Università degli Studi di Salerno
Dipartimento di Informatica

Tesi di Laurea di I livello in
Informatica

Adversarial Attacks on Vision-based Deep Neural Networks in Autonomous Driving Vehicles

Relatore
Giuseppe Scanniello
Correlatore
Dott. Nome Cognome

Candidato
Michelangelo Esposito

Academic Year 2021-2022

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Contents

List of Figures

List of Acronyms and Abbreviations

Chapter 1

Introduction

Chapters

- Testing in the software development life cycle
- Limitations of traditional Testing
- Test Driven Development with its advantages and integrations with the agile model

Chapter 2

Problem formulation

2.1 Software Development Lifecycle

2.1.1 Introduction

General introduction on what SDL is and why it is needed in the first place

2.1.2 The waterfall model

Start with the introduction of the waterfall model with a focus on its limitations (i.e. lack of feedback from the client, no possibility to revision requirements, etc...)

2.1.3 Agile techniques

Extreme programming, CI/CD, DevOps, ...

2.1.4 Test Driven Development

Comparison with other agile methods

2.2 Testing embedded systems

2.2.1 Introduction

Reference the old survey papers (i.e. X in the loop) that provide a summary of the main techniques

2.2.2 Test Driven Development fro Embedded systems

Reference to "TDD for Embedded C" and other books/papers

Chapter 3

Literature

Chapter 4

Conclusions

Bibliography

[1] Ross B. Girshick et al. "Rich Feature Hierarchies for Accurate Object Detection and Semantic Segmentation". In: *2014 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2014, Columbus, OH, USA, June 23-28, 2014*. IEEE Computer Society, 2014, pp. 580–587. DOI: 10.1109/CVPR.2014.81. URL: https://doi.org/10.1109/CVPR.2014.81.

[2] Jindi Zhang et al. "Evaluating Adversarial Attacks on Driving Safety in Vision-Based Autonomous Vehicles". In: *IEEE Internet Things J.* 9.5 (2022), pp. 3443–3456. DOI: 10.1109/JIOT.2021.3099164. URL: https://doi.org/10.1109/JIOT.2021.3099164.

[3] Edmund K. Burke and Graham Kendall. *Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques*. Springer US, 2014, pp. 403–449.

[4] *Check: framework for unit testing in C*. URL: https://libcheck.github.io/check/.

[5] A. Author and A. Author. *Book reference example*. Publisher, 2099.

[6] A. Author. "Article title". In: *Journal name* (2099).

[7] *Example*. URL: https://www.isislab.it.

[8] A. Author. "Tesi di esempio ISISLab". 2099.