FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

Fahreridentifikation mittels Machine-Learning

Driver identification by Machine-Learning

Masterarbeit

Zur Erlangung des akademischen Grades

Master of Science in Engineering

der Fachhochschule Campus Wien
Masterstudiengang: ITS-20

Vorgelegt von:
David Lechner

Personenkennzeichen:
1810537012

ErstbetreuerIn / ErstbegutachterIn:
Dr. Martin Schmiedecker

ZweitbetreuerIn / ZweitbegutachterIn:
Kevin Koch

Eingereicht am:
tt.mm.jjjj

Erklärung:

Ich erkläre, dass die vorliegende Masterarbeit von mir selbst verfasst wurde und ich keine anderen als die angeführten Behelfe verwendet bzw. mich auch sonst keiner unerlaubter Hilfe bedient habe.

Ich versichere, dass ich diese Masterarbeit bisher weder im In- noch im Ausland (einer Beurteilerin/einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Weiters versichere ich, dass die von mir eingereichten Exemplare (ausgedruckt und elektronisch) identisch sind.

Datum: Unterschrift:

Kurzfassung

(Z.B. “Diese Arbeit beschäftigt sich mit...”)

Abstract

(E.g. “This thesis deals with...”)

List of Abbreviations

ARP	Address Resolution Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
WLAN	Wireless Local Area Network

Key Terms

Machine Learning
CAN-Bus
Driver Fingerprinting

Contents

1. Einführung

Der Präfix Smart ist in der heutigen Alltagsprache täglich in Verwendung. Entweder wird es in Verbindung mit einem Telekommunikationsgerät oder mit anderen sogenannten Wearables gebracht. Damit ist gemeint, dass diese mit Funktechnologien ausgestattet sind und Daten übermitteln. Der Bereich Internet of Things (IoT) ist noch einmal eine Weiterentwicklung, bei dem jegliches technische Gerät – von der Lampe bis hin zur Fertigungsmaschinen – mit dem Internet verbunden ist. Dieser Trend macht auch vor Fahrzeugen keinen Halt. Schon längst sind moderne Autos mit LTE-, GPS und Wifi-Modulen ausgestattet und senden Daten unter anderem zum Hersteller. Gartner prognostiziert für das Jahr 2020 470 Millionen vernetzte Fahrzeuge [Gar19]. In Zukunft werden wahrscheinlich alle Fahrzeuge mit etlichen Sensoren ausgestattet sein und kommunizieren untereinander, mit der Umwelt, dem Fahrer oder sonstige Service-Anbieter. Dies gründet vor allem auf den wachsenden Themen Vehicle-to-Everything (V2X) und autonomes Fahren. Insbesondere beim letztgenannten wird zudem eine riesige Menge an Daten aus tausenden Sensoren gewonnen. Schon heute senden Electronic Control Units (ECUs) Daten, wie zum Beispiel Lenkradwinkel, Gangposition und Bremsdruck, welche für Sicherheits- und Komfortfunktionen genutzt werden. Durch diese Vielzahl an verschiedenen Daten ergeben sich viele weitere Möglichkeiten. Eine davon ist, den Lenker eines Autos während der Fahrt nur durch das Fahrverhalten zu identifizieren.

Daraus lassen sich unterschiedliche Anwendungen ableiten. Einige von ihnen schaffen Komfort und erleichtern in gewisser Weise das Leben des Fahrers. Andere indes könnten gegen den Fahrzeughalter und der Fahrerin selbst eingesetzt werden, diese gehen mit datenschutzrechtlichen Bedenken einher.

Doch zunächst zu diesen, welche eine positive Auswirkung haben können. Moderne Autos – vor allem jene mit einem Automatik Getriebe – bieten die Möglichkeit sich an den Fahrstil anzupassen. Wenn beispielsweise eine Person zum schnelleren Beschleunigen neigt, lernt dies das Auto und schaltet demnach erst bei einer höheren Motordrehzahl in den nächsthöheren Gang. Dasselbe gilt bei einem gemächlichen Fahrstil, wobei hier eher früher geschalten wird. Lernt das Auto nun von einer Person mit dem zweitgenannten Stil und wird aber auch hin und wieder mit anderen Personen, zum Beispiel Familienmitglieder, geteilt, kann es für diese ein Komfortverlust darstellen. Identifiziert das Auto jedoch durch das Fahrverhalten eine andere Person, könnte es den gelernten Stil temporär vergessen oder gar ein neues Profil anlegen und erneut lernen.

Der Mechanismus kann weiters dazu verwendet werden, Fahrzeug-Funktionen und Leistung fahrerabhängig zu steuern. Ein Familienvater ist so etwa in der Lage, die zur Verfügung stehenden PS einzuschränken, wenn seine Kinder mit dem Auto fahren.

Überdies ist eine Art Diebstahlwarnung zu realisieren. Wird eine unautorisierte Fahrerin eines Autos erkannt, kann beispielsweise eine Benachrichtigung an den Fahrzeughalter versendet, oder die Fahrerin zum Anhalten gebracht werden.

Durch das Aufzeichnen und Analysieren von personenbezogenen Daten kommen natürlich auch datenschutzrechtliche Bedenken auf. Werden die Daten in eine Cloud – sei es eine vom Hersteller, Versicherung oder einer anderer Drittpartei – gesendet und ausgewertet, können Personen von diesen Unternehmen oder Organisationen eindeutig identifiziert und geortet

werden. Dies kann in einigen Fällen problematisch werden. Des Weiteren könnte der Hersteller bestimmte Services anbieten, welche personalisierte Werbungen während dem Fahren anzeigen. Eventuell ist es dadurch möglich, bevorzugte Restaurants in der Navigationsansicht hervorzuheben.

Die angeführten Beispiele zeigen, dass ein System, welches die Person hinter dem Lenkrad eines Fahrzeuges eindeutig identifiziert, Benutzervorteile bringen kann. Zudem erschließt sich ein neues Geschäftsfeld für Autohersteller, um vielleicht Premium-Features anbieten zu können. Jedoch stellen sich auch Fragen zur Privatsphäre und wie mit solch sensiblen Daten umgegangen wird.

Bibliography

[Gar19] Inc. Gartner. Gartner says 5.8 billion enterprise and automotive iot endpoints will be in use in 2020. Technical report, 2019. 1

List of Figures

List of Tables

A. Anhang/Ergänzende Information

EIGENER ANHANG

(Hier können Schaltpläne, Programme usw. eingefügt werden.)