Vehicular Networks to Intelligent Transportation Systems

Felipe Cunha, Guilherme Maia, Heitor S. Ramos, Bruno Perreira, Clayson Celes, André Campolina, Paulo Rettore, Daniel Guidoni, Fernanda Sumika, Leandro Villas, Raquel Mini and Antonio Loureiro

Abstract Urban mobility is a current problem of modern society and large cities, which leads to economic and time losses, high fuel consumption, and high CO_2 emission. Some studies point out Intelligent Transportation Systems (ITS) as a solution to this problem. Hence, Vehicular Ad hoc Networks (VANETs) emerge as a component of ITS that provides cooperative communication among vehicles and the necessary infrastructure to improve the flow of vehicles in large cities. The primary goal of this chapter is to discuss ITS, present an overview of the area, its challenges, and opportunities. This chapter will introduce the main concepts involved in the ITS architecture, the role of vehicular networks to promote communication, and its integration with other computer networks. We will also show applications that leverage the existence of ITS, as well as challenges and opportunities related to VANETs such as data collection and fusion, characterization, prediction, security, and privacy.

1 Introduction

The disorderly growth of large urban centers has caused severe socioeconomic and structural problems for the population, which contributes to the increase of social inequalities and a significant stress on the structure of cities. In this way, services

F. Cunha (✉) · R. Mini
Department of Computer Science, Pontifical Catholic University of Minas Gerais,
Belo Horizonte, Brazil
e-mail: felipe@pucminas.br

G. Maia · B. Perreira · C. Celes · A. Campolina · P. Rettore · A. Loureiro
Federal University of Minas Gerais, Belo Horizonte, Brazil

H. S. Ramos
Federal University of Alagoas, Maceio, Brazil

D. Guidoni · F. Sumika
Federal University of São João del-Rei, São João del-Rei, Brazil

L. Villas
University of Campinas, Campinas, Brazil

K. V. Arya et al. (eds.), *Emerging Wireless Communication and Network Technologies*,
https://doi.org/10.1007/978-981-13-0396-8_15

and resources must be provided in a way that tackles and minimizes these problems. Among them, it can be mentioned the incorrect occupation of the urban space that collaborates to generate diverse problems of mobility in big cities. In this context, public transport systems are an essential part of improving urban mobility. For example, in São Paulo—Brazil, 23% of the residents spend at least 2 hours commuting to their destination every day [1, 2].

Over the years, traffic-related problems have been increasing due to the number of vehicles in circulation and the vast concentration of people in the same region. According to studies conducted by IBM, the current quantity of automotive vehicles in the world currently exceeds 1 billion, and this number can double in the year 2020. With this, big cities are the most affected by this increase of vehicles, with the constant presence of traffic jams. For example, recent surveys show that São Paulo has an annulling loss of 20 billion, and this loss is related to 85% lost time in traffic; 13% increase in fuel consumption; And only 2% of the growth in the emission of polluting gases. Which also contributes to the increase in warming in these urban centers.

Aiming to solve the problem of mobility, some solutions are proposed, for e.g., the plate casters and incentives for the use of public transport. However, these solutions have not been very successful. In many scenarios, they affect the routine of the population and do not achieve engagement. On the other hand, intelligent solutions that make use of communication can contribute to greater success, improving traffic in these scenarios. These solutions can provide applications that enable the control and management of traffic, with services ranging from a more assertive control of the schedules and routes of public transport to the intelligent synchronization of traffic lights. These services make up the Intelligent Transportation Systems (ITS) [3].

ITS use data, communication, and processing to provide services and applications to solve various transportation problems. These systems, in addition to providing services to manage and improve security for people in transit, also can enable comfort services for drivers and passengers, such as access to social networks and video stream services while traveling. These applications rely on collaboration between the elements that integrate the system such as vehicles, sensors and other mobile devices. Each of these elements plays an important role, collaborating and sensing data that will be evaluated by the system. All this collaboration of elements is made possible by the communication between them. For this, elements such as antennas and control stations can intermediate this communication. In the context of the direct communication between the vehicles, vehicular networks arise, a type of network that has been exerting a significant influence on the scene of the ITS [4].

The services and applications provided by ITS have their characteristics and peculiarities, which differs to other traditional applications. They are services that generate and consume a varied amount of data, use different communication technologies with different bandwidths, reach, and latency. Besides, vehicles have high mobility, moreover, speed limits and directions determined by public roads become communication a challenging task in this scenario. For this reason, designing a service part of these systems becomes a major challenge. In this chapter, we discuss ITS and present an overview of the area, defining its central concepts, integration, the role of VANETS to provide communication, and the cooperation with other networks. Also, we describe challenges of the infrastructure to promote the services and the open issues about data and security.

The remainder of this chapter is organized as follows. Section 2 discusses the concept of ITS presenting all definitions, architecture, and integration with other networks. Section 3 presents features and challenges related to infrastructure and services in ITS. Section 4 discusses opportunities for the current research topics related to data and security in ITS. Finally, Sect. 5 presents the conclusion.

2 Intelligent Transportation Systems

Intelligent Transportation Systems (ITS) aims to improve transport safety and mobility, as well as to increase people's productivity and reducing the harmful effects of traffic. This improvement is achieved through the integration of communication technologies in vehicles and infrastructure.

ITS is not only proposed to improve vehicle traffic conditions but also intends to make the transportation safer, more sustainable, and efficient, avoiding the inconvenience caused by traffic congestion and the effects of climate problems on traffic. To this end, the focus is on improving the management of cities' resources and increasing the convenience of people using information and alert services. This improvement, therefore, helps to ease the flow in the city, reducing the time spent on congestion and consequently reducing fuel consumption, CO_2 emissions and monetary losses. In the following sections, the central concepts related to ITS will be presented.

2.1 Architecture

Considering the evolution of computing and communication technologies and the increasing demand for ITS services with different requirements, the necessity for standardization to define how devices and components can interact with each other arises. Among the proposed architectures, it is worth to mention the North American, the European, and the Japanese.

The National ITS Architecture, defined by the US Department of Transportation, describes how communication between its elements and subsystems occurs, with a precise definition of the role of each one of them. This architecture is divided into four classes: *Center*, *Fields*, *Vehicles*, and *Travelers*. *Center* defines the center of control and management of the whole system, in which the services are executed. *Field* encompasses all the infrastructure of the environment (RSU, monitoring sensors, cameras). *Vehicles*, which are vehicles and embedded sensors, and *Travelers* that are defined by the devices people use during the trip.

The Japanese architecture proposed by the *SmartWay* defines the communication among vehicles and among vehicles and all the intelligent infrastructure of the roads (sensors, RSU, traffic lights) and uses as the standard of the DSRC [2], along with the proposed ARIB standard (similar to the WAVE protocol). The European architecture (ITS ISO CALM) has very similar characteristics to other architectures such as the adoption of RSUs and the DSRC [2] for communication. However, this architecture has the greatest difference in the utilization of the CALM communication protocol, which provides a communication interface between the transmission technologies such as 3G/4G, Wi-Fi, infra-red, and others.

Both Japanese and European architectures have disadvantages compared to North American architecture because they lack the flexibility to use new communication technologies and new paradigms of computing such as cloud and fog computing. Hence, one can observe a requirement to design architectures that allow the easy integration of new technologies, since they can cooperate for the development and improvement of services offered by ITS.

2.2 Vehicular Ad Hoc Networks

Vehicular networks are a type of emerging network that has attracted the interest of many research groups. These networks are made up of vehicles with processing capacity and wireless communication, traveling on streets and highways, sending and receiving information from other vehicles. They differ from traditional networks in many ways. The first of these is the nature of the nodes that form them, such as automobiles, trucks, buses, etc., which have wireless communication interfaces, and equipment attached to the roads. Also, these nodes have high mobility, and their trajectory follows the limits and direction defined by public roads [5–7].

Vehicles participating in the network are equipped with an onboard system with computing capability, communication interfaces, sensors, and user interfaces. The system supports a range of applications to improve transport security and also provide services to users. A network infrastructure along roadsides and streets called the Roadside Unit (RSU) is also part of VANETs and facilitates the communication of network nodes to the Internet. Also, passenger handhelds and the vehicle system can connect to the Internet through the RSU infrastructure. A management system can be adapted to control and authenticate the entrance of vehicles in the network, mainly in the aspect of computer security, such as the distribution of cryptographic keys, authentication servers, etc. The system can also provide services and manage node mobility during network exchanges.

Due to high node mobility, vehicular networks allow nodes to exchange information along with their trajectory without the need of any infrastructure, in an ad hoc fashion. Hence, vehicular networks can be considered as a type of Mobile Ad hoc Network (MANETs). However, there is a possibility of nodes communicating with the infrastructure of the highways, allowing an infrastructural communication [8–10]. In this way, considering these peculiar characteristics, the communication between the vehicles can be classified in three ways (as illustrated in Fig. 1).

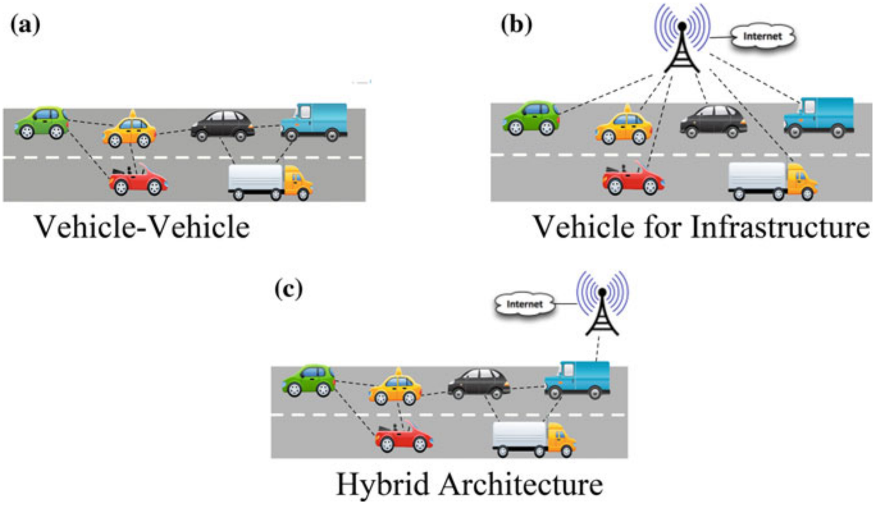

Fig. 1 Types of communication in vehicular networks

- Vehicle-to-Vehicle (V2V): It allows a direct communication of vehicles without relying on fixed infrastructure support. In this type of communication, vehicles can exchange data of the conditions of the highway, detect the presence of other vehicles, and even information about vehicles in unsafe movement.
- Infrastructure-to-Vehicle (V2I): It allows a vehicle to communicate with the road infrastructure. In this way, the vehicle can receive from the road infrastructure information about obstacles and the presence of pedestrians, road conditions data, advertisements, and safety information.
- Hybrid Architecture: It combines V2V and V2I solutions. In this case, a vehicle can communicate with the road infrastructure in a single or multiple hops according to its location about the point of connection with the infrastructure for different purposes.

Currently, car manufacturers already put into circulation cars with onboard computers, wireless communication devices, sensors, and navigation systems. These resources enable the establishment of the vehicular networks. An example of the application of these features is vehicles that have sensors to collect weather conditions, vehicle status, road conditions, and even road speed limit. In this scenario, vehicles can interact with the infrastructure of the highways, obtaining information of traffic which generates improvements in the conditions for the driver to make decisions about the traffic.

An interaction between vehicles can prevent the occurrence of collisions on public roads. Traffic surveys show that in Brazil an average of 110,000 traffic accidents occurs per year, around 300 per day. Also, 6 thousand people die, and another 68 thousand are injured, generating to the government an expense about US$7 billion [11]. The primary cause of these accidents was the lack of attention of the drivers, followed by drivers who do not obey the safety distance and speed limit [12]. Studies show that about 60% of accidents can be avoided if the driver is warned a second before the collision. In this context, the use of vehicular networks can provide the reduction of these accidents rates, through the vehicle–vehicle interaction the drivers can be alerted of hazards on roads [13].

In vehicle networks, information should usually be delivered within vehicles in a region of interest, taking into account the geographical position of the node and the relevance of the information to the node. One challenge in this context is how to distribute information to vehicles efficiently, considering the dynamics and mobility of vehicles on the network and even the urgency of delivering information to avoid a collision. For this, an important tool to be studied is the routing protocol, which must be efficient, reliable, support multi-hop communication, and delay intolerant. Moreover, it is important that the vehicle receives the warning of the possible obstacle, even if they are not in the same range of communication [14].

2.3 Integration with Other Networks

Wireless technologies are becoming ubiquitous. It provides network access to a variety of standards, such as IEEE 802.11, 3G/4G, LTE and Bluetooth, which can be used to equip sensor networks, unmanned vehicle networks, and vehicular networks. Hence, cellular networks (4G/LTE) may provide long-distance communication and Internet access for vehicles, and, in short distance, DSRC (Dedicated short-range communications) ad hoc should be more suitable. Hence, ITSs must provide services to drivers and passengers at any time and place. And the success and availability of this service will depend on the integration of different technologies and networks.

In [15], the authors present a performance analysis of the two communication patterns in vehicular networks for different scenarios, densities, and speeds of vehicles. It can be observed that the DSRC scores good results in scattered networks. But because of its communication radius limitations, its support for vehicle mobility is limited. On the other hand, the LTE standard presented a good performance regarding scalability, reliability, and mobility support. However, it presents some challenges in dealing with the delay constraints in some applications.

Regarding data collection, ITSs should make use of an integration with sensor networks (WSN) and unmanned vehicle networks (FANET). Sensory data can be combined with other data collected by the vehicles to, for example, infer the positioning of a network node (vehicle, RSU, mobile user device), provide vehicle density in roads, point out the presence of points of floods and obstacles, etc. Taking into account the unmanned vehicles, they can be applied in special occasions like accidents or floods, to aid in the collection and dissemination of data. In such cases, they would assist in the diffusion of alert messages by establishing communication links in places where RSU infrastructure is in operation or unavailable.

Considering other aspects of data transmission technology, these standards can also be used to establish communication between ITSs and all intelligent traffic infrastructure. For instance, reprogramming traffic lights, reading data from cameras and sensors installed on public roads, communication with radars, etc., all such devices must be able to communicate with traffic monitoring centers to provide data that can assist with the management of all traffic.

3 Infrastructure and Services

In this section, we present the main current research topics related to infrastructure and services of traffic prediction and mobility in ITS. We listed the key features and opportunities of this topic.

3.1 ITS Infrastructure

The dynamic scenario of a transportation system has as main characteristic the high mobility of its components in an urban environment. Although people and goods' mobility are present for many years, it has never reached such a high scale as nowadays. Therefore, problems faced along those years, such as accidents, congestions, and dangerous situations have also worsened with the mobility increasing.

With the technology advancement, the communication evolved from radio, signs, and alerts from own drivers to onboard computers, sensors, smartphones, and other devices that receive real time notifications through wireless communication. New technologies enabled a more dynamic and instant communication.

ITSs have a flexible hybrid architecture, allowing the operation within Internet connectivity, either by infrastructure or taking full autonomy of the system, in an ad hoc manner. This architecture has benefits such as scalability and delay reduction, but it faces some challenges to perform efficiently and guarantees quality and safety, besides representing an additional cost that is not always feasible.

Many devices compose such architecture, including sensors, OBUs (*onboard units*), RSUs (*roadside units*), GPS (global positioning system), intelligent traffic lights, access points, portable devices (smartphones, tablets, laptops), satellites, specialized servers, and the Internet. To allow communication among those components, diverse technologies can be adopted, such as Wi-Fi, WiMAX, LTE, GSM, 3G, 4G, satellite, and Bluetooth, among others.

One of the biggest challenges consists of designing new communication solutions in this heterogeneous set of available technologies. Since an intelligent system operates in a collaborative manner, it is necessary to define standards to enable the integration of all components. Moreover, due to the high mobility, the infrastructure deployment becomes an issue (for instance, consider access points or RSUs location), besides delay and fault tolerance, inherent in such systems.

The components of ITS can be equipped with multiple types of wireless transceivers and can communicate over more than one wireless data channel.

The IEEE 802.11p protocol, a variant of Wi-Fi technology, provides the allocation of bandwidth for specific V2V and V2I communication. Communication can take place in short range, enabling V2V and V2I communication, through GPS and DSRC radios or long range, mainly for V2I and I2I, using cellular data transceivers, GSM-based, GPRS, UMTS.

The work [16] highlights the importance and the role played by the Internet infrastructure in the context of vehicular networks. Being ubiquitous and available in various urban environments, the wired Internet infrastructure can provide support to a variety of applications. For instance, the downloading of advertisements and entertainment or the storage of data gathered and sent by the vehicles. Also, content that is already in the possession of some vehicle may also be shared by opportunistic P2P connections between vehicles and other devices. The authors conclude that a big trend for the Future Internet is the interaction between wireless P2P communication side by side with a support infrastructure for the adequate provisioning of applications and services. Among them, we have navigation safety, navigation efficiency, entertainment, vehicle monitoring, urban sensing, participatory sensing, and emergencies.

In the following, we highlight some works on integrating infrastructure and ad hoc networks to show how ITS can become complete and efficient by using a hybrid architecture.

The problem of RSUs deployment for V2I communication through IEEE 802.11p is studied in [17]. The main goal consists of analyzing urban features' impacts, along with a suitable RSU deployment and communication configurations to guarantee a successful V2I communication. Results presented for a large set of experiments conducted in the city of Bologna show that the quality of V2I communication through IEEE 802.11p is strongly affected by street layout, terrain elevation, trees and vegetation, traffic density, and presence of heavy vehicles. Thus, it is necessary to take such factors into consideration in the proper deployment of RSUs and radio configuration. The authors propose guidelines to be followed for an efficient deployment in the design of vehicular networks.

In [18], the I2V data delivery problem is investigated. It consists of accurately estimating the destination position, considering the temporal and spatial encounter of the packet and destination vehicle. The proposed solution, named Trajectory-based Statistical Forwarding (TSF), uses a packet delay distribution and a vehicle delay distribution to select a target point aiming to minimize packet delivery delay while satisfying the packet delivery probability requested by the user. They consider the installation of RSUs as infrastructure, vehicles equipped with OBUs and DSRC communication, GPS present in both vehicles and stationary nodes and knowledge of the trajectory of the vehicle, which is shared on the Internet periodically through access points.

Infrastructure on the design of ITS is explored in many works of the literature. The employment of RSUs can be found in [19, 20]. The integration of VANETs and cloud computing is treated in [21–23]. Security strategies are studied in [24, 25].

3.2 Traffic Prediction

Traffic congestion impacts not only congested roads but also nearby streets and highways which are alternative paths to drivers avoiding it. A solution to avoid these situations is tracing more efficient routes, which depend on updated traffic information. Since obtaining real-time traffic state of all roads in a city is a hard task, alternative ways of sensing such aspect were developed.

Lippi et al. [26] presented a comparison between multiple short-term traffic prediction strategies. Predicting traffic state in shorter windows of time is an easier task and more effective, given that routes will be traced taking into consideration more recent information. Tostes et al. [27] and Abadi et al. [28] developed predictors of traffic levels in urban areas based on statistical tools. Regression models are especially useful in predicting short-term traffic because they capture the typical behavior of congestion levels and adapt in face of unusual situations, like accidents and roadblocks.

Recent communication technology advances have enabled vehicles to communicate among themselves and with a city's underlying infrastructure. Being able to communicate, vehicles can share sensor data which contains reflexes of traffic state. Wan et al. [29] and Pan et al. [30] present methods to aggregate sensor data from multiple individuals and extract traffic information to trace less crowded routes in a city.

3.3 Mobility and Traffic

Urban problems, especially regarding mobility and traffic, are one of the main research challenges related to the quality of life of people in the cities. In this sense, several efforts have been made to reduce congestion, provide safe means of locomotion, reduce environmental pollution, reduce noise pollution, among other objectives. ITSs can play a key role regarding technological solutions to achieve those objectives.

Understand the dynamics of cities is a fundamental aspect to provide mobility and traffic solutions. Thanks to the popularization of devices with the capacity for sensing and the evolution of ITSs, an enormous amount of data has been generated and made available to analyze the behavior of the entities (e.g., vehicles, people, and objects) in the cities, thus facilitating the understanding of human mobility and the behavior of traffic through the days. Many cities around the world provide several open datasets that can be freely used for the study of mobility, for example, Rio de Janeiro,[1] London,[2] and New York.[3]

[1] http://data.rio/.

[2] http://data.london.gov.uk/.

[3] http://opendata.cityofnewyork.us/.

Data sources such as social networks and applications (*Waze*[4] and *Bing Maps*[5]) also are a powerful form of data collection for the study of mobility and traffic. For example, [31] analyzed social network data (*Instagram*[6] and *Foursquare*[7]), [32] used Bing Maps data to analyze and predict congestion points in Chicago in the United States. These studies show how the discipline of data analysis can be interesting to facilitate the understanding of the dynamics of cities. For example, to identify the main routes used by the population, collect information on the demand for private and public vehicles, find out the causes of congestion, etc. Also, there are several opportunities related to the use of heterogeneous data sources, large-volume data manipulation and processing, and techniques for summarizing and understanding the semantics of the data.

In addition to the analysis to understand the mobility of the population in the cities, another critical perspective is the offer of services that optimize resources and efficiently use the means of transport, considering the particularities of each city such as territorial and population size, road topology, culture, and other aspects. In that sense, the remainder of this section focuses on exposing mobility and transit solutions, highlighting the key opportunities and challenges associated with them, as is illustrated in Fig. 2.

Shared mobility: In this case, new transport solutions allow users to use systems of shared means of transportation such as cars and bicycles for a particular time. Generally, in these systems, vehicles are available at stations and users can use them for a fee. In this context, several research challenges are related. Yang et al. [33] proposed a predictive method for balancing bicycles in stations based on the study of mobility data in Hangzhou in China. Similarly, some efforts have focused on studying vehicle sharing [34, 35].

Carpooling: A common occurrence in several cities is the action of drivers offering car rides to lower travel costs by considering their mobility routines. The digital media leveraged this behavior, as people started to organize themselves in social networks and message groups to plan the rides like the service provided by BlaBlaCar.[8] In this sense, one of the main challenges for this type of system is the creation of recommendation services that explore the infrastructure of ITS such as VANET and data generated by vehicles and people.

Integrated systems and multimodal transport: This refers to integrating the various modes of transport to provide the mobility of people. For example, an integrated system between bus lines, subways, bicycles, or shared cars. Therefore, several challenges must be considered when designing multimodal transport systems, such as real-time information manipulation, multicriteria analysis, making route recommendations, and user preferences.

[4] http://www.waze.com/.

[5] http://www.bing.com/maps/.

[6] http://www.instagram.com/.

[7] http://www.foursquare.com/.

[8] http://www.blablacar.com.br/.

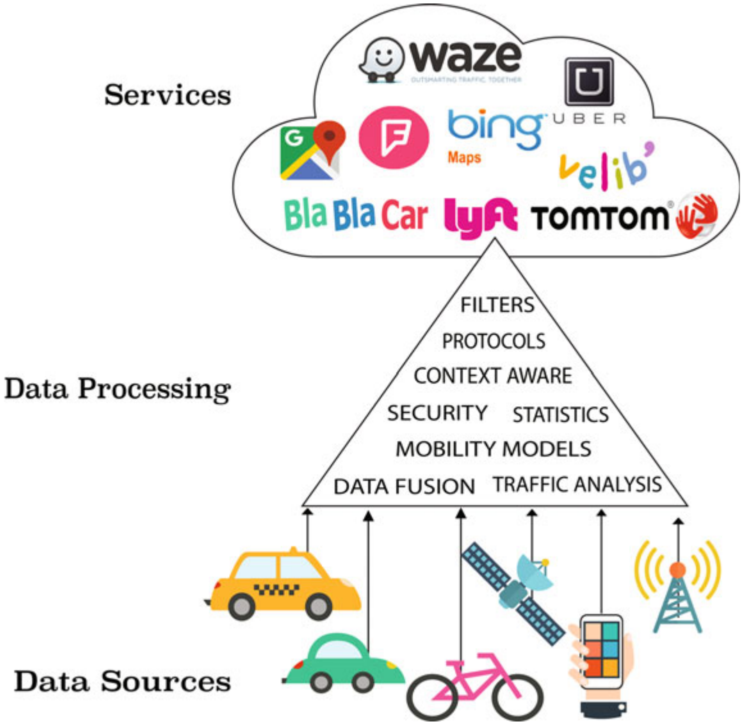

Fig. 2 Data flow to promote the services in ITS

Mobile applications: The popularization of smartphones has leveraged the development of mobile applications that provide services for both mobilities (e.g., Uber[9] and Lyft[10]) to get traffic information (e.g., Waze[11]). In this sense, new initiatives exploring supportive technologies (e.g., mobile and ubiquitous computing, things based on location systems) to ITS are highly recommended in the current scenario.

Traffic control: Monitoring and controlling traffic flow of vehicles (traffic) is an important topic in ITSs. Tian et al. [36] have reviewed the literature on studies that use cameras to monitor and assist the traffic in urban areas. They proposed a taxonomy of methods for detecting, tracking, and recognizing vehicles. Another topic related to the problem of vehicle traffic is the control of intersections, especially at peak times, to improve the flow of vehicles and safety of drivers and pedestrians. In this case, the challenge is to manage traffic lights and intersections for the synchronization of traffic between lanes as discussed in [37, 38].

Detection and management of traffic incidents: Detection and mitigation of traffic incidents is one of the leading research opportunities in the context of ITS,

[9] https://www.uber.com.

[10] https://www.lyft.com/.

[11] https://www.waze.com.

since it is possible to explore the large volume of data generated by vehicles or made available by users through mobile applications and social networks. Pan et al. [39] proposed a system for detecting incidents (e.g., accidents, sporting events) and suggested routes using vehicle location data and information shared by social networks. In this topic, there are some open challenges such as spatially determining the impact of an incident, time duration, and semantics.

In summary, technological solutions in mobility and traffic seek people to spend less time in traffic safely using the various types of transport, prioritizing the conscious consumption of energy resources and reducing the environmental impact.

4 Data and Security in ITS

Data and security become important research topics in ITS due to a series of restricts and challenges to deal with personal data and its peculiarities. Thus, we discuss aspects of data collection, quality, and security issues in ITS, highlighting some research opportunities in the following.

4.1 Data Collection and Quality

Nowadays, modern vehicles have high-technology embedded systems that aim to improve driving safety, performance, and fuel consumption. To achieve these goals, manufacturers have invested both in the quantity and quality of sensors that vehicles have [40]. Currently, a vehicle collects information from hundreds of sensors that are connected to the Engine Control Unit (ECU) through an internal wired sensor network [3] and the Output data is accessible via an Onboard Diagnostic (OBD) interface.

The control system of modern vehicles relies on data collected from embedded sensors. These systems allow to control vehicle's stability and contribute to safer driving. Sensor data is available through the OBD interface, which has been introduced for regulatory and maintenance issues but has been exploited for various other purposes due to the information it provides.

Some of the data collected from vehicle's sensors do not represent relevant information for drivers since most of this data is used by the ECU and does not have a clear meaning for the driver (e.g. oxygen and fuel pressure sensors). Besides, sensors that indicate meaningful information to the driver are displayed by indicators in vehicles such as rotation per minute, speed, and temperature of the engine.

Thus, the challenge is to extract useful information from vehicle's sensors to correlate them with internal and external variables, enabling personalized services for drivers and a transportation system. To better illustrate this subject, data were collected from Bluetooth adapters connected to the OBD interface and *smartphones*.

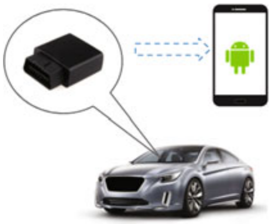

Fig. 3 Data collection schematic using the OBD interface and smartphone

Table 1 Used protocols of the OBD interface

Protocols	Bitrate (kbit/s)
SAE J1850 PWM	41.6
SAE J1850 VPW	10.4
ISO 9141-2	10.4
ISO 14230 KWP 2000	10.4
ISO 15765 CAN	250 or 500

The OBD-II interface was introduced to standardize the physical connector, protocols, and message formats. The system is used to monitor and regulate gas emission, and it is present in all produced cars in Europe and the United States since 1996. The OBD interface also assists maintenance services, tracking the origin of mechanical problems [41]. By enabling the storage of engine failure codes, this information provides a history of problems and possible associated sources. Figure 3 illustrates the collection process: the acquired data from the sensors through the OBD interface are transferred to a smartphone with the Android operating system where they are processed and registered.

Table 1 shows five protocols allowed with the OBD interface. These protocols use the same OBD connector, but the pins have different functions except those that provide battery power. The collected data from sensors are available through OBD parameters IDs (PIDs). Table 2 shows some of the information available considering *smartphone*, vehicle, and data from virtual sensors (values are generated from physical sensor data and mathematical processing and data fusion). There are also hundreds of other sensors that can be accessed through PIDs, some of which are defined by OBD standards and others by vehicle manufacturers.

It is important to note that data from physical sensors are inherently subject to errors caused by some reasons, including the accuracy of the sensor itself, and even operation failures of the vehicle and sensor [42]. Therefore, the first step of the processing and analysis of virtual sensor data is its verification to ensure it is in correlation to the measured data. Among the observed issues at this stage we can highlight discrepant or outliers' data, conflicting information from two or more sensors, incomplete or ambiguous data. Once the data are verified, it is possible to apply

Table 2 Data collected from ECU and mobile phone

Data collected				
Mobile phone		Vehicle		Virtual sensor
Device time	Trip distance	Engine load	Engine RPM	Acceleration
GPS location	Fuel remaining	Fuel flow	Speed	Reaction time
GPS speed	Ambient air temp	Engine coolant temp	CO_2 average	Air drag force
GPS precision	Barometer	Adapter voltage	CO_2 instant	KPL instant
GPS bearing	GPS altitude	Fuel level	Pedal	Speed/RPM relation
Gravity		Intake air temp		Gear

data fusion, which aims to obtain new values with a more significant meaning than the individual data.

4.2 Security

This section presents data security and privacy as a major issue when developing ITSs. ITS services data may contain personal information, enabling people and vehicles tracking. Because data can be transmitted through multiple hops and administrative domains, malicious entities can capture this data. By implementing security in ITSs, one can mitigate those issues and avoid high degradation of ITSs services factors such as response time, network overload, and desirable quality of service. The overview presented in the following was based on [43–45], which introduced guidelines and good practices for Internet security, cyber security for general propose ITS and intelligent public transport, respectively.

One can define the security in ITS into three aspects: *objectives, threats, and services*. *Security objectives* are the goals to keep the ITS as safe as possible. *Security threats* may affect the security objectives causing degradation of ITS services. Finally, *security services* are aimed to counter the threats and to drive the system towards the security objectives. Each security component is discussed in more details in the following section.

4.2.1 Security Objectives

One can divide security objectives for ITSs into four major categories[12]: confidentiality, availability, integrity, and peer authentication.

[12] Note that different authors can consider others security objectives [43–45].

Confidentiality: It aims to keep user and system data free of unauthorized malicious entities, processes, or systems. Hence, the ITSs may selectively grant access only for entities, processes or system with right permissions.

Availability: This objective intends to keep ITSs information available when it is needed. ITS available is accessible at all times and has ways to overcome threats (such as natural disasters, accidental, or intentional ones) to its proper functioning.

Integrity: The basic goal here is to ensure that ITS data sent and received was the same. In another word, the data over the communication channel should maintain its meaning, completeness, and consistency.

Peer authentication: It is aimed to make sure that the one in the endpoint of the communication is the one intended to be. In [43], the authors highlight that without peer authentication, it is hard to reach confidentiality and integrity.

4.2.2 Security Threats in ITS

This section concerns security threats in ITS. Here, threats are everything that potentially can cause problems to proper ITS functioning. One can loosely divide ITS security threats according to its consequences to a system (such as unauthorized usage, denial of service, manipulation). Also, one can classify ITS security threats concerning its origins: *natural disasters, accidental, or intentional ones*. These understanding promote a basis to create security services to counter or mitigate threats. The remaining section discusses mainly threats and consequences to the system, which are pertinent to a wide range of ITSs and applications.

Unauthorized usage: ITS must not be freely accessible to most of the public. Indeed, only authorized users with worth permission level have to receive access to a given ITS function. Although several ITS are available for public users, some subservices are intended to specific users. Suppose, for instance, ITS RESTFUL service like Google Maps[13] or HERE,[14] the servers will serve data to its ordinary users, but they restrict the ability to modify data from the servers or even insert/remove data to specific users. Thus, if the regular users perform service data modification, it would be an unauthorized usage, and then action would be taken. Unauthorized usage arises from accidental or intentional origins ranging from misconfiguration to malicious attackers.

Denial of Service (DoS): One can classify an attack as DoS when actions are taken to block access or interrupt the proper ITS functioning. DoS arises from intentional, accidental, or natural events. However, usually, the cause of DoS is an intentional insertion of malicious codes into the system or by executing inappropriate actions. Critical hazards can emerge when DoS attacks occur in ITS. For instance, if a system of safe driving detection suffers a DoS, then accidents can happen.

Manipulation: The practice of altering data and other information from systems to produce unauthorized effects is namely known as manipulation. Natural, accidental,

[13] https://developers.google.com/maps/.

[14] https://developer.here.com/.

or intentional events can cause manipulation issues. Within ITS, consider a sign system controlling speed limits in roadways. If system manipulations are made in the signs to display incorrect or inappropriate information, several traffic issues might happen such as poor system performance, traffic jams or even accidents.

Replay: In such threat, an attacker records a sequence of data messages and sends them back to the intended receiver.[15] Thus, an attacker replays valid data under invalid circumstances to promote unauthorized effects to the system. In the ITS context, consider a toll system being used by Alice to perform a payment. Bob (an attacker) could capture the messages of the Alice payment and replays it, although he cannot read the messages, he causes twice transactions.

Message insertion, deletion, or modification: Several threats come from insertion, deletion, or modification of spurious messages. On the message insertion case, an attacker forges a message and inserts it into the system to promote malicious effects, for example, in a DoS, the attacker can open a bulk of TCP connections with the victim to drain memory resources and deny the service quickly. On message deletion cases, messages are dropped from the system. An example is the black hole attack [46], where a misconfigured router has zero cost to any destination, and then all traffic loads are forwarded to this router. Consequently, the router does not support the burden and fails. Finally, on the modification case, the attacker removes a message from the system, modifies it, and then reinserts the modified message again into the ITS network. Consider a ITS fast food service, where a user does an order to the service. An attacker wants to attack the order and receives the food. The attacker does not know the victim credit card number. Thus, the attacker waits for the victim to perform an order, then he intercepts the messages order, modifies them by replacing some properties (such as address, goods, and order description) and put the messages again to the system.

Repudiation: When users deny that they performed actions or transaction in the system, one can say a repudiation has occurred. Hence, repudiation attacks are hard to prove without an auditing. Repudiation arises from accidental or intentional events. Such threat usually affects the system integrity and peer authentication. In the ITS context, repudiation, usually, occurs in electronic transactions, for instance, suppose an order service facility. Using an automatic payment scheme without proper security audition, the user could deny ordering a service and refuse to pay.

4.2.3 Security Services

Developing security services is a natural step derived from the identification of security objectives and threats categories. Security services are protections usually employed to enhance confidentiality, availability, integrity, and peer authentication. In the following, it is listed some useful security services for ITS[16]:

[15] The attacker does not need to know the message content to replay messages.

[16] In [44], the reader can find a more exhaustive list of ITS security services.

- **Authentication service**: It aims to verify entities identity and ensure that the ones in the endpoints or even in the middle of the communication channel are those who are supposed to be. Usually, the own entity performs its identification to the system. Such services, enhance the system confidentiality, integrity, and peer authentication objectives.
- **Integrity services**: These services support integrity analyses over information flowing through the system, aiming to minimize manipulation threats. Error detection and correction, cryptographic checksums, digital signatures are basic integrity services that provide some confidence that the data has not been modified during the communication.
- **Access control services**: It aims to provide specific permissions/limits for system entities (such as users, managers, process) to access system resources, according to entity rule in the system. Usually after an entity authentication action, then it is applied some system access permission level to the entity. Access control helps to mitigate unauthorized usage, DoS, manipulation and furthers.

5 Conclusion

This chapter discusses the main concepts related to intelligent transportation systems. Issues related to existing architectures, communication network standards, and integration of systems with different types of communication were pointed out and discussed, showing the demand for the standardization and integration of these systems.

Additionally, it is presented the main types of ITS applications, to show the works found in the literature that already uses these concepts, giving some directions of new works. Finally, it points out the main topics of current research and the challenges that are found in ITS with the purpose of guiding future research in the area. We believe that there are new challenges that can arise as these systems evolve and new users join.

References

1. M. Cintra, “A crise do trânsito em São Paulo e seus custos,” *GV-executivo*, vol. 12, no. 2, pp. 58–61, 2013.
2. “Intelligent Transport Systems—Communications Access for Land Mobiles ({CALM})—Architecture,” ISO, Geneva, Switzerland, Apr. 2010.
3. F. Qu, F. Y. Wang, and L. Yang, “Intelligent transportation spaces: Vehicles, traffic, communications, and beyond,” *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 136–142, Nov. 2010.
4. G. Karagiannis *et al.*, “Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions,” *Commun. Surv. Tutorials, IEEE*, vol. 13, no. 4, pp. 584–616, 2011.
5. M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, “Progress and Challenges in Intelligent Vehicle Area Networks,” *Commun. ACM*, vol. 55, no. 2, pp. 90–100, 2012.

6. A. Boukerche *et al.*, "A new solution for the time-space localization problem in wireless sensor network using UAV," in *DIVANet 2013 - Proceedings of the 3rd ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Co-located with ACM MSWiM 2013*, 2013, pp. 153–160.
7. A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems," *Comput. Commun.*, vol. 31, no. 12, pp. 2838–2849, Jul. 2008.
8. R. S. Alves *et al.*, "Redes veiculares: Princípios, aplicações e desafios," in *Minicursos do Simpósio Brasileiro de Redes de Computadores*, 2009, pp. 199–254.
9. H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *Commun. Mag. IEEE*, vol. 46, no. 6, pp. 164–171, 2008.
10. S. Yousefi, M. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives," *... Proceedings, 2006 6th ...*, pp. 761–766, 2006.
11. I. -, "Instituto Brasileiro de Pesquisas Econômicas." May-2012.
12. CESVI, "Centro de Experimentação e Segurança Viária." May-2012.
13. X. Yang, J. Liu, F. Zhao, and N. Vaidya, "A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning," in *First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04)*, 2004, pp. 114–123.
14. F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *Veh. Technol. Mag. IEEE*, vol. 2, no. 2, pp. 12–22, Jun. 2007.
15. Z. Hameed Mir and F. Filali, "LTE and IEEE 802.11p for vehicular networking: a performance evaluation," *EURASIP J. Wirel. Commun. Netw.*, vol. 2014, no. 1, p. 89, 2014.
16. M. Gerla and L. Kleinrock, "Vehicular networks and the future of the mobile internet," *Comput. Networks*, vol. 55, no. 2, pp. 457–469, 2011.
17. J. Gozálvez, M. Sepulcre, and R. Bauza, "IEEE 802.11 p vehicle to infrastructure communications in urban environments," *IEEE Commun. Mag.*, vol. 50, no. 5, 2012.
18. J. Jeong, S. Guo, Y. Gu, T. He, and D. H. C. Du, "TSF: Trajectory-based statistical forwarding for infrastructure-to-vehicle data delivery in vehicular networks," in *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference On*, 2010, pp. 557–566.
19. Y. Peng, Z. Abichar, and J. M. Chang, "Roadside-aided routing (RAR) in vehicular networks," in *Communications, 2006. ICC'06. IEEE International Conference on*, 2006, vol. 8, pp. 3602–3607.
20. O. Trullols, M. Fiore, C. Casetti, C. F. Chiasserini, and J. M. B. Ordinas, "Planning roadside infrastructure for information dissemination in intelligent transportation systems," *Comput. Commun.*, vol. 33, no. 4, pp. 432–442, 2010.
21. S. Olariu, I. Khalil, and M. Abuelela, "Taking VANET to the clouds," *Int. J. Pervasive Comput. Commun.*, vol. 7, no. 1, pp. 7–21, 2011.
22. R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking vehicular communications: Merging VANET with cloud computing," in *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, 2012, pp. 606–609.
23. W. He, G. Yan, and L. Da Xu, "Developing vehicular data cloud services in the IoT environment," *IEEE Trans. Ind. Informatics*, vol. 10, no. 2, pp. 1587–1595, 2014.
24. K. Plößl and H. Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks," *Comput. Stand. Interfaces*, vol. 30, no. 6, pp. 390–397, 2008.
25. A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on*, 2009, pp. 1–9.
26. M. Lippi, M. Bertini, and P. Frasconi, "Short-term traffic flow forecasting: An experimental comparison of time-series analysis and supervised learning," *Intell. Transp. Syst. IEEE Trans.*, vol. 14, no. 2, pp. 871–882, 2013.
27. A. I. J. Tostes, F. de L. P. Duarte-Figueiredo, R. Assunção, J. Salles, and A. A. F. Loureiro, "From Data to Knowledge: City-wide Traffic Flows Analysis and Prediction Using Bing Maps," in *Proceedings of the 2Nd ACM SIGKDD International Workshop on Urban Computing*, 2013, p. 12:1–12:8.

28. A. Abadi, T. Rajabioun, and P. A. Ioannou, "Traffic Flow Prediction for Road Transportation Networks With Limited Traffic Data," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 653–662, Apr. 2015.
29. J. Wan, J. Liu, Z. Shao, A. V Vasilakos, M. Imran, and K. Zhou, "Mobile crowd sensing for traffic prediction in internet of vehicles," *Sensors*, vol. 16, no. 1, p. 88, 2016.
30. B. Pan, Y. Zheng, D. Wilkie, and C. Shahabi, "Crowd Sensing of Traffic Anomalies Based on Human Mobility and Social Media," in *Proceedings of the 21st ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, 2013, pp. 344–353.
31. T. H. Silva, P. O. S. V. De Melo, J. M. Almeida, and A. A. F. Loureiro, "Large-scale study of city dynamics and urban social behavior using participatory sensing," *IEEE Wirel. Commun.*, vol. 21, no. 1, pp. 42–51, 2014.
32. A. I. J. Tostes, F. de LP Duarte-Figueiredo, R. Assunção, J. Salles, and A. A. F. Loureiro, "From data to knowledge: city-wide traffic flows analysis and prediction using bing maps," in *Proceedings of the 2nd ACM SIGKDD International Workshop on Urban Computing*, 2013, p. 12.
33. Z. Yang, J. Hu, Y. Shu, P. Cheng, J. Chen, and T. Moscibroda, "Mobility Modeling and Prediction in Bike-Sharing Systems," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, 2016, pp. 165–178.
34. R. Nair, E. Miller-Hooks, R. C. Hampshire, and A. Bušić, "Large-scale vehicle sharing systems: analysis of V{é}lib'," *Int. J. Sustain. Transp.*, vol. 7, no. 1, pp. 85–106, 2013.
35. C. Boldrini, R. Bruno, and M. Conti, "Characterising demand and usage patterns in a large station-based car sharing system," in *Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on*, 2016, pp. 572–577.
36. B. Tian *et al.*, "Hierarchical and networked vehicle surveillance in its: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 1, pp. 25–48, 2017.
37. Z. Ye and M. Xu, "Decision Model for Resolving Conflicting Transit Signal Priority Requests," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 1, pp. 59–68, 2017.
38. M. S. Shirazi and B. T. Morris, "Looking at Intersections: A Survey of Intersection Monitoring, Behavior and Safety Analysis of Recent Studies," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 1, pp. 4–24, 2017.
39. B. Pan, Y. Zheng, D. Wilkie, and C. Shahabi, "Crowd sensing of traffic anomalies based on human mobility and social media," in *Proceedings of the 21st ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, 2013, pp. 344–353.
40. W. J. Fleming, "Overview of Automotive Sensors," *IEEE Sens. J.*, vol. 1, no. 4, pp. 296–308, 2001.
41. J. Lin, S. Chen, Y. Shih, and S. Chen, "A study on remote on-line diagnostic system for vehicles by integrating the technology of OBD, GPS, and 3G," *World Acad. Sci. Eng. Technol.*, vol. 32, no. 8, pp. 435–441, 2009.
42. P. H. Rettore, B. P. S. André, Campolina, L. A. Villas, and A. A.F. Loureiro, "Towards Intra-Vehicular Sensor Data Fusion," in *Advanced perception, Machine learning and Data sets (AMD'16) as part of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC 2016)*, 2016.
43. E. Rescorla and B. Korver, "Guidelines for writing RFC text on security considerations," 2003.
44. K. Biesecker, E. Foreman, K. Jones, and B. Staples, "Intelligent Transportation Systems (ITS) Information Security Analysis," 1997.
45. C. Levy-Bencheton and E. Darra, "Cyber security and resilience of intelligent public transport: good practices and recommendations," 2015.
46. J. R. Vacca, "Front Matter," in *Computer and Information Security Handbook (Third Edition)*, Third Edit., Boston: Morgan Kaufmann, 2017, p. iii.