Guest Editorial
Special Issue on Sensor Technologies for Connected Cars: Devices, Systems and Modeling

VEHICULAR accidents are a major global problem, leading to human injury, damages to property, financial losses and other negative impacts on the general public. In most cases, vehicular accidents are caused by avoidable human error and improper driving practices. With recent advances in sensing technologies, self-driving, connected cars and autonomous vehicles are becoming more and more practicable. The sensor data contribution to the peer to peer vehicle sharing system reduces occurrences of road accidents by the use of vehicle to vehicle (V2V) interaction, along with use of sensors for maintaining safe driving distances and preempting accidents. Sensor technology in connected cars also improves the overall driving experience by using vehicle to infrastructure (V2I) interaction. This enables the reception of warnings from a network of roadside units, functioning as stationary waypoints and the relaying of warnings messages and information regarding availability of crucial services. Such information is particularly beneficial to users in remote areas where it cannot be obtained reliably through conventional communication channels.

The first part of this Special Issue deals with driving maneuver classification, in a comparative study between three window-based feature extraction methods for driving maneuver classification which are statistical values, automatically extracted features using principal component analysis and stacked sparse auto-encoders. This study emphasizes the need for driving manoeuvre classification technology as an effort to eliminate road accidents and to assist automotive users with fuel consumption optimization methods. In this comparative study, Xie *et al.* used smartphones embedded sensors to generate window based data, then use principal component analysis and stacked sparse auto-encoder to extract features using the windowed. A technical consideration made from this work is that, in most cases, a smaller window size leads to better performance for both acceleration and deceleration operations.

The next part of the Special Issue deals with an advanced driver assistance system, whereby, a concept of dangerous driving intensity (DDI) is introduced. In this section, Yin *et al.* proposed a fuzzy-set-optimized framework via a particle swarm optimization for modelling driver, vehicle, and lane attributes. The input sensors are used in this approach to obtain driving conditions and driver conditions.

The third part of the Special Issue deals with, IoT Cloud System for Traffic Monitoring and vehicular accidents prevention based on mobile sensor data processing.

In the third part, Celesti *et al.* proposed an IoT cloud system for traffic monitoring and alert notifications based on Open GTS and Mongo DB. Their system collected Geo-location and speed data by using the GSM/GPRS/GPS TK103 system tracker installed in some of the vehicles.

The fourth part of this Special Issue addresses the measurement of traffic flow parameters with radar-based sensor. López *et al.* proposed a based on a Frequency-Modulated Continuous Wave radar with satellite mounted installation which is operating at 24 GHz. Their proposed prototype performs clutter cancellation and target speed estimations by using the phase information from target echoes.

The fifth part of this Special Issue focuses on the emergency broadcast strategy for vehicular ad hoc networks. In this final part, Chou *et al.* proposed an emergency broadcast system, which is called Appropriate Vehicular Emergency Dissemination (AVED) scheme to ensure when a car accident occurs, the vehicle's sensors detect impact signals and immediately send emergency messages to inform other vehicles nearby to assist in avoiding redundant broadcast messages. The final part of the Special Issue deals with Proactive Threat Detection for Connected Cars. Here, al-Khateeb *et al.* investigated remote or cyber hijacking of connected vehicles. They introduced proactive anomaly detection technique for cyber threat prevention by using behavioral analysis and profiling concepts through Bayesian estimation techniques.

REZA MALEKIAN, *Lead Guest Editor*
Department of Electrical, Electronic and Computer Engineering
University of Pretoria
Pretoria 0002, South Africa
(e-mail: reza.malekian@ieee.org)

KEVIN CURRAN, *Guest Editor*
School of Computing
Ulster University
Coleraine, Northern Ireland
(e-mail: kj.curran@ulster.ac.uk)

Digital Object Identifier 10.1109/JSEN.2018.2830478

CHRISTIAN FISCHER PEDERSEN, *Guest Editor*
Department of Engineering
Aarhus University
8200 Aarhus, Denmark
(e-mail: cfp@eng.au.dk)

BIN CAO, *Guest Editor*
ChongQing University of Posts and Telecommunications
Chongqing 400065, China
(e-mail: caobin@cqupt.edu.cn)

XUEWEI QI, *Guest Editor*
Autonomous Vehicle Technology Laboratory
General Motors
USA
qixuewei@gmail.com