ICASSP 2025 - 2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) | 979-8-3503-6874-1/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICASSP49660.2025.10889589

Imperceptible Adversarial Attacks on Point Clouds Guided by Point-to-Surface Field

Keke Tang
Guangzhou University
tangbohutbh@gmail.com

Weiyao Ke
Guangzhou University
weiyaoke08@gmail.com

Weilong Peng
Guangzhou University
wlpeng@tju.edu.cn

Xiaofei Wang
SmartMore Corporation
wxf9545@mail.ustc.edu.cn

Ziyong Du
Guangzhou University
duxiaoshuaicst@gmail.com

Zhize Wu
Hefei University
wuzz@hfuu.edu.cn

Peizan Zhu
Northwestern Polytechnical University
ericcan@nwpu.edu.cn

Zhihong Tian
Guangzhou University
tianzhihong@gzhu.edu.cn

***Abstract*—Adversarial attacks on point clouds are crucial for assessing and improving the adversarial robustness of 3D deep learning models. Traditional solutions strictly limit point displacement during attacks, making it challenging to balance imperceptibility with adversarial effectiveness. In this paper, we attribute the inadequate imperceptibility of adversarial attacks on point clouds to deviations from the underlying surface. To address this, we introduce a novel point-to-surface (P2S) field that adjusts adversarial perturbation directions by dragging points back to their original underlying surface. Specifically, we use a denoising network to learn the gradient field of the logarithmic density function encoding the shape's surface, and apply a distance-aware adjustment to perturbation directions during attacks, thereby enhancing imperceptibility. Extensive experiments show that adversarial attacks guided by our P2S field are more imperceptible, outperforming state-of-the-art methods.**

***Index Terms*—deep neural network, adversarial attacks, imperceptibility, point clouds, surface**

I. Introduction

With the advancement of deep learning techniques [1], [2] and the increased availability of affordable depth-sensing devices, 3D point cloud perception using deep neural networks (DNNs) has become a prominent solution [3]–[5]. However, recent studies have demonstrated that DNN classifiers are susceptible to adversarial attacks [6], [7], where imperceptible perturbations to input point clouds can result in incorrect predictions. This vulnerability poses significant challenges for their application in real-world scenarios. Therefore, investigating adversarial attacks on 3D DNN classifiers is essential for evaluating and improving their adversarial robustness [8]–[10].

To achieve imperceptible attacks on 3D point clouds, a classic approach is to employ constraints such as the l_2-norm, Chamfer distance, and Hausdorff distance to restrict point displacements [6]. However, for adversarial attacks to be effective, these points must be displaced, making it challenging to balance imperceptibility and adversarial effectiveness. In practice, the displacement of points is not the primary cause of perceptibility; rather, it is the deviation of these points from the underlying surface of the point cloud that makes them noticeable [11]. Therefore, as long as the points remain on the original surface, slightly larger displacements during attacks can still achieve imperceptibility.

In this paper, we introduce a novel point-to-surface (P2S) field for dragging perturbed points onto the surface during attacks, achieving enhanced imperceptibility. Specifically, we train a denoising network to learn the gradient field of the logarithmic density function encoding the shape surface. This field directs any point in Euclidean space toward the surface. Considering that points farther from the surface need more significant adjustments, we define a distance-aware P2S field magnitude. By iteratively dragging the initial perturbation direction onto the surface and then determining the perturbation magnitude, our adversarial attacks become more imperceptible. We validate the effectiveness of our solution by attacking various common 3D DNN classifiers. Extensive experimental results show that the generated adversarial point clouds are significantly more imperceptible than those produced by state-of-the-art methods.

Overall, our contribution is summarized as follows:

- We are the first to attribute the inadequate imperceptibility of adversarial attacks on 3D point clouds to the deviation from the underlying surface.
- We devise a point-to-surface (P2S) field and a novel adversarial attack framework that employs this field to drag perturbed points onto the surface.
- We show by experiments that adversarial attacks guided by the P2S field achieve superior performance in terms of imperceptibility.

II. Related Work

Adversarial Attacks on Point Clouds. Adversarial attacks [12]–[18], aimed at generating samples that can mislead target networks, originated in 2D image classification and have been successfully extended to 3D point clouds. Existing point cloud attacks are categorized into three types: addition-based, introducing independent points to induce errors [6];

This work was supported in part by the National Natural Science Foundation of China (62472117, U2436208, 62406095), the Guangdong Basic and Applied Basic Research Foundation (2024A1515012064), and the Science and Technology Projects in Guangzhou (2025A03J0137).

Keke Tang and Weiyao Ke contributed equally. Weilong Peng and Peican Zhu are joint corresponding authors.

deletion-based, involving the removal of critical points to affect classification [19]–[22]; and perturbation-based, which involves altering existing points to facilitate attacks [6], [23]–[28]. This paper focuses on perturbation-based methods.

To achieve imperceptibility of attacks, a common approach is to apply constraints such as the l_2-norm, Chamfer distance, and Hausdorff distance between the original and adversarial point clouds [6], [7], [29]. Beyond these standard constraints, GeoA^3 [30] maintains local curvatures after the attack. More recent solutions guide perturbations along normal or tangential directions [31]–[33]. In contrast, our approach achieves imperceptibility by dragging the perturbed points onto the surface.

Surface Modeling of Point Clouds. Surface modeling of point clouds encompasses traditional geometric methods, such as Poisson surface reconstruction [34], implicit surface techniques like Signed Distance Functions [35], and recent deep learning approaches [36]. In our work, we also employ deep learning to implicitly represent the surface. Our goal is to drag adversarially perturbed points back to the surface to achieve imperceptibility.

III. Problem Formulation

Preliminary on Adversarial Attacks. Given a point cloud $P \in \mathbb{R}^{n\times 3}$ sampled from an object surface S and its label $y \in \{1, \ldots, K\}$, adversarial attack aims to mislead a 3D DNN classifier f by feeding a perturbed point cloud P':

$$p'_i = p_i + \sigma_{p_i} \cdot \overrightarrow{d_{p_i}}, \tag{1}$$

where σ_{p_i} is the perturbation size for the i-th point in P, i.e., p_i, and $\overrightarrow{d_{p_i}}$ is the unit perturbation direction. Formally, this perturbation, $\sigma_{p_i} \cdot \overrightarrow{d_{p_i}}$, can be computed by solving the following optimization problem, iteratively:

$$\min_{\sigma_{p_i}, \overrightarrow{d_{p_i}}} L_{mis}(f, P', y) + \lambda_1 C(P, P'), \tag{2}$$

where $L_{mis}(\cdot,\cdot,\cdot)$ is the misclassification loss (e.g., the negated cross-entropy loss), P' is the adversarial point clouds consists of $\{p'_i\}_{i=1:n}$, $C(\cdot,\cdot)$ is a constraint to ensure imperceptibility, and λ_1 is a weighting parameter. In particular, our focus is on untargeted attacks, and targeted attacks can be similarly addressed.

Discussion. Common choices for $C(\cdot,\cdot)$, such as the l_2-norm, Chamfer distance, and Hausdorff distance, impose strict limits on point displacements, making it challenging to balance imperceptibility and adversarial effectiveness. In practice, if the points remain on the original surface S, slightly larger displacements can still achieve imperceptibility. Therefore, a feasible approach to achieving imperceptible adversarial attacks is to apply perturbations while dragging the points back towards the surface S.

Point-to-Surface Field-Guided Attacks. Suppose there is a point-to-surface (P2S) field $\mathcal{F}$ that, given a point q, drags it closer to the surface S, such that

$$D(q, S) > D(q + \mathcal{F}(q), S), \tag{3}$$

where $D(\cdot,\cdot)$ measures the point-to-surface distance.

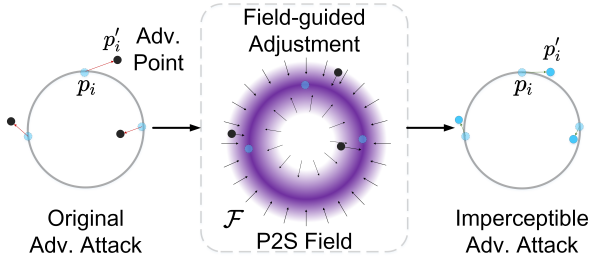

Fig. 1: Illustration of our point-to-surface (P2S) field-guided adversarial attacks. For each adversarial point in a point cloud, we adjust its direction using the P2S field to bring it closer to the surface, making the perturbation imperceptible.

Therefore, adversarial points generated by P2S field-guided attacks can be formulated as:

$$p'_i \leftarrow p'_i + \mathcal{F}(p'_i). \tag{4}$$

Compared to the original point, the updated point p'_i is closer to the surface S.

IV. Method

In this section, we first introduce how to construct the point-to-surface (P2S) field using DNN, and then outline our P2S field-guided adversarial attack framework. Please refer to Fig. 1 for a demonstration.

A. DNN-based Point-to-Surface Field

We learn the point-to-surface (P2S) field using a DNN network. Specifically, we train the network to predict the gradient field from noisy point cloud data by minimizing the l_2 loss between the predicted gradients of the logarithmic density function encoding a shape and the ground-truth gradients estimated from the input point cloud, following [36].

Since the network has learned how to move points towards high-density regions, i.e., the shape's surface S, the P2S field at the position q can be estimated as follows:

$$\mathcal{F}(q) := \nabla_q \log Q_S(q), \tag{5}$$

where $Q_S(\cdot)$ approximates the true data distribution whose density concentrates near the surface S.

B. P2S Field-guided Imperceptible Adversarial Attacks

Given the clean point cloud P, we first randomly initializes the perturbation to form the 0-iteration adversarial point cloud $P'^{(0)}$, and then iteratively applying the following three steps.

Generating Initial Perturbations. We employ IFGM [37] to generate initial perturbation directions for all points. It is noteworthy that alternative methods could also be employed to achieve similar effects.

Adjusting Perturbation Directions with P2S Field. To ensure that perturbed points remain close to the surface, we use the P2S field $\mathcal{F}$ to adjust the perturbation directions. Specifically, for the t-iteration adversarial point $p'^{(t)}_i$, we

TABLE I: Comparison on the perturbation sizes required by different methods to reach their highest achievable ASR in the untargeted attack setting. The evaluation is conducted across different DNN classifiers on ModelNet40 and ShapeNet Part.

Model	Attack	ModelNet40							ShapeNet Part						
		ASR (%)	CD (10^{-4})	HD (10^{-2})	l_2	GR	Curv (10^{-2})	EMD (10^{-2})	ASR (%)	CD (10^{-4})	HD (10^{-2})	l_2	GR	Curv (10^{-2})	EMD (10^{-2})
PointNet	PGD	100	7.155	5.025	0.981	0.302	1.624	2.315	100	13.172	17.068	1.569	0.521	3.679	3.358
	IFGM	100	4.039	5.565	0.789	0.314	0.775	0.864	100	3.328	10.269	0.785	0.408	0.619	0.556
	GeoA^3	100	4.646	0.497	1.307	0.121	0.396	2.319	100	7.531	1.444	2.655	0.146	0.465	4.104
	3d-Adv	100	6.115	4.372	0.863	0.250	1.215	1.410	100	15.659	5.495	1.787	0.279	4.006	3.693
	SI-Adv	100	2.768	2.595	0.731	0.220	0.271	0.725	100	3.435	3.692	0.881	0.233	**0.441**	0.825
	ITA	100	2.747	0.414	0.534	0.122	0.555	1.214	100	5.872	1.917	1.002	0.181	1.016	2.035
	Ours	100	**1.110**	**0.358**	**0.366**	**0.115**	**0.260**	**0.449**	100	**2.822**	**1.347**	**0.780**	**0.145**	0.492	**0.543**
DGCNN	PGD	100	19.968	5.098	1.933	0.267	4.924	4.785	100	63.556	27.557	5.224	0.511	7.275	9.233
	IFGM	100	15.791	12.391	1.622	0.363	2.849	3.777	100	19.623	26.040	2.069	0.504	4.954	4.387
	GeoA^3	100	7.566	0.546	1.585	0.119	0.741	3.083	100	27.612	3.748	5.798	0.199	**1.695**	7.502
	3d-Adv	100	10.345	3.807	3.589	0.227	5.997	6.685	100	21.553	8.531	2.258	0.282	5.119	4.628
	SI-Adv	100	7.146	1.691	1.087	0.143	0.666	2.495	100	11.685	3.019	1.772	0.160	2.054	3.646
	ITA	100	3.249	0.524	**0.552**	0.114	0.971	1.359	100	27.633	4.597	2.492	0.244	3.847	4.696
	Ours	100	**1.898**	**0.316**	0.619	**0.110**	**0.516**	**1.016**	100	**7.013**	**1.339**	**1.668**	**0.137**	2.521	**2.663**
PointConv	PGD	100	14.551	2.216	1.442	0.184	3.491	3.862	100	42.202	9.949	3.784	0.252	6.866	7.277
	IFGM	100	7.959	2.608	1.015	0.184	1.741	2.427	100	16.139	8.776	1.812	0.231	3.526	3.807
	GeoA^3	100	6.809	0.644	2.169	0.119	1.119	3.556	100	9.383	1.222	4.224	0.120	**1.190**	5.391
	3d-Adv	100	11.213	1.763	1.179	0.163	3.279	2.807	100	21.034	3.687	2.277	0.193	4.912	4.548
	SI-Adv	100	6.060	1.784	0.977	0.144	0.576	2.081	100	11.281	3.500	1.741	0.165	1.949	3.514
	ITA	100	5.539	0.480	0.833	0.111	1.904	1.971	100	9.082	1.452	1.375	0.146	3.645	2.925
	Ours	100	**1.801**	**0.248**	**0.528**	**0.105**	**0.504**	**0.959**	100	**7.193**	**1.195**	**1.237**	**0.112**	2.318	**2.636**

sample the P2S vector $\mathcal{F}(p_i'^{(t)})$ and adjust the direction $\overrightarrow{d_{p_i'^{(t)}}}$ as follows:

$$\overrightarrow{d_{p_i'^{(t)}}} \leftarrow \overrightarrow{d_{p_i'^{(t)}}} + \theta||p_i'^{(t)} - p_i|| \cdot \frac{\mathcal{F}(p_i'^{(t)})}{||\mathcal{F}(p_i')^{(t)}||}, \quad (6)$$

where θ is a weighting hyperparameter.

Determining Perturbation Magnitudes. With the refined perturbation directions established, we proceed to determine the perturbation magnitude $\sigma_{p_i'^{(t)}}$ for point $p_i'^{(t)}$ following [31]. The $t+1$-iteration adversarial point $p_i'^{(t+1)}$ is then obtained as follows:

$$p_i'^{(t+1)} = p_i'^{(t)} + \sigma_{p_i'}^{(t)} \cdot \overrightarrow{d_{p_i'^{(t)}}}. \quad (7)$$

By iteratively executing the above three steps, our approach creates highly imperceptible adversarial point clouds.

V. Experimental Results

A. Experimental Setup

Implementation. We implement our framework and baseline solutions using PyTorch. The weighting hyperparameter $\theta = 0.5$. All experiments are conducted on a workstation with dual 2.40 GHz CPUs, 128 GB of RAM, and eight NVIDIA RTX 3090 GPUs.

Datasets. We utilize two public datasets for evaluation: ModelNet40 [38] and ShapeNet Part [39]. Specifically, we randomly sample 1,024 points from each point cloud.

Victim Models. We select three commonly used DNN classifiers for the attacks: PointNet [40], DGCNN [41], and PointConv [42]. These models are trained following the procedures outlined in their respective original papers.

Baseline Attack Methods. We select six state-of-the-art techniques as baselines: IFGM [37], PGD [37], SI-Adv [32], ITA [31], GeoA^3 [30] and 3d-Adv [6].

Evaluation Setting and Metrics. We configure each attack method to achieve its maximum attack success rate (ASR), defined as the percentage of adversarial point clouds that successfully mislead the victim model. Under this maximal adversarialness condition [43], [44], we evaluate the imperceptibility of the attacks using six widely recognized metrics: Chamfer distance (CD) [45], Hausdorff distance (HD) [46], l_2-norm (l_2), curvature (Curv), geometric regularity (GR) [30], and earth mover's distance (EMD) [47]. Unless stated otherwise, all results discussed pertain to untargeted attacks.

B. Performance Comparison and Analysis

Comparisons with State-of-the-art Methods. We evaluate the ASR and imperceptibility of various adversarial attack methods, with the results presented in Tab. I. While all methods achieve a 100% ASR, approaches like PGD exhibit higher distortion, leading to lower performance across most metrics due to their lack of subtlety. In contrast, direction-based methods such as SI-Adv and ITA demonstrate lower distortion, highlighting their effectiveness in maintaining attack imperceptibility. Notably, our P2S field-guided approach surpasses these state-of-the-art methods across the majority of metrics, emphasizing its superior effectiveness in achieving imperceptible adversarial attacks.

Visualization of Adversarial Point Clouds. We visualize adversarial point clouds generated by various attack methods targeting PointNet on ModelNet40 in Fig. 2. Adversarial point clouds from PGD and IFGM show significant outliers, while GeoA^3 reduces them with curvature constraints. Directional attacks such as SI-Adv and ITA further minimize visible outliers. Notably, our P2S field-guided solution, which aligns adversarial points with the surface, produces nearly outlier-free point clouds, highlighting the effectiveness and superiority of our method in achieving imperceptibility.

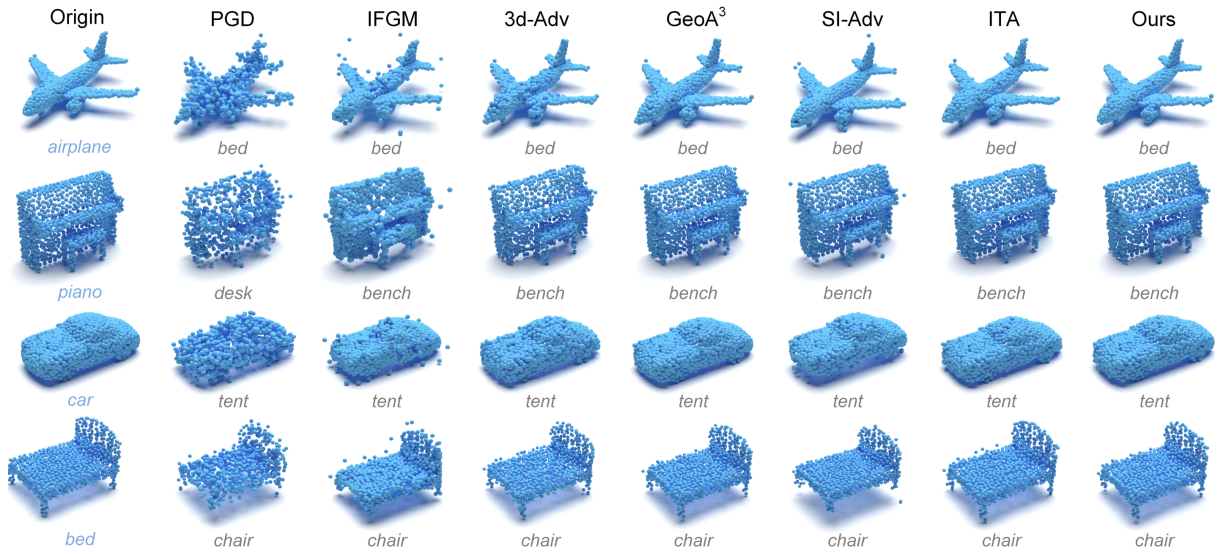

Fig. 2: Visualizations of original and adversarial point clouds generated to fool PointNet on ModelNet40 by various adversarial attack methods. The ground truth and predicted labels are marked in blue and gray below the images.

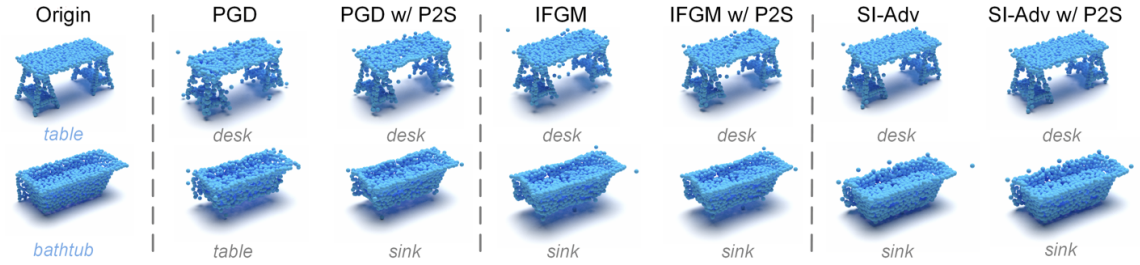

Fig. 3: Visualization of adversarial point clouds generated by various attack methods in attacking PointNet, with and without guidance from the P2S field. The ground truth and predicted labels are marked in blue and gray below the images.

TABLE II: Imperceptibility of different variants of our solution: without using the P2S field (w/o), using the P2S field in the forward direction (w/ +), and using it in reverse (w/ -).

P2S Field	ASR (%)	CD (10^{-4})	HD (10^{-2})	l_2	GR	Curv (10^{-2})	EMD (10^{-2})
w/o	100	2.267	0.524	0.719	0.118	0.499	0.989
w/ -	100	2.573	0.537	0.821	0.119	0.569	1.192
w/ +	100	**1.110**	**0.358**	**0.366**	**0.115**	**0.260**	**0.449**

Ablative Analysis of P2S Field. To validate the importance of the P2S field, we compare the results of three configurations: without the field, using the field in reverse, and using the field in its intended forward direction to guide perturbations. The results in Tab. II show that utilizing the P2S field in the forward direction significantly enhances imperceptibility. Conversely, when the field is applied in reverse, causing adversarial points to move further away from the surface, the imperceptibility of the attacks decreases. Therefore, we conclude the critical role of the P2S field in improving the imperceptibility of adversarial attacks.

Generalization of P2S Field. To evaluate the generalizability of the P2S field, we integrate it into three established iterative attack methods: PGD [37], IFGM [37], and SI-Adv [32]. As shown in Tab. III, these methods, when guided by the P2S field, demonstrate significant improvements across most performance metrics under identical parameter settings. Additionally, we visualize the adversarial samples generated with and without the P2S field in Fig. 3. It is evident that the adversarial point clouds guided by the P2S field exhibit less pronounced outlier points. These results confirm the broad applicability and effectiveness of the P2S field.

TABLE III: Comparison of imperceptibility of various attack solutions with and without P2S field guidance.

Attack	ASR (%)	CD (10^{-4})	HD (10^{-2})	l_2	GR	Curv (10^{-2})	EMD (10^{-2})
PGD w/o P2S	100	7.155	5.025	0.981	0.302	1.624	2.315
PGD w/ P2S	100	**4.300**	**4.402**	**0.784**	**0.276**	**0.740**	**1.491**
IFGM w/o P2S	100	4.039	5.565	0.789	0.314	0.775	0.864
IFGM w/ P2S	100	**3.366**	**4.371**	**0.712**	**0.275**	**0.614**	**0.793**
SI-Adv w/o P2S	100	2.768	2.595	0.731	0.220	0.271	**0.725**
SI-Adv w/ P2S	100	**2.537**	**1.778**	**0.644**	**0.160**	**0.206**	0.743

VI. Conclusion

This paper has introduced a novel point-to-surface (P2S) field-guided framework for imperceptible 3D point cloud attacks. The core idea is to guide perturbed points back to their original underlying surface during attacks. Comprehensive experiments validate the effectiveness of our P2S field-guided attacks in achieving high imperceptibility.

REFERENCES

[1] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[2] K. Tang, Y. Ma, D. Miao, P. Song, Z. Gu, Z. Tian, and W. Wang, "Decision fusion networks for image classification," *IEEE TNNLS*, pp. 1–14, 2022.

[3] Y. Guo, H. Wang, Q. Hu, H. Liu, L. Liu, and M. Bennamoun, "Deep learning for 3d point clouds: A survey," *IEEE TPAMI*, vol. 43, no. 12, pp. 4338–4364, 2020.

[4] A. Ioannidou, E. Chatzilari, S. Nikolopoulos, and I. Kompatsiaris, "Deep learning advances in computer vision with 3d data: A survey," *ACM computing surveys (CSUR)*, vol. 50, no. 2, pp. 1–38, 2017.

[5] K. Tang, Y. Chen, W. Peng, Y. Zhang, M. Fang, Z. Wang, and P. Song, "Reppvconv: attentively fusing reparameterized voxel features for efficient 3d point cloud perception," *The Visual Computer*, vol. 39, no. 11, pp. 5577–5588, 2023.

[6] C. Xiang, C. R. Qi, and B. Li, "Generating 3d adversarial point clouds," in *CVPR*, 2019, pp. 9136–9144.

[7] D. Liu, R. Yu, and H. Su, "Extending adversarial attacks and defenses to deep 3d point cloud classifiers," in *ICIP*, 2019, pp. 2279–2283.

[8] K. Tang, T. Lou, X. He, Y. Shi, P. Zhu, and Z. Gu, "Enhancing adversarial robustness via anomaly-aware adversarial training," in *KSEM*, 2023, pp. 328–342.

[9] P. Zhu, Z. Fan, S. Guo, K. Tang, and X. Li, "Improving adversarial transferability through hybrid augmentation," *Computers & Security*, p. 103674, 2023.

[10] K. Tang, T. Lou, W. Peng, N. Chen, Y. Shi, and W. Wang, "Effective single-step adversarial training with energy-based models," *TETCI*, vol. 8, no. 5, pp. 3396–3407, 2024.

[11] F. Pistilli, G. Fracastoro, D. Valsesia, and E. Magli, "Learning graph-convolutional representations for point cloud denoising," in *ECCV*, 2020, pp. 103–118.

[12] Q. Li, X. Li, X. Cui, K. Tang, and P. Zhu, "Hept attack: Heuristic perpendicular trial for hard-label attacks under limited query budgets," in *CIKM*, 2023, pp. 4064–4068.

[13] P. Zhu, J. Hong, X. Li, K. Tang, and Z. Wang, "Sgma: a novel adversarial attack approach with improved transferability," *Complex & Intelligent Systems*, pp. 1–13, 2023.

[14] P. Zhu, Z. Pan, Y. Liu, J. Tian, K. Tang, and Z. Wang, "A general black-box adversarial attack on graph-based fake news detectors," in *IJCAI*, 2024, pp. 568–576.

[15] Y. Zhang, J. Hong, Q. Bai, H. Liang, P. Zhu, and Q. Song, "Enhancing adversarial transferability with local transformation," *Complex & Intelligent Systems*, vol. 11, no. 4, pp. 1–13, 2024.

[16] Z. Fan, P. Zhu, C. Gao, J. Hong, and K. Tang, "Dba: An efficient approach to boost transfer-based adversarial attack performance through information deletion," in *KSEM*, 2023, p. 276–288.

[17] M. He, P. Zhu, K. Tang, and Y. Guo, "Hypergraph attacks via injecting homogeneous nodes into elite hyperedges," in *AAAI*, 2025.

[18] P. Zhu, Z. Pan, K. Tang, X. Cui, J. Wang, and Q. Xuan, "Node injection attack based on label propagation against graph neural network," *TCSS*, vol. 11, no. 5, pp. 5858–5870, 2024.

[19] T. Zheng, C. Chen, J. Yuan, B. Li, and K. Ren, "Pointcloud saliency maps," in *ICCV*, 2019, pp. 1598–1606.

[20] J. Yang, Q. Zhang, R. Fang, B. Ni, J. Liu, and Q. Tian, "Adversarial attack and defense on point sets," *arXiv preprint arXiv:1902.10899*, 2019.

[21] M. Wicker and M. Kwiatkowska, "Robustness of 3d deep learning in an adversarial setting," in *CVPR*, 2019, pp. 11 767–11 775.

[22] J. Zhang, C. Jiang, X. Wang, and M. Cai, "Td-net: Topology destruction network for generating adversarial point cloud," in *ICIP*, 2021, pp. 3098–3102.

[23] Y. Zhao, Y. Wu, C. Chen, and A. Lim, "On isometry robustness of deep 3d point cloud models under adversarial attacks," in *CVPR*, 2020, pp. 1201–1210.

[24] J. Kim, B.-S. Hua, T. Nguyen, and S.-K. Yeung, "Minimal adversarial examples for deep learning on 3d point clouds," in *ICCV*, 2021, pp. 7797–7806.

[25] K. Tang, Z. Wang, W. Peng, L. Huang, L. Wang, P. Zhu, W. Wang, and Z. Tian, "Symattack: Symmetry-aware imperceptible adversarial attacks on 3d point clouds," in *ACM Multimedia*, 2024.

[26] K. Tang, L. Huang, W. Peng, D. Liu, X. Wang, Y. Ma, L. Liu, and Z. Tian, "Flat: Flux-aware imperceptible adversarial attacks on 3d point clouds," in *ECCV*, 2024, pp. 198–215.

[27] Z. Wang, W. Peng, L. Wang, Z. Wu, P. Zhu, and K. Tang, "Eia: Edge-aware imperceptible adversarial attacks on 3d point clouds," in *MMM*, 2025.

[28] K. Tang, Z. Du, W. Peng, X. Wang, D. Liu, L. Liu, and Z. Tian, "Imperceptible 3d point cloud attacks on lattice-based barycentric coordinates," in *AAAI*, 2025.

[29] H. Zhou, D. Chen, J. Liao, K. Chen, X. Dong, K. Liu, W. Zhang, G. Hua, and N. Yu, "Lg-gan: Label guided adversarial network for flexible targeted attack of point cloud based deep networks," in *CVPR*, 2020, pp. 10 356–10 365.

[30] Y. Wen, J. Lin, K. Chen, C. P. Chen, and K. Jia, "Geometry-aware generation of adversarial point clouds," *IEEE TPAMI*, vol. 44, no. 6, pp. 2984–2999, 2022.

[31] D. Liu and W. Hu, "Imperceptible transfer attack and defense on 3d point cloud classification," *IEEE TPAMI*, vol. 45, no. 4, pp. 4727–4746, 2023.

[32] Q. Huang, X. Dong, D. Chen, H. Zhou, W. Zhang, and N. Yu, "Shape-invariant 3d adversarial point clouds," in *CVPR*, 2022, pp. 15 335–15 344.

[33] K. Tang, Y. Shi, T. Lou, W. Peng, X. He, P. Zhu, Z. Gu, and Z. Tian, "Rethinking perturbation directions for imperceptible adversarial attacks on point clouds," *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 5158–5169, 2023.

[34] M. Kazhdan, M. Bolitho, and H. Hoppe, "Poisson surface reconstruction," in *SGP*, vol. 7, no. 4, 2006.

[35] J. J. Park, P. Florence, J. Straub, R. Newcombe, and S. Lovegrove, "Deepsdf: Learning continuous signed distance functions for shape representation," in *CVPR*, 2019, pp. 165–174.

[36] R. Cai, G. Yang, H. Averbuch-Elor, Z. Hao, S. Belongie, N. Snavely, and B. Hariharan, "Learning gradient fields for shape generation," in *ECCV*, 2020, pp. 364–381.

[37] X. Dong, D. Chen, H. Zhou, G. Hua, W. Zhang, and N. Yu, "Self-robust 3d point recognition via gather-vector guidance," in *CVPR*, 2020, pp. 11 513–11 521.

[38] Z. Wu, S. Song, A. Khosla, F. Yu, L. Zhang, X. Tang, and J. Xiao, "3d shapenets: A deep representation for volumetric shapes," in *CVPR*, 2015, pp. 1912–1920.

[39] A. X. Chang, T. Funkhouser, L. Guibas, P. Hanrahan, Q. Huang, Z. Li, S. Savarese, M. Savva, S. Song, H. Su *et al.*, "Shapenet: An information-rich 3d model repository," *arXiv preprint arXiv:1512.03012*, 2015.

[40] C. R. Qi, H. Su, K. Mo, and L. J. Guibas, "Pointnet: Deep learning on point sets for 3d classification and segmentation," in *CVPR*, 2017, pp. 652–660.

[41] Y. Wang, Y. Sun, Z. Liu, S. E. Sarma, M. M. Bronstein, and J. M. Solomon, "Dynamic graph cnn for learning on point clouds," *ACM TOG (SIGGRAPH)*, vol. 38, no. 5, pp. 1–12, 2019.

[42] W. Wu, Z. Qi, and L. Fuxin, "Pointconv: Deep convolutional networks on 3d point clouds," in *CVPR*, 2019, pp. 9621–9630.

[43] K. Tang, J. Wu, W. Peng, Y. Shi, P. Song, Z. Gu, Z. Tian, and W. Wang, "Deep manifold attack on point clouds via parameter plane stretching," in *AAAI*, vol. 37, no. 2, 2023, pp. 2420–2428.

[44] K. Tang, X. He, W. Peng, J. Wu, Y. Shi, D. Liu, P. Zhou, W. Wang, and Z. Tian, "Manifold constraints for imperceptible adversarial attacks on point clouds," in *AAAI*, vol. 38, no. 6, 2024, pp. 5127–5135.

[45] H. Fan, H. Su, and L. J. Guibas, "A point set generation network for 3d object reconstruction from a single image," in *CVPR*, 2017, pp. 605–613.

[46] A. A. Taha and A. Hanbury, "Metrics for evaluating 3d medical image segmentation: analysis, selection, and tool," *BMC medical imaging*, vol. 15, pp. 1–28, 2015.

[47] Y. Rubner, C. Tomasi, and L. J. Guibas, "The earth mover's distance as a metric for image retrieval," *IJCV*, vol. 40, pp. 99–121, 2000.