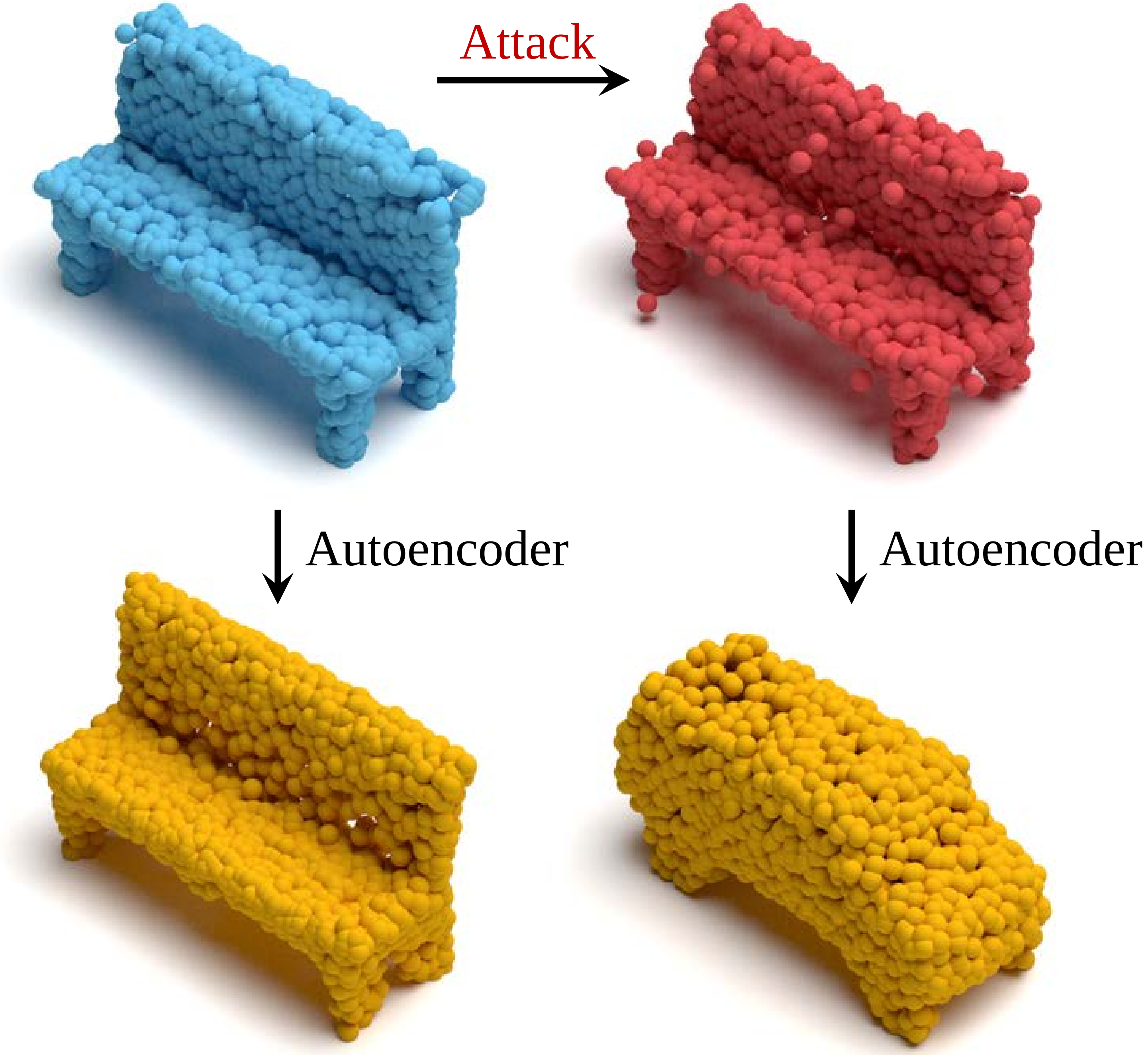
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

3DV 2021
International Conference on 3D Vision
Online, December 1-3, 2021

Geometric Adversarial Attacks and Defenses on 3D Point Clouds

Itai Lang, Uriel Kotlicki, Shai Avidan

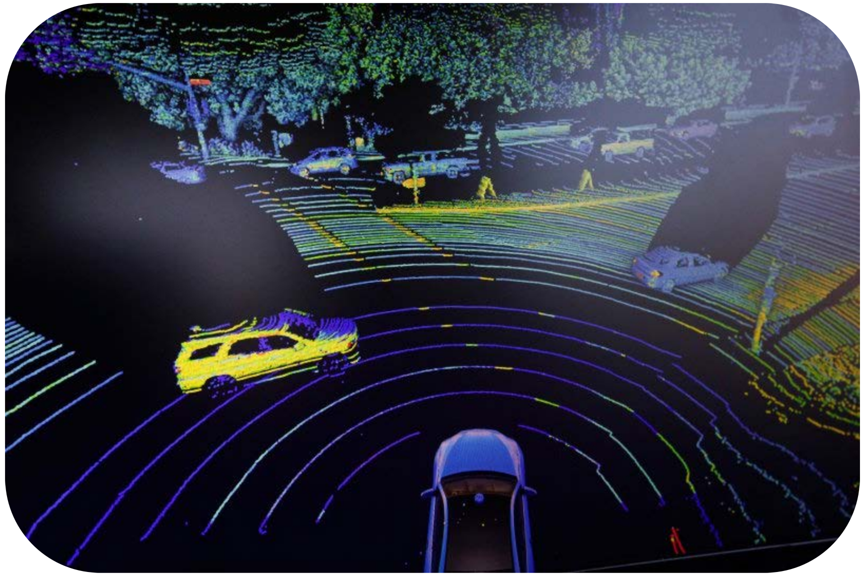


Attack

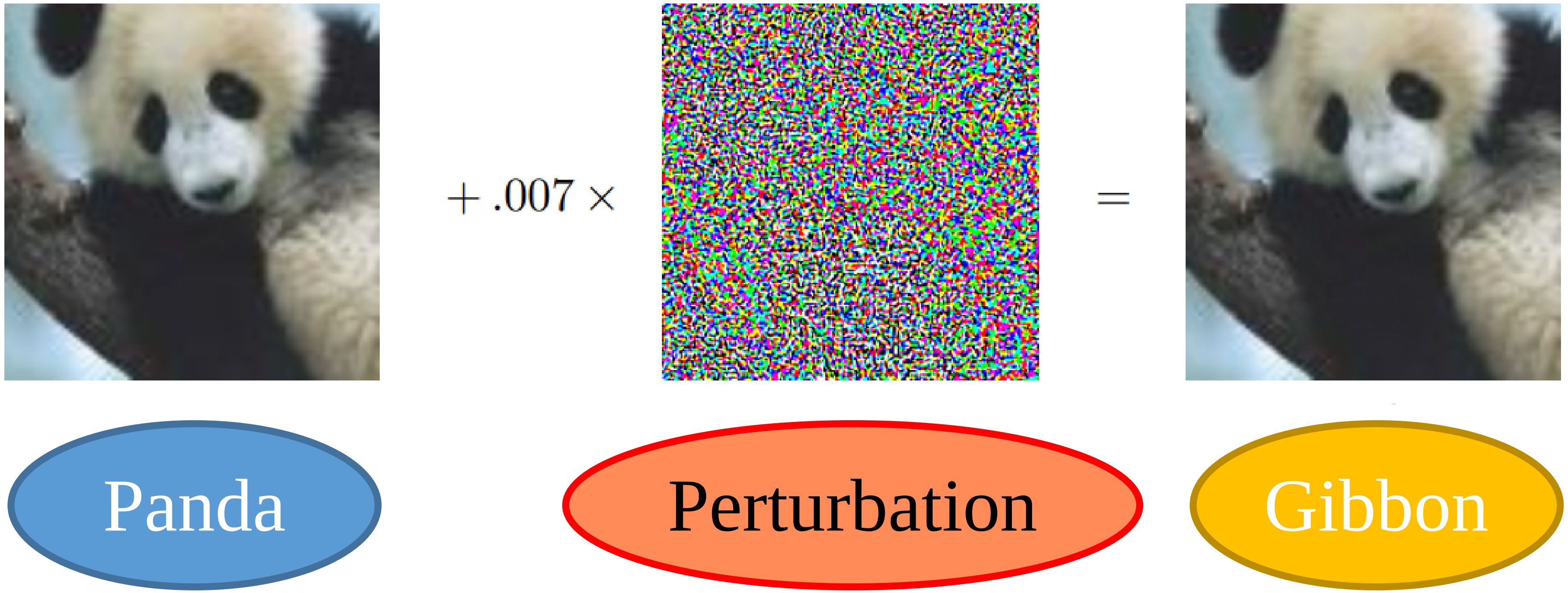
Autoencoder

Autoencoder

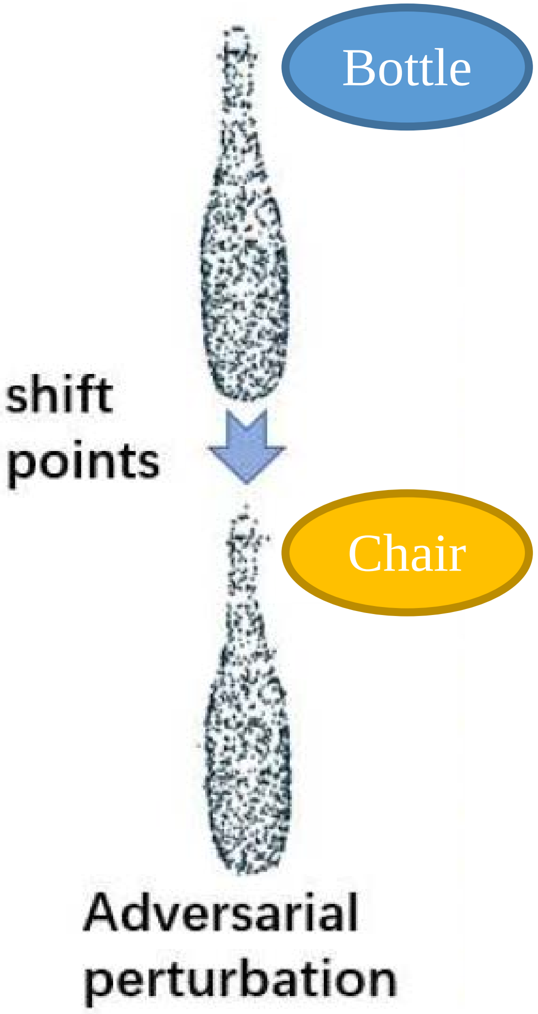
3D & AI in Safety-critical Systems



Neural Networks are Vulnerable!



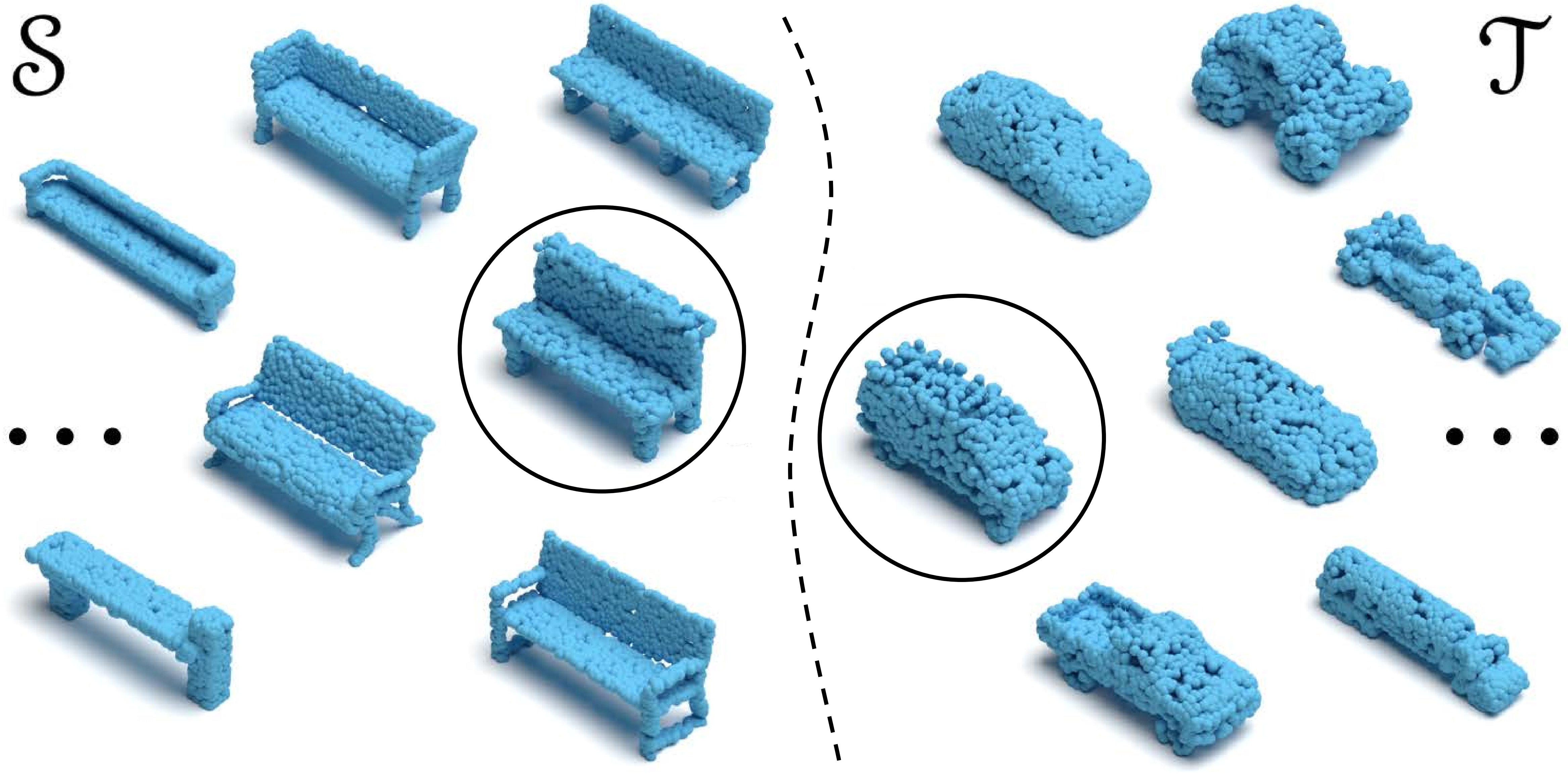
Goodfellow *et al.*, 2015



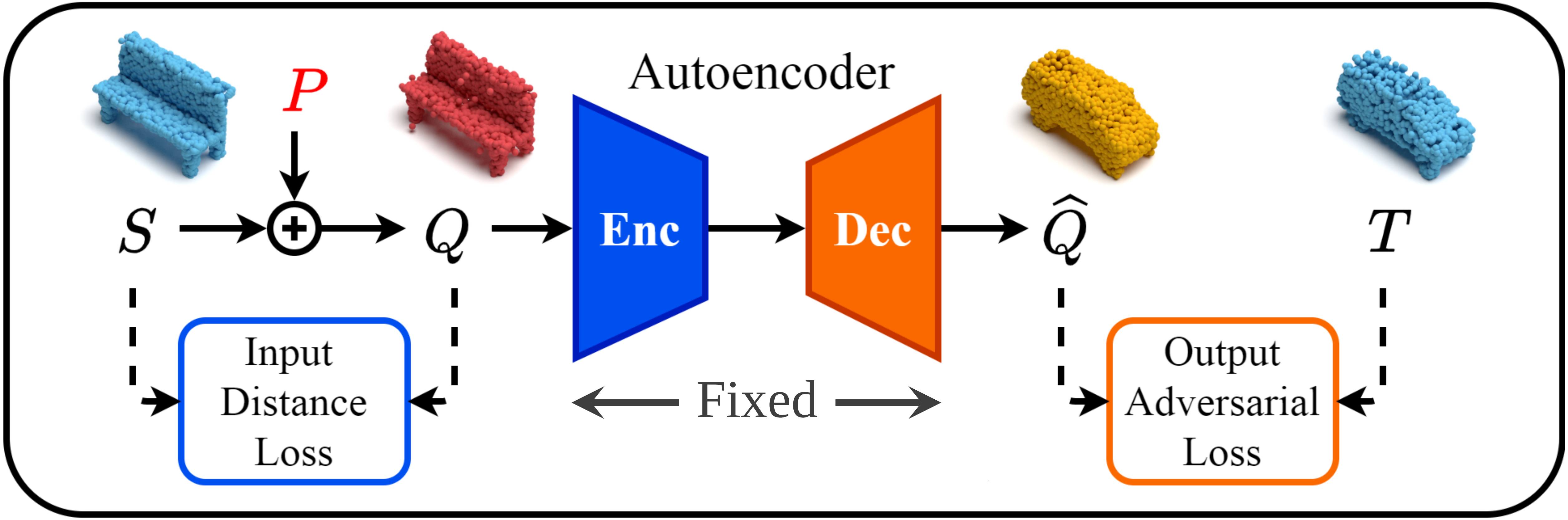
Xiang *et al.*, 2019

Can we make a small perturbation to an input point cloud to change the reconstructed geometry by an autoencoder model?

Problem Statement



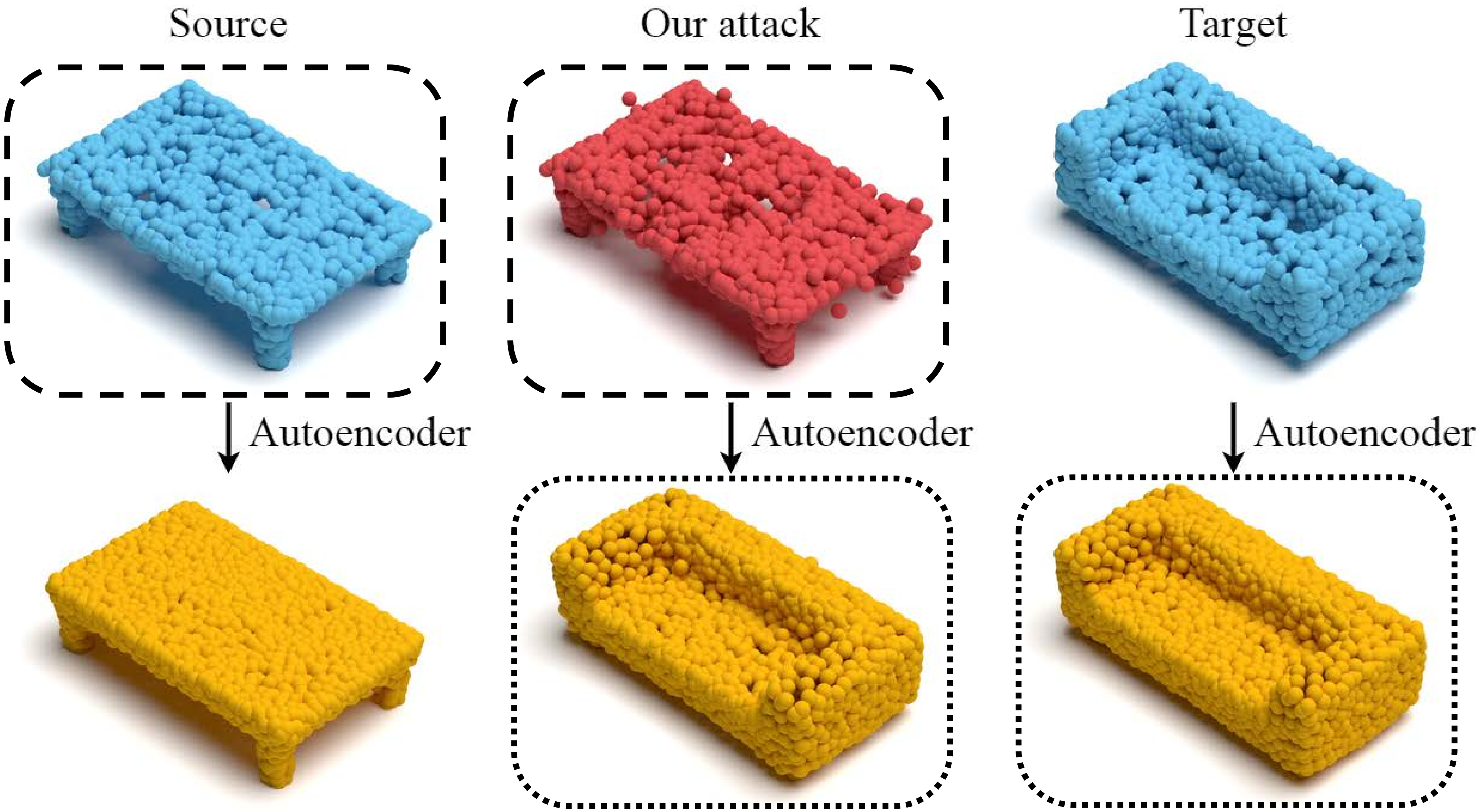
The Proposed Attack



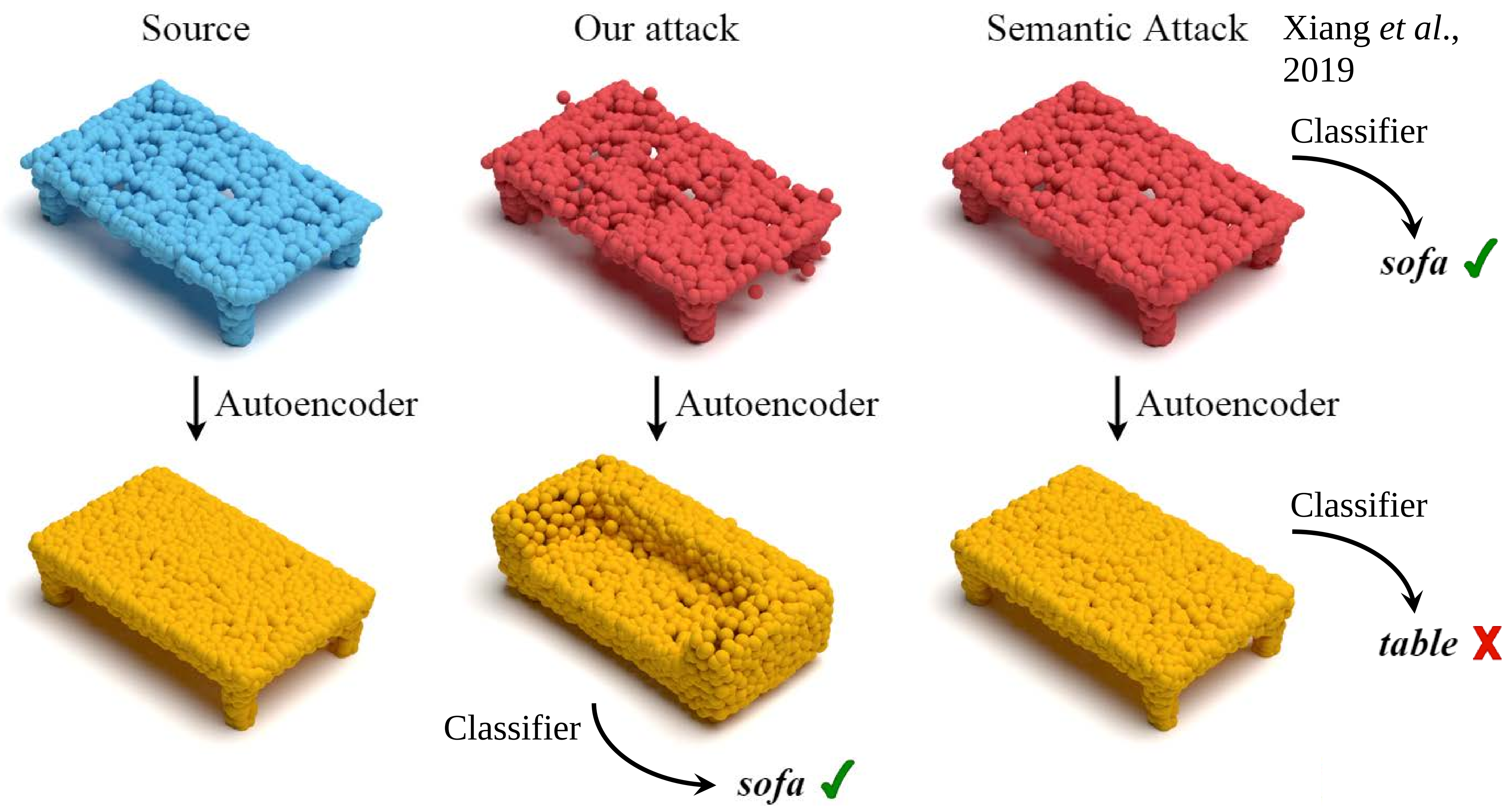
→ Data flow - -→ Loss flow

The attacked autoencoder is from the work of Achlioptas *et al.*, 2018

Attack Results



Attack Comparison



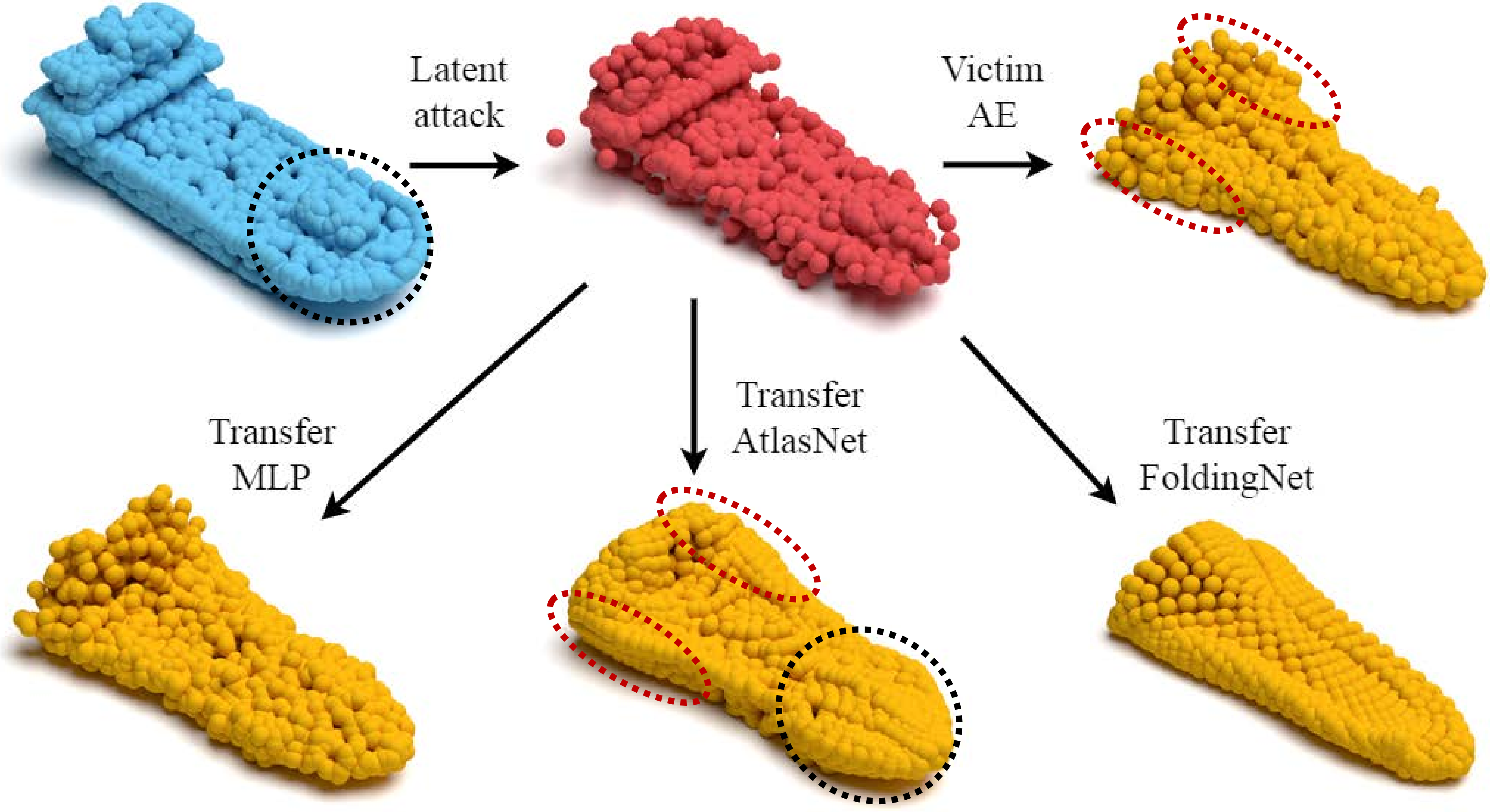
Xiang *et al.*, 2019

Semantics of the Reconstructions

Input type	Hit Target	Avoid Source
Our attack	**76.0%**	**94.7%**
Semantic attack	1.0%	9.6%

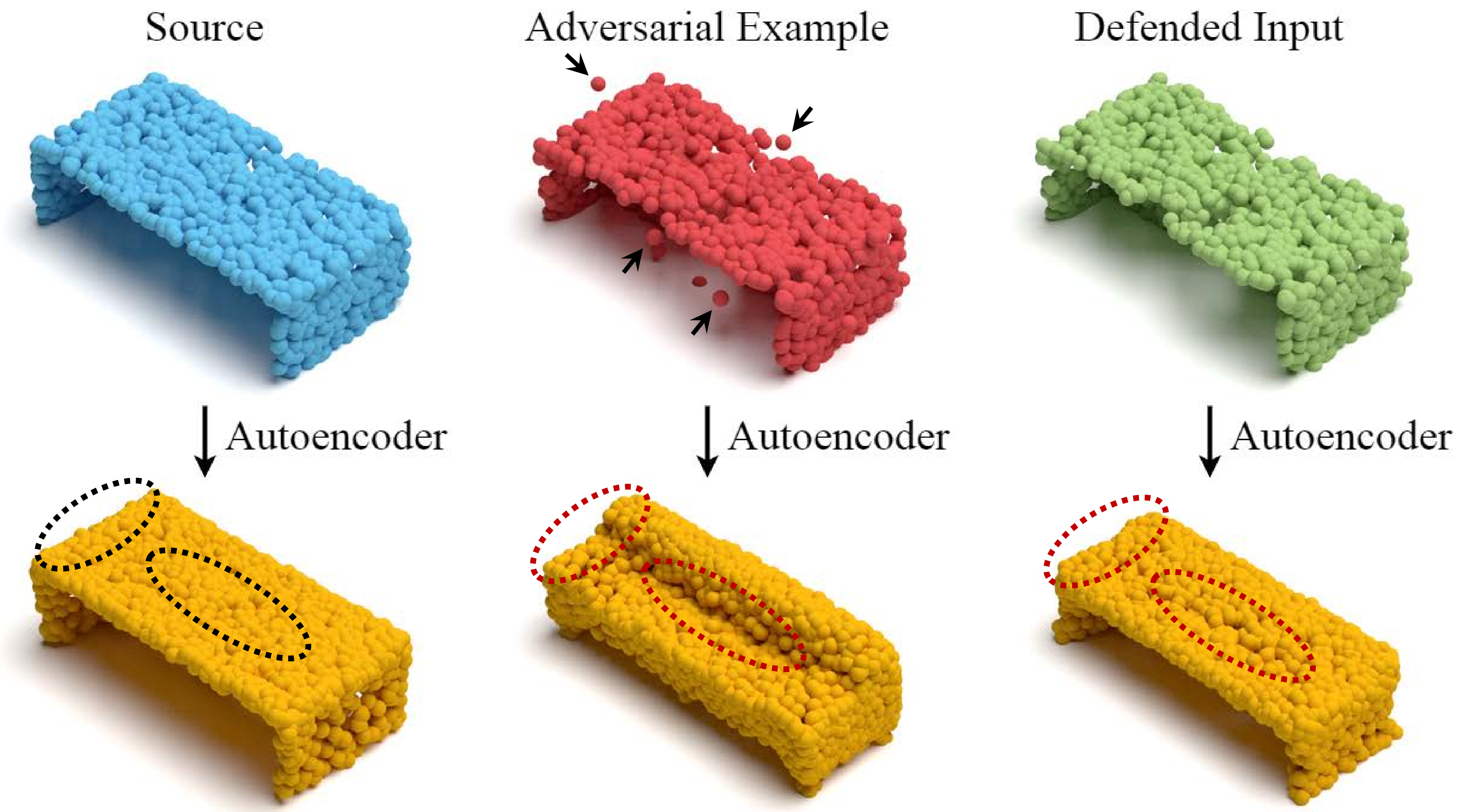
The semantic attack is from the work of Xiang *et al*., 2019

Attack Transfer



MLP AE, Achlioptas *et al.*, 2018 AtlasNet, Groueix *et al.*, 2018 FoldingNet, Yang *et al.*, 2018

Attack Robustness to Defense



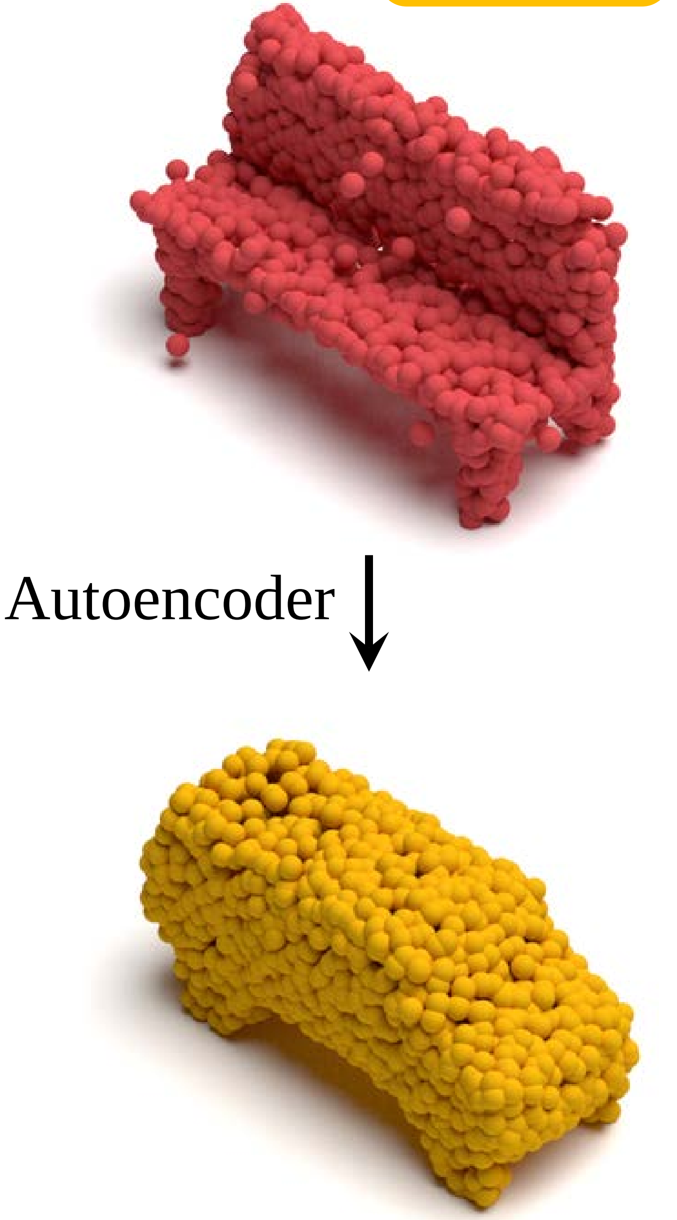
TEL AVIV UNIVERSITY אוניברסיטת תל אביב

3DV 2021
International Conference on 3D Vision
Online, December 1-3, 2021

Summary

- Geometric adversarial attack – changes the reconstructed shape
- Not entirely defendable – a residual effect remains
- Paper and code are available – github.com/itailang/geometric_adv

THANK YOU!


Autoencoder