Improving Vehicle Safety through a Fog Collaborative Infrastructure

Gianpiero Costantino, Fabio Martinelli, Ilaria Matteucci, Francesco Mercaldo
IIT - CNR, Pisa,Italy
Email:firstname.lastname@iit.cnr.it

***Abstract*—The introduction of Information and Communication Technology in modern cities enhances quality, performance, and interactivity of urban services. The ultimate goal is twofold: the reduction of costs and of resource consumption and the increasing number of services offered to citizens. As drawback, smart cities become more vulnerable from the point of view of safety, security, and preservation of citizen privacy. In this paper, we propose a fog-computing based infrastructure to manage the sharing of information among vehicles and smart traffic lights in a urban network, with the aim of improving the safety of end-users of the network. For this purpose, our infrastructure provides to drivers several services to retrieve information in a private and secure way. The services we consider, are mainly four and are oriented to the traffic prediction, incident prevention, managing of emergency, and driver recognition.**

Keyword: smart city, automotive domain, fog computing, collaborative infrastructure, service analytics.

I. Introduction

The smart city integrates Information and Communication Technology (ICT), and various physical devices connected to the network to optimize the efficiency of city operations and services. Several issues related to security and privacy of data circulating among different end-users (drivers, citizens, pedestrians) of the environment may arise, due to the high connectivity of heterogeneous devices in a smart city and the distributive nature of the scenario we consider. Indeed, let us focus on the urban network as part of a smart city. It is made of, for instance, the roadside infrastructure, vehicles circulating on urban and extra-urban area, pedestrians, and so on. All these actors are able to generate information about, e.g., traffic, weather, occurrence of emergency situations, and share them with other actors in the network. The main communication technologies we consider are Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2X) relying on WiFi connections, so subject to issues related to security and privacy of possible shared information.

To manage the secure and private data sharing among both different vehicles and between vehicles and the roadside infrastructure, we describe an infrastructure based on smart systems able collect, manage, exchange, and analyse data. Considering the distributive nature of a smart city, we base our infrastructure on *Fog computing* [1], [2], [3] and we consider as main end-users of the proposed infrastructure smart traffic lights belonging to the roadside network that collaborate one another to carry out a substantial amount of storage of information coming from sensors, analyse such data and manage the sharing of useful information to vehicles circulating on the considered urban or extra-urban area. We enhance the smart traffic lights with two components able both to manage the sharing of data in a secure way, i.e., according to some pre established security policies, and to analyse and process collected information to derived useful information that may again be shared to guarantee the safety of urban network end-users. This analysis are provided to the end-users as a set of *service analytics* that improve the driver experience. Examples of such services are the possibility of predicting traffic congestion on the basis of information related to the number of vehicles travelling across a traffic light met (*Traffic prediction*); managing the *occurrence of an emergency situation* by exploiting the distributive nature of the fog infrastructure, for instance, in order to spread the information about ambulance approaching; recognizing a driver by using in-vehicle sensors that share with the fog collaborative infrastructure the travel information on the actual trip (*Driver recognition*). This service can be useful also from an insurance prospective to establish the actual evolution of an occurred incident; finally, by using again the in-vehicle sensors to collect vehicles information, it is possible to use an analytic service able to understand the meaningful behaviour of driver in a segment of road. The aim of this analytic is to provide other vehicles circulating in that segment information about the most appropriate drive behaviour to, for instance, avoid incidents (*Traffic Incident Prevention*). Note that, the services we describe in this paper are only examples of possible services that can be exposed by our infrastructure.

The paper is structured as follows: next section introduces our reference smart environment scenario in which we pinpoint and discuss safety, security, and privacy issues. In §III we propose a fog collaborative infrastructure aiming at overcoming those issues. §IV describes four possible analytic services belonging to the fog collaborative infrastructure we propose. All these services aim at improving the safety, security, and privacy of end-users of the urban network. §V discusses and compares our work with results already existing in literature. Finally, §VI draws the conclusion of the paper and introduces hints for future work along this line of research.

II. The Reference Smart Environment Scenario

Let us consider a smart city in which there are several sensors to collect data to supply information used to manage assets and resources efficiently. Data we are going to include in

978-1-5386-4705-9/18/$31.00 ©2018 IEEE
DOI 10.1109/SMARTCOMP.2018.00044

our reference scenario are collected from citizens, devices, and assets. In particular, we suppose that data related to vehicles circulating on the roadside as well as context attributes are collected by exploiting in-vehicle and environmental sensors, respectively.

The scenario we are going to consider is made of several smart systems, such as, sensors, smart traffic lights, smart vehicles circulating of the road (Fig. 1). These smart systems communicate one another by mean of three infrastructures: the roadside infrastructure that communicate with vehicles through *Vehicle to Infrastructure* communication (V2X), the *Vehicle to Vehicle* communications (V2V) infrastructure, and the *Urban Network*, a typical WSN-based Urban Traffic Management System (W-UTMS) [4].

A. Security and Privacy Aspects

Since cyber and physical worlds are increasingly linked, cyber-security attacks become a critical issues and have serious consequences for both security and safety. Indeed, ICT services generate a huge number of information regarding several events, such as weather conditions, exceptional events on a roadside network, such as, work area, strikes, footraces or cycling races, traffic conditions, and incidents. The sharing of such information among different systems in a infrastructure may lead to several benefits in terms of, for instance, incident prevention, traffic prediction, emergency management, and so on. However, the collection of information about environment as well as about vehicles and drivers circulating on a roadside network, arises several issues concerning security and privacy due to sensitive nature of the collected information. Thus, it must be treated appropriately in terms of storage, sharing, and manipulation. Indeed, the ultimate goal of the collection of these data is to aggregate them to recognize, prevent, and eventually overcome cyber-attacks.

B. Safety Aspects

Security and privacy aspects can impact also on the safety of drivers and pedestrians. Indeed, recent studies [5] proves that in real world, cyber-security attacks have been perpetrated to vehicles as a demonstration of the vulnerabilities of connected vehicles (vehicles connected with other vehicles or with the roadside infrastructure) may impact on the core functionalities of the vehicle itself. A typical attack to this kind of system is the Denial of Service attack (DoS) that would not allow the car to be remotely locked/unlocked/started and in some cases it may be possible to unlock/start the car without the proper key fob [5]. In 2010, some security researchers showed how to "kill"a car engine remotely, i.e., make the car engine exploitable, by turning off the brakes so that the vehicle would not stop, and making instruments give false readings[1]. In July 2015 an hijacking has been perpetrated to a Jeep Cherokee[2] and also to General Motors (GM)[3]. Hackers remotely took the control of the engine or stole the data from the infotainment system, respectively, by exploiting the internet connection of the infotainment system and a malicious version of the infotainment software installed on the car. In September 2016, researchers have hacked a TESLA Model S[4] by using bugs on the TESLA's bounty program through which vehicles received firmware update. In [6], Koscher et al. experimentally evaluate the security features of a modern vehicles and prove that, at a certain point in time, an attacker able to infiltrate virtually any ECU can leverage this ability to completely circumvent a broad array of safety-critical systems, and to control a wide range of automotive functions, including disabling the brakes, stopping the engine, and so on.

III. The Proposed Infrastructure

To overcome the issues presented in §II, hereafter, we propose an infrastructure based on *Fog computing* [1], [2], [3] and smart systems able to collect, manage, exchange, and analyse data in a safe, secure, and privacy preserving way. Within our proposed infrastructure, the end-users are smart traffic lights belonging to the roadside network that collaborate one another to carry out a substantial amount of storage of information coming from sensors, analyse such data and manage the sharing of useful information to vehicles circulating on the considered urban or extra-urban area.

Hence, the proposed infrastructure is based on two components: one able to manage and share collected information, named *Information Sharing Infrastructure* (ISI), and one to analyse and process the such information, named *Information Analytic Infrastructure* (IAI)[5]. We assume that, each vehicle has a embedded *Local ISI* (§III-A) and each traffic light is enhanced by both components, ISI and IAI (§III-B).

A. The Local-ISI

A ISI module is embedded in each vehicle travelling on the road and it is referred as *Local-ISI*. It aims at preparing the data shared with the Fog infrastructure and, in particular by setting up policies on how to manage and share collected information and their *derived data*, i.e., the data derived from initial information through some data manipulation, such as, by performing *service analytics* (some examples of such services are described in §IV). In addition, the Local ISI is in charge of performing the Data Manipulation Operations (DMO) that allows a vehicle to protect sensitive data before the sharing. To this aspect, we foresee two levels of DMO operations; the first level is composed by the data-anonymisation, which anonymises the data, and the data-filtering, which is obtained by removing sensitive fields from the data. The second level of DMO is composed by a more challenging set of encrypted-operations that are performed using the homomorphic encryption [7]. In this case, the data are encrypted and the operations made on the data do not reveal any sensitive information to the third-party infrastructure that will make the computation.

[1] http://goo.gl/46ojKC
[2] http://goo.gl/fAUfBv
[3] http://goo.gl/aXaWzl
[4] http://goo.gl/RrgBR2
[5] This nomenclature is inherited form the European H2020 Project on Collaborative and Confidential Information Sharing and Analysis for Cyber Protection - C3ISP (http://c3isp.eu).

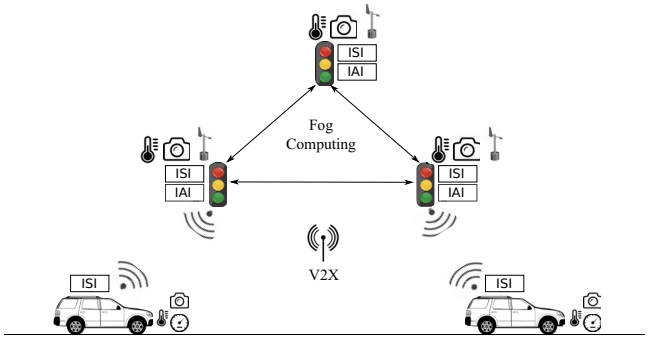

Fig. 1: The Smart Environment Scenario for Automotive.

The DMO operations are thought to adapt their performance and their confidentiality metric depending on the kind operation used. In fact, if the first level of DMO operations is selected, they allow the vehicle to achieve a good level of data-confidentiality maintaining, however, a very good level of performance when the data are processed by the analytics. Instead, the second level of DMO, i.e., homomorphic encryption, provides a strong solution to protect the data-confidentiality, but the analytics executed in the data provide lower performances.

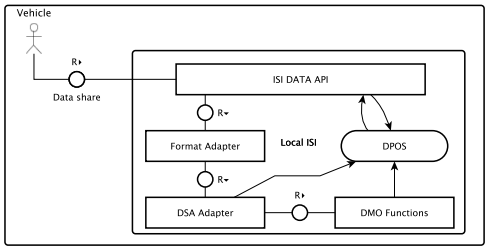

Fig. 2: The local-ISI module.

Figure 2 illustrates the Local-ISI in detail. When a vehicle wants to share data with the Fog infrastructure, it selects the data to share and calls the proper interface, which is provided by the *ISI Data Api*, to prepare the data before offloading them into the Fog infrastructure. In particular, the phase may require that the data need to be adapted in a format that the remote ISI and IAI are able to process. So, the *Format Adapter* is the component in charge of this formatting (if needed). As subsequent step, the *DSA Adapter* component will analyse the policies, which have been previously established, to verify whether specific DMO operations must be applied in the data. In case of positive outcome, the data pass through the *DMO functions* component that will apply the DMO operations as specified in the policies. As final step, the data formatted and sanitised, which means that a DMO operation was applied, are stored into a local file system, which is represented by the *Data Manipulation Object Storage* (DPOS) component. At this stage, the data are ready to be offload into the Fog infrastructure and this operation is in charge of the ISI Data Api that through a specific interface, for instance *upload*, will share the data.

B. The Fog Collaborative Infrastructure: ISI and IAI modules

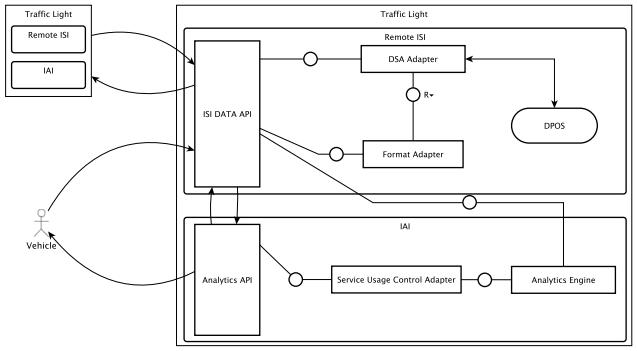

Fig. 3: The Fog layer.

In Figure 3 we show how a traffic light, which belongs to the Fog infrastructure, is composed with the inclusion of the ISI and IAI modules and, their interactions with the vehicles and other traffic lights. We expect that every time that a vehicle has data to be shared, it contacts the ISI Data API component, in the remote ISI module. This allows a vehicle to store its data remotely into the remote DPOS. Then, when a traffic light needs to process the data of vehicles, the Analytics API module retrieve the data from the DPOS, contained in the ISI module. However, before this action is completed, there are two intermediate steps: the first one is the *DSA Adapter* that checks if the analytic can access the data that it needs for the elaboration and this depends on the policies written before the submission. The additional step is given by the *Format Adapter* that will convert, the format of data stored in the DPOS, in such a format that analytics is able to process. In particular, with *service analytic* we intend those techniques and algorithms that will make use of the vehicles shared data to infer knowledge useful to, for instance, identify a possible and possibly mitigate cyber-attacks, as well as, to implement a traffic prediction algorithm or to help car insurance in case of incident. Analytic functions are performed and managed by

the IAI. In fact, once data are collected by several sources, it is possible to combine and analyse them in such a way to derive some further information coming from the aggregation of such heterogeneous data. So, once the data are grabbed by the analytics module, the *Analytics Engine* is invoked since it represents the core of data elaboration. In fact, it contains the algorithms that are executed when an analytic is required. In addition, during the data elaboration phase, the *Service Usage Control Adapter* will verify that the data processed by the analytics engine do not violate what is written in the policies. In case of violation found, the service usage control adapter will block the execution of the analytics.

Data processed by the analytics engine will produce pieces of information that can be shared also with other traffic lights that belong to the same Fog distributed infrastructure. This operation allows other traffic lights, and as consequence other vehicles, to retrieve data already processed. However, the data distribution among other traffic lights and other vehicles is enforced as well by the DSA adapter of the other ISI modules.

C. Data Acquisition

The first step of the proposed approach consists of *Data Acquisition* to have as much information as possible coming from both environmental and in-vehicle sensors. In particular, a typical W-UTMS involves four different activities: (i) information collection; (ii) data diffusion; (iii) processing of data to plan the required activities; and (iv) implementation of the suitable actions [4]. At different degree of implementation, the UTMS involved different physical devices, such as, wireless sensors, Traffic Management Centres (TMC), a Road Side Units (RSU), and On-Board Units (OBU). Information about a vehicle, such as, parking sensors, car doors opened, engine information and so on, circulate into the vehicles itself on the Controller Area Network (CAN) bus. The CAN bus is a standard used by Electronic Control Units (ECUs) into vehicles to exchange messages containing such information. There are several ways to acquire vehicle information: i) by physically accessing to the On Board Diagnostics Interface (OBDII) or ii) by remotely downloading data circulating on the CAN bus through the infotainment system. Originally, ECUs work in isolation, now, instead, in order to provide information to the driver, in the new generation of car the CAN bus network is attached to the infotainment system, that represents an external access to the internal network.

Even though the physical access through the OBDII provides more information about the car, it is not always feasible. For this reason and according to [8], by using vehicle's information circulating on the CAN Bus it is possible to characterize the behaviour of the driver, the *Driver DNA*. Hence, we consider to exploit infotainment system and its Wi-Fi connection to remotely access and acquire vehicle information. For instance, Android In-Vehicle infotainment systems, named *Android Automotive* systems, have a built-in APP that shows CAN bus information that are collected by a hardware, called CAN bus decoder. Some data that can be obtained from the built-in APP are: water temperature; seat belt attached or not; handbrake pulled or not; car doors status; remaining fuel; voltage of the battery; engine rpm; Speed of the car; air conditioning system status; distance from an obstacle if the rear gear was selected.

IV. Service Analytics

Once the proposed architecture is put in place, it is able to provide several services analytic to improve the safety, the quality of life, and the drive experience of drivers as well as pedestrians. Four possible services are i) Traffic prediction, ii) Occurrence of an Emergency Situation, iii) the Driver recognition and iv) the Traffic Incident Prevention.

It is worth noting that other services can be designed and implemented by using the same architecture. Furthermore, the same services can be refined with additional data in such a way that the derived information are more accurate.

A. Traffic prediction

One service analytic that we discuss is called *Traffic Prediction*. The goal of this service is to collect information from each vehicles about their frequency of travelling across the traffic light met. In this way, a traffic light of a specific place, for instance of a road intersection, is able to learn the amount of traffic depending on the hour and on the day. The vehicle information is received every time that the vehicle is in proximity of the traffic light, and this is able to store the data the will be processed then by the corresponding analytic. An important aspect of the data sharing is the possibility of the vehicle to establish, a priori, how the data must be processed by the traffic lights and, in particular, by the service analytic. In addition, the vehicle can also decide to sanitise the data filtering out some pieces of information that it does not want to disclose out with third-parties.

When several vehicles have shared their data with the traffic light, it can decide to process the data using the analytic as expressed in §III. The outcome of the services analytics will give a traffic prediction for each hour of the days of a week. The traffic prediction will be shared with the vehicles that pass in proximity of the traffic light. In this way, when a vehicle needs to establish the more convenient path, it will use the information got from the traffic light. In addition, with our Fog infrastructure the result of analytics can be shared of other traffic lights of the same infrastructure allowing all the end-users to have an indirect and complete knowledge of the traffic in different points, for instance, of a city.

B. Occurrence of an Emergency Situation

Similar to the previous service analytic, the *Emergency Situation* aims at collecting information from vehicles, processed by the traffic light and shared with the Fog infrastructure. Basically, here we suppose that an ambulance that is approaching the traffic light is able to share its position and the path that it will do to reach the destination places, e.g., the hospital. We suppose that these pieces of information once retrieved by the traffic light, they will be processed and the information obtained will be also shared with other traffic lights, which

belong to the same Fog infrastructure. So, we expect that the sharing of the elaborated information can be used to facilitate the way taken by the emergency vehicle to reach in a faster manner the destination place. In fact, if a traffic light knows in advance that an ambulance is approaching it, then the traffic light can turn the light to green and as consequence adapt the traffic to allow the stream of vehicles and the ambulance to pass without wasting additional time.

C. Driver Identification

The proposed architecture permits to silently and continuously verify the identity of the car owner by discriminating different driving styles on the bases of a set of features related to the vehicle. Using a machine learning service analytic on all data acquired from a vehicle it is possible to infer behavioural characteristics that identify the driver. This may solve authentication issues, for instance, by authenticating the owner of the vehicle as the current driver, (*anti-theft*). Indeed, once a possible theft is able to unlock the door and to start the engine, the attacker has full access to the vehicle.

Other actors that can benefits from the continuous and silent driver identification are the insurance companies: new insurance paradigms, as the "Usage-based insurance", are emerging. Basically, the Usage-based insurance, also known as *pay as you drive* and *pay how you drive* and *mile-based auto* insurance, is a type of vehicle insurance whereby the costs are dependent upon type of vehicle used, measured against time, distance, behaviour and place [9].

D. Traffic Incident Prevention

Another service analytic that exploits the infrastructure we propose is the traffic incident prevention based on real-time driving style identification. We assume that several cars are running on the same road, we expect that drivers have a similar driving style. When a driver assumes a driving style different from the other drivers, the FOG infrastructure communicates with the driver to invite it to change its own driving style following the most of the drivers. This is the reason why we consider the proposed approach as context-awareness: depending on the type of road, the proposed infrastructure can be exploited to avoid traffic incidents.

V. Related Work

In literature there are several works about the four services discussed in §IV. In this section, we recall some of them without aiming at being exhaustive.

A. Traffic Prediction

De Fabritiis *et al.* [10] consider real-time Floating-Car Data, based on traces of GPS positions to gather travel times and speeds in a road network. They improve short-term predictions of travel conditions. The designed system updates every three minutes link travel speeds along the Italian motorway network.

A traffic prediction system is proposed in [11]. Basically this approach considers the floating car data in urban networks and the average density, flow, and speed at every interval for different demand levels to predict traffic congestion.

Gora [12] proposes a simulation-based traffic management system with the ability to evaluate traffic conditions for different traffic control strategies (e.g., different traffic signal settings, route assignments) using fast traffic simulations and neural networks. It also employs meta-heuristics (for instance, genetic algorithms) to find optimal traffic control strategies.

The model proposed in [13] examines traffic flow, average speed, and average detector occupancy in real-time. Authors consider a statistical model to filter noisy traffic data for traffic short time prediction and a real-time prediction model to provide the input flows.

B. Occurrence of an Emergency Situation

Zhao *et al.* [14] propose an user-friendly decision support tool aiming at facilitating the process of optimizing urban emergency rescue facility locations in urban areas. Their results provide evidences that the designed method is able to generate Pareto-optimal frontier and capture a pool of alternative solutions to the decision maker for trade-off in urban emergency situations.

Researchers in [15] focus on specific problem of traffic management for emergency services, for which a delay of few minutes may cause human lives risks as well as financial losses. In detail, the aim is to reduce the latency of emergency services for vehicles such as ambulances and police cars, with minimum unnecessary disruption to the regular traffic, and preventing potential misuses. This is the reason why they propose a framework in which the Traffic Management System may adapt by dynamically adjusting traffic lights, changing related driving policies, recommending behaviour change to drivers, and applying essential security controls.

Chai *et al.* [16] discuss a framework for smart travel planning project from a space-time behaviour approach. They exploit individual activity-travel data collection. GPS tracking technology had been integrated into a web-based activity-travel diary survey to collect data with high spatial and temporal resolution and with detailed activity-travel information.

C. Driver Identification

Researchers in [17] classify a set of features gathered from the power-train signals of the vehicle, showing that the considered features are able to classify the human driving style based on the power demands placed on the vehicle power-train.

Van Ly *et al.* [18] investigate the possibility of using the inertial sensors of the vehicle gathered from the CAN bus in order to build a profile of the driver observing braking and turning events to characterize a single driver compared to acceleration events.

The driver behaviour is also modelled in [19] using data from steering wheel angle, brake status, acceleration status, and vehicle speed through Hidden Markov Models (HMMs) and GMMs employed in order to capture the sequence of driving characteristics gathered from the CAN bus.

Authors in [20] propose a method based on driving pattern of the car. They analyse features gathered from the CAN bus evaluating them with different supervised classification

algorithms. They evaluate the proposed solution on the same car with 10 different drivers on the same track.

D. Traffic Incident Prevention

Several methods have been deployed in the automotive context to prevent and detect traffic incidents. As a matter of fact, researchers in [21] developed a mobile application with the aim to monitor the vehicle using the OBD interface in order to detect accidents. This application exploits the G force experienced by the passengers in case of a frontal collision.

Another approach considering the adoption of the mobile technologies is the one proposed in [22]: authors describe how mobile devices can automatically detect traffic accidents through accelerometers and acoustic features. They design a central emergency dispatch server able to receive notification from mobile devices after an accident in order to provide situational awareness through photographs, GPS coordinates, and VOIP communication channels.

Li *et al.* [23] examine the significant factors for a better Fatal-injury crash identification: Driver Conduct, Vehicle Action, Roadway Surface Condition, Driver Restraint, and Driver Age. They propose a data-driven model with the aim to combines the Non-dominated Sorting Genetic Algorithm with the Neural Network architecture to predict traffic incidents.

VI. Conclusions and Future Work

In this paper, we proposed a Fog Collaborative Infrastructure in a Smart City with the aim of sharing information among end-users of urban and extra-urban network in such a way that security, as privacy aspects are preserved and guaranteed. In addition to the collection and management of the obtained information, the infrastructure is also able to process such data to produce derived ones useful to enhance the safety of drivers, pedestrians, and so on. To illustrate potential services of the proposed infrastructure, we have designed four analytics related to traffic prediction, emergency, driver identification and incident prevention.

As future work, we will implement service analytics to show their effectiveness in real test cases, and we will work to extend the set of analytic services managed by our infrastructure.

Acknowledgment

This work has been partially supported by H2020 EU-funded projects NeCS, C3ISP, "CyberSure", EIT-Digital Project HII, and PRIN "GAUSS-Governing Adaptive and Unplanned Systems of Systems".

References

[1] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for vm-based cloudlets in mobile computing," *IEEE Pervasive Computing*, vol. 8, no. 4, pp. 14–23, Oct. 2009. [Online]. Available: http://dx.doi.org/10.1109/MPRV.2009.82

[2] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, Oct. 2014. [Online]. Available: http://doi.acm.org/10.1145/2677046.2677052

[3] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, Warsaw, Poland, September 7-10, 2014.*, 2014, pp. 1–8.

[4] K. Nellore and G. P. Hancke, "A survey on urban traffic management system using wireless sensor networks," *Sensors*, vol. 16, no. 2, p. 157, 2016. [Online]. Available: https://doi.org/10.3390/s16020157

[5] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *Black Hat USA*, 2014.

[6] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *Proceedings of IEEE Symposium on Security and Privacy*, 2010, pp. 447–462.

[7] S. Carpov, T. H. Nguyen, R. Sirdey, G. Costantino, and F. Martinelli, "Practical privacy-preserving medical diagnosis using homomorphic encryption," in *9th IEEE International Conference on Cloud Computing, CLOUD 2016, San Francisco, CA, USA, June 27 - July 2, 2016*, 2016, pp. 593–599.

[8] U. Fugiglando, P. Santi, S. Milardo, K. Abida, and C. Ratti, "Characterizing the "driver dna" through can bus data analysis," in *Proceedings of the 2Nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services*, ser. CarSys '17. New York, NY, USA: ACM, 2017, pp. 37–41. [Online]. Available: http://doi.acm.org/10.1145/3131944.3133939

[9] A. Marotta, F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin, "Cyber-insurance survey," *Computer Science Review*, 2017.

[10] C. De Fabritiis, R. Ragona, and G. Valenti, "Traffic estimation and prediction based on real time floating car data," in *Intelligent Transportation Systems, 2008. ITSC 2008. 11th International IEEE Conference on*. IEEE, 2008, pp. 197–203.

[11] Y. Lin and H. Song, "Dynachina: Specially-built real-time traffic prediction system for china," Tech. Rep., 2007.

[12] P. Gora, "Simulation-based traffic management system for connected and autonomous vehicles," in *Road Vehicle Automation 4*. Springer, 2018, pp. 257–266.

[13] M. Ben-Akiva, E. Cascetta, and H. Gunn, "An on-line dynamic traffic prediction model for an inter-urban motorway network," in *Urban Traffic Networks*. Springer, 1995, pp. 83–122.

[14] M. Zhao and X. Liu, "Development of decision support tool for optimizing urban emergency rescue facility locations to improve humanitarian logistics management," *Safety science*, vol. 102, pp. 110–117, 2018.

[15] S. Djahel, M. Salehie, I. Tal, and P. Jamshidi, "Adaptive traffic management for secure and efficient emergency services in smart cities," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference on*. IEEE, 2013, pp. 340–343.

[16] Y. Chai and Z. Chen, "Towards mobility turn in urban planning: Smart travel planning based on space-time behavior in beijing, china," in *Big Data Support of Urban Planning and Management*. Springer, 2018, pp. 319–337.

[17] G. Kedar-Dongarkar and M. Das, "Driver classification for optimization of energy usage in a vehicle," *Procedia Computer Science*, vol. 8, pp. 388–393, 2012.

[18] M. Van Ly, S. Martin, and M. M. Trivedi, "Driver classification and driving style recognition using inertial sensors," in *Intelligent Vehicles Symposium (IV), 2013 IEEE*. IEEE, 2013, pp. 1040–1045.

[19] S. Choi, J. Kim, D. Kwak, P. Angkititrakul, and J. H. Hansen, "Analysis and classification of driver behavior using in-vehicle can-bus information," in *Biennial Workshop on DSP for In-Vehicle and Mobile Systems*, 2007, pp. 17–19.

[20] F. Martinelli, F. Mercaldo, A. Orlando, V. Nardone, A. Santone, and A. K. Sangaiah, "Human behavior characterization for driving style recognition in vehicle system," *Computers & Electrical Engineering*, 2018.

[21] J. Zaldivar, C. T. Calafate, J. C. Cano, and P. Manzoni, "Providing accident detection in vehicular networks through obd-ii devices and android-based smartphones," in *Local Computer Networks (LCN), 2011 IEEE 36th Conference on*. IEEE, 2011, pp. 813–819.

[22] J. White, C. Thompson, H. Turner, B. Dougherty, and D. C. Schmidt, "Wreckwatch: Automatic traffic accident detection and notification with smartphones," *Mobile Networks and Applications*, vol. 16, no. 3, p. 285, 2011.

[23] Y. Li, D. Ma, M. Zhu, Z. Zeng, and Y. Wang, "Identification of significant factors in fatal-injury highway crashes using genetic algorithm and neural network," *Accident Analysis & Prevention*, vol. 111, pp. 354–363, 2018.