Chair for Integrated Systems
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Understanding Adversarial Robustness in the Context of 3D-Object Detection

Adversarial attacks present a threat to convolutional neural networks deployed in real-time critical applications, such as autonomous driving. These attacks can be performed on the target classifier in the form of black box or white box attacks. In the second case, the attacker may transfer a generalized attack from one network to another. These attacks have been well studied for CNNs applied to 2D classifiers. In this seminar, the extended effect of these attacks on 3D classifiers will be studied.

Contact

Manoj Vemparala

Email: Manoj-Rohit.Vemparala@bmw.de

Advisors

Manoj Rohit Vemparala, Nael Yousef Abdullah Al-Fasfous