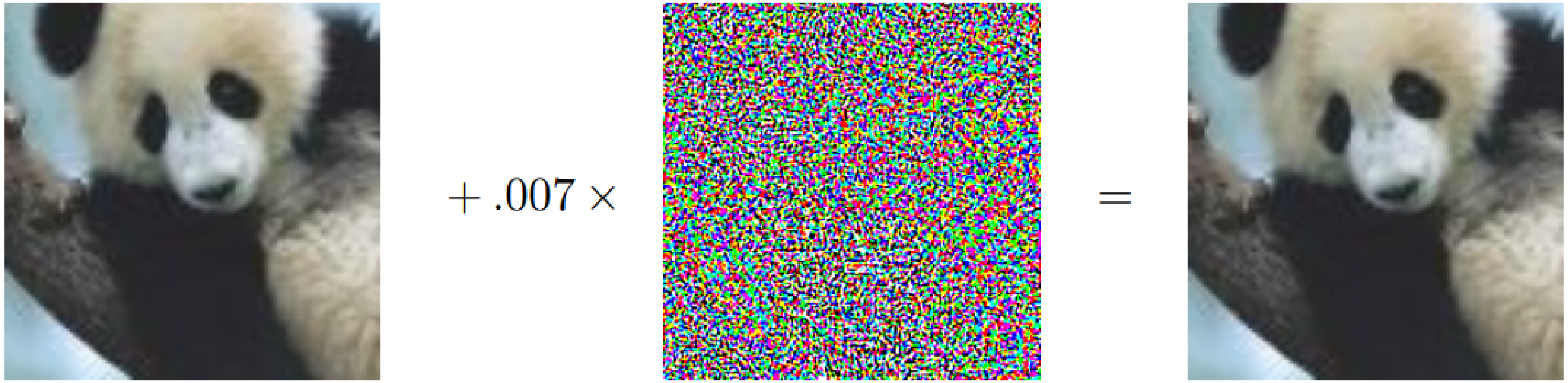
TEL AVIV UNIVERSITY
אוניברסיטת תל אביב

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

Neural Networks are Vulnerable!

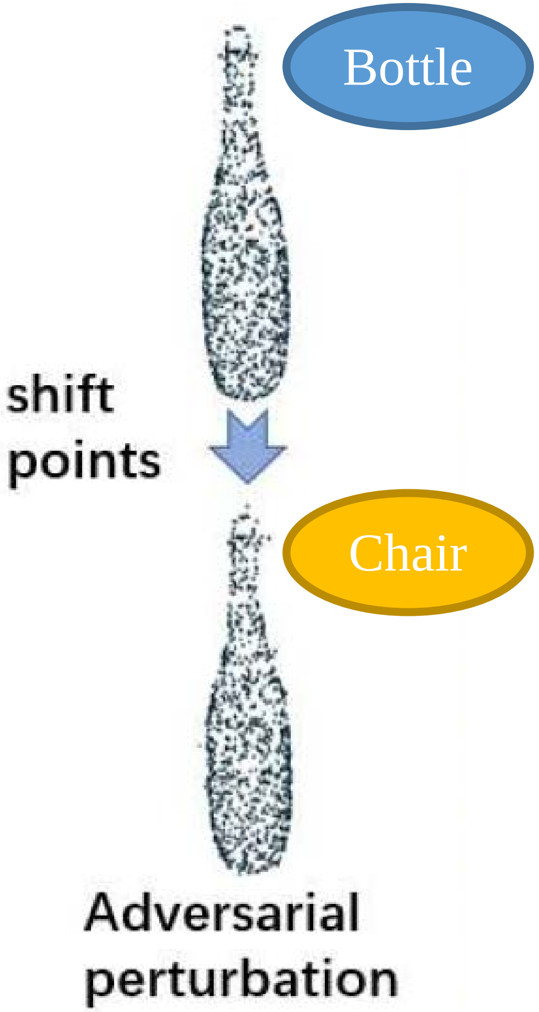


Panda

Perturbation

Gibbon

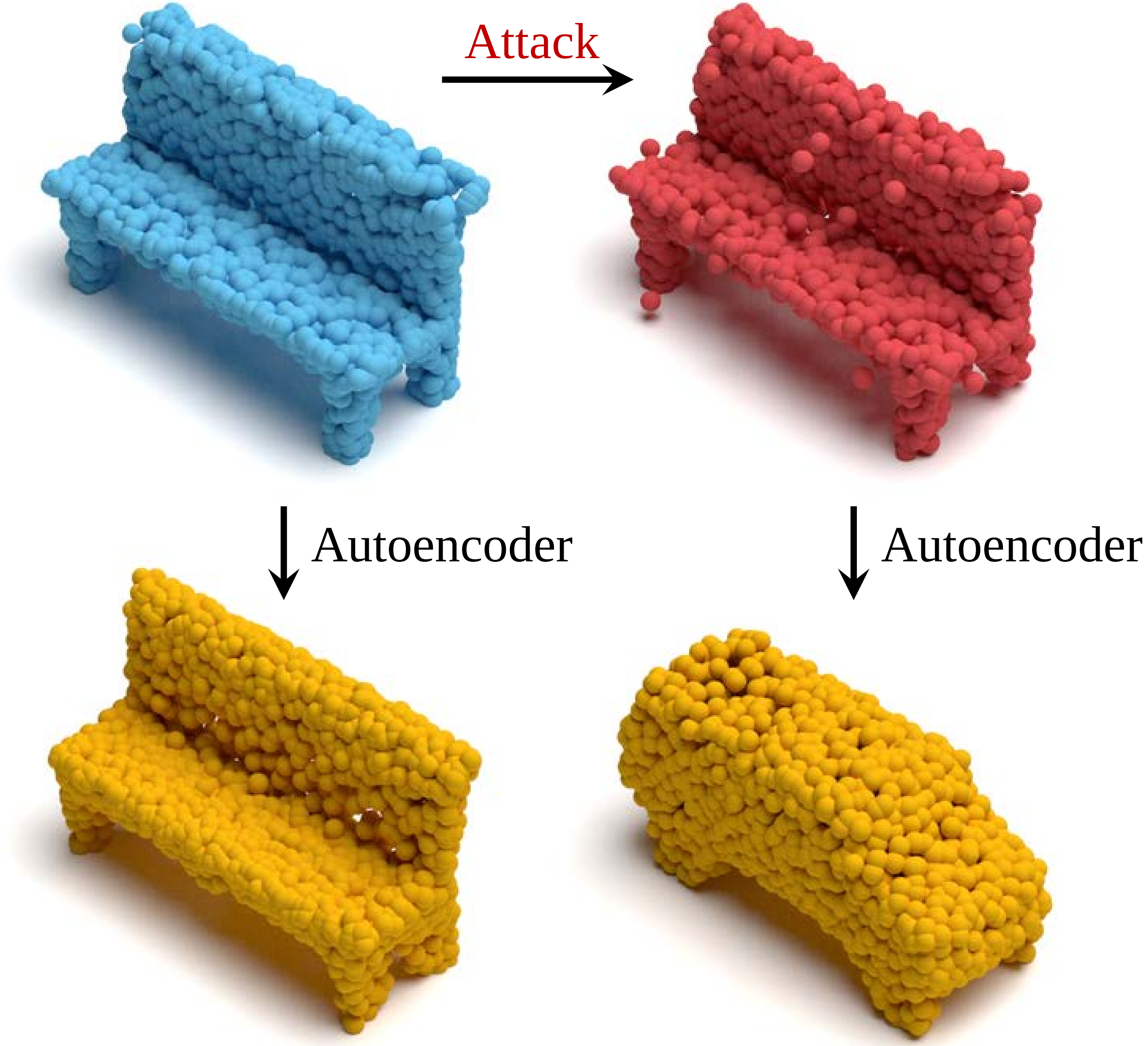
Goodfellow *et al.*, 2015


Bottle

Chair

Xiang *et al.*, 2019

Make a small perturbation to an input point cloud to change the reconstructed geometry by an autoencoder model


Attack
Autoencoder
Autoencoder

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

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

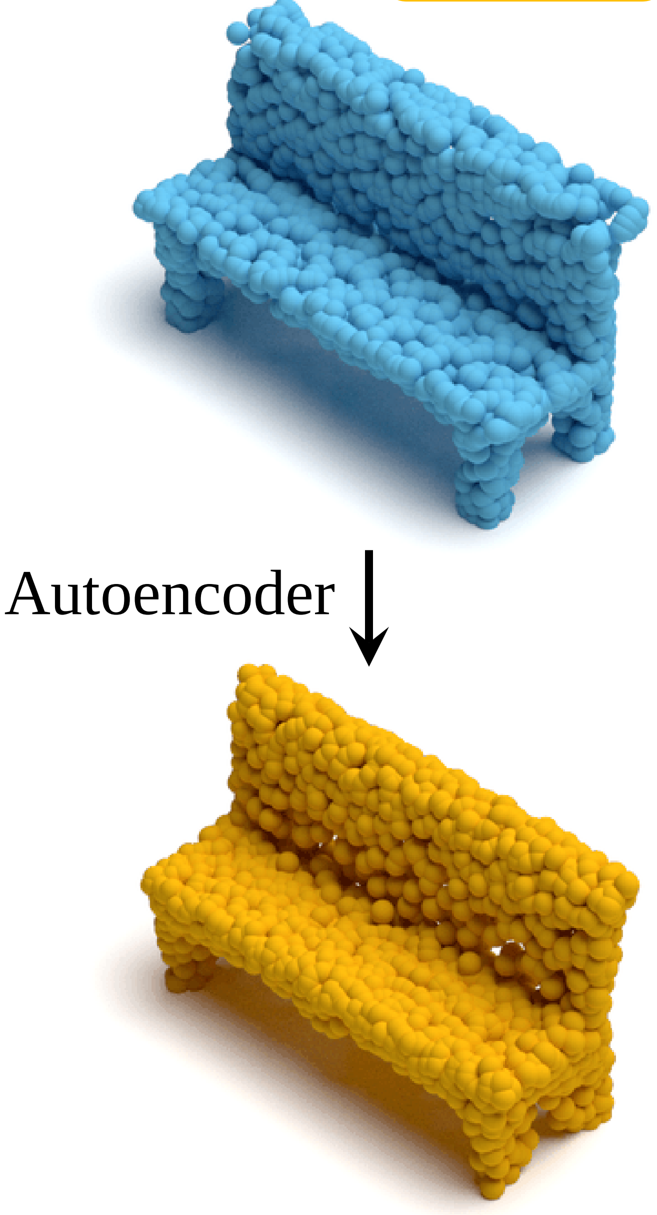
Summary

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