BlurNet: Defense by Filtering the Feature Maps

Ravi Raju

September 25, 2019

Outline

Introduction

Introduction

Vulnerabilities in NNs