

STELLENAUSSCHREIBUNG

Bachelorarbeit, Hilfskraftstelle, Masterarbeit, Studentische Abschlussarbeit

ADVERSARIALE ANGRIFFE AUF AUTONOM FAHRENDE FAHRZEUGE

UMFELD

Im Bereich des autonomen Fahrens wurden große Fortschritte in den letzten Jahren erzielt. Trotzdem bleibt fraglich inwieweit sicheres Fahren gewährleistet werden kann. Da aktuelle autonome Fahrzeuge stark auf Deep Learning Algorithmen basieren, ist es nötig die Entscheidungsfindung neuronaler Netze zu verstehen, um zu garantieren, dass diese robust funktionieren und um Sicherheitsaussagen treffen zu können.

Das FZI Forschungszentrum Informatik arbeitet unter anderem an robusten und erklärbaren Deep Learning Ansätzen. Wir forschen an neuen Methoden um autonome Fahrzeuge vor unbeabsichtigten (d. H. Fehlfunktionen) und beabsichtigten (d. H. Hacking) Unfällen zu schützen. Dafür benötigen wir Unterstützung in zahlreichen Bereichen, wobei man sich seinen Stärken entsprechend einbringen kann. Die möglichen Themen sind Adversarial Attacks und Defenses (vor allem Angriffe auf neuronale Netze in der realen Umgebungen), Interpretierbarkeit und Plausibilisierung neuronaler Netze mit Fokus auf autonomes Fahren.

AUFGABEN

- Literaturrecherche und Analyse des Standes der Technik
- Implementierung und Anpassung von ausgewählten Algorithmen in Python

WIR BIETEN

- Ein interdisziplinäres Arbeitsumfeld mit Partnern aus Wissenschaft, Wirtschaft und Anwendern
- Arbeit in einem spannenden und hochaktuellen Themengebiet
- Praktische Anwendung der entwickelten Algorithmen im realen Straßenverkehr
- Aktuelle Hardware zum Training der Algorithmen
- Eine angenehme Arbeitsatmosphäre
- Konstruktive Zusammenarbeit

WIR ERWARTEN

- Gute Programmierkenntnisse in Python
- Theoretische Kenntnisse im Bereich Deep Learning
- Erfahrung mit PyTorch und/oder Tensorflow
- Kenntnisse in Linux
- Selbständiges Denken und Arbeiten
- Motivation und Engagement
- Sehr gute Deutsch- oder Englischkenntnisse

BEWERBUNG

Wir freuen uns auf Deine PDF-Bewerbung an [Svetlana Pavlitskaya](#) mit folgenden Unterlagen:

- aktueller Notenauszug
- tabellarischer Lebenslauf
- kurze Beschreibung deiner Erfahrung im Bereich Deep Learning

WEITERE INFORMATIONEN

Start: ab sofort.

- Themen-Schwerpunkt: Maschinelles Lernen, Mobilität, Sichere und intelligente Fahrzeuge
- Studiengänge: Informatik, Informationstechnik, Informationswirtschaft, Verwandte Studiengänge
- Kontakt: [Svetlana Pavlitskaya](#), pavlitsk@fzi.de, Tel.: +49 721 9654-374