	28.61	78.24	73.66	73.87	75.89	84.85	84.24	84.48	85.58	84.20	85.37	76.27
	w/o ConvONet	71.19	79.38	73.91	79.17	83.99	87.97	80.96	87.36	89.10	89.63	89.83	82.95
	Ours	70.14	80.67	76.50	83.79	81.77	86.30	85.53	86.83	87.88	87.52	86.95	**83.08**
PCT	w/o SOR	74.11	68.03	66.05	77.80	77.15	79.38	81.28	81.40	73.66	83.31	83.18	76.85
	w/o Hybrid Training	45.83	75.24	73.45	72.85	79.42	85.86	85.29	86.35	87.16	85.94	86.83	78.57
	Ours w/o ConvONet	74.84	76.99	74.11	79.74	72.45	82.25	78.36	82.09	82.05	83.43	82.74	79.00
	Ours	73.91	78.32	75.77	76.86	79.66	82.41	80.71	81.60	82.78	82.21	83.710	**79.81**
Curvenet	w/o SOR	76.22	65.88	67.83	80.75	83.51	79.50	84.16	86.10	76.05	86.79	87.72	79.50
	w/o Hybrid Training	45.38	76.18	75.45	74.19	80.51	85.45	86.02	86.14	88.01	86.75	86.67	79.16
	w/o ConvONet	78.85	80.06	76.70	82.74	82.74	86.43	82.66	86.43	87.88	88.25	87.16	83.63
	Ours	76.13	80.26	78.16	83.67	83.59	87.20	84.97	86.14	88.05	86.99	87.88	**83.91**
RPC	w/o SOR	73.50	70.10	69.65	81.77	83.10	83.31	85.58	86.47	73.74	86.69	88.37	80.21
	w/o Hybrid Training	40.44	76.13	73.62	73.58	77.43	83.95	86.06	84.60	87.72	85.90	87.64	77.92
	w/o ConvONet	74.11	83.55	73.62	82.33	81.65	88.17	83.02	87.07	89.06	89.63	89.63	83.80
	Ours	74.11	82.66	78.20	82.98	84.48	87.93	85.49	87.40	88.01	88.45	88.13	**84.35**
GDANet	w/o SOR	75.89	68.56	71.52	80.96	83.23	80.75	83.79	86.79	74.84	87.44	88.09	80.17
	w/o Hybrid Training	38.05	81.65	75.45	72.37	80.92	85.41	85.94	85.21	87.72	86.10	86.87	78.69
	w/o ConvONet	76.66	79.66	74.84	80.55	81.48	87.12	81.12	86.18	87.97	89.06	88.61	83.02
	Ours	75.32	80.79	77.31	83.59	83.75	86.59	84.44	86.63	88.65	86.95	87.28	**83.75**

Furthermore, we process the hypothesis testing to different components in Table 2. Table 2 presents the p-value for each part of Our defense framework. At 95% confidence level, SOR and hybrid training improve robustness in most point cloud

Table 2. The one-tailed p-value of different components. HT: hyrbid training. Conv: ConvONet

	PointNet	PointNet++	DGCNN	PointConv	PCT	CurveNet	RPC	GDA
W/O SOR	0.008	0.012	0.021	0.091	0.027	0.013	0.013	0.014
W/O HT	0.011	0.025	0.049	0.042	0336	0.057	0.025	0.052
W/O Conv	0.024	0.337	0.131	0.439	0.163	0.250	0.187	0.031

DNNs. Despite the p-value not affirming ConvONet's effectiveness, ConvONet has significant efficacy in removing points attacks, hence we regard ConvONet as a crucial part of Our defense framework.

B.2. Evaluation on Hybrid Training

In order to evaluate the effectiveness of hybrid training, we conduct a comparative analysis between various augmentation configurations. As depicted in Table 3, hybrid training consistently outperforms other methods across a majority of attack scenarios, which means that hybrid training can improve the adversarial robustness of augmentation.

Table 3. The effectiveness of augmentation methods with different settings. Bold: the best in column.

	PGD	SIA	L3A	Drop	AOF	KNN	GeoA3	AdvPC	IFGM	Add	Perturb	ACC
PGD	**86.35**	53.32	48.22	62.20	67.50	55.83	70.38	82.29	81.44	79.05	87.52	70.38
Drop	48.26	44.57	48.30	**85.09**	72.29	60.82	76.74	**87.64**	86.91	84.00	90.68	71.39
Add	36.26	36.91	47.81	68.52	61.91	49.35	70.62	88.33	**90.11**	**86.95**	**95.66**	66.58
Hybrid Training	44.89	**68.60**	**68.76**	65.19	**75.28**	**82.46**	**82.74**	83.79	85.41	82.86	85.01	**74.99**

B.3. Evaluation on Attack Transferability

The transferability of adversarial examples is essential for their effectiveness in real-world applications. In this section, we investigate the attack success rate of adversarial examples generated using three prevalent point cloud deep neural networks (DNNs) as surrogate models, including PointNet [7], PointNet++ [8], and DGCNN [11]. We then evaluate their performance against all victim models. The results, as presented in Table 5, reveal that adversarial examples generated by PointNet++ demonstrate lower transferability compared to those produced by the other two surrogate models. For example, AOF adversarial example generated by PointNet++ has lower attack success rate than PointNet and DGCNN.

B.4. Evaluation on Attack imperceptibility

In Table 4, we present our imperceptibility evaluation results, where attack methods are ordered from left to right according to their distance values. Notably, the selection of a distance metric influences the ranking of attack methods, which could be attributed to variations in the distance loss functions incorporated in the objective functions. Consequently, to guarantee a fair assessment of the imperceptibility of attack approaches, it is crucial to adopt a consistent distance loss in the objective function.

Table 4. The leaderboard of attack imperceptible. CD: Chamfer measurement. HD: Hausdorff distance.

	Perturb	IFGM	KNN	GeoA3	SIA	AOF	L3A	PGD	AdvPC
CD ($\times 10^3$)	0.017	0.054	0.290	0.340	0.490	0.900	1.500	3.400	59.00
	Perturb	IFGM	AOF	GeoA3	KNN	SIA	PGD	L3A	AdvPC
HD ($\times 10^{-2}$)	0.160	0.350	0.720	0.730	1.200	1.200	1.700	2.000	15.10

B.5. Evaluation on adversarial loss function

In untargeted adversarial attacks, two primary loss functions can be employed: logit loss (C&W) and cross-entropy loss. To evaluate the efficacy of these loss functions, we investigate the attack success rate with different adversarial loss functions, as illustrated in Figure 2. Our findings suggest that in the untargeted attacks, adversarial examples utilizing cross-entropy loss exhibit enhanced transferability compared to those employing logit loss (C&W).

Table 5. The leaderboard of attack transferability.

Surrogate Model	Attack	PointNet	PointNet++	DGCNN	PointConv	PCT	Curvenet	RPC	GDANet	Avg.ASR
PointNet	PGD	34.32	17.60	21.35	8.63	32.78	25.65	36.18	18.44	77.05
	SIA	31.40	17.00	45.34	28.28	41.77	34.20	45.26	43.40	63.54
	L3A	45.38	44.89	54.29	50.00	54.21	51.28	53.40	57.21	47.82
	KNN	45.10	54.25	70.10	71.80	67.08	66.73	70.58	72.20	32.47
	AOF	62.84	65.24	71.88	69.57	72.00	71.15	68.60	73.14	29.77
	Add	59.64	71.47	73.10	76.50	71.27	71.29	69.89	72.33	27.74
	Drop	71.76	72.37	83.71	85.15	82.33	79.86	80.75	83.47	18.91
	GeoA3	76.94	81.77	82.98	76.90	82.58	84.48	83.67	85.13	17.79
	AdvPC	61.26	85.00	87.00	71.80	87.20	87.32	77.92	79.25	17.49
	IFGM	74.59	81.22	86.91	86.51	85.62	85.09	83.55	86.63	14.92
	Perturb	85.58	88.17	88.74	88.09	89.22	88.33	85.98	88.33	11.87
PointNet++	PGD	38.05	9.56	17.71	9.12	30.31	22.71	35.33	15.76	75.86
	SIA	40.19	9.04	31.08	14.10	33.14	27.96	45.50	29.66	68.34
	KNN	61.43	25.14	57.27	61.89	59.00	60.27	64.91	62.16	39.01
	L3A	70.12	36.31	64.31	64.16	66.41	66.24	60.96	68.78	34.14
	Drop	72.77	67.75	70.95	74.31	72.77	74.19	71.35	70.99	27.52
	AdvPC	81.69	61.22	71.92	65.19	76.86	79.54	80.71	78.57	23.65
	IFGM	73.87	51.78	79.78	81.28	76.46	81.82	79.54	80.11	21.02
	Perturb	85.94	87.14	88.68	87.74	88.59	88.08	86.03	87.91	12.43
	GeoA3	88.05	89.87	89.47	88.65	89.14	89.10	87.20	89.71	11.24
	AOF	87.64	89.14	89.47	88.21	89.79	89.38	89.59	89.42	10.93
	Add	89.91	89.79	90.13	89.09	90.00	89.79	87.01	89.70	10.62
DGCNN	PGD	48.10	19.08	17.22	8.35	38.09	30.31	41.14	19.33	70.80
	SIA	47.77	19.25	20.79	12.68	36.14	35.45	47.89	23.46	68.19
	AOF	70.90	52.30	36.04	50.93	44.17	53.20	63.85	50.57	44.87
	KNN	69.25	53.28	45.14	44.69	60.45	61.91	46.96	49.72	44.82
	L3A	77.45	66.24	57.14	72.06	69.18	72.90	75.92	67.20	28.44
	AdvPC	79.66	70.79	62.88	57.82	73.22	76.82	77.27	70.34	27.73
	Drop	74.92	73.87	69.00	75.85	72.04	73.78	68.52	69.49	27.36
	IFGM	82.9	82.09	82.29	85.90	84.85	84.81	83.63	83.87	15.99
	GeoA3	84.56	85.01	83.14	84.48	86.39	86.43	83.87	85.62	14.81
	Add	85.29	83.79	87.03	87.56	87.76	87.16	86.06	87.16	13.60
	Perturb	87.76	88.17	88.05	88.25	88.33	87.97	85.75	87.72	12.29

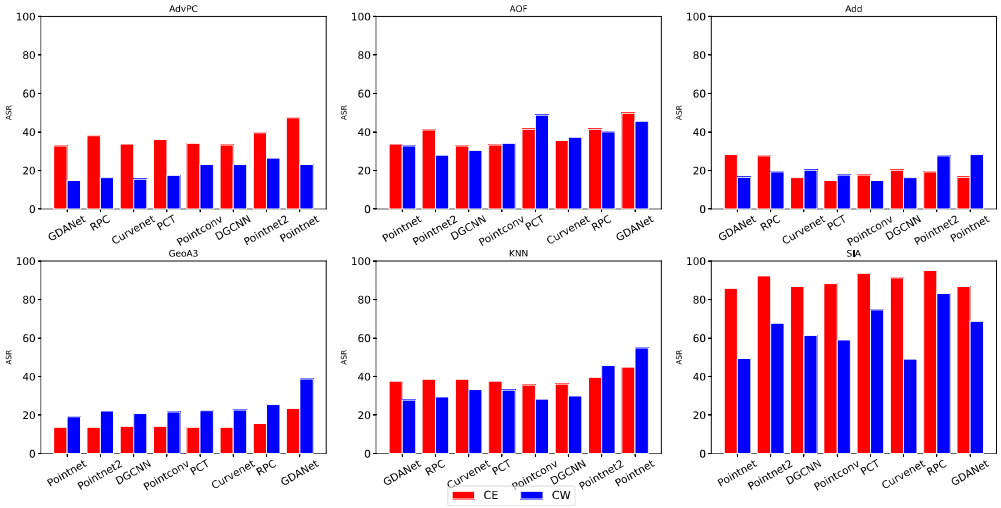

Figure 2. Attack success rate on different adversarial loss function. All adversarial examples are generate with PointNet surrogate model and test on eight victim models.

B.6. Full Adversarial Robustness Leaderboard

We shows full adversarial robustness leaderboard in Table 6. Compared with other defense strategies, our defense framework achieves the best adversarial robustenss.

Table 6. Full leaderboard. Bold: best in column. Underline: second best in column.Blue: second best in row. Red: worst in row.

Defense & (Acc)	Model	Clean	PGD	SIA	L3A	Drop	AOF	KNN	GeoA3	AdvPC	Add	IFGM	Perturb
Ours (83.45)	PointNet	87.36	76.70	76.26	75.04	80.79	81.60	85.53	84.04	86.22	87.28	86.26	86.35
	PointNet++	88.65	71.56	78.61	76.70	83.14	84.12	86.87	85.78	**87.40**	88.45	88.17	88.70
	DGCNN	87.97	72.93	81.81	77.96	82.94	84.08	86.39	84.81	86.71	88.17	87.76	87.32
	Pointconv	87.12	70.14	80.67	76.50	83.79	81.77	86.30	85.53	86.83	87.88	87.52	86.95
	PCT	83.27	73.91	78.32	75.77	76.86	79.66	82.41	80.71	81.60	82.78	82.21	83.71
	Curvenet	88.57	76.13	80.26	78.16	83.67	83.59	87.20	84.97	86.14	88.05	86.99	87.88
	RPC	88.86	74.11	**82.66**	**78.20**	82.98	**84.48**	**87.93**	85.49	87.38	88.01	88.45	88.13
	GDANet	88.57	75.32	80.79	77.31	83.59	83.75	86.59	84.44	86.63	88.65	86.95	87.28
Hybrid Training* (79.35)	PointNet	88.57	80.15	53.08	50.28	77.55	73.34	64.71	75.45	84.12	83.39	85.17	87.64
	PointNet++	89.75	77.39	52.80	57.74	85.74	79.85	74.68	82.74	86.08	85.45	88.29	89.00
	DGCNN	89.47	81.40	66.29	61.14	86.14	80.19	80.59	82.74	87.28	87.76	88.53	89.95
	Pointconv	90.19	80.06	45.30	57.37	**86.47**	69.65	81.69	83.31	85.13	88.82	**89.83**	**90.28**
	PCT	87.44	45.95	75.97	76.70	72.69	78.57	85.86	83.02	86.35	87.12	87.86	87.24
	Curvenet	87.16	44.57	76.22	76	74.15	81.48	85.45	83.43	86.14	87.40	87.84	86.35
	RPC	85.45	53.85	76.46	74.80	70.30	80.31	83.95	82.17	84.60	84.52	85.90	84.68
	GDANet	87.24	38.74	79.01	75.04	72.16	80.71	85.41	82.86	85.21	86.43	86.87	86.67
IF-Denfens (78.4)	PointNet	85.33	44.89	68.6	68.76	65.19	75.28	82.46	82.74	83.79	85.41	82.86	85.01
	PointNet++	87.52	38.61	72.45	72.33	73.01	78.28	85.56	85.17	85.66	87.20	85.37	87.12
	DGCNN	87.88	40.32	77.92	76.05	71.48	80.35	85.78	85.41	85.49	86.75	85.86	87.32
	Pointconv	85.53	28.61	78.24	73.66	73.87	75.89	84.85	84.24	84.48	85.58	84.20	85.37
	PCT	88.33	45.83	75.24	73.45	72.85	79.42	85.86	85.29	86.35	87.16	85.94	86.83
	Curvenet	88.33	45.38	76.18	75.45	74.19	80.51	85.45	86.02	86.14	88.01	86.75	86.67
	RPC	88.05	40.44	76.13	73.62	73.58	77.43	83.95	**86.06**	84.60	87.72	85.90	87.64
	GDANet	87.93	38.05	81.65	75.45	72.37	80.92	85.41	85.94	85.21	87.72	86.10	86.87
AT (76.32)	PointNet	87.03	82.82	51.46	48.78	60.37	64.63	56.73	69.41	79.94	78.57	80.06	85.82
	PointNet++	88.13	84.40	53.81	54.17	68.76	77.51	68.35	79.46	84.76	80.31	84.48	87.76
	DGCNN	88.78	84.56	60.80	58.31	73.82	79.42	73.62	81.77	85.82	84.40	86.71	88.21
	Pointconv	88.49	84.72	44.94	57.70	74.27	72.69	74.43	78.44	82.94	85.53	87.24	88.29
	PCT	82.01	78.89	63.70	57.01	67.67	76.01	72.65	76.99	79.17	77.43	79.94	81.32
	Curvenet	88.17	85.17	61.55	58.83	72.00	80.31	73.58	82.37	85.82	83.63	85.25	88.21
	RPC	86.59	83.02	60.09	54.98	69.45	77.76	71.43	79.17	83.67	80.47	85.21	86.18
	GDANet	88.70	**85.86**	60.94	59.00	71.72	80.06	74.64	82.01	85.86	84.36	86.35	88.17
SOR (75.19)	PointNet	86.95	42.10	63.21	63.70	57.86	68.48	80.06	73.22	80.49	86.10	84.16	85.53
	PointNet++	88.57	25.00	64.30	72.49	66.25	71.31	85.13	80.23	84.89	88.70	87.72	88.98
	DGCNN	88.57	18.00	73.58	69.89	66.94	66.25	85.25	74.24	82.33	87.88	87.64	87.44
	Pointconv	72.12	11.70	71.84	69.73	72.12	65.92	85.53	77.47	84.68	88.49	86.02	87.12
	PCT	88.41	38.94	72.97	70.75	67.50	74.84	85.01	80.31	84.52	88.65	86.79	87.76
	Curvenet	88.33	33.63	74.51	76.86	69.81	76.62	86.43	83.39	85.17	89.10	86.83	87.72
	RPC	89.43	15.07	72.57	69.17	69.00	69.85	85.53	78.04	84.04	88.86	87.44	87.72
	GDANet	89.26	17.34	79.90	72.12	68.40	74.39	86.59	82.29	85.94	88.85	88.01	87.88
DUP-Net (75.07)	PointNet	86.14	45.62	62.97	62.76	61.83	68.23	79.21	72.59	79.82	85.82	81.97	83.87
	PointNet++	88.53	24.92	67.06	66.13	67.18	70.79	84.48	78.81	82.86	88.21	86.10	87.36
	DGCNN	88.94	22.53	77.15	68.40	70.91	70.42	85.86	74.92	84.60	85.94	87.32	87.82
	Pointconv	87.36	13.37	75.97	68.00	69.98	68.64	85.49	79.38	84.20	87.52	85.98	86.43
	PCT	88.98	37.80	71.72	69.00	69.04	73.58	84.44	77.92	84.24	86.39	86.63	86.71
	Curvenet	88.00	35.53	74.51	72.16	71.64	76.34	85.66	81.16	85.41	87.93	86.26	87.16
	RPC	88.41	19.53	70.58	68.84	67.67	66.90	84.32	72.20	82.29	85.86	86.67	87.40
	GDANet	88.33	24.11	78.20	70.87	71.35	73.58	85.90	78.73	85.05	86.63	87.24	87.28
PointCutmix (73.27)	PointNet	86.84	35.84	37.66	52.48	73.03	63.51	60.77	71.02	81.82	86.51	81.90	85.35
	PointNet++	89.10	24.47	35.35	53.45	79.52	66.44	74.41	79.30	83.12	89.43	86.28	88.68
	DGCNN	89.02	18.74	70.00	66.88	81.00	72.08	83.02	82.71	84.86	89.10	87.62	88.68
	Pointconv	88.02	7.87	55.36	63.15	83.02	60.23	83.18	82.43	84.05	87.79	87.18	87.70
	PCT	89.97	29.06	53.08	63.23	81.66	70.17	78.91	82.51	85.23	**89.84**	87.42	88.76
	Curvenet	89.98	17.53	48.46	59.70	79.48	69.97	76.97	82.87	85.87	89.06	86.24	88.31
	RPC	88.49	23.01	61.32	63.6	78.17	68.99	79.40	80.84	83.97	87.87	86.20	86.89
	GDANet	89.56	17.16	71.05	70.13	80.67	71.27	83.06	84.62	86.57	89.23	88.76	88.88
SRS (61.43)	PointNet	87.40	43.72	40.96	50.45	54.78	58.31	58.11	66.13	77.67	78.65	78.53	84.89
	PointNet++	89.10	11.41	23.87	47.57	56.93	58.39	64.71	76.62	81.97	81.28	84.24	87.90
	DGCNN	79.17	8.51	26.62	48.00	28.11	44.29	60.62	73.91	66.09	81.20	73.91	77.15
	Pointconv	85.53	9.20	52.76	55.51	52.67	58.71	76.50	76.09	78.56	86.30	84.64	84.72
	PCT	82.46	33.87	46.39	56.52	38.90	62.40	69.00	71.68	76.00	81.00	79.21	82.13
	Curvenet	85.33	22.85	45.79	57.15	61.22	66.05	71.47	77.92	81.08	82.29	83.27	84.32
	RPC	89.71	8.35	30.39	42.59	23.42	39.22	53.12	61.59	61.14	78.08	71.88	77.11
	GDANet	89.71	8.59	16.53	46.35	21.43	42.30	60.29	65.44	63.29	81.85	75.41	78.40
Avg.ASR		-	53.84	36.78	35.62	29.36	27.67	21.37	20.31	16.77	14.07	14.70	13.35

References

[1] Thomas Cover and Peter Hart. Nearest neighbor pattern classification. *IEEE transactions on information theory*, 13(1):21–27, 1967.

[2] Abdullah Hamdi, Sara Rojas, Ali Thabet, and Bernard Ghanem. Advpc: Transferable adversarial perturbations on 3d point clouds. In *European Conference on Computer Vision*, pages 241–257. Springer, 2020.

[3] Qidong Huang, Xiaoyi Dong, Dongdong Chen, Hang Zhou, Weiming Zhang, and Nenghai Yu. Shape-invariant 3d adversarial point clouds. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 15335–15344, 2022.

[4] Binbin Liu, Jinlai Zhang, and Jihong Zhu. Boosting 3d adversarial attacks with attacking on frequency. *IEEE Access*, 10:50974–50984, 2022.

[5] Daniel Liu, Ronald Yu, and Hao Su. Extending adversarial attacks and defenses to deep 3d point cloud classifiers. In *2019 IEEE International Conference on Image Processing (ICIP)*, pages 2279–2283. IEEE, 2019.

[6] Songyou Peng, Michael Niemeyer, Lars Mescheder, Marc Pollefeys, and Andreas Geiger. Convolutional occupancy networks. In *European Conference on Computer Vision*, pages 523–540. Springer, 2020.

[7] 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.

[8] Charles Ruizhongtai Qi, Li Yi, Hao Su, and Leonidas J Guibas. Pointnet++: Deep hierarchical feature learning on point sets in a metric space. *Advances in neural information processing systems*, 30, 2017.

[9] Yiming Sun, Feng Chen, Zhiyu Chen, and Mingjie Wang. Local aggressive adversarial attacks on 3d point cloud. In *Asian Conference on Machine Learning*, pages 65–80. PMLR, 2021.

[10] Tzungyu Tsai, Kaichen Yang, Tsung-Yi Ho, and Yier Jin. Robust adversarial objects against deep learning models. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 34, pages 954–962, 2020.

[11] Yue Wang, Yongbin Sun, Ziwei Liu, Sanjay E Sarma, Michael M Bronstein, and Justin M Solomon. Dynamic graph cnn for learning on point clouds. *Acm Transactions On Graphics (tog)*, 38(5):1–12, 2019.

[12] Yuxin Wen, Jiehong Lin, Ke Chen, CL Philip Chen, and Kui Jia. Geometry-aware generation of adversarial point clouds. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2020.

[13] Ziyi Wu, Yueqi Duan, He Wang, Qingnan Fan, and Leonidas J Guibas. If-defense: 3d adversarial point cloud defense via implicit function based restoration. *arXiv preprint arXiv:2010.05272*, 2020.

[14] Chong Xiang, Charles R Qi, and Bo Li. Generating 3d adversarial point clouds. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 9136–9144, 2019.

[15] Jiancheng Yang, Qiang Zhang, Rongyao Fang, Bingbing Ni, Jinxian Liu, and Qi Tian. Adversarial attack and defense on point sets. *arXiv preprint arXiv:1902.10899*, 2019.

[16] Lequan Yu, Xianzhi Li, Chi-Wing Fu, Daniel Cohen-Or, and Pheng-Ann Heng. Pu-net: Point cloud upsampling network. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 2790–2799, 2018.

[17] Jinlai Zhang, Lyujie Chen, Bo Ouyang, Binbin Liu, Jihong Zhu, Yujing Chen, Yanmei Meng, and Danfeng Wu. Pointcutmix: Regularization strategy for point cloud classification. *arXiv preprint arXiv:2101.01461*, 2021.

[18] Hang Zhou, Kejiang Chen, Weiming Zhang, Han Fang, Wenbo Zhou, and Nenghai Yu. Dup-net: Denoiser and upsampler network for 3d adversarial point clouds defense. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pages 1961–1970, 2019.