Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 487–491 DOI: 10.15439/2019F263
ISSN 2300-5963 ACSIS, Vol. 18

Inference of driver behavior using correlated IoT data from the vehicle telemetry and the driver mobile phone

Daniel Alves da Silva, José Alberto Sousa Torres, Alexandre Pinheiro, Francisco L. de Caldas Filho,
Fabio L. L. Mendonça, Bruno J. G Praciano, Guilherme de Oliveira Kfouri and Rafael T. de Sousa Jr.
Department of Electrical Engineering
University of Brasília, Brasília, Brasil
{daniel.alves, albero.torres ,alexandre.pinheiro, francisco.lopes,
fabio.mendonca, bruno.praciano, guilherme.kfouri}@redes.unb.br, desousa@unb.br

***Abstract*—Drivers' behavior in traffic is a determining factor for the rate of accidents on roads and highways. This paper presents the design of an intelligent IoT system capable of inferring and warning about road traffic risks and danger zones, based on data obtained from the vehicles and their drivers mobile phones, thus helping to avoid accidents and seeking to preserve the lives of the passengers. The proposed approach is to collect vehicle telemetry data and mobile phone sensors data through an IoT network and then to analyze the driver's behavior while driving, along with data from the environment. The results of the inference serve to alert drivers about incidents in their trajectory as well as to provide feedback on how they are driving. The proposal is validated using a developed prototype to test its data collection and inference features in a small scale experiment.**

***Index Terms*—Internet of Things; Vehicular networks; Driving behavior; Inference; OBD-II; Android.**

I. Introduction

THE WAY drivers behave in traffic is a determining factor for high accident rates on roads and highways. In 2018, there were 69114 serious accidents on Brazilian highways [1]. In such context [2], by analyzing the driver's profile, it is possible to analyze the phenomenon and create mechanisms to positively influence driver behavior, thus making the routes safer and energy use more efficient.

Over time, technologies, such as smartphones, have become easily accessible to the population and have aided drivers. According to FGV-SP [3], the number of smartphones in Brazil already exceeds 230 million. Since most of these mobile phone models have sensors, such as GPS (Global Positioning System), accelerometer, gyroscope, 3-axis magnetometer (lateral, longitudinal and vertical or in coordinates x, y and z), we can use their data, as indicated by other studies, such as [4] or [5], to contribute to the driver behavior study.

Internet of Things (IoT) is a paradigm that combines aspects and technologies of different approaches: ubiquitous computing, communication protocols and technologies, sensors and actuators, composing a system in which the real world and the digital world interact symbiotically [6]. The IoT connected devices installed base comprised around 23.14 billion devices in 2018 and it is projected to increase to 75.44 billion ones worldwide by 2025 [7].

The increasing number of internet-connected objects ranging from cell phones to air conditioners is a compelling force for a more comprehensive study of how such devices connect. The ease to share information among IoT devices open up a new environment for different uses, where objects with traditional use can turn into objects with a certain intelligence, as shown in [8].

The IoT concept is based on data sharing between several different devices, be they vehicles or, in their simplest form, smartphones. Thus, shared data can be treated in a way that generates different interpretations and providing significant indicators to, for example, influence users behavior [9]. Then, the device can be part of several IoT networks and with intelligence to infer actions.

For the proposed project development, firstly it was necessary to fully understand the IoT concept, which is used for new technology development and it is the assumption on which the Smart Drive project is based, developed and discussed in this article.

Like all new technologies, the IoT development also faces several challenges. One of main topics addressed in our IoT study is network security. The need for in-depth study of this topic is observed when analyzing the steps necessary for system operation, i.e. information sharing may be subject to malicious actions, which will compromise the network operation and even the user privacy. Some methods are employed to mitigate this problem, as explained in [10]. This topic was approached with its necessary applications in the project being registered in this paper.

The rest of this article is divided into four parts. Section II briefly highlights the main related works. Section III presents the Smart Drive project proposal as well as an overview of what was developed. Section IV encompasses the project development and implementation. Section V focuses on the main contribution of this paper regarding inferences of driver behavior. Finally, Section VI presents the conclusions about the validation of the proposal and comments on future work.

II. Related works

In order to start the proposed project, it was necessary to first investigate some related works, i.e. already published articles that had some ideas correlated with the objectives here exposed. Therefore, the following articles were analyzed:

- Driver Behavior Profiling Using Smartphones: A Low-Cost Platform for Driver Monitoring [11]: In this article, it is analyzed how smartphone sensors can be used to identify maneuvers. SenseFleet is proposed, a steering profile platform that is able to detect risky events direction; and
- Driver Profile Analysis: Event Detection through Smartphones and Machine Learning [2]: This article conducts an investigation with different sensors, present in an Android smartphone, and different classification algorithms, in order to evaluate which sensor set/method allows classification with greater accuracy. The results show that specific combinations of sensors and intelligent methods allow to improve rate performance.

It is important to note that other articles were also considered for the realization of the project and are cited hereafter.

III. Methodology

For the project development, it was necessary to define what should be inferred and what should be returned to the user.

The project scope was based on the environment in which the car will be present, as well as its movement, given data sampling of several routes performed. So, it was possible to predict user behavior and to correlate data with streets that the car would go through. Thus, user's mobile phone can inform the best route as well as possible dangers in its trajectory.

The referred paper [12] is very useful regarding the functionality developed in the project, as well as the data to be inferred and corresponding interpretations. Also interesting is [2], which provides a good basis for the driver profile analysis.

A. Objectives

Six specific objectives, that will provide a project progress vision, have been defined:

1) Collect telemetry data from vehicular computer. Such data will be captured from OBD-II (On-board diagnostics) device, as indicated in [5];
2) Collect data from user Android device sensors, as indicated in [13] and [14];
3) Develop mobile application gateway to receive collected data and transmit to server called Smart Driver;
4) Develop secure server, using Hypertext Transfer Protocol Secure protocol, with auto registration function to receive collected data and transmit it to application;
5) Execute inferences, both at application and server layers, using collected data, to identify driver behavior, as well as to send geographic information on the risk areas;
6) Develop application for users administration, access to collected data and inference results.

B. Project phases

The architecture development has occurred in five phases, detailed as follows: in phase 1 data were collected from an OBD-II device, connected to the car, and the individual's smartphone; phase 2 consists of access to Smart Driver platform, from an application installed on smartphone; in phase 3 each user direction characteristics are verified by inference; Phase 4 consists of indications to the user about incidents generated from his driving and information about safety of certain routes; and phase 5 provides user administration interface, data and inferred information. Figure 1 shows, in an illustrative way, the phases related above.

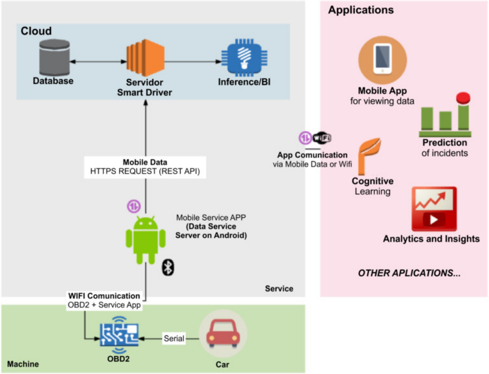


Figure 1. The project general architecture

C. Sensors for an Android device

Some data have been set to be used from the user's Android device. These data are considered from the cell phone capability of acquiring them, for that, the work presented in [13] was useful. The data are quoted below:

- accelerometer - abrupt acceleration or deceleration can be inferred according to the acceleration vector provided by the sensor;
- GPS - provides the speed (m/s), making it possible to compare this value with the allowed track speed;
- orientation - according to the magnetometer and the gravity sensor, azimuth (-pi, pi) is obtained in radians. The change rate at the steering wheel is found by calculating the change after two subsequent samples, giving the idea of how sharp is the car turning.

The Android operating system was chosen as basis to this research because it is installed on almost seven times more devices than the iOS operating system in Brazil.

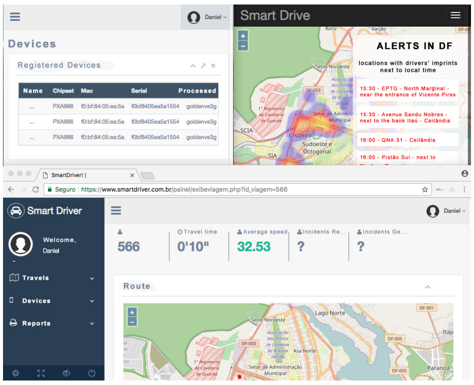
IV. Proposed Solution

This topic reports the development of proposed application for recording incidents and events while driving. The application module is responsible for receiving information generated by user and present it to the UIOT, a middleware responsible for data storage and sharing, developed and maintained by IoT research team, at the University of Brasilia. The tools used to develop the application module were Java, Android Studio IDE and Google Firebase.

A. *SmartDriver Platform*

The SmartDriver platform development objective was to create a secure service for communication of stealthy data about user location, requiring that this service being scalable and highly available through the "Raise Middleware" use. Another important goal was the development of the user administration interface, the data and the plotting of the routes and cluster of incidents as heat zones on the map.

In Figure 2 is possible to visualize the reference region heat map, where heat points (red scales), present regions in which there were incidents, such as, abrupt acceleration and stops.


Daniel
Devices
Registered Devices
Smart Drive
ALERTS IN DF
locations with drivers' imprints next to local time
SmartDriver! |
Seguro https://www.smartdriver.com.br/painel/exibeviagem.php?id_viagem=566
Smart Driver
Welcome, Daniel
Travels
Devices
Reports
Route

Name	Chipset	Mac	Serial	Processed
...	PXA986	f0:bf:84:05:ea:5a	f0bf8405ea5a1554	goldenve3g
...	PXA986	f0:bf:84:05:ea:5a	f0bf8405ea5a1554	goldenve3g
...	PXA986	f0:bf:84:05:ea:5a	f0bf8405ea5a1554	goldenve3g

15:30 - EPTG - North Marginal - near the entrance of Vicente Pires

15:30 - Avenue Sandu Nobres - next to the bank Itaú - Ceilândia

16:00 - QNA 31 - Ceilândia

16:00 - Pistão Sul - next to

	Travel time	Average speed	Incidents Re...	Incidents Ge...
566	0'10"	32.53	?	?

Figure 2. SmartDriver Platform

In this platform, in addition to presenting the risky areas on the roads, with their respective history of alerts, it is also possible to register new users. In order to do that, the Log in / Register window must be accessed to allow user will to set the requested email and password.

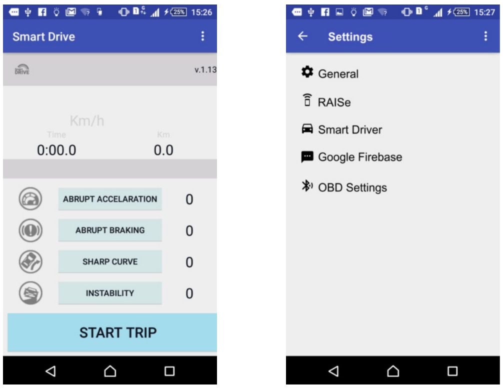
B. *Proposed mobile application*

The application for capturing events has two main screens: Home and Settings.

The application starting screen is shown in Figure 3a. The user's trip will be initiated by clicking the Start Trip option. In this screen, the user's car speed will be displayed as well as the traveled time, the distance traveled and all events like abrupt acceleration, abrupt breaking, sharp curve and instability.

When starting the trip, in addition to tracking possible events while driving, user can report third-party events by clicking on event name buttons, as shown in Figure 3a.

Finally, the user will also have access to application settings, as shown in Figure 3b. In this menu, it is possible to access general application settings; connectivity function with Raise; connectivity settings with Smart Driver server; OBD-II device settings and the Firebase function that stores the updated Firebase token value, which identifies each device/user. This value will be used by the inference to send the results (data to be presented to the user) directly to device, which will be read by application and presented to user.



(a) Main screen (b) Settings screen

Figure 3. Application screens

C. *Self-registration*

The self-registration mechanism was developed as a way to facilitate the entry and management of devices in IOT networks, allowing sensors and actuators, aware of their context, to enter autonomously and securely in an environment capable of receiving massive volumes of data and control actuators safely. As explained in [15], the middlware responsible for receiving and processing data in cloud has two main components, the REST API Approach for IoT Services (RAISe) and the User Interface Management System (UIMS). RAISe is the web services interface responsible for responding to client requests, storing data provided by these clients. UIMS is the visual interface through which a user can consult data manipulated by the middleware.

The solution implements a complete self-registering architecture for the Smart Device from sending basic device data, such as serial number, MAC address and other identification data, thus forming a unique composite primary key for any device that enters into that network. After registration, the device can be associated with one or more users, keeping track of who handled the device during its life cycle. Thus, the sensor data recording is associated to user, promoting individual definition of their steering profile.

The entire information transit process between the device and the self-registering middleware is performed through a Secure Sockets Layer (SSL) connection. In addition, sender authenticity is verified based on a token generated randomly and periodically by the middleware and sent to the device after its registration process. Thus, in order to allow the call of service from a device, it must send an authentication token which must be within its validity.

Due to need for additional processing, the communication architecture between device and middleware is asynchronous. Thus, although the device makes repeated calls to the service to perform the data sending, the inference answer is performed only after processing data step, with message sending through an operating system API call. This solution was adopted because the constant data sending process from client requires a real-time response from the server.

V. Inference

The inference process is the base for the *insights* obtained from the collected raw data of the IoT devices. In the proposed model, part of the data processing and analysis is performed in the device itself, such as the identification of sharp braking and curves, and part is performed in a centralized way, mainly heuristics that depend on collective knowledge, that is, involving joint analysis of data coming from different devices.

Heuristics involving collective knowledge are precisely the main contribution of this project. The centralized analysis allows not only heuristics creation involving large volume of data, due to the difference of processing and storage capacities in relation to IoT devices, as it creates a bidirectional channel of communication, allowing the collectively generated *insights* to arrive at each of the individual devices. It is important to emphasize that, although several studies propose Vehicle-to-Vehicle communication models (V2V communication), the cloud-based communication strategy is more adequate at the present moment, since, while the mobile data communication technologies are more consolidated and provide good coverage and high speeds, V2V technologies are still in the early stages of deployment.

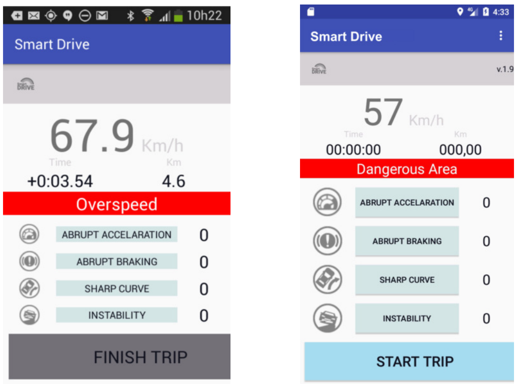
A. Clustering and Alerts

From the collected data, the incident point clustering is performed to calculate the region hazard index and, thus, define the hazardous areas. The clustering groups points that they are at a distance of three meters from each other; this distance is necessary because it is very unlikely that two incidents will be marked exactly in the same geographic coordinate. Thus, the clustering process assists in the identification of areas where there is incident point concentration.

It was considered as an alternative the fact that, from the existing data sample, an inference was made to prove the proposed IoT architecture intelligence layer from the service layer, as well as to provide practical and efficient results regarding solution benefits. In this way, an automatic inference was developed, based on data from the Android device sensors, which analyzes if the speed sent to the Smartdrive server (middleware) is greater than track speed by 10%, if so, using Firebase, the server sends an "Over Speed" alert to the application and to the Android device's messaging system by means of a standard message class that logs all sent alerts as shown in Figure 4a.

Speed alerts are generated by regulatory speed capturing of route on which user is traveling. This is done through a geographic consult to the Openstreetmap geographic database, which was imported into the inference layer local database, a postgreSQL DBMS with the postGIS extension.

User sends his geographical coordinate every 0.5 seconds; others sensor data are activated if the system identifies that the coordinate sent by user is within 50 meters of a hazardous area. Thus, a notification is sent to user informing that he is approaching a hazardous area as shown in Figure 4b.



(a) Speed Alert (b) Danger Zone Alert

Figure 4. Alert screens

B. Execution Layer Inference

Inferences executed only at service layer would not characterize an IoT solution. Given the application on smartphone could not be considered a smart object whether it did not have embedded intelligence, it was decided to make inferences about driver behavior directly in execution layer, so that its results can be sent to server in followed or simultaneously, depending on packet sending time configuration.

Again, to prove initial hypothesis in the work of the available data sample, we opted to identify two physical phenomena: abrupt acceleration and abrupt braking, from reading the three axes (x, y, and z) of the Android device's linear acceleration sensor.

Using simple logic without noise (Kalman), and as reference, the gravity acceleration (9.8 m/s) and threshold defined in [16] [17], the following equation has been set up to alert whether values exceed thresholds set for abrupt braking and acceleration (1): a is accelerometer X axis sensor measurement, b is Y axis measurement and c the measuring of Z axis.

$$0.4g < \sqrt{a^2 + b^2 + c^2} \tag{1}$$

Another inference implemented in execution layer is to use vehicular computer data through OBD-II protocol, in which, whenever vehicular sensor acceleration is greater than 1, both application and trip will start automatically. Besides that, the trip will be automatically interrupted when speed and engine rotation are both equal to ZERO.

VI. Conclusion

With goal of validating the system and scaling a cloud solution capable of meeting the demand of a large number of users, we invited 50 volunteers to use our software for a period of 30 days, with an average usage of three hours per day and we obtained the following results:

1) 24 users (50% of the sample) did not have EML327 interface in their car;
2) 5 users (10% of the sample) had communication problems with the OBD-II adapter;

3) 3 users (6% of the sample) have managed to install the OBD-II adapter but did not use the application at suggested frequency; and
4) 18 users (36% of the sample) used the application with suggested daily frequency.

Analyzing the last group of 18 users, we have the following statistics:

1) smartphone sensors collected a mean of 160 Bytes/s;
2) OBD-II interface captured a mean volume of 80 Bytes/s.

Therefore, the average data rate generated by the solution was 250 Bytes per second. With these values, we can conclude that in a journey of one hour, each mobile phone will need to transmit to the middleware 900 MB of data collected.

After the data collection sent by the group of volunteers, we arrived at the following conclusions:

1) Some manufacturers have not yet fully adhered to the OBD-II protocol, either for reasons of industrial secrecy or for adhering to underlying standards as proposed by the European Union and some Asian countries.
2) The generated data volume by each mobile phone is very high. This fact is leading us to research solutions where the mobile phone does not send all the data to central middleware. Taking advantage of today's phones large processing capacity, we state as future work a pre-processing at the edge, sending to the middleware only alert information and summary statistical data.
3) The client side processing and data analysis to identify individual events, such as sharp braking and presence of curves, seems to be a good alternative to reduce the need for processing capacity in central server.
4) The proposal heuristics involving collective knowledge creates a bidirectional channel of communication, allowing the collectively generated insights to arrive at each of the individual devices.
5) At this moment, the cloud-based communication strategy seems to be more adequate to provide communication among vehicles, mainly because V2V technologies are still in the early stages of deployment.

The security aspects or GDPR were not addressed in depth in this work since the goal was to evaluate the proposed platform operational capability. A deeper analysis of these security and privacy issues and the conduction of new tests with a higher number of users are considered for future work.

Acknowledgment

This research work is supported by the Brazilian research and innovation Agencies CAPES (Grants 23038.007604/2014-69 FORTE and 88887.115692/2016-00), CNPq (Grant 465741 /2014-2 INCT-CyberSecurity), and FAPDF (Grants 0193.001 366/2016 UIoT and 0193.001365/2016 SSDDC), as well as the LATITUDE/UnB Laboratory (Grant 23106.099441/2016-43 SDN), the Ministry of the Economy (Grants 005/2016 DIPLA, 011/2016 SEST and 083/2016 ENAP), the Institutional Security Office of the Presidency of the Republic of Brazil (Grant 002/2017), and the IEEE VTS Centro-Norte Brasil Chapter.

References

[1] Brasil. (2019) Portal oficial de notícias da Polícia Rodoviária Federal: Balanço PRF 2018. [Online]. Available: https://www.prf.gov.br/agencia/prf-registra-diminuicao-no-numero-de-acidentes-e-mortes-nas-rodovias-federais-em-2018

[2] J. Ferreira Júnior and G. Pessin, "Análise de perfil de motoristas: Detecção de eventos por meio de smartphones e aprendizado de máquina," in *Anais do WOCCES 2016 Workshop de Comunicação em Sistemas Embarcados Críticos*, 2016, pp. 76–85.

[3] FGV-SP. (2019) Pesquisa anual do uso de TI da Fundação Getúlio Vargas-SP. [Online]. Available: https://eaesp.fgv.br/ensinoeconhecimento/centros/cia/pesquisa

[4] S. R. Muramudalige and H. D. Bandara, "Demo: Cloud-based vehicular data analytics platform," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services Companion*, ser. MobiSys '16 Companion. New York, NY, USA: ACM, 2016. doi: 10.1145/2938559.2948849. ISBN 978-1-4503-4416-6 pp. 1–1. [Online]. Available: http://doi.acm.org/10.1145/2938559.2948849

[5] M. Amarasinghe, S. Kottegoda, A. L. Arachchi, S. Muramudalige, H. M. N. Dilum Bandara, and A. Azeez, "Cloud-based driver monitoring and vehicle diagnostic with obd2 telematics," in *2015 IEEE International Conference on Electro/Information Technology (EIT)*, May 2015. doi: 10.1109/EIT.2015.7293433. ISSN 2154-0373 pp. 505–510.

[6] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, Dec. 2014. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2014.09.008

[7] S. R. Department. (2016) Internet of things (iot) connected devices installed base worldwide from 2015 to 2025 (in billions). [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. . Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015. doi: 10.1109/COMST.2015.2444095

[9] B. Xiao, R. Rahmani, Yuhong Li, D. Gillblad, and T. Kanter, "Intelligent data-intensive iot: A survey," in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Oct 2016. doi: 10.1109/CompComm.2016.7925122 pp. 2362–2368.

[10] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of iot systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Nov 2014. doi: 10.1109/ICCAD.2014.7001385. ISSN 1092-3152 pp. 417–423.

[11] G. Castignani, T. Derrmann, R. Frank, and T. Engel, "Driver behavior profiling using smartphones: A low-cost platform for driver monitoring," *IEEE Intelligent Transportation Systems Magazine*, vol. 7, no. 1, pp. 91–102, Spring 2015.

[12] G. Castignani, T. Derrmann, R. Frank, and T. Engel, "Driver behavior profiling using smartphones: A low-cost platform for driver monitoring," *IEEE Intelligent Transportation Systems Magazine*, vol. 7, no. 1, pp. 91–102, 2015.

[13] V. Astarita, G. Guido, D. Mongelli, and V. P. Giofrè, "A co-operative methodology to estimate car fuel consumption by using smartphone sensors," *Transport*, vol. 30, no. 3, pp. 307–311, 2015.

[14] B. P. Puig, "Smartphones for smart driving: a proof of concept," *unpublished master's thesis for master's degree, Universitat Politecnica de Catalunya, Barcelona*, 2013.

[15] C. C. d. M. Silva, F. L. d. Caldas, F. D. Machado, F. L. Mendonça, and R. T. de Sousa Júnior, "Proposta de auto-registro de serviços pelos dispositivos em ambientes de iot," *34^o Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*, 2016.

[16] Hongyang Zhao, Huan Zhou, Canfeng Chen, and J. Chen, "Join driving: A smart phone-based driving behavior evaluation system," in *2013 IEEE Global Communications Conference (GLOBECOM)*, Dec 2013. doi: 10.1109/GLOCOM.2013.6831046. ISSN 1930-529X pp. 48–53.

[17] J. Paefgen, F. Kehr, Y. Zhai, and F. Michahelles, "Driving behavior analysis with smartphones: Insights from a controlled field study," in *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia*, ser. MUM '12. New York, NY, USA: ACM, 2012. doi: 10.1145/2406367.2406412. ISBN 978-1-4503-1815-0 pp. 36:1–36:8. [Online]. Available: http://doi.acm.org/10.1145/2406367.2406412