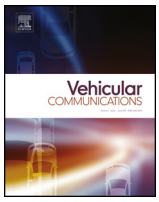
Vehicular Communications 31 (2021) 100349

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom



A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications

Hwanseok (Harrison) Jeong [a], Yiwen (Chris) Shen [a], Jaehoon (Paul) Jeong [b,*], Tae (Tom) Oh [c]

[a] Department of Electrical & Computer Engineering, Sungkyunkwan University, Suwon, 16419, Republic of Korea
[b] Department of Computer Science & Engineering, Sungkyunkwan University, Suwon, 16419, Republic of Korea
[c] School of Information, Rochester Institute of Technology, USA

ARTICLE INFO

Article history:
Received 22 August 2020
Received in revised form 23 February 2021
Accepted 14 March 2021
Available online 16 April 2021

Keywords:
Smart transportation
Vehicular networks
Driving safety
Driving efficiency
Protocol
Security

ABSTRACT

Dramatic increase in road traffic volume has made driving safety and traffic efficiency more challenging, but smart transportation has been spotlighted as a promising technology for improving driving safety and efficiency. This paper surveys safe and efficient driving in the smart transportation with a focus on the aspects of systems, protocols, applications, and security, especially for autonomous vehicles. This smart transportation requires to monitor road surfaces precisely and identify hazards, and vehicles also need to share sensing information to avoid dangerous situations or environments through wireless communication in vehicular networks. For this purpose, dedicated short-range communications (DSRC) have achieved the international standards of the IEEE Wireless Access in Vehicular Environments (WAVE), and applications are now common that use the global positioning systems (GPS) for a dedicated navigation system navigator or smartphone application. This combination of vehicular networking and navigation enables systems and applications not only to enhance driving safety, but also to increase traffic efficiency. To support the vehicular systems and applications efficiently, the protocols need to be designed carefully and implemented effectively. This paper summarizes and analyzes the state-of-the-art research based on standardization activities for smart transportation systems, protocols, applications, and security. This paper also provides the comparison between the different technologies composing vehicular systems, protocols, applications, and security in terms of advantages, disadvantages, analysis, simulation, implementation, and complexity to provide a trend of overall technologies. Lastly, this paper suggests research directions for the smart transportation.

1. Introduction

Recently, smart transportation has been spotlighted as an important part of smart cities. There are multiple components to smart transportation, such as road networks, railways, and subways. In particular, road networks are people's primary locations for driving and have many infrastructure elements (e.g., traffic lights, road-side units, and ramps) and moving objects (e.g., vehicles, motorcycles, bicycles, and pedestrians). Vehicles can play a critical role in smart transportation by monitoring these environments to sense obstacles and hazards. For such monitoring, the vehicles use motion sensors (e.g., gyroscope, accelerometer, barometer, and magnetometer), obstacle detection sensors (e.g., ultrasonic sensors, laser sensors, and lidars), and cameras (e.g., on-board and smartphone cameras) in vehicles. In smart transportation, precise monitoring of road surfaces for possible hazards is critical, and different vehicles (e.g., personal vehicles and subway trains) can act as mobile sensors to detect these hazards. Through vehicular communications such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), infrastructure-to-vehicle (I2V), and vehicle-to-everything (V2X), vehicles can then share the sensing information with neighboring vehicles and pedestrians to help travelers avoid possible accidents and dangerous situations.

Wireless communication among vehicles has generated much interest to both academia and industry. It enables vehicles to take instantaneous actions in response to dynamic transportation scenarios and neighboring vehicles through prompt data exchange

* Corresponding author.
E-mail addresses: harryjeong@skku.edu (H.H. Jeong), chrisshen@skku.edu (Y.C. Shen), pauljeong@skku.edu (J.P. Jeong), tom.oh@rit.edu (T.T. Oh).

https://doi.org/10.1016/j.vehcom.2021.100349
2214-2096/

Table 1
Comparison of this survey and related surveys.

Year	Survey	Focus	Tutorial	Protocol	System	Application	Network security	Emergency management	Challenges & research issues
2021	[15]	Emerging security issues in SDN-based VANET.	✓	×	✓	✓	✓	×	✓
2021	[16]	IP-based VNs and standardizations.	✓	×	✓	✓	×	×	✓
2020	[17]	Safety and traffic management based on car-following sensor and data.	×	×	✓	✓	×	×	✓
2019	[18]	Integration of intra- and inter-vehicle communications for autonomous driving.	✓	✓	×	×	×	×	✓
2018	[19]	Several aspects of cooperative vehicular networking.	✓	✓	×	×	✓	×	✓
This survey		Approaches in vehicular networking for driving safety and efficiency	✓	✓	✓	✓	✓	✓	✓

over wireless links. The dedicated short-range communications (DSRC) [1] technology allocates wireless channels for communications among vehicles, and the Institute of Electrical and Electronics Engineers (IEEE) has developed standards for Wireless Access in Vehicular Environments (WAVE): IEEE 802.11p and IEEE 1609 [2–6]. Note that IEEE 802.11p was revised into IEEE 802.11-OCB (Outside the Context of a Basic Service Set) [7] in 2012. This trend of DSRC-based vehicular networking and navigation enhancement has opened a new door for smart transportation.

On the other hand, the 3rd Generation Partnership Project (3GPP) has announced technical specifications of Cellular V2X (C-V2X) [8] in 4G-LTE network, and has been developing new use cases and technical requirements in 5G networks [9,10]. The US Federal Communications Commission (FCC) [1] and the Commission Decision of European Union (EU) [11] assigned wireless channels in the range of 5.850∼5.925 GHz and in the 5.875∼5.905 GHz, respectively, for enabling vehicular networking. The technology of DSRC/ITS-G5 or C-V2X enables the communications for V2I, I2V, V2V and V2X, and will be an important technical element for Intelligent Transportation Systems (ITS) applications such as a neighbor-vehicle-aware navigation protocol for collision avoidance [12], a pedestrian protection smartphone application [13], and a car speed recommendation system for energy efficiency [14]. Drivers today rely on global positioning system (GPS)-based navigation for efficient road travels. A navigator for a vehicle can be a dedicated device embedded into dashboard, or an application in smartphones or other mobile devices.

1.1. Related work

There are many related surveys that introduce different topics in vehicular networks (VNs). Sultana et al. [15] investigated emerging issues in software-defined networking (SDN) based VANET. Jeong et al. [16] surveyed various architectures and approaches in the IP-based VNs. Talal et al. [17] systematically reviewed safety and traffic management based on car-following sensors and data in ITS. Wang et al. [18] paid special attention to the integration of intra- and inter-networking for autonomous vehicles. Ahmed et al. [19] focused on the cooperative vehicular networking that mostly investigated technologies and approaches for the network efficiency. However, most of these surveys focus more on the networking part, such as network security issues, IP-based VNs, and intra- and inter-vehicle integrated networking, which did not investigate much about the approaches that can improve driving safety and efficiency based on VNs.

1.2. Current survey

To fill the gap, in this paper, we survey systems, protocols, and applications of the smart transportation that is based on VNs with regard to driving safety and traffic efficiency. To show the differences between our survey and other related surveys, Table 1 summarizes a comparison from different perspectives, such as focus, tutorial, protocol, system, application, and challenges and research issues. Our survey focuses on the latest advances in driving safety and traffic efficiency. We provide several comparison tables (e.g., Table 3 and 4) for studies on systems, protocols, applications as well as security in smart transportation systems. Thus, the analysis on the surveyed schemes of this paper allows the audience to understand the trend of the studies on driving safety and efficiency based on VNs.

As mentioned earlier, the IEEE WAVE standard comprises several parts, and each part regulates different functions for vehicle communications [3–6], as shown in Fig. 2. For example, for the MAC layer, IEEE WAVE standard 1609.4 utilizes enhanced distributed channel access (EDCA) [7] and multiple-channel operation. Many research results have demonstrated that the IEEE WAVE standard performs poorly in certain scenarios. An improved vehicle communication protocol can enhance vehicle driving safety and efficiency [20,21], and, as noted above, the aim of this paper is to highlight the current research on systems, protocols, applications, and security related to smart transportation. The major contributions of this paper are as follows:

- A comprehensive survey focuses on the particular angle of driving safety and efficiency based on VNs.
- Various systems, protocols, and applications for driving safety and efficiency are reviewed and analyzed.
- We compare different technologies for vehicular applications, protocols, and applications for their advantages and disadvantages.
- Along with the security issues and emergency management in VNs, several research issues and challenges are presented.

The remainder of this paper is organized as follows. Section 2 briefly introduces the background knowledge and the definitions used in this paper. Section 3 comprises a discussion of the research work related to driving safety, and Section 4 discusses driving efficiency. Section 5 presents the issues and requirements of security and privacy in VNs along with possible solutions, and Section 6 provides a safety and emergency management schemes during emergency situations. Section 7 suggests research issues and challenges in smart transportation. Section 8 analyzes and summarizes the identified papers on traffic safety and driving efficiency related to smart transportation. Finally, Section 9 concludes this paper along with future work.

We use a set of acronyms and abbreviations shown in Table 2 for simplicity. The structure of this paper is also provided in Fig. 3 to make it easy to understand the overall structure of this survey.

Fig. 1. Smart car.

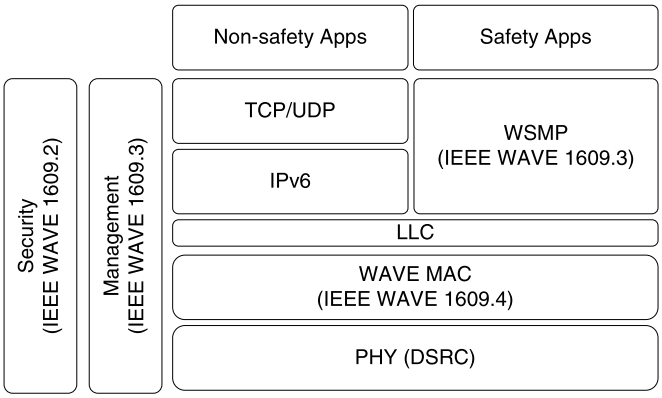


Fig. 2. IEEE WAVE protocol stack [3–6].

Table 2
Acronyms and abbreviations.

Acronym	Description
SANA [13]	Safety-Aware Navigation Application
CBPRS [22]	Cloud-Based Pedestrian Road-Safety
FTRA [23]	Fair Transmission Rate Adjustment
WPCF [24]	WAVE Point Coordination Function
LMA [25]	Location- and Mobility-Aware MAC protocol
DMMAC [26]	Distributed Multichannel and Mobility-Aware Cluster-based MAC Protocol
STMAC [27]	Spatio-Temporal Coordination-Based MAC Protocol
D2D [28]	Device-to-Device communication for Intelligent Transportation Systems
V-D2D [29]	Vehicular D2D communication
LORA [30]	LOss differentiation Rate Adaptation scheme
SS-MAC [31]	time Slot-Sharing MAC
CASD [12]	A framework of Context-Awareness Safety Driving
CNAC [32]	Context and Network Aware Communication strategies
AAOSM [33]	An Android ITS Driving Safety Application Based on V2V Communications
SafeDrive [34]	An Autonomous Driver Safety Application
BRO [35]	Beacon Rate Optimization for Vehicular Safety Applications
SBUS [36]	Cloud-based Battery Replacement Scheme for Smart e-Bus
ORBR [37]	Online Routing and Battery Reservations
SAINT+ [21]	Self-Adaptive Interactive Navigation Tool+
SignalGuru [14]	Leveraging Mobile Phones for Collaborative Traffic Signal Schedule Advisory
CRATER [38]	A Crowd Sensing Application to Estimate Road Conditions
TBD [39]	Trajectory-Based Data Forwarding
TSF [40]	Trajectory-based Statistical packet Forwarding scheme
TPD [41]	Travel Prediction-based Data Forwarding
VRU [42]	A Vehicular Routing protocol with UAV-assisted
BDAC [43]	A traffic Big Data Assisted V2X Communications
GDRP [44]	A Global and Dynamic Route Planning application
STFC [45]	Smart Transportation applications in Fog Computing paradigm
EEEC [46]	Energy-Efficient Edge Computing Service Provisioning
UAV ITS [47]	Unmanned Aerial Vehicles enabled ITS

2. Background in VNs for driving efficiency and safety

In this section, we introduce the background knowledge for driving efficiency and safety based on VNs. Along with that, we also give several definitions for systems and applications in ITS and clarify the distinction between a system and an application in our definition.

For driving efficiency, sensors (e.g., radars and cameras) mounted on vehicles can measure road congestion and, via DSRC links or cellular links (e.g., 3G, 4G-LTE and 5G), the vehicles can periodically report road congestion conditions and their navigation routes to a traffic control center (TCC) [20]. A TCC is a central node in vehicular clouds for road traffic management. A TCC efficiently coordinates vehicles in real-time for better navigation paths that can reduce the traffic congestion [48]. A TCC can also acquire these optimized routes by synchronizing traffic signals at different intersections and navigation systems in vehicles, which is particularly useful during rush hours. In addition to increasing efficiency during heavy traffic time, a smart transportation navigation service can support the rapid delivery of emergency vehicles such as fire and police vehicles [21].

For driving safety, various kinds of in-vehicle sensors shown in Fig. 1 can sense road environments, such as motion sensors, obstacle detection sensors, and image sensors. Accurately monitoring road surfaces and detecting hazards on highway environments can provide drivers with important information, alerting them to dangerous and questionable roads. Monitoring the road environment can give drivers many benefits. For example, in a vehicle, a smartphone installed with an accelerometer can be used to detect potholes and speed bumps for safe driving [38]. Vehicles can also measure inter-distance spacing for safe driving with radar and lidar sensors; if two vehicles have a high probability of colliding with each other, their drivers can detect this situation and warn each other to avoid a crash. Furthermore, the vehicles themselves can collaborate through wireless communication to calculate and execute safe maneuvers (i.e., moving paths) to avoid a collision. To prevent hackers from causing hazards in cooperative driving environments with false information, security and privacy should be protected through well-designed protocols.

2.1. Systems

A system defined in this paper is an entity that manages hardware resources and provides functions that allow applications to control and use these resources. It is designed to provide a platform on which many different applications can run. It can be a large-scale centralized cloud platform, and it can also be an in-vehicle system that conducts different tasks such as monitoring, sensing, decision-making, and path planning. Sensors on the road for traffic monitoring are also included in the systems. Considering the collaboration between infrastructures and vehicles, a system can cross multiple entities to work together for the driving efficiency and safety. For example, an edge computing cloud (ECC) system can receive the offloaded tasks from vehicles, and the ECC can also distribute tasks to several vehicles to cooperatively calculate efficient paths for both general and special cases.

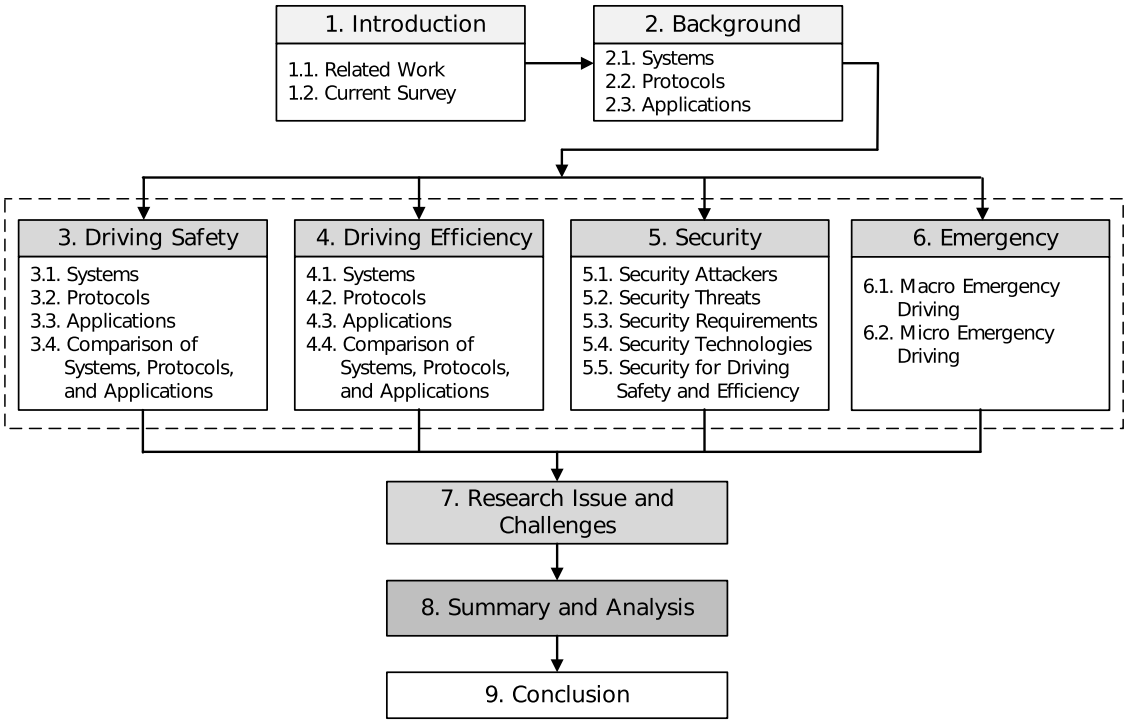


Fig. 3. Structure of this paper.

2.2. Protocols

A protocol in smart transportation systems needs to be designed and implemented to allow applications to run efficiently and effectively. As an aside, self-driving vehicles are being developed by major IT companies (e.g., Google and Apple) and major automobile companies (e.g., Tesla, GM, BMW, Hyundai, Honda, and Toyota). The smart transportation technologies surveyed in this paper can support these self-driving vehicles for driving safety and efficiency. These self-driving vehicles can collaborate and communicate with each other using wireless communications directly or with infrastructure nodes comprising road-side units (RSUs) and relay nodes (RNs) [40]. Note that RSUs are gateways that have DSRC interfaces for vehicular ad hoc networks (VANETs) and Ethernet interfaces for wired networks. However, RNs are packet holders that have sufficient memory for keeping a vehicle's packets in delay-tolerant networks, which deliver the packets from a source node to a destination node based on forward-and-carry data delivery.

2.3. Applications

An application is a user-oriented software, and it provides functions that users directly control or that are utilized in other applications provided by the system. An application can be operated through mutual interaction of components such as a system and a protocol. A smart transportation system can refer to an application software and networking functions so that multiple nodes, such as vehicles and RSUs, can share information for safe driving or efficient driving. In addition, systems can reduce battery consumption and control safe messages delivery through resource coordination between communication devices. An application can also be software for services used by users, which can exchange notifications between a vehicle and a pedestrian using a smartphone that operates in the upper layer of the service structure. Such use cases include a road information service, a navigator considering current and future traffic conditions, and a vehicle-pedestrian collision warning app.

In the next section, we will introduce systems, protocols, and applications for driving safety based on VNs.

3. Driving safety

Driving safety is one of the critical issues for smart transportation. We surveyed papers related to driving safety in terms of systems, protocols, and applications for smart transportation. Driving safety is usually about collision detection and avoidance, and can be improved with the frequent exchange of driving information among vehicles in a vicinity.

3.1. Systems

Hwang et al. proposed SANA [13] to protect pedestrians in VANET whereby smartphones alert drivers to predicted dangers. The communication between pedestrians and drivers is performed via RSUs at the intersections through DSRC channels. Both smartphones and vehicles share trajectories (e.g., travel paths) and motion vector (e.g., vehicle position, speed, and direction) with the RSUs, which use the data to calculate collision probabilities and travel delays. SANA is designed to increase the safety of pedestrians while decreasing the battery consumption of smartphones through an efficient communication device scheduling. To address the efficiency of the collision prediction and energy consumption, the SANA scheduling algorithm filters out collision unrelated vehicles for specific pedestrians and decides sleeping time for communication with each smartphone. In SANA, there are two notification types, which are pre-warning and warning, depending on the pedestrian protection warning areas. As shown in Fig. 4, the warning area is in the inner circle and the pre-warning area is from the outer circle to the inner circle. A pre-warning area is an area in which any vehicle can arrive at the perimeter of the pedestrian area within the pre-safety time (e.g., 4 seconds which are the rendezvous time of the vehicle and pedestrian). In a warning area, a

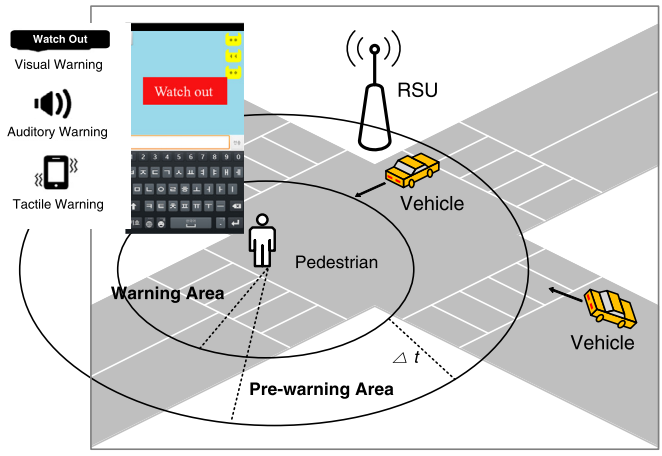


Fig. 4. Pedestrian protection area [13].

vehicle can arrive at a pedestrian within the safety time (e.g., 2 seconds which are the time for a pedestrian to avoid the collision with an approaching vehicle). Note that many European nations regard 2 seconds as the safety time as part of pedestrian protection requirements. Compared with previous solutions such as Always-On and Duty-Cycle, SANA gives more efficient energy consumption and fewer delayed warning messages.

Bagheri et al. proposed a cloud-based pedestrian road safety (CBPRS) [22] system with adaptive multi-mode for energy efficient communication and condition-aware beaconing; the system reduces power consumption by controlling beacon transmission rates. CBPRS is a cloud system, and a mobile application in CBPRS controls the frequency of beaconing between the pedestrian and the cloud according to the collision risk level: no, low, or high risk. Under no risk, there is no probability of collision, whereas under high risk, a vehicle is approaching a pedestrian at a high speed and there is a high probability for collision. The client-side application for road safety in the pedestrian smartphone operates in three different modes: sleep, low rate, and full rate modes; each mode corresponds to the level of collision risk, such as risk free, low risk, and high risk. On the server side, the application runs an algorithm to analyze and predict the collision risk. The algorithm checks paired beacon signals received from pedestrians and vehicles that are moving closer to each other. If the cloud server recognizes a high-risk situation, the server sends notification messages to the target pedestrians, and the pedestrians' smartphones convert to full-rate mode. The authors used a simulation of urban mobility (SUMO) [49] to establish a street network of a city from OpenStreetMap [50] for VN simulation. The simulation result showed that CBPRS with the adaptive multi-mode road-safety system was practical and realistic in a real-world environment. However, frequent beacon messages consumed additional power when the smartphone operates in full-rate mode. Simulation with the assumption of 50% market penetration of CBPRS with adaptive mode showed an increase of 40% battery lifetime compared with the non-adaptive approach.

Cooperative vehicle safety systems (CVSS) use VNs to track positions and movements of vehicles in a vicinity from the state update messages of those vehicles. A high vehicle density can cause a severe packet loss and reduce a tracking accuracy. Zhang et al. in [23] proposed a distributed fair transmission rate adjustment (FTRA) scheme based on multi-agent model predictive control (MPC) to ensure fair allocation of channel resources and provide high tracking accuracy among vehicles even under continuous changes of a wireless network topology in VNs due to the dynamic movement of vehicles. The FTRA is built based on an information dissemination rate (IDR) model that tries to catch the continuous changes in vehicle density over time. The IDR model counts the packets received by all neighbors of a vehicle per unit time, considering the channel access probability of both senders and receivers. Then, by characterizing interconnections among vehicles and the dynamics of a single vehicle, the FTRA formulates a multi-agent transmission rate control optimization problem with the objective of finding both the fairness of transmissions and the high tracking accuracy in the CVSS. To work in a distributed environment, FTRA also proposed an augmented Lagrangian-based coordinated decision-making approach to determine the optimal message transmission rate for the channel utilization to guarantee both fairness and efficiency. Although proponents of other proposals consider the fairness of channel utilization, they do not consider the efficiency of resource allocation; they depend on the other nodes' transmission adjustment, not using coordinated control of each node's transmission adjustment. In contrast, this proposal focuses on integrating fair channel utilization and efficient resource allocation at the same time. Simulation results showed that this transmission control proposal was effective in vehicle networks with frequent changes of vehicle density.

3.2. Protocols

A communication protocol can increase vehicle driving safety in that more efficient and reliable protocols can provide vehicles with more reliable safety information.

Chung et al. proposed a WAVE PCF-based MAC protocol (WPCF) [24] to reduce channel collision and to increase user capacity in I2V communication in VNs. WPCF is based on the point coordination function (PCF) [7] in IEEE 802.11p. In WPCF, an RSU is a coordinator to schedule communication between vehicles and itself. When a vehicle approaches an RSU's communication range, the vehicle receives beacon messages from the RSU at the current intersection, called the timing advertisement frame (TAF). After receiving the TAF, the vehicle registers its mobility information (e.g., location, speed, direction to move, and trajectory) with the RSU. The RSU assigns time slots for message transmissions of the registered vehicles. Moreover, WPCF uses a WAVE handover controller to reduce service allocation time. However, WPCF has a few disadvantages as follows. For example, vehicles need to communicate with each other via an RSU, but the RSU could increase communication delay as a relay, resulting in bottlenecks in system performance if the RSU is congested or malfunctions. Another potential issue is that the channel utilization of WPCF may not be efficient because the contention period [7], that is the time period to register the mobility information of in-coming vehicles with an RSU, may not be optimized according to the vehicle number. Also, the contention-free period [7] of WPCF for the actual data exchange between an RSU and vehicles cannot fully utilize wireless channels by relay delay via the RSU in the wireless communication among the vehicles in a vicinity because the RSU needs to relay a vehicle's data frame to another vehicle.

Feng proposed an LMA MAC protocol [25], which was based on the distributed coordination function (DCF) in IEEE 802.11 with a directional antenna. LMA provides vehicles with V2V communication without an RSU and uses the carrier sensing multiple access with collision avoidance (CSMA/CA) mechanism [7]. LMA predicts the locations and movements of target vehicles in order to transmit packets to them, effectively using the directional transmission and antenna beam forming. LMA has good channel efficiency because it allows multiple V2V communications simultaneously in non-overlapped transmission coverage with directional antennas. A potential issue of LMA is the low channel utilization due to the frequent control frame collision, which is caused by request-to-send (RTS)/clear-to-send (CTS) frames whose exchanges are required to reserve the channel for the transmission of data frames.

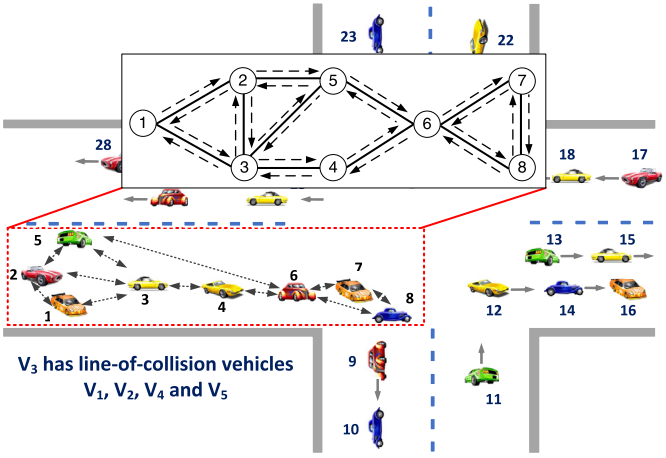


Fig. 5. Spatio-temporal coordination-based MAC protocol [27].

Hafeez et al. proposed a distributed MAC protocol (DMMAC) [26] for VANETs that exploited the characteristics of multiple channels, mobility awareness, and node clustering. This protocol used the position, speed, and acceleration of neighboring vehicles to decide an exponential-weighted stabilization factor, which is used to select a cluster head (CH). To decide future acceleration of a vehicle, DMMAC proposes a rule-based fuzzy logic, and to address adaptability in the fuzzy logic system, an adaptive learning process is developed. During the clustering process, vehicles periodically exchange status messages that contain the stabilization factor, and the vehicle with the highest stabilization factor becomes the CH. In every control channel interval, the CH sends three additional messages to announce transmission schedules and subchannel identifiers for the current cluster. For emergency message transmission, DMMAC leverages the EDCA mechanism [7] to give emergency messages the highest priority with a minimum contention window. CHs relay emergency messages as a virtual backbone, and eventually a distant destination vehicle can receive the emergency messages with a low delay.

Jeong et al. proposed a spatio-temporal coordination-based MAC protocol (STMAC) [27], considering the topology of vehicles. STMAC is designed to efficiently exchange driving information among vehicles in congested urban traffic environments, especially during rush hours. STMAC defines a line-of-collision (LoC) graph indicating that vehicles could physically collide with each other, as shown in Fig. 5. Adjacent vehicles in an LoC graph exchange safety messages to share driving mobility information, such as the current position, driving speed, direction, and conditions of each vehicle, in order to prevent vehicles from having a physical collision. STMAC suggests an enhanced set-cover algorithm to minimize the number of time slots in which vehicles need to transmit safety messages to neighboring vehicles. The optimized scheduling of time slots can be formulated as follows:

$$S^* \leftarrow \arg\min_{S \in 2^N} |S|, \tag{1}$$

where $S = \{S_i | S_i$ is a cover-set for time slot $i\}$ and 2^N is a power set of natural number set N as a set of time slots, such as $2^N = \{\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \ldots\}$. STMAC also optimizes the length of the contention period for registering vehicle information with an RSU according to the number of vehicles entering the covering area of the RSU at a road intersection. The authors compared STMAC with the other state-of-the-art protocols in VNs (i.e., WPCF, LMA, DMMAC, and EDCA [24–26,51]) using theoretical analysis and computer simulation and found that STMAC outperformed them in CP length, end-to-end (E2E) delay, and packet loss. As in STMAC, Integrating V2V and V2I communications is becoming a key issue in VNs. Effective and efficient integration of V2V and V2I communications is an important factor in the success of next-generation ITS.

Direct communication is classified into two cases, such as, device-to-device (D2D) communication and machine-to-machine (M2M) communication. V2V communication is a kind of M2M communications. D2D communications have recently emerged as a solution to an effective V2V and V2I integration in cellular networks. In D2D communications, two adjacent users can communicate with each other using a direct link between two devices bypassing a base station. D2D communication is done with human intervention. But V2V communication to form a D2D network is done without human intervention and without base station involvement. Different from cellular communication, D2D and V2V communications are similar in that they connect directly between the two devices without utilizing a base station [52,53].

Cheng et al. in [28] proposed a practical and beneficial D2D architecture for ITS based on both D2D communication and VNs. They proposed an architecture of D2D operations with high performance and low complexity under the features of VNs. Cheng et al. focused on the D2D underlay reuse mode. In the D2D underlay mode, D2D devices can directly transmit data by reusing some resources for either uplink or downlink communications in cellular networks. This mode coordinates the interference of transmissions and allocates frequency resources according to the positions of vehicles. Transmission power for cellular users and D2D pairs can be optimized under the sum of total power, considering the sum of the maximum data rates. The authors proposed an improved scheduling algorithm by cooperating with adjacent RSUs in VNs; via backhaul connections between RSUs, the RSUs collaborate on resource allocation. Through extensive simulation, the authors found that the D2D underlay mode allowed for the best spectrum efficiency at all D2D transceiver distances. They concluded that the ITS D2D technology is promising to improve frequency utilization of vehicular applications.

Cheng et al. [29] proposed vehicular device-to-device (V-D2D) communications to provide alternative links for vehicular data transmission in addition to the cellular network and DSRC. A joint power control scheme and a mode selection strategy according to variable channel quality are adopted. A channel inversion power control scheme is adopted to avoid high interference level and to keep the receive power threshold. Based on channel condition, biased mode selection scheme was exploited according to the optimal portion of vehicle users to select D2D mode or cellular mode. When the quality of biased D2D link was the same or better than that of cellular link, they choose D2D link to transmit data rather than cellular link. They examined the effectiveness of V-D2D communications underlaying the cellular uplink resources in two metrics, such as, signal-to-interference-plus-noise ratio (SINR) failure probability and network throughput. According to their simulation, the increase of SINR outage shows that of the outage threshold. The increased biased factor resulted in the higher level of interference and increased average SINR failure. However a probability of average SINR failure did not necessarily contradict to the cell throughput. A higher value of channel inversion threshold leads to increased throughput. They made a theoretical analysis for the performance of V-D2D communications considering the unique characteristics of VANETs.

Single-hop broadcasting in V2V communications is a good method to guarantee a delay requirement, but it does not guarantee the reliability. Rate adaptation promotes efficient system performance in the dynamic topology change of VNs due to continuous vehicle movement. Differentiated interference loss should be provided for this rate adaptation in V2V communications. To decide an optimal data transmission rate for driving safety in V2V

communications on highways, Yao et al. proposed loss differentiation rate adaptation (LORA) [30]. The authors first built a hybrid model considering highway scenarios, MAC-layer backoff, and PHY-layer propagation. Based on the hybrid model, the authors designed an algorithm to evaluate packet loss and channel conditions. Then, through the proposed algorithm, the LORA scheme was proposed to select a transmission rate rapidly and appropriately by a self-organizing fuzzy neural network according to the dynamic environment parameters. They compared LORA with an up-to-date decentralized congestion control protocol standardized by the European Telecommunications Standards Institute (ETSI) [54]. LORA outperformed the decentralized congestion control protocol in terms of reliability for V2V safety applications and average received packets to a dynamic topology in VNs.

Lyu et al. in [31] proposed an SS-MAC (Time Slot Sharing MAC) protocol for broadcasting which is used to transmit and receive safety messages. It supports a variety of periodic speeds so that the vehicle can occupy the media according to the priority of safety. The main algorithms of the SS-MAC are a distributed time slot sharing (DTSS) algorithm and a random index first fit (RIFF) algorithm. SS-MAC uses a circular recording queue to detect whether a time slot is available in real-time or not. A circular recording queue is periodically broadcasted to the vehicles to record the most recent status. DTSS is a decentralized time slot sharing scheme for a common agreement of time slot sharing and is to control the time slot sharing process between vehicles. RIFF is designed to help the vehicles occupy a proper time slot for sharing in the condition of the commitment of periodic broadcast requirements of all the vehicles and optimal utilization of channel resources in VANETs. DTSS is efficiently to share time slots and the RIFF algorithm is to create online vehicle slot matching, respectively. They showed the efficiency and high performance of SS-MAC through theoretical analysis and various simulations with MATLAB under the various driving scenarios and resource parameters. It is shown that SS-MAC is a time slot sharing MAC with reliability and minimal delay for safe message broadcasting and wide scalability of various scenarios in VANETs.

3.3. Applications

Shen et al. proposed CASD [12] that three-level safety actions to vehicles with regard to LoS (line-of-sight) and safety are classified into class 1 (in LoS and unsafe range), class 2 (in non-LoS but unsafe range), and class 3 (just in a safe range), as shown in Fig. 6. CASD [12] is designed to improve driving safety according to traffic conditions by exploiting a GPS navigation and VNs. It is assumed that vehicles share driving information such as trajectory, velocity, and distance between any two vehicles, and individual driver actions. In emergencies, CASD proactively uses this information to reduce the possibilities of accidents using avoidance maneuvers, as shown in Fig. 7. Thus, CASD works for cooperative driving with an action plan for neighboring vehicles and a dynamic path moving plan.

In an emergency environment, a user can observe the surrounding situation through a user interface. CASD exploits a hybrid action scheme. The first reaction is performed by a driver. The control system takes control of the vehicle in the absence of a proper driver action within a threshold time. The threshold time to take an action is optimized by exploiting vehicle mobility information (e.g., speed, position, and direction), driving behavior, and the distance between any two vehicles. For consistent coordination, only one vehicle can coordinate the maneuver plan for the sake of nearby vehicles, and other vehicles follow that plan.

To mitigate the scalability issue for safety applications in connected vehicle environments, Fallah et al. in [32] suggest making these applications aware of communication and network conditions by a combined design of application and communication layers. One of the challenges for such a combined design is to find safety performance measures to reflect system performance. The authors used vehicle tracking accuracy by relating it with vehicle warning system accuracy to demonstrate system performance. The analysis of the different measures particularly showed that network load control could correct physical layer packet losses. Moreover, the authors found that using a time-average packet error rate to compensate for the packet losses caused inefficiency, but the performance was improved when vehicle velocity accuracy was improved by altering the communication timing. The authors showed that application performance can be improved through hazard detection accuracy and alert generation delay. The main idea from the paper is that, instead of conventionally separating the application and communication layers, combining the layers can bring significant gains for connected vehicle safety applications.

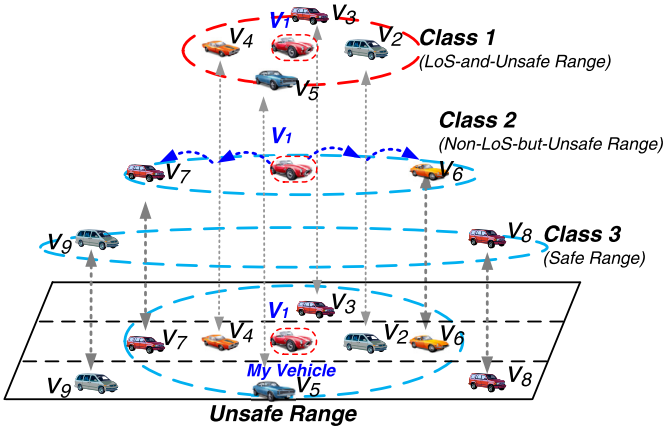


Fig. 6. Context-aware safety driving structure [12].

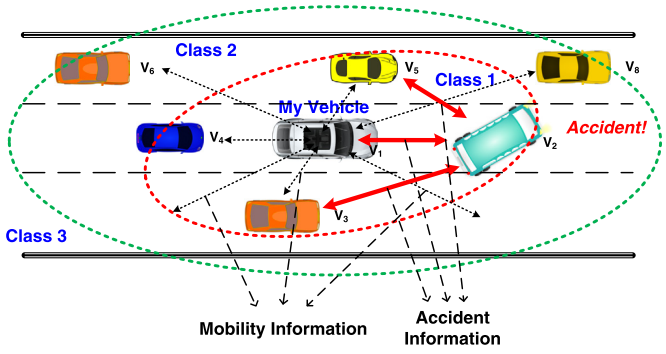


Fig. 7. Context-aware safety driving information [12].

Hadiwardoyo et al. proposed an OsmAnd [55] safe driving application for Android but modified OsmAnd to meet a smart navigation function that would create a network of vehicles [33]. This function gives a driver a warning message about the presence of approaching emergency vehicles including police cars and fire engines in a timely manner; this warning message allows the driver to take other routes. This can be used by cars, bicycles, or pedestrians; it is a plug-in application for OsmAnd and can construct a VANET where vehicles can send and receive notifying messages for the presence of nearby vehicles. The application is based on message dissemination, runs on GRCBox hardware, and is designed to provide V2V communication to commercial Android terminals. GRCBox used as a router inside a vehicle connects local networks to Android devices for external V2V communication; it has three modes: administrative, SOS, and civil mode. In the administrative

mode, emergency vehicles can broadcast messages received from other vehicles on current locations, routes, and destinations. In the SOS mode, vehicles can create SOS beacons that alert neighboring vehicles that a vehicle in the vicinity needs help. In the civil mode, the app in the vehicle only disseminates messages to neighboring vehicles in V2V communication, and the message is displayed on the screen in each vehicle. A message in this VN contains the following information fields: node id, time stamp, message type, a sender's current location, tracing route, and destination. The results of the field tests showed that GRCBox can run properly even in non-line-of-sight conditions in urban scenarios at up to 80 meters when the sender and receiver are on different streets. However, there were some disadvantages. The proposed system is based on V2V communication in VNs, but it is inefficient in one-way message dissemination in either administrative or SOS mode. This V2I communication lowers congestion conflict by avoiding heavy radio frequency occupation; in a traffic-congested intersection, the radio traffic conflict will dramatically increase in V2V communication. Another disadvantage is that it is impossible to prepare and decide in advance in the absence of overall traffic information from the TCC.

Sadeghi et al. proposed SafeDrive [34]. It is an autonomous application for driving safety in cities. SafeDrive assumes that a driver is equipped with brain sensors connected to a smartphone. A vehicle's devices, such as wheel speed sensor, front camera, and rear camera, are monitored, and their sensing data are transmitted to other vehicles or infrastructure nodes via a smartphone. A transportation control system (TCS), which is also called a traffic control center (TCC), collects information from the smartphone, which includes the vehicle speed, the mental fatigue of drivers, and the detailed driving information through step 1 and step 2. The TCS calculates a collision probability by exploiting the mental fatigue levels of drivers and the current states of moving vehicles. Using the probability, the TCS alerts each driver about possible dangers by sending warning messages through step 3 and step 4, as shown in Fig. 8.

In VNs, beaconing is an important mechanism for safety message exchange that provides driving information to safety applications. Luong et al. in [35] proposed beacon rate optimization (BRO) scheme in safety message exchange through an analytical model that evaluates the performance of single-hop broadcast and considers the impact of hidden terminals, direct collisions, and traffic density. The authors also proposed a utility maximization framework to optimize the beacon rate in highway scenarios; the framework considers the reliability of safety messages as well as neighbor vehicle information and provides an analytical solution through the Karush-Kuhn-Tucker conditions. Based on the analytical solution, the results showed that the optimal communication rate in different traffic densities can fulfill safety requirements. Furthermore, the authors also obtained feasible regions for different packet delivery ratios (PDRs) and found that when the traffic density increases, the feasible region shrinks.

3.4. Comparison of systems, protocols, and applications

Table 3 presents a comparison of the different smart transportation systems, protocols, and applications for driving safety in terms of advantages and disadvantages. The comparisons in terms of theoretical analysis, simulation, real implementation, and complexity are also presented in the Table 3. Complexity means the degree to which the related scenario is complex and difficult to implement in a real environment, such as a real vehicle or real mobile node.

SANA [13] is a navigation system designed to protect vehicle drivers and pedestrians and to provide efficient smartphone power consumption while vehicle and pedestrians meet at a roadway

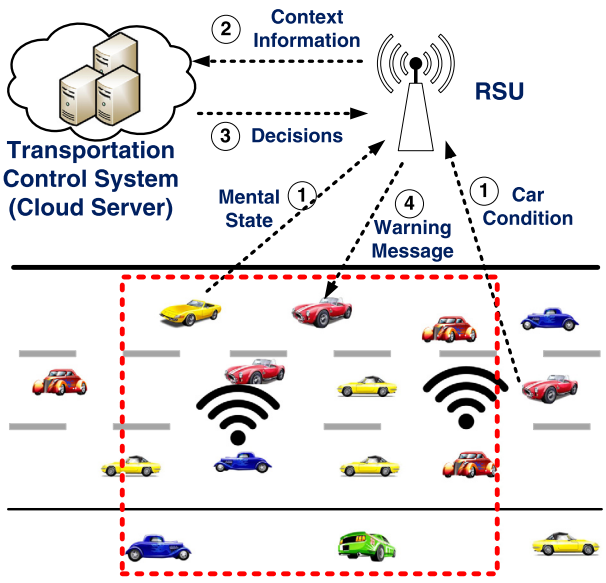


Fig. 8. Operation of SafeDrive application using HumanNet [34].

or an intersection. However, the battery consumption in pedestrians' smartphones increases rapidly at crowded intersections. CBPRS [22] is a cloud-based system that focuses on protecting pedestrians considering traffic situations; however, there is no clear transition from driver mode to pedestrian mode, and no power guarantees can be made. FTRA [23] uses a distributed node control scheme rather than a centralized cloud-based strategy to make fair transmission rate, but because of the distributed node control scheme, transmission power and message delivery rate are not optimized with interconnection. This proposal also does not consider the dramatically changing vehicle density, the traffic conditions according to urban traffic signaling systems, or the integration of transmission power and transmission rate.

Based on I2V communication, WPCF [24] reduces channel collisions so that safety messages between vehicles can be delivered efficiently. It is efficient in that infrastructure components such as RSUs can quickly transmit messages to vehicles, but it is inefficient because the messages must go through the infrastructure having RSUs for V2V communication, that is, V2I2V communication. LMA [25] is based on V2V communication and a scheme to deliver safety messages among vehicles without infrastructure elements such as RSUs. V2V communication is efficient, but this is not desired in heavy traffic areas because of contention-based processes. DMMAC [26] proposes channel scheduling based on vehicle behavior information; it is a distributed protocol and provides mobility-based clustering. STMAC [27] is a scheme to increase message transmission efficiency in rush hours by considering both spatial and temporal coordination at the same time. To support efficient V2V communication, message transmission scheduling of infrastructure is desired.

D2D [28] uses communication between devices; it is similar to V2V and V2I communication, but there are no detailed optimized techniques. V-D2D [29] employed vehicular device-to-device (V-D2D) communications to provide complementary channel for data transmission as well as cellular network and DSRC in VANETs. LORA [30] proposes a hybrid system that integrates physical layer and MAC layer in highway scenarios; it uses fuzzy neural network training and has a complex system.

CASD [12] provides three-step action plans with a pure communication-based safe driving strategy, but there are high costs for system implementation. CNAC [32] is a proposal for safety awareness that combines application and communication layers, but sophisticated information is needed in order to measure a neighbor-

Table 3
Comparison of systems, protocols, and applications for driving safety.

Domain	Name	Advantages	Disadvantages	Theoretical analysis	Simulation	Implementation	Complexity
Systems	SANA [13]	Low energy consumption and message delays by filtering out collision-irrelevant vehicles.	Quick consumption of smartphone battery in vehicle crowded places.	✓	✓	×	Low
	CBPRS [22]	Low smartphone battery consumption for switching an App's operation mode according to a collision risk level.	Without explicit mode changing in the smartphone app, no guarantee of power saving after switching mode from driver to pedestrian.	✓	✓	×	High
	FTRA [23]	Integrating cooperative vehicle safety systems and distributed fair transmission rate control into an optimization problem.	Without jointly optimizing the transmission power and transmission rate.	✓	✓	×	High
Protocols	WPCF [24]	Efficient V2I communication with PIF; Efficient handover.	Low communication efficiency via RSU for V2V communication, that is, the increased delay by V2I2V.	✓	✓	×	Mid
	LMA [25]	Space reuse due to directional antenna based the DCF protocol; Location and mobility awareness.	Packet collision due to a contention-based process.	✓	✓	×	Mid
	DMMAC [26]	Distributed protocol; Mobility-aware clustering	EDCA-based clustering process is required.	✓	✓	×	High
	STMAC [27]	Efficient V2V communication; Space reuse by using directional antenna and Tx power control	Infrastructure-assisted transmission scheduling.	✓	✓	×	High
	D2D [28]	Similar transmission rate in traditional V2V and V2I mode; accommodating V2V and V2I connections in a D2D mode.	Lack of detailed calibration and optimization in the proposal.	✓	✓	×	Low
	V-D2D [29]	First trial to model the urban road topology as a square area.	No validation on rural area.	✓	✓	×	Low
	LORA [30]	A hybrid system considering highway scenario, MAC-layer backoff, and PHY-layer propagation.	System complexity; Fuzzy neural network training process is needed.	✓	✓	×	High
	SS-MAC [31]	Similar results in highway and urban scenarios under many kinds of resource conditions.	Considering static resource assignment.	✓	✓	×	Mid
Applications	CASD [12]	Compatible with IEEE WAVE; Class-based vehicle category; Emergency motion planning.	Pure communication-based safe driving strategy; Implementation costs are high.	×	×	×	High
	CNAC [32]	Safety applications aware of communication and network conditions; The performance of safety applications is improved by the information of network conditions.	Needing more accurate information to estimate neighbors.	×	✓	×	Mid
	AAOSM [33]	OsmAnd safe driving Android application with a smart navigation function; Seamless running just with GRCBox hardware.	Need to integrate vehicles with infrastructure for V2X communications.	×	✓	✓	Low
	SafeDrive [34]	Autonomous driver safety application with brain sensor-based collision prediction.	The cost of implementation and communication of the SafeDrive is high.	✓	✓	×	Low
	BRO [35]	An optimal beacon rate control obtained through a utility maximization framework.	Higher beacon rate is required for various safety applications.	✓	✓	×	Mid

ing vehicle. For effective driving safety, SafeDrive [34] is an application for autonomous driving that uses information obtained from various sensors attached to vehicles, such as front camera, rear camera, and wheel speed sensor. BRO [35] adjusts beacon rates to increase channel utilization and is effective in highway scenarios. In the next section, we will survey studies related to driving efficiency.

4. Driving efficiency

In smart transportation, another important issue is driving efficiency. In most cases, driving efficiency focuses on vehicle travel time and fuel efficiency. Current real-time traffic-based navigation methods may bring poor driving efficiency because traffic congestion can occur in any road segments due to the lack of network-wide traffic coordination. Also, as electric vehicles become increasingly popular, efficient battery exchange is important as well. In this section, we survey driving efficiency related studies.

4.1. Systems

Kim et al. proposed a smart e-bus battery substitution scheme (SBUS) [36] for public transportation service using electric bus (e-Bus). SBUS executes efficient cloud-based e-Bus battery replacement at e-Bus stations using the buses' trajectories in urban road networks. SBUS suggests a scheduling algorithm to optimally minimize the waiting time for each e-Bus. TCC considers each bus's arrival time at a station and each bus's remaining energy to travel to another station for battery replacement given current road traf-

fic conditions to optimize the average waiting time of each e-Bus. Using the arrival and departure times for each e-Bus to and from each station, the optimization problem can be formulated as

$$q^* \leftarrow \arg \min_{q_i \in Q_{reachable}} \{T_{q_i} + T_s\}, \tag{2}$$

where q_i is a quick battery changing machine (QCM), $Q_{reachable}$ is the set of reachable QCMs for an e-Bus, T_{q_i} is the waiting time for q_i, and T_s is battery changing time. If an e-Bus has less battery power than the predefined threshold, it requests a list of e-Bus stations, $Q_{reachable}$, which it can reach with its remaining battery power so that its battery can be replaced, to the TCC for QCM selection. Specifically, the TCC compares the arrival and departure times for each e-Bus to a given reachable station and assigns a given e-Bus to the station with the shortest waiting time. They compared SBUS with two baselines (i.e., random and farthest), and the results showed that SBUS needed shorter average waiting times than the baselines.

Adler et al. in [37] proposed an online routing and battery reservation (ORBR) scheme to minimize the average waiting time of all electric vehicles at battery swap stations by recommending a travel path for each vehicle to meet overall benefits of all vehicles. ORBR suggests an algorithm that can balance the trip time of electric vehicles and the battery swap loads at the stations. The algorithm can also make reservation of the battery replacement of electric vehicles, considering all the battery changing stations in the driving routes of the electric vehicles. Based on a Markov decision process [56], dynamic programming with a linear model is used to quickly provide vehicle routing solutions using vehicle-mounted software that is connected to a central computer through wireless networks.

Shen et al. proposed a self-adaptive interactive navigation tool (SAINT+) [21], as a road navigation system that performs cloud-based vehicular traffic optimization in road networks. SAINT+ was particularly tailored to optimize both emergency service delivery to accident sites and navigation detour routes around the sites. The existing navigation systems (e.g., Tmap [57] and Waze [58]) suggest driving routes based on the current road traffic conditions, but these legacy navigation systems provide drivers with locally rather than globally (i.e., network-wide) optimal trajectories. A currently idle road can become congested if a navigation system directs all vehicles to travel that path. To improve traffic flow efficiency on the overall road network, SAINT+ [21] exploits a traffic congestion metric (called congestion contribution) with congestion contribution value per road segment in a target road network. Note that congestion contribution per road segment (as a virtual metric) is an estimated traffic congestion increase by a vehicle that enters the road segment or will visit it in near future.

In SAINT+ [21], for a vehicle V_a with a route P_{V_a} having a sequence of nodes (i.e., intersections): $P_{V_a} = \langle n_1, n_2, \ldots, n_u \rangle$, the E2E delay ($D$) can be formulated as:

$$D_u^{V_a} = \sum_{k=1}^{u-1} d_{(n_k, n_{k+1})}, \tag{3}$$

where $d_{(n_k, n_{k+1})}$ is road segment delay from the intersection n_k to n_{k+1}.

The Congestion Contribution (CC) $c_i^{V_a}$ [21] for vehicle V_a is modeled as:

$$c_i^{V_a} = 1 - \frac{D_i^{V_a}}{D_u^{V_a}}, \tag{4}$$

where $D_u^{V_a}$ is the E2E delay of a vehicle for a route P_{V_a} with u intersections, i.e., the travel time from its source n_1 to its destination n_u, and $D_i^{V_a}$ is the *sub-route delay* from the source n_1 to an intermediate intersection n_i:

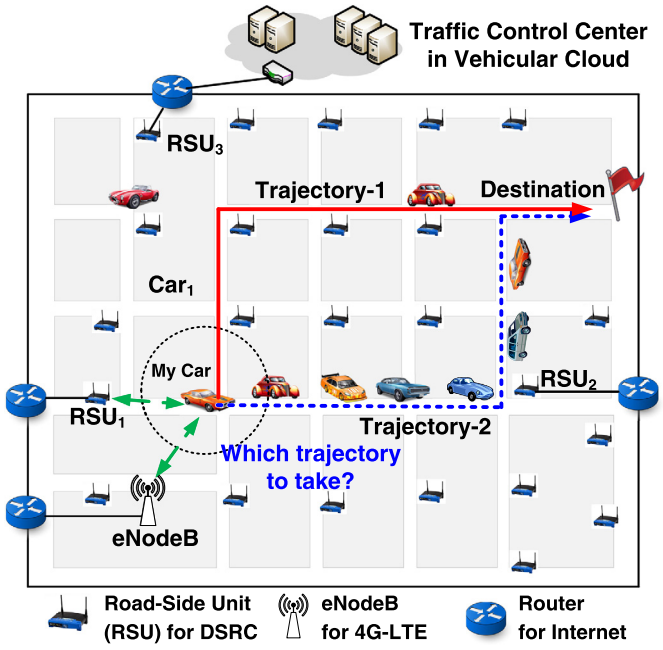


Fig. 9. SAINT+ navigation process [21].

$$D_i^{V_a} = \begin{cases} \sum_{k=1}^{i-1} d_{(n_k, n_{k+1})} & \text{for } i \geq 2, \\ 0 & \text{for } i = 1, \end{cases} \tag{5}$$

where $d_{(n_k, n_{k+1})}$ is the delay for a road segment (n_k, n_{k+1}) in the vehicle's route. Here we define $D_1^{V_a}$ as 0 because it is travel delay at the beginning of the route, then the corresponding CC $c_1^{V_a}$ is 1.

In the design of SAINT+, the $c_i^{V_a}$ on each road segment of a route is constant, so a Congestion Contribution Step Function (CCSF) $C_i^{V_a}(x)$ is defined for the sub-route delay x from a vehicle's source to an intermediate location on its path:

$$C_i^{V_a}(x) = c_i^{V_a} \cdot u(x - D_i^{V_a}), \tag{6}$$

where $u(x - D_i^{V_a})$ is a shifted unit step function defined as:

$$\begin{cases} 1 & x \geq D_i^{V_a} \\ 0 & x < D_i^{V_a} \end{cases} \text{for } i \in (1, u). \tag{7}$$

For a directed road network graph G with n vertices (i.e., intersections), a Congestion Contribution Matrix (CCM) is defined as:

$$M = \begin{bmatrix} 0 & m_{1,2} & \ldots & \ldots & m_{1,n} \\ m_{2,1} & 0 & & m_{i,j} & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & & m_{n-1,n} \\ m_{n,1} & \ldots & \ldots & m_{n,n-1} & 0 \end{bmatrix}, \tag{8}$$

where $m_{i,j}$ is a *cumulative link CC* of edge $e_{i,j}$, i.e., the sum of CCs from all vehicles that are passing and will pass through edge $e_{i,j}$.

As shown in Fig. 9, the TCC in the vehicular cloud calculates globally optimal route (i.e., My Car in Fig. 9) based on the congestion contribution matrix. The optimal route is sent to the vehicle via vehicular or cellular networks. As shown in Fig. 10, each road segment has an accumulated congestion contribution value that indicates the current and future congestion caused by the current and near-future passing vehicles in the road segment; a road segment has a higher congestion contribution value when the TCC

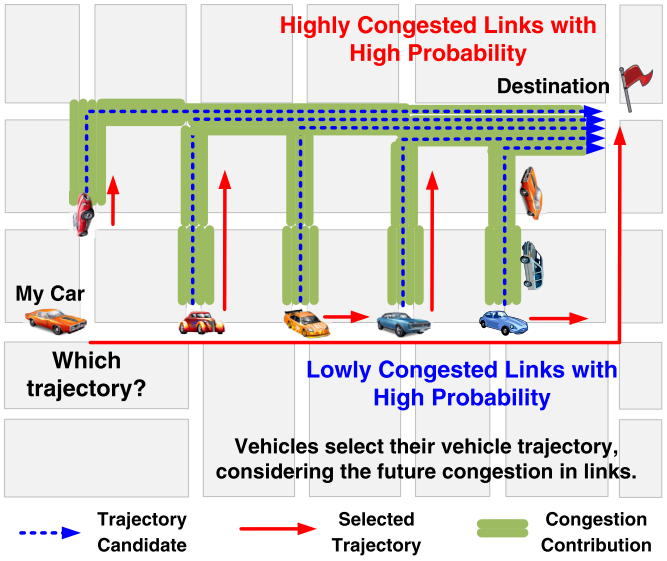


Fig. 10. Self-adaptive interactive navigation tool+ [21].

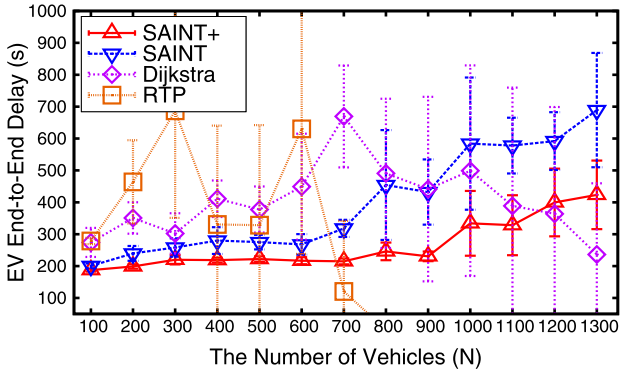


Fig. 11. The E2E delay comparison of multiple emergency vehicles delivery between SAINT, Dijkstra [48] and RTP.

guides more vehicles to use that segment. For global traffic optimization, SAINT+ suggests routes with minimal congestion contributions. Occasionally, this requires that vehicles detour within a bounded distance, that is, with a predefined extended travel time, compared with the shortest travel time based on the current vehicular traffic statistics.

In emergencies, it is important to deliver emergency vehicles to accident sites but also to relieve traffic congestion around the sites. SAINT+ is based on the congestion contribution model to enhance globally optimization of vehicle path, but to guarantee the fast delivery of an emergency vehicle to the accident spot, SAINT+ increases the congestion contribution values along the road segments of the route taken by the emergency vehicle to artificially create a congested path. Other vehicles then cannot use the path of the emergency vehicle and are guided to detour to the other shortest paths with lower congestion contribution values. After an emergency vehicle passes by the road segments on the path with the artificial congestion contribution values, the road segments of the path are restored with original congestion contribution values, so other vehicles can use the path as usual. For reducing congestion around an accident area, SAINT+ divides an emergency area into three zones, as shown in Fig. 12. Vehicles in Zone 0, the road segment with the accident, are guided to quickly leave the accident area. Vehicles in Zone 1, that is, the one-hop road segments neighboring the accident road segment, can travel to Zone 1 and Zone 2, that is, the road segments outside Zone 1, but they can-

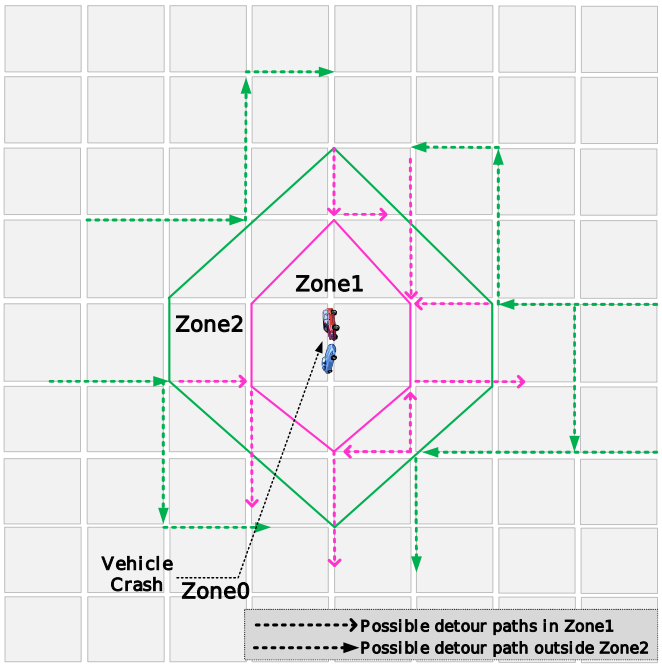


Fig. 12. Evolved self-adaptive interactive navigation tool for emergency service [21].

not travel to Zone 0. In Zone 2, vehicles can travel through Zone 1 when the traffic is light in Zone 1. In this way, this zone-based navigation scheme shows effective detouring for vehicles around an accident area. As shown in Fig. 11, the E2E delay of multiple emergency vehicles in SAINT+ scheme outperformed SAINT [48] as the number of vehicles increases. The performance of the Dijkstra [59] and RTP showed feasible results in a small number of vehicles. However, as the number of vehicles increased, the performance looked enhanced. This result might be caused by the shortage of data due to the decrease of the delivery success ratio. Through the extensive and realistic simulations based on SUMO [49] and OpenStreetMap [50] using a real-world road network in Minneapolis, MN, US, SAINT+ outperformed other schemes for the travel time of the emergency vehicles.

Koukoumidis et al. suggested SignalGuru [14], a green driving assistant system. SignalGuru provides an optimal driving speed for a driver to enhance the vehicle efficiency in terms of fuel consumption, air contamination, and better traffic flow by avoiding sudden or frequent stop-and-go. A vehicle driver with SignalGuru can manipulate the vehicle speed to avoid a sudden stop by leveraging the traffic signal changing information when heading toward an intersection. In the current SignalGuru system, the V2I communication is based on a cellular link [14]. This system has three merits: (i) it can monitor and predict traffic signal changes by leveraging a windshield-mounted smartphone with a camera and taking pictures of the traffic lights to record the traffic light scheduling, as shown in Fig. 13. This traffic light scheduling reverse engineering can provide vehicles with green light optimized speed advisory (GLOSA); (ii) it also enhances processing accuracy and speed by concatenating information from a smartphone obtained from inertial sensors, reducing the image processing overhead for detecting traffic signal phases (i.e., patterns and timing); and (iii) several user-based applications can be layered over the traffic signal prediction system. SignalGuru also suggests traffic signal-adaptive navigation (TSAN) to provide an efficient detour route for minimizing stop duration time and red-light encounter frequency at intersections, as shown in Fig. 13. SignalGuru with GLOSA and TSAN outperforms the other legacy schemes in fuel consumption, and it increases average vehicle driving distance.

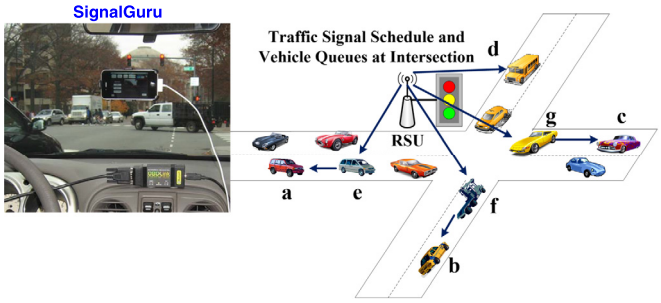


Fig. 13. SignalGuru enabled iPhone display [14].

Kalim et al. [38] proposed a crowd-sensing application to estimate road conditions (CRATER). CRATER is a smartphone app that supports participatory users to upload multiple sensor data to a cloud server. A centralized database in the cloud server aggregates the sensor data from multiple users to estimate the conditions of road networks. CRATER sensors do not require any user input; the server periodically retrieves data from the centralized database, processes the data, and places the results in the database. They presented a public website that could show the real-time road conditions in a road network: Through real-world testing, CRATER's detection rates were approximately 90% for potholes and 95% for speed bumps.

4.2. Protocols

To improve driving efficiency, low-latency packet forwarding with high packet delivery is required. We survey different papers related to packet forwarding in VNs in the aspect of I2V, V2V, V2I, and V2U (Vehicle to UAV) communications.

To improve the performance of V2I packet forwarding in light-traffic environments, Jeong et al. in [39] proposed trajectory-based data forwarding (TBD) for light-traffic VNs. Fig. 14 shows the V2I data-forwarding process in VNs. TBD [39] leverages vehicle trajectory information to formulate a carry-and-forward delivery model. A packet carrier based on the expected delivery delay (EDD) model selects a vehicle to relay a packet. The main features of TBD are: (i) an accurate link delay model; (ii) the geographically shortest path instead of the smallest-angle path toward the destination of a packet at the selection of a next-hop vehicle; and (iii) a trajectory-based forwarding model.

Assume that a packet is with a vehicle that will travel along a trajectory through a sequence of intersections: $1 \rightarrow 2 \rightarrow \cdots \rightarrow M$. The total time for carrying the packet from the intersection i to j along the vehicle's trajectory, C_{ij}, can be formulated as, $C_{ij} = \sum_{k=i}^{j-1} l_{k,k+1}/v$.

The expected E2E delay D for the vehicle can be calculated as follows:

$$D = \sum_{j=1}^{M} ((\prod_{h=1}^{j-1} P^c_{h,h+1}) \times (C_{1j} + \sum_{k \in N(j)} P'_{jk} D_{jk})), \tag{9}$$

where $P^c_{h,h+1}$ is the carry probability for a vehicle traveling from the intersection h to the adjacent intersection $h+1$, and $\prod_{h=1}^{j-1} P^c_{h,h+1}$ is the carry probability for a vehicle traveling from the intersection 1 to j. $\sum_{k \in N(j)} P'_{jk} D_{jk}$ is the EDD when the packet is forwarded from the current vehicle to a next-hop vehicle moving toward the intersection k where P'_{jk} is forwarding probability.

Furthermore, TBD also explores the scenario where packets are forwarded to multiple RSUs or Access Points (APs). Through theoretical analysis and simulation, it is shown that TBD outperforms previous V2I communication scheme in different aspects.

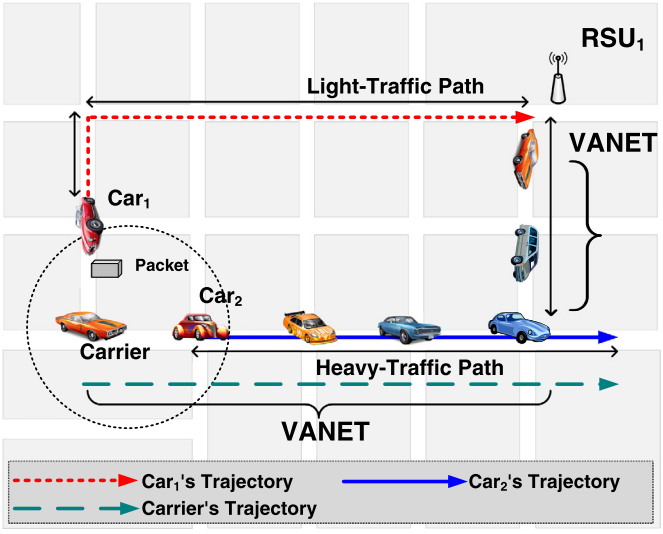


Fig. 14. Packet-forwarding process in V2I communication.

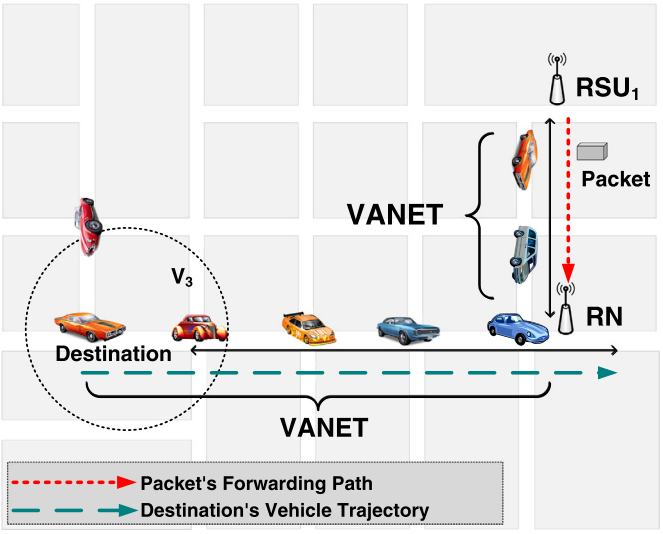


Fig. 15. Packet-forwarding process in I2V communication.

There are many scenarios that require a vehicle or a TCC to quickly distribute data packets to a target moving vehicle as a packet destination in an area. Jeong et al. in [40] proposed a trajectory-based statistical packet forwarding (TSF) for multi-hop I2V communication. The goal of TSF is to deliver packets as quickly as possible from an RSU (or AP) to a destination vehicle using relay nodes at the intersections that are used as temporary packet holders. Traditional packet-forwarding schemes (e.g., TBD [39]) mainly explored forwarding packets from a moving vehicle to a fixed destination in the multi-hop V2I communication. In contrast, TSF aims to improve the rate of successful packet forwarding from an RSU (or AP) to the moving vehicle in the multi-hop I2V communication and also maintains a low packet delivery delay. Fig. 15 shows the I2V data-forwarding process in VNs. An RSU as a packet source delivers a packet along the packet's forwarding path toward a target point at an intersection having a relay node, where the packet destination vehicle will pass through. To achieve the multi-hop I2V data delivery, TSF calculates an optimal rendezvous point (as a target point) of a packet and the destination vehicle of the packet, and then the packet is forwarded to the target point.

Formally, given a desired delivery probability α, an optimal rendezvous point selection can be formulated as:

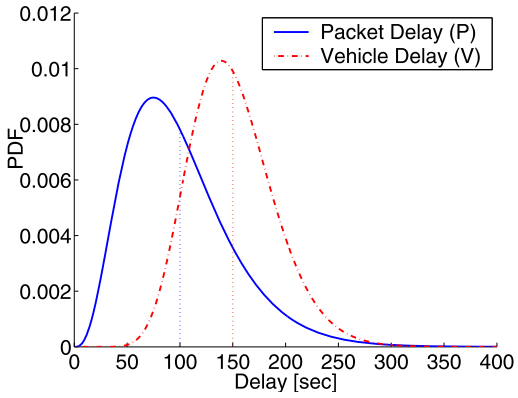


Fig. 16. An example of packet delay distribution and vehicle delay distribution [40].

$$i^* \leftarrow \arg\min_{i \in I} E[V_i], \quad \text{subject to } P[P_i \le V_i] \ge \alpha, \tag{10}$$

where I is the set of intersections that the destination vehicle will pass through, P_i is the packet delay after which a packet would be forwarded to target intersection i, V_i is the travel time of the destination vehicle moving from its current position to target intersection i, and $P[P_i \le V_i]$ is the probability for a packet that will arrive at an intersection i earlier than the arrival of the destination vehicle. $P[P_i \le V_i]$ can be calculated as:

$$P[P_i \le V_i] = \int_0^{TTL} \int_0^{v} f(p)g(v)dpdv, \tag{11}$$

where $f(p)$ and $g(v)$ are the probability density function (PDF) of packet delay p and vehicle travel time v, and TTL is a packet's lifetime Time-To-Live. The authors theoretically analyze the optimal value of packet delivery delay by utilizing the delivery delay distribution of packets and the travel delay distribution of the destination vehicle. Fig. 16 shows an example of PDFs of packet delay P and vehicle delay V.

Both TBD and TSF can be used for V2V packet forwarding where a packet can be forwarded from a source vehicle to an RSU (or AP) via the TBD protocol and then forwarded from the RSU (or AP) to a destination vehicle via the TSF protocol. To explore better V2V packet forwarding without using infrastructure nodes (i.e., RNs) as temporary packet holders in a road network, Jeong et al. proposed travel prediction-based data forwarding (TPD) [41] for light-traffic VNs. TPD is designed for multi-hop V2V communication based on a graph that predicts vehicle encounter events. The events are modeled by the encounter probability on a road segment and at an intersection.

The probability that two vehicles V_a and V_b will encounter each other on a road segment can be calculated as follows:

$$\mathrm{P}(V_a \otimes_{1,2} V_b) = \mathrm{P}(T_{a1} \le T_{b1} \cap T_{a2} \ge T_{b2}), \tag{12}$$

where "$\otimes_{1,2}$" is defined as "encountering on road segment $E_{1,2}$". Assume that n_1 and n_2 are the endpoints of the encountered road segment $E_{1,2}$ for vehicles V_a and V_b. V_a travels from n_1 to n_2, while V_b travels from n_2 to n_1. T_{a1} and T_{a2} are the time instants when V_a passes through n_1 and n_2, respectively. Similarly, T_{b1} and T_{b2} are the time when V_b passes through n_1 and n_2, respectively.

The probability that V_a and V_b encounter and communicate with each other at an intersection n_x where V_a arrives at intersection n_x earlier than V_b can be calculated as follows:

$$\mathrm{P}(V_a \otimes_x V_b) = \mathrm{P}\Big(T_{b(j,x)} \ge T_{a(i,x)} \cap (T_{b(j,x)} - T_{a(i,x)})S_b \le R\Big), \tag{13}$$

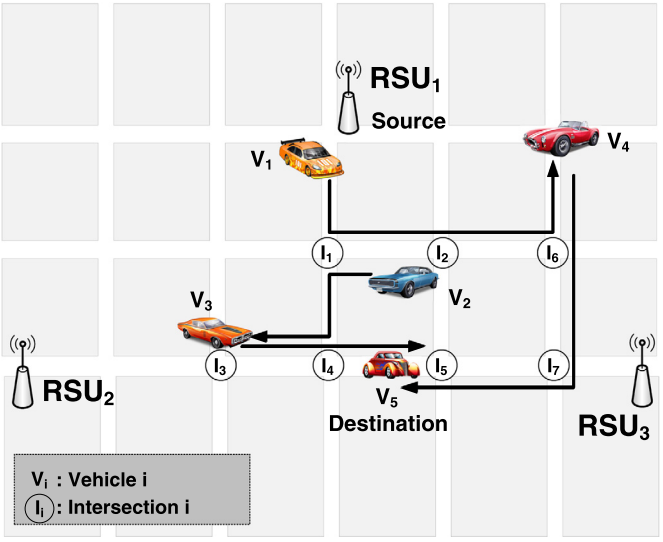


Fig. 17. The encounter graph construction in TPD for V2V communication [41].

where "$\otimes_x$" is defined as "encountering at intersection n_x" and R is the communication range. $T_{a(i,x)}$ and $T_{b(j,x)}$ are the arrival time at n_x when V_a and V_b move from n_i of $E_{i,x}$ and n_j of $E_{j,x}$ to n_x, respectively. S_b is the expected speed of vehicle V_b. The probability that V_a and V_b encounter and communicate with each other at an intersection n_x where V_a arrives at intersection n_x later than V_b can be calculated as follows:

$$\mathrm{P}(V_a \otimes_x V_b) = \mathrm{P}\Big(T_{a(i,x)} \ge T_{b(j,x)} \cap (T_{a(i,x)} - T_{b(j,x)})S_b \le R\Big). \tag{14}$$

In TPD, a vehicle encounter graph is also proposed based on shared trajectory information for packet forwarding. Fig. 17 shows that the encounter graph is constructed based on the trajectories of the vehicles. Through the vehicle encounter graph, TPD formulates an optimal forwarding sequence for a packet from a packet source to a packet destination. TPD also seeks to minimize E2E packet delivery delay under a defined delivery ratio threshold by selecting a subset of encountered vehicles. In Fig. 17, V_i and I_j mean vehicle i and intersection j, respectively. Vehicles V_1 to V_5 are moving on the target road network, and intersections I_1 to I_7 are in the road network. A vehicle V_5 was selected as the packet destination. It is supposed that vehicle V_1 wants to forward packets to a destination. First, vehicle V_1 expects to meet vehicles V_2 and V_4, so intersection I_2 and I_4 are selected according to the expected encounter sequence. Since the vehicle V_2 can meet the vehicle V_3 under the condition that V_1 meets V_2 first, the intersection I_3 is selected after I_2 is selected. The intersection I_3 precedes I_4 because the expected meeting time of V_2 and V_3 is earlier than the expected meeting time of V_1 and V_4. The extensive simulation demonstrates that TPD can achieve a short delivery delay and a high delivery ratio.

Fatemidokht et al. in [42] propose a routing protocol named VRU, which is composed of two data routing schemes such as VRU_vu and VRU_u. This protocol is designed to connect communication links and detect malicious nodes in VANETs using an unmanned aerial vehicle (UAV) when a network link is disconnected between vehicles. The VRU_vu uses UAV to progressively select road segments and to collect information about road segment connection. The VRU_u is a reactive routing scheme to find routes between UAVs, which uses the Ant Colony Optimization (ACO) algorithm [60] to find the best path between UAVs. Through extensive simulation, it is demonstrated that the VRU routing protocol can not only reduce E2E latency and routing overhead, but also increase packet delivery rate. The advantage is that the UAVs

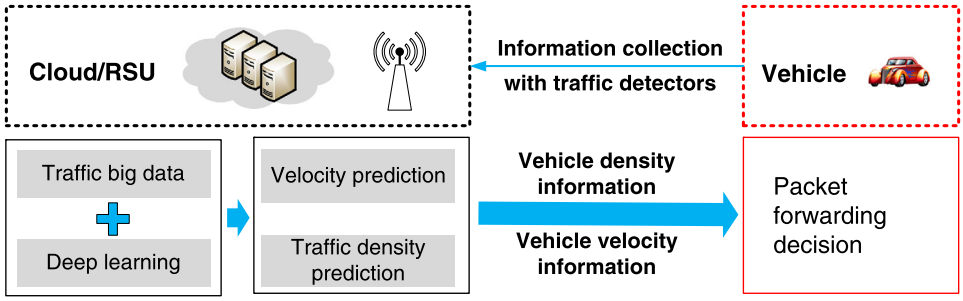


Fig. 18. Big data collection and prediction result dissemination [43].

can connect the stations where communication disconnection occurs in VANETs, thereby achieving good performance. The potential issue is that this protocol cannot be exploited continuously, due to the limitation of continuous flying time of UAVs in the air.

An et al. in [43] propose an offline traffic big data assisted communication scheme (BDAC) for VANETs. This scheme uses one month of historical traffic big data to obtain vehicle density and speed, and then uses the prediction results for the next 5 minutes to improve the multi-hop broadcast V2X communication protocol for VANETs. This protocol consists of the prediction part and the forwarding part. The predictions of average vehicle speed and traffic density based on offline traffic big data are performed in the cloud or an RSU at 5 minute intervals, as shown in Fig. 18. The predicted results are disseminated in a bundle (accumulated data at least 5 minutes) from an RSU to vehicles in a vicinity with low communication overhead. Thus each vehicle uses the predicted information for online packet forwarding.

4.3. Applications

Sun et al. proposed a global and dynamic route planning (GDRP) scheme [44] for smart transportation to release urban traffic congestion. GDRP is based on wireless sensor networks to monitor congestion in real-time and provides an optimal solution through a global and dynamic travel path planning algorithm. Smart sensing devices installed in crash barriers along the road can monitor the traffic flow by counting the passing vehicles. This measured information is gathered by local sink nodes using the IEEE 802.11 or Zigbee protocol. A data center concatenated all data collected from all the local sink nodes via long-distance wireless communication (e.g., WiMax, 3G, and 4G-LTE) to share traffic information for the whole city. GDRP suggests an improved Dijkstra's algorithm for weight change of routes. The simulation of the proposed algorithm, which is based on MATLAB, shows that the efficiency of road traffic flows can be improved, road capacity can increase, and the overall traffic congestion of the transportation network is well-balanced in the whole road network.

Giang et al. proposed smart transportation fog computing [45] called STFC for VANET applications. Although many VANETs use cloud infrastructures, they cannot fully satisfy VANET requirements due to the frequent movement of vehicles and their strict delay requirements. Fog computing is a promising paradigm because computation infrastructures are closer to the network edge, supporting latency-sensitive applications, but it is challenging to spread fog computing functions across networks due to the distribution natures of application development, such as message transferring and data sharing models in fog systems. STFC [45] provides an overview of development requirements for an application model in smart transportation. Fig. 19 shows the layer of cloud, content delivery network (CDN), and peer-to-peer (P2P) edge in a fog computing system.

The requirements of the application model and programming abstraction in fog computing for smart transportation systems

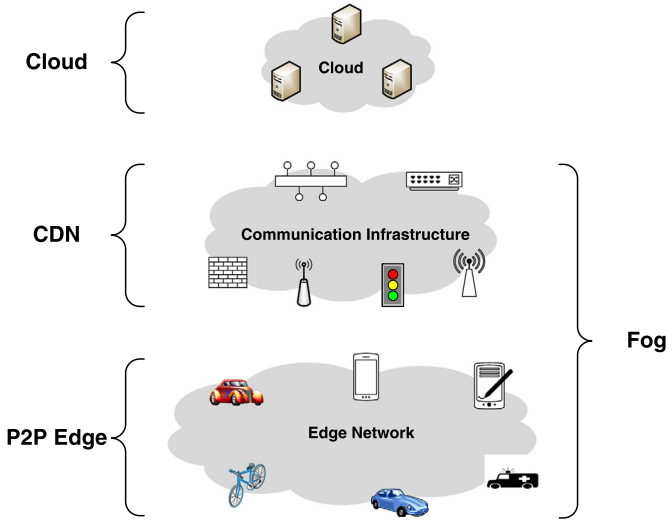


Fig. 19. Smart transportation application in fog computing [45].

are (i) modularity, (ii) reusability, (iii) scalability, (iv) context-awareness, and (v) high-level abstraction. Modularity means that an application can be deployed without affecting the whole system. Reusability means the module can be used by other applications without needing to be changed. Scalability allows an application to manipulate a large amount of vision data from cameras in a large area in smart transportation systems. Context-awareness refers to providing context information (e.g., a vehicle's physical location and in-vehicle devices' states) to developers so that they can make context-aware applications. The meaning of high-level abstraction is how heterogeneous computations in various devices can be described and coordinated or how they interact with each other. The requirements of fog computing platforms in smart transportation systems include (i) guaranteed low latency networks in particular, (ii) decentralized computation applications, and (iii) data-flow-based communications among a lot of devices.

Zhou et al. in [46] proposed a workload offloading algorithm considering energy-efficiency with low-complexity distributed vehicular edge computing, which is based on a consensus alternating direction method of multipliers (ADMM). ADMM is a solution to handle distributed convex optimization problems and takes iterative decomposition coordination procedures, which means that a problem is decomposed into subproblems and processed in parallel. Offloading workload in an energy-efficient manner can be formulated to minimize the overall energy consumption and the latency of all the user equipment as nodes. Latency includes local computing latency, data transmission latency, waiting latency, and handover latency. They suggested an extension of ADMM, so-called, a consensus ADMM-based distributed algorithm with the features of decreasing signaling overhead and increasing scalability, compared to the central approach ADMM. It is different from

Table 4
Comparison of systems, protocols, and applications for driving efficiency.

Domain	Name	Advantages	Disadvantages	Theoretical Analysis	Simulation	Implementation	Complexity
Systems	SBUS [36]	The reduction of overall waiting time for e-Bus battery exchange.	Restricted performance evaluation; Simple scheduling algorithm; No considering for a global optimization.	✓	✓	×	Low
	ORBR [37]	Balance between travel time and battery swap loads; Guaranteed battery replacement via reservations.	Centralized battery swap scheduling.	✓	✓	×	High
	SAINT+ [21]	Virtual path reservation scheme; Zone-based emergency event protection; Dynamic traffic flow control around an emergency event location.	Centralized navigation process; Storing double congestion matrices for multiple emergency vehicles.	✓	✓	×	Mid
	SignalGuru [14]	Optimal routing using traffic light states instead of traffic condition in the road.	The cost for the implementation of the SignalGuru; Overhead of TCC or edge computing to process many data.	×	×	✓	Mid
	CRATER [38]	Sensing without user input; Multiple machine learning techniques for prediction; Results freely accessed by the public.	Quick power consumption for smartphone.	×	×	✓	Mid
Protocols	TBD [39]	Efficient multi-hop V2I communication using a vehicle trajectory; Geographical-shortest-path-based metric to select a relay vehicle.	The cost of probability computation and implementation; A less realistic vehicle traffic environment.	✓	✓	×	Mid
	TSF [40]	Packet forwarding to moving vehicles for multi-hop I2V communication; Utilizing shared trajectory information; An optimal rendezvous point model.	The cost of implementation and communication; Privacy issue by trajectory sharing.	✓	✓	×	High
	TPD [41]	A multi-hop V2V or I2V communication with intermediate carry vehicles; Light traffic environment; Vehicle encounter graph; Without infrastructure.	The cost of implementation and communication; Privacy issue by trajectory sharing.	✓	✓	×	High
	VRU [42]	Lowering the E2E delay and overhead; AI assisted protocol.	Limitation of consistent flight of UAVs.	✓	✓	×	Mid
	BDAC [43]	Low data communication overhead; No real-time routing computation required.	Storage to gather and store past traffic big data.	×	✓	×	Mid
Applications	GDRP [44]	Optimal solution through a global and dynamic travel path planning algorithm based on real-time traffic condition and road capability.	The cost of implementation and communication protocol.	×	✓	✓	Low
	STFC [45]	Using fog computing instead of cloud computing for latency sensitive services.	Battery restriction of edge devices to process data as edge computers.	×	×	×	Mid
	EEEC [46]	Higher performance with dynamic offloading.	No deals to minimize delay.	✓	✓	×	High
	UAV ITS [47]	UAV used instead of report agents, fixed RSU, speed camera, and police eye.	Restriction of unmanned aerial vehicle.	×	✓	×	Mid

the ADMM approach in the following points. ADMM employs alternating or sequential primal variables to update. On the other hand, the distributed approach uses a series of local variables to separate related objectives and constraints for the optimization problem. The hierarchy of this framework is composed of three layers, i.e., the control layer, the Vehicular Edge Computing (VEC) server layer, and the VN layer. A centralized controller in the control layer is for the resource allocation and handover management between two adjacent cells. In the VEC server layer, VEC nodes co-locate with homogeneous servers. In the VN layer, the road is divided into the corresponding segments according to the transmission coverage of RSUs. They validated their algorithm with a SUMO [49] simulator and a map of OpenStreetMap [50]. The proposed algorithm can reduce the energy consumption by dynamically adjusting the offloading portion, so it outperforms the static offloading algorithm.

Menouar et al. [47] introduced an unmanned aerial vehicle-enabled intelligent transportation system (UAV ITS); the next generation of ITS involves integrating connected and autonomous vehicles. These two technologies are important for fully self-driving transportation systems and are currently verified in many countries; they are also crucial for ITS UAVs to connect wireless links with vehicles in proximity for driving efficiency and road safety. Menouar et al. expected that ITS UAVs will play a crucial role in enforcing traffic laws and providing efficient traffic information to road users. The authors suggested several applications and challenges with ITS UAVs such as flying accident report agents, flying RSUs, flying speed cameras, flying police eyes, and flying dynamic

traffic signals. For example, an ITS UAV can be present at an accident and assist the rescue team by identifying the shortest and fastest path for the rescue team to reach the accident location and sending detailed information about the situation, such as the extent of an accident and the number of related persons through videos and photos. ITS UAVs can be used as flying RSUs equipped with DSRC to monitor traffic where there are no fixed RSUs on highways. Menouar et al. also suggested several challenges to utilizing UAVs for ITS applications, including regulations for ITS services, security and privacy, and limitations of UAV hardware such as limited battery life (usually half an hour), signal transmission range, and maximum flying speed.

4.4. Comparison of systems, protocols, and applications

We compare different systems, protocols, and applications for driving efficiency in smart transportation in terms of advantages and disadvantages in Table 4. SBUS [36] provides battery replacement for electric buses using predefined routes, while ORBR [37] provides battery reservation for electric vehicles using random travel paths; ORBR uses centralized battery exchange scheduling. SAINT [48] is a cloud-based efficient navigation tool, and SAINT+ [21] is an advanced version of SAINT that provides optimized navigation paths, considering the fast movement of emergency vehicles as well as usual vehicles. SAINT+ is a centralized scheme to provide navigation. SignalGuru [14] provides optimal routing using traffic lights instead of traffic conditions; it focuses on optimizing driving speed to reduce frequent stop-and-go at the intersections. A smartphone application, CRATER [38], uses sensor information provided by smartphones; it makes quick power consumption for smartphone batteries.

TBD [39] is based on V2I communication and provides vehicles with efficient data forwarding by considering vehicle trajectory, although it is evaluated in a less real vehicle traffic environment. TSF [40] also presents an efficient data forwarding scheme by utilizing shared vehicle trajectory information in I2V communication. TPD [41] is different in that it is path prediction-based data forwarding, and it uses V2V communication. VRU [42] is a routing protocol with UAV's support to link road segment connections in VANETs. Due to a limitation of flight capacity of UAV, VRU [42] cannot be employed continuously. BDAC [43] is a V2X communication protocol assisted with past traffic big data from RSU in VANETs.

GDRP [44] is a proposal to monitor urban traffic congestion and suggest efficient travel paths. STFC [45] is a smart transportation application to provide efficient vehicular transmission utilizing fog computing; edge devices have battery restrictions to process data as edge computers. In the next section, we survey several security issues in smart transportation.

5. Security

Smart transportation encompasses both pedestrians and all types of vehicles, and security in smart transportation is deeply related to the safety of travelers as well as drivers and pedestrians. The VNs for smart transportation should support secure communication among vehicles, including simple authentication processes for fast V2I or I2V communication. However, it is challenging to provide vehicles with mobile authentications with firewalls in wireless networks due to the high mobility of vehicles. Wireless networks make these mobile communications possible, but they can be easily exposed to hackers. In the following subsections, we survey security in smart transportation.

5.1. Security attackers

Systems attackers are grouped into four categories: outsider/insider, malicious/rational, active/passive, and local/extended [61]. Inside attackers have privileged access to information technology systems and can include current or former employees, contractors and business partners. Inside threats can also come from non-employees, and it can often be difficult to detect inside attackers. Outside attackers are considered strangers to a system who infiltrate from outside. The difference between malicious and rational attacks are the intention of the attacks: Malicious attacks aim at simple destruction (of a network or other organization infrastructure for instance), whereas rational attacks aim at personal gain rather than harm to others. Active versus passive attacks differ in performing versus monitoring attack activities: Active attacks cause actual interference, whereas passive attacks only monitor networks and eavesdrop to look for any useful information. In terms of local versus extended attackers, the difference is geographic distance: Local attackers operate within a limited range, whereas extended attackers can operate across a network.

5.2. Security threats

The security threats in smart transportation include false information, denial of service (DoS), impersonation, eavesdropping, and hardware tampering [62–64]. False information attacks include fake data, false certificates, and false warning messages. For example, a Sybil attack [65] can give one vehicle multiple vehicle identities, which are false identities, by fabricating and sending multiple messages to the vehicle. Such an attack can cause vehicles to collide by spreading false vehicle position information to other vehicles.

DoS attacks overwhelm VNs by sending a large volume of packets to vehicles in a short period of time, causing their systems to be overloaded [66]. These attacks can pose serious threats, for instance by preventing emergency vehicle information from being delivered to vehicles in the area of an accident; when surrounding vehicles fail to receive the emergency vehicle information during a DoS attack, the accident can worsen because the communication in the VN has entirely broken down.

An impersonation attack is an attack in which a hacker disguises himself or herself to be an innocent vehicle or RSU and sends malicious messages throughout VNs as well as intercepting important messages [66]. An eavesdropping attack attempts to overhear communication messages within VNs and can collect confidential vehicle and driver information for malicious purposes [65] such as threats to drivers.

Message suspension attacks occur when an attacker removes packets from a network that hold critical information [67]. This causes incomplete messages to be received by the destination. Additionally, the attacker could inject the collected packets back to the networks to cause confusion and miscommunication in the network. Hardware tampering attacks intend to manipulate onboard hardware in a vehicle. For example, a brake system can be tampered and cause a life-threatening situation to the driver [64].

5.3. Security requirements

Preventing security attacks in VNs requires confidentiality, integrity, availability, non-repudiation, and privacy protection [67, 68]. Confidentiality could be implemented by the encapsulating security payload (ESP) of Internet protocol security (IPsec) [69]. Integrity can be provided by the IP authentication header [70], which provides vehicles with connectionless integrity and data origin authentication for IP datagrams. Availability means that a vehicle can

always access the wireless network. For example, a vehicle can obtain the wireless channel information from an RSU by an electronic signature (i.e., digital signature) to access DSRC channels. Service denial prevents vehicles or RSUs from receiving incoming messages.

Privacy protection in VNs is also important and can prevent a vehicle from being illegally identified or tracked while the vehicle is communicating with other vehicles. For this purpose, the vehicle is required to change its wireless network interface card's MAC address and IP address periodically which is called MAC address pseudonym. It is important that vehicles should be able to maintain a TCP connection transparently when they change their MAC and IP addresses [71].

5.4. Security technologies

Authentication and digital signature are two common ways to address security. Authentication provides the assurance that the contents of the message are not altered in any ways, and also determines the message source. In a VN, it is critical to be able to detect hackers pretending to be normal vehicle operators. To achieve authentication, public key infrastructure (PKI) is adopted and included in IEEE1609.2 [4]. Basically, PKI uses public and private key pairs to secure message exchange, but the conventional PKI is not secure enough for VANET requirements since verification time is too long, and conditional privacy, which guarantees that traceability is not achievable, is not addressed [72].

Digital signature is a common way to provide PKI to determine the integrity and authentication, and plays a very important role in VANET security. Digital signature can add to the existing authentication, and there are various digital signature algorithms. A digital signature implementation depends on the speed and size of the signature. Symmetric cryptography (i.e., shared key) and asymmetric cryptography (i.e., private and public keys) are two classes of cryptography, but the symmetric cryptography is not attractive in VANET in terms of key management (e.g., key distribution and key revocation). The most common adaption in VNs is based on the asymmetric cryptography using RSA, elliptic curve cryptography (ECC), and elliptic curve digital signature algorithms. [73]

5.5. Security for driving safety and efficiency

Bhoi et al. [74] proposed a secure routing protocol (SRP) for VANET for ITS services to eliminate road accidents and traffic congestion. SRP is a position-based hybrid routing protocol that uses the concepts of most forward within a radius (MFR) and border-node based most forward within a radius (B-MFR) [75]. Both are used to search for optimal nodes to relay data packets, and also to support data confidentiality by preventing vehicles from performing malicious attacks. SRP can search for efficient routes and forward data encrypted with a session key (SK) [76,77] and consists of three steps: (i) initialization, (ii) optimal node selection, and (iii) security module addition. In the last step, the station-to-station key agreement [78] is used to generate an SK [79] that can check whether a message is trapped from a malicious intruder. In the performance comparison among SRP, MFR, and B-MFR, SRP has a higher E2E delay than MFR and B-MFR due to the security mechanism to check the packet dropping attack. Because of the correct data forwarding to the genuine nodes rather than the malicious nodes, the packet delivery ratio of SRP is higher than the MFR and B-MFR protocols.

Fernandez et al. proposed secure vehicular IPv6 communication (SVIPv6) for the IPv6 network [80]. SVIPv6 focuses on V2I communication but uses hop-by-hop communication between vehicles, which depends on two main IPv6 security technologies (i.e., Internet Protocol Security [81,82,70,69] and Internet Key Exchange version 2 [83]). The two IPv6 security technologies provide vehicles with secure communication between a mobile router (MR) in a vehicle and a mobile server in a vehicular cloud. The MR has multiple wireless interfaces, such as 3G, IEEE 802.11p, WiFi, and WiMax, and can provide network connectivity to users and on-board devices in the vehicle, which are the vehicle's hosts (i.e., in-vehicle hosts). SVIPv6 proposes an architecture consisting of a vehicle ITS station (vehicle ITS-S), a roadside ITS station (roadside ITS-S), and a central ITS station (central ITS-S). A vehicle ITS-S is a vehicle with mobile network functions, having in-vehicle hosts and an MR. A roadside ITS-S is an RSU as a gateway for connecting a vehicle to a mobile network. A central ITS-S is a TCC that functions as a home agent for mobility management. SVIPv6 provides IPv6 continuity to in-vehicle hosts by supporting basic network mobility for control and data traffic. If no connection is available between a roadside ITS-S and a vehicle ITS-S, the vehicle ITS-S connects to a central ITS-S via cellular networks. SVIPv6 is implemented and analyzed in a real testbed that supports 3G and IEEE 802.11p wireless networks. The communication between the in-vehicle hosts and MR in the vehicle ITS-S is via IEEE 802.11g. The results show that SVIPv6 can provide secure communication to vehicle ITS-S, roadside ITS-S, and central ITS-S.

Moustafa et al. proposed authentication, authorization, and accounting (AAA) [84] to support security in VNs. The safety and reliability of data services in VNs are the goals of AAA, which authenticates vehicles as mobile clients. Vehicles can access the network and use various services provided by service providers. The protocol uses IEEE 802.11i for secure layer-2 links to ensure confidential data transfer between communication nodes, such as vehicles and infrastructure nodes. In an access network, wireless mobile ad hoc networks (MANETs) and APs are the components of the VN architecture in AAA. An access network is the back end of the network architecture, and a MANET is the front end that contains moving vehicles. APs provide the connection between the front-end and back-end networks following the standard of IEEE 802.11 WLAN architecture. The Kerberos authentication model [84] is used for AAA services. Kerberos authenticates the vehicles at an entry point of the network architecture only once, which can minimize the overhead and decrease communication delay on the layer 2 (i.e., data link layer) using 802.11i. Kerberos can also authorize access to a variety of other services. In the next section, we will summarize further research issues and challenges.

6. Safety and emergency management

This section describes safety and emergency management schemes that can affect network functions during the operations of emergency situations. In VNs, emergency situations can be automatically managed in terms of systems, protocols, and applications. In this section, these works were classified into two divisions in terms of macro emergency driving and micro emergency driving. Macro emergency driving is a method to increase the navigation effect from a macroscopic perspective in navigation, such as providing vehicles with an effective detour to avoid traffic jam in an emergency situation such as a road accident. Micro emergency driving is a method to overcome a dangerous situation through communication messages between neighboring vehicles from a microscopic perspective in driving.

6.1. Macro emergency driving

Santamaria et al. in [85] proposed the scheme of optimizing traffic flow in a vehicle environment with vehicle-to-roadside capabilities. This proposal utilizes information gathered at the roadside level to redirect traffic flows (by vehicle) to less congested

roads. This will optimize the entire system and contribute to reducing carbon dioxide emissions. This paper devised a new traffic rerouting algorithm that can manage vehicle mobility patterns to evaluate new routes on roads with low traffic density. RSU analyzes the average mobility for vehicle's behavior and uses the mobile host's orientation preference statistics when rerouting. The vehicle network is modeled and dynamically updated as a weighted graph that considers the direction and the number of vehicles at different distances. The new route is evaluated, taking into account the average level of congestion. This paper does not consider only the current level of congestion, but also statistically predicts the road dynamics of the geographic map by considering the future movement of the mobile host.

Santamaria et al. in [86] focused on the design for vehicular environments which was able to collect data during mobile node traveling and can alert a message of dangerous or emergency conditions by exploiting on-board sensors and GPS equipped on each vehicle. A sensing platform can monitor the vehicular environment conditions, such as obstacles, accidents, emergent situations. On-board units transmit and receive the collected information from a sensing platform with the surrounding RSUs. GPS is used to handle the accurate location of an event. By exploiting this information, vehicles approaching the event location can detour and avoid dangerous situations. They proposed a layered architecture to control dangerous situations. An architecture of three layers, such as cloud layer, edge layer, and end system layer, was suggested. A cloud layer is designed for global management. An edge layer is for local and distributed management. For the integration of heterogeneous technology, an end system layer is provided. Some messages for 802.11p have been redefined for a new scheme. A simulation has been run in terms of traffic decentralization and traveling time saving.

Fazio et al. in [87] proposed an application with V2V and V2I message exchange in VANETs to reduce risk from an accident by advising a danger or emergency situation. The message exchange protocol, multi-channel operation, Security services, resource management in WAVE were defined. After receiving an accident notification message in V2V communication, vehicles intended to come across the accident area will avoid the road in traffic jams or dangerous situations. Due to the detouring of these vehicles, the traffic density of the area near the accident will be decreased. Emergency vehicles calculate the faster path to the destination. Dijkstra's algorithm is used for optimal path planning. In V2I communication, an RSU sends the request message to a server and receives a message related to the accident. SUMO and JiST/SWANS [88] combined with VSimRTI [89] were used to simulate the traffic on the VN and the communication between nodes, respectively.

As mentioned in Subsection 4.1, Shen et al. proposed SAINT+ [21], which was focused on optimization and guarantee of both fast delivery of the emergency vehicle to an accident area and navigation detouring traces around the accident area. In emergencies and accidents, other vehicles cannot tour the path of the emergency vehicle and are guided to detour to the other paths with lower congestion contribution values. To reduce congestion around an accident area, SAINT+ divides an emergency area into three zones and guides vehicle action; Zone 0 (the road segment with the accident), Zone 1 (the one-hop road segments from Zone 0), and Zone 2 (outside Zone 1).

6.2. Micro emergency driving

SafeSmart [90] is an emergency vehicle warning system using V2I communication. It focuses on the design of application scenarios at traffic intersections as it is to establish faster routes for emergency vehicles by controlling traffic lights. At the intersection, sensors are connected to each traffic light, and it is composed of a master node traffic light and a slave node that is in each direction traffic light. The sensor connected to the slave traffic light has been delegated the authority to control the traffic light. The emergency vehicle's transmitter sends the emergency vehicle's status information data such as position, speed, and direction to the master node. At this time, the master node has already created a secure communication channel with the slave node according to the security mechanism of ITS-G5 and established the network topology. After receiving data from the incoming emergency vehicle, the master node adjusts the traffic lights to create a faster route for the emergency vehicle.

Hafeez et al. in [91] proposed a new mobility model that accurately derives the relationship between average vehicle speed and density, taking into account the vehicle's follow-on safety rules. They analyzed the broadcasting service in the DSRC protocol considering the frequent changes of road topology, the collision probability, the hidden terminal problem, and the non saturation condition. It also identifies the delay in which urgent messages are delivered to their intended recipients. It analyzes the relationship between the speeds of the transmitter and the receiver, and the relationship between the connectivity and the packet reception speed. In order to maintain a safe distance between vehicles, a rapid increase in vehicle density due to traffic jam, accident, or any event) can be controlled, and a packet reception rate is derived taking into account the distance between the transmitter and all potential receivers and their speed. Through the Markov Chain approach, the packet transmission and delay probability is derived in the busy channel. By exploiting the adaptive mobility recognition algorithm, it was found that the performance of the DSRC was improved compared to other algorithms as a simulation result.

Liu et al. proposed Non-Redundant Communication Range Broadcast (NRCR-CAST) protocol [92] which supports a sparse or dense topology, and asymmetric radius vehicle communication in heterogeneous VANETs. It is a distributed broadcast protocol employing local topology information to propagate safety messages and focuses on the highway scenario. This protocol utilizes a broadcast storm suppression mechanism and local topology information obtained through the sending and receiving of periodic HELLO messages. The NRCR-CAST protocol performed good results in terms of packet reception rate, E2E packet delivery delay, and network overhead.

Jat et al. in [93] proposed a solution to the hidden node problem in the VANETs. There has been a fundamental problem known as the hidden node problem [94] in the VANET system, which is that one vehicle is hidden to another vehicle so that the one node has no vehicle information (i.e., vehicle position, speed, and direction) of near but hidden nodes. Consequently, it results in increases in traffic crashes and road accidents due to the lack and difficulty of broadcasting messages in real-time among vehicles to notify information for dangerous conditions. In [93], the location-based protocols and RSU and On-Board Unit (OBU) are used to communicate between vehicles taking into account a rotating node. The cluster is also considered to decide the maximum frequency. They constructed a four-lane path on SUMO [49] simulator and analyzed the result using the nets.

As mentioned in Subsection 3.3, Shen et al. proposed CASD [12] that three-level safety actions to vehicles; LoS and unsafe range, non-LoS but unsafe range, and just in a safe range, as shown in Fig. 6. In emergency and dangerous situations, CASD [12] is designed to decrease accidents using avoidance maneuvers. A user can recognize the near situations through a user interface. First of all, a driver can take an action in an accidental situation. After the threshold time without proper driver's action, CASD takes control and an action to the vehicles.

7. Research issues and challenges

For future smart transportation, several general difficulties need to be considered such as real-time, scalability, resiliency, safety, applicability, heterogeneity, and fault tolerance. In the autonomous driving that we focus on, there are not only the difficulties considered in smart transportation, but also more extensive and various considerations. These are included in the areas of security, heterogeneous vehicle network management, artificial intelligence for autonomous vehicles, radar interference management, and edge computing in an autonomous driving in [95]. Therefore, new models, theories, and methods may need to be considered to tackle these issues.

Several research issues and challenges for smart transportation can be summarized as follows:

- Due to vehicles' interaction with each other in real time, physical dynamics (i.e., kinematics) continuously changes.
- Heterogeneous device collaboration is required, such as various devices in vehicles and smart devices on pedestrians.
- Some vital devices in smart transportation may fail to function, so a reliable and fault-tolerant network system is required.
- Dynamic resource allocation procedure based on safety-awareness is required under various kinds of resource conditions.
- The exploration of more functions is required for edge computing in smart transportation.

In particular, new research challenges and issues for autonomous vehicles can be listed as follows:

- Autonomous vehicles move continuously and cause frequent changes of network topology in a heterogeneous vehicular environments. Heterogeneous VNs include DSRC, LTE, and 5G. There are several considerations, such as short coverage of DSRC, a limited network capacity for massive vehicles in LTE, and integration of multiple VNs. A more adaptable, more flexible, and faster network is required to connect heterogeneous devices in smart transportation.
- Online machine learning (ML) in artificial intelligence technology can cause massive vehicles to control vehicle motion and decision-making in selective conditions. There is a lack of solution for real-time analysis using massive data collected from autonomous vehicles. It will bring a new horizon to data processing schemes for autonomous vehicles in smart transportation.
- Edge computing can help to process an amount of data from autonomous vehicles. However, there is a limitation to scalability in terms of functionality, administration, and load. Production of a massive amount of data can disrupt the edge nodes for analysis on the amount of data.
- Autonomous vehicles are based on Cyber-Physical System (CPS). CPS is vulnerable to cyber attacks. Autonomous vehicles are exposed to not only traditional attacks (i.e., lidar sensor attacks, GPS jamming, etc.), but also new attacks (i.e., ransomware and vehicle theft.

8. Summary and analysis

In this paper, we have surveyed various research works on systems, protocols, applications, and security in smart transportation related to road safety and traffic efficiency. Through this survey, researchers can obtain the state-of-the-art research results in smart transportation. Traffic information gathered from smartphone sensors is used to enhance driving safety, and traffic information is shared between smartphones and vehicles in vehicular networks.

For safe driving, systems can predict the probabilities of collisions and deliver information in a timely manner to prevent accidents. Because of the limited power of smartphones, it is important to reduce the power consumption of smartphones that provide pedestrian safety services; for this purpose, condition adaptive multi-mode schemes are used. There are proposals to increase the efficiency of the power consumption by adjusting the beacon transmission rate of smartphones according to the emergency level. Cloud servers can analyze and predict collision risk to adjust the distributed fair transmission rate to improve the resource utilization and tracking accuracy of a radio channel. Central scheduling by RSUs can also provide communication between vehicles to reduce collision risk.

There is also a distributed protocol among vehicles based on vehicle location and movement information. Vehicle driving direction and position are predicted and sent to neighboring vehicles using a directional antenna. There is also a hybrid centralized and distributed system that pulls out a clustering head from a cluster of vehicles, allocates a clustering head to a channel, and manages the information of vehicle movements. There is also a proposal to receive and forward safety messages considering the spatial and temporal information of vehicles. It prevents collisions during data transmission by utilizing the gap in vehicle data transmission and reduces the possibility of wireless frame collisions in space by using directional antennas. This method can increase the transmission rate of safety messages. Using the self-organizing fuzzy model, the hybrid system model was proposed that could quickly and appropriately choose the transfer rate. Other safety proposals for smart transportation utilize a line of sight vehicle position information and GPS-based navigation. One Android-based safe driving app alerts drivers to emergency vehicles in one of three modes such as civil, admin, and SOS. The app is useful for drivers and motorcyclists to drive safely and for pedestrians to walk safely. There is also a cloud-based driver safety app where a smartphone acts as a mobile sensor. Based on information collected from sensors inside vehicles, such as velocity and position of vehicles, a central server calculates the collision prediction and alerts the driver of each vehicle. There is also an analysis model-based app that can find optimal beacon transmission rates for safety messages.

We also surveyed various research works on smart transportation systems, protocols, and applications for driving efficiency. In terms of systems, TCC can calculate globally minimal wait times for electric vehicles with the arriving time information at the battery exchange stations. To ensure efficient battery exchange of electric vehicles, the TCC informs each electric vehicle of the optimal battery replacement time at each station where it will be able to replace its battery with the minimal prediction waiting time. The TCC suggests the travel route of each vehicle to minimize the average waiting time for an electric vehicle at a battery exchange station. The existing navigation algorithms provide a local optimal path by current traffic measurement instead of a globally optimal navigation path. SAINT+ [21] was suggested to provide overall optimal travel routes by predicting traffic congestion through self-adaptive interaction navigation. It was cloud-based vehicle traffic optimization algorithms and focused on optimization of emergency service delivery and navigation detour routes. A system called SignalGuru [14] was also proposed to control the speed of a vehicle in advance, which can suggest that a driver reduces vehicle speed before moving into an intersection with a traffic-light switching by receiving predicted messages of traffic-light switchings. The system proposed efficient navigation routes to reduce total traffic-light wait times by providing bypass routes that can reduce the probability of encountering a red light. The cloud database only retains useful information collected from the various sensors attached to each smartphone, which supports efficient vehicle operations.

TBD [39] is a network protocol for driving efficiency in smart transportation, which is a data-forwarding algorithm for V2I applications. TBD uses vehicle trajectory information, an accurate link delay model, and the geographically shortest vehicle paths to formulate the forward-and-carry model. An efficient protocol called TSF [40] for I2V communications was also proposed to enable RSUs to transmit data. V2V communications can be normally performed using protocols for V2I and I2V purposes, but the delay can occur through relay nodes. To eliminate these bottlenecks, an improved protocol called TPD [41] was proposed by establishing the encounter probability model.

There are also many proposed smart transportation applications. There is a proposal called GDRP [44] to enable the traffic data center to gather data from the local link node to find the best path using a global and dynamic travel path planning algorithm, and fog computing called STFC [45] has also been proposed for VANET applications; fog computing performs fast computation of traffic information through a hierarchy composed of clouds, CDNs, and P2P edges. Unmanned aerial vehicles can play an important role in road traffic [47] by efficiently collecting and transmitting traffic information to vehicle drivers and pedestrians, monitoring traffic speed for police officers, communicating relevant information to emergency vehicles and neighboring vehicles in accidents, and serving as mobile RSUs. However, UAVs face many limitations, including limited battery life, radio transmission range, and maximum flying speed.

9. Conclusion

In this paper, we surveyed systems, protocols, applications, and security for two areas in smart transportation, driving safety and driving efficiency; we introduced research in each area and analyzed it in detail to provide a comprehensive understanding of the state of the art in smart transportation. In particular, we compared and analyzed different schemes in terms of advantages and disadvantages. From this survey, other researchers can obtain new perspectives and insights about the current research related to smart transportation systems. We also suggest research issues and challenges in smart transportation, so researchers will be able to discover new research directions for each application domain (i.e., safety and efficiency) in future smart transportation. As future work, we will design and implement a VN architecture for smart transportation using software-defined networking, network functions virtualization, and edge computing (or fog computing). In addition, we will design and implement smart transportation applications and services such as context-aware, traffic-signal-synchronized, and in-situ emergency navigators as well as high-speed intersection passing.

Declaration of competing interest

The authors declare that there is no conflict of interest.

Acknowledgements

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-2017-0-01633) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation). This research was also supported in part by the DGIST R&D Program of the MSIT under Grant 18-EE-01.

References

[1] Y.L. Morgan, Notes on DSRC & WAVE standards suite: its architecture, design, and characteristics, IEEE Commun. Surv. Tutor. 12 (4) (2010) 504–518.
[2] IEEE 802.11 Working Group, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Wireless Access in Vehicular Environments, IEEE Std 802.11p-2010, 2010.
[3] IEEE 1609 Working Group, IEEE Guide for Wireless Access in Vehicular Environments (WAVE) – Architecture, IEEE Std 1609.0-2013, 2014.
[4] IEEE 1609 Working Group, IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages, IEEE Std 1609.2-2016, 2016.
[5] IEEE 1609 Working Group, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services, IEEE Std 1609.3-2016, 2016.
[6] IEEE 1609 Working Group, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operation, IEEE Std 1609.4-2016, 2016.
[7] IEEE 802.11 Working Group, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2012, 2012.
[8] 3GPP, Architecture enhancements for V2X services, Technical specification (TS), 2019.
[9] 3GPP, Study on enhancement of 3GPP support for 5G V2X services, Technical report (TR), 2018.
[10] 3GPP, Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services, Technical specification (TS), 2019.
[11] European Union, Commission Decision of 5 August 2008 on the harmonised use of radio spectrum in the 5875–5905 MHz frequency band for safety-related applications of Intelligent Transport Systems (ITS), Technical specification (TS), 2008.
[12] Y. Shen, J. Jeong, T. Oh, S.H. Son, CASD: a framework of context-awareness safety driving in vehicular networks, in: 2016 30th International Conference on Advanced Information Networking and Applications Workshops, WAINA, 2016, pp. 252–257.
[13] T. Hwang, J.P. Jeong, SANA: Safety-Aware Navigation Application for Pedestrian Protection in Vehicular Networks, Springer International Publishing, 2015.
[14] E. Koukoumidis, L.-S. Peh, M.R. Martonosi, SignalGuru: leveraging mobile phones for collaborative traffic signal schedule advisory, in: Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services, MobiSys '11, ACM, New York, NY, USA, 2011, pp. 127–140.
[15] R. Sultana, J. Grover, M. Tripathi, Security of SDN-based vehicular ad hoc networks: state-of-the-art and challenges, Veh. Commun. 27 (2021) 100284, https://doi.org/10.1016/j.vehcom.2020.100284.
[16] J. Jeong, Y. Shen, T. Oh, S. Céspedes, N. Benamar, M. Wetterwald, J. Härri, A comprehensive survey on vehicular networks for smart roads: a focus on IP-based approaches, Veh. Commun. 29 (2021) 100334, https://doi.org/10.1016/j.vehcom.2021.100334.
[17] M. Talal, K.N. Ramli, A. Zaidan, B. Zaidan, F. Jumaa, Review on car-following sensor based and data-generation mapping for safety and traffic management and road map toward ITS, Veh. Commun. 25 (2020) 100280, https://doi.org/10.1016/j.vehcom.2020.100280.
[18] J. Wang, J. Liu, N. Kato, Networking and communications in autonomous driving: a survey, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1243–1274, https://doi.org/10.1109/COMST.2018.2888904.
[19] E. Ahmed, H. Gharavi, Cooperative vehicular networking: a survey, IEEE Trans. Intell. Transp. Syst. 19 (3) (2018) 996–1014, https://doi.org/10.1109/TITS.2018.2795381.
[20] R. Sundar, S. Hebbar, V. Golla, Implementing intelligent traffic control system for congestion control, ambulance clearance, and stolen vehicle detection, IEEE Sens. J. 15 (1) (2014) 1109–1113.
[21] Y. Shen, J. Lee, H. Jeong, J. Jeong, E. Lee, D.H.C. Du, SAINT+: self-adaptive interactive navigation tool+ for emergency service delivery optimization, IEEE Trans. Intell. Transp. Syst. PP 99 (2017) 1–16, https://doi.org/10.1109/TITS.2017.2710881.
[22] M. Bagheri, M. Siekkinen, J.K. Nurminen, Cloud-based pedestrian road-safety with situation-adaptive energy-efficient communication, IEEE Intell. Transp. Syst. Mag. 8 (3) (2016) 45–62, https://doi.org/10.1109/MITS.2016.2573338.
[23] F. Zhang, G. Tan, C. Yu, N. Ding, C. Song, M. Liu, Fair transmission rate adjustment in cooperative vehicle safety systems based on multi-agent model predictive control, IEEE Trans. Veh. Technol. 66 (7) (2017) 6115–6129, https://doi.org/10.1109/TVT.2016.2645682.
[24] J.M. Chung, M. Kim, Y.S. Park, M. Choi, S. Lee, H.S. Oh, Time coordinated V2I communications and handover for WAVE networks, IEEE J. Sel. Areas Commun. 29 (3) (2011) 545–558, https://doi.org/10.1109/JSAC.2011.110305.
[25] K.-T. Feng, LMA: location- and mobility-aware medium-access control protocols for vehicular ad hoc networks using directional antenna, IEEE Trans. Veh. Technol. 56 (6) (2007) 3324–3336.
[26] K.A. Hafeez, L. Zhao, J.W. Mark, X. Shen, Z. Niu, Distributed multichannel and mobility-aware cluster-based MAC protocol for vehicular ad hoc networks, IEEE Trans. Veh. Technol. 62 (8) (2013) 3886–3902, https://doi.org/10.1109/TVT.2013.2258361.
[27] J. Jeong, Y. Shen, S. Jeong, S. Lee, H. Jeong, T. Oh, T. Park, M.U. Ilyas, S.H. Son, D.H.C. Du, STMAC: spatio-temporal coordination-based MAC protocol for driving safety in urban vehicular networks, IEEE Trans. Intell. Transp. Syst. (2017) 1–17, https://doi.org/10.1109/TITS.2017.2723946.

[28] X. Cheng, L. Yang, X. Shen, D2D for intelligent transportation systems: a feasibility study, IEEE Trans. Intell. Transp. Syst. 16 (4) (2015) 1784–1793, https://doi.org/10.1109/TITS.2014.2377074.
[29] N. Cheng, H. Zhou, L. Lei, N. Zhang, Y. Zhou, X. Shen, F. Bai, Performance analysis of vehicular device-to-device underlay communication, IEEE Trans. Veh. Technol. 66 (6) (2017) 5409–5421.
[30] Y. Yao, X. Chen, L. Rao, X. Liu, X. Zhou, LORA: loss differentiation rate adaptation scheme for vehicle-to-vehicle safety communications, IEEE Trans. Veh. Technol. 66 (3) (2017) 2499–2512, https://doi.org/10.1109/TVT.2016.2573924.
[31] F. Lyu, H. Zhu, H. Zhou, W. Xu, N. Zhang, M. Li, X. Shen, SS-MAC: a novel time slot-sharing MAC for safety messages broadcasting in VANETs, IEEE Trans. Veh. Technol. 67 (4) (2018) 3586–3597.
[32] Y.P. Fallah, M.K. Khandani, Context and network aware communication strategies for connected vehicle safety applications, IEEE Intell. Transp. Syst. Mag. 8 (4) (2016) 92–101, https://doi.org/10.1109/MITS.2016.2593672.
[33] S.A. Hadiwardoyo, S. Patra, C.T. Calafate, J. Cano, P. Manzoni, An Android ITS driving safety application based on vehicle-to-vehicle (V2V) communications, in: 2017 26th International Conference on Computer Communication and Networks, ICCCN, 2017, pp. 1–6.
[34] K. Sadeghi, A. Banerjee, J. Sohankar, S.K.S. Gupta, SafeDrive: an autonomous driver safety application in aware cities, in: 2016 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops, 2016, pp. 1–6.
[35] H.P. Luong, M. Panda, H.L. Vu, B.Q. Vo, Beacon rate optimization for vehicular safety applications in highway scenarios, IEEE Trans. Veh. Technol. 67 (1) (2018) 524–536, https://doi.org/10.1109/TVT.2017.2739830.
[36] J. Kim, J. Jeong, H. Kim, J. Park, Cloud-based battery replacement scheme for smart electric bus system, IETE J. Res. (July 2018), https://doi.org/10.1080/03772063.2018.1488627.
[37] J.D. Adler, P.B. Mirchandani, Online routing and battery reservations for electric vehicles with swappable batteries, Transp. Res., Part B, Methodol. 70 (2014) 285–302, https://doi.org/10.1016/j.trb.2014.09.005.
[38] F. Kalim, J.P. Jeong, M.U. Ilyas, CRATER: a crowd sensing application to estimate road conditions, IEEE Access 4 (2016) 8317–8326, https://doi.org/10.1109/ACCESS.2016.2607719.
[39] J. Jeong, S. Guo, Y. Gu, T. He, D. Du, Trajectory-based data forwarding for light-traffic vehicular ad-hoc networks, IEEE Trans. Parallel Distrib. Syst. 22 (5) (2011) 743–757.
[40] J. Jeong, S. Guo, Y. Gu, T. He, D. Du, Trajectory-based statistical forwarding for multihop infrastructure-to-vehicle data delivery, IEEE Trans. Mob. Comput. 11 (10) (2012) 1523–1537.
[41] J.P. Jeong, J. Kim, T. Hwang, F. Xu, S. Guo, Y.J. Gu, Q. Cao, M. Liu, T. He, TPD: travel prediction-based data forwarding for light-traffic vehicular networks, Comput. Netw. 93 (2015) 166–182, https://doi.org/10.1016/j.comnet.2015.10.016.
[42] H. Fatemidokht, M.K. Rafsanjani, B.B. Gupta, C.H. Hsu, Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems, IEEE Trans. Intell. Transp. Syst. (2021) 1–13, https://doi.org/10.1109/TITS.2020.3041746.
[43] C. An, C. Wu, Traffic big data assisted V2X communications toward smart transportation, Wirel. Netw. 26 (2020) 1601–1610, https://doi.org/10.1007/s11276-019-02181-6.
[44] N. Sun, G. Han, P. Duan, J. Tan, A global and dynamic route planning application for smart transportation, in: 2015 First International Conference on Computational Intelligence Theory, Systems and Applications, CCITSA, 2015, pp. 203–208.
[45] N.K. Giang, V.C. Leung, R. Lea, On developing smart transportation applications in fog computing paradigm, in: Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, DIVANet '16, ACM, New York, NY, USA, 2016, pp. 91–98.
[46] Z. Zhou, J. Feng, Z. Chang, X. Shen, Energy-efficient edge computing service provisioning for vehicular networks: a consensus ADMM approach, IEEE Trans. Veh. Technol. 68 (5) (2019) 5087–5099.
[47] H. Menouar, I. Guvenc, K. Akkaya, A.S. Uluagac, A. Kadri, A. Tuncer, UAV-enabled intelligent transportation systems for the smart city: applications and challenges, IEEE Commun. Mag. 55 (3) (2017) 22–28.
[48] J. Jeong, H. Jeong, E. Lee, T. Oh, D.H.C. Du, SAINT: self-adaptive interactive navigation tool for cloud-based vehicular traffic optimization, IEEE Trans. Veh. Technol. 65 (6) (2016) 4053–4067, https://doi.org/10.1109/TVT.2015.2476958.
[49] D. Krajzewicz, J. Erdmann, M. Behrisch, L. Bieker, Recent development and applications of SUMO – Simulation of Urban MObility, Int. J. Adv. Syst. Meas. 5 (3&4) (2012) 128–138.
[50] O. Foundation, OpenStreetMap, Online, https://wiki.osmfoundation.org/wiki/Main_Page, 2017. (Accessed 1 September 2017).
[51] I. Inan, F. Keceli, E. Ayanoglu, Analysis of the 802.11e enhanced distributed channel access function, IEEE Trans. Commun. 57 (2009) 1753–1764, https://doi.org/10.1109/TCOMM.2009.06.0701132.
[52] A. Asadi, Q. Wang, V. Mancuso, A survey on device-to-device communication in cellular networks, IEEE Commun. Surv. Tutor. 16 (4) (2014) 1801–1819.
[53] J. Kim, J. Lee, J. Kim, J. Yun, M2M service platforms: survey, issues, and enabling technologies, IEEE Commun. Surv. Tutor. 16 (1) (2014) 61–76.
[54] E. T.. V1.1.1, Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems Operating in the 5 GHz Range; Access Layer Part, IEEE Std 802.11p, Jul. 2011.
[55] O. O. automated navigation direction, Online, http://osmand.net. (Accessed 19 January 2017).
[56] M.L. Puterman, Markov Decision Processes: Discrete Stochastic Dynamic Programming, 1st edition, John Wiley & Sons, Inc., New York, NY, USA, 1994.
[57] SKT, SKT Tmap, Online, https://www.tmap.co.kr. (Accessed 1 September 2017).
[58] W. Mobile, Waze, Online, https://www.waze.com. (Accessed 1 September 2017).
[59] E.W. Dijkstra, A note on two problems in connexion with graphs, Numer. Math. 1 (1) (1959) 269–271, https://doi.org/10.1109/MCI.2006.329691.
[60] M. Dorigo, M. Birattari, T. Stutzle, Ant colony optimization, IEEE Comput. Intell. Mag. 1 (4) (2006) 28–39, https://doi.org/10.1109/MCI.2006.329691.
[61] M. Raya, J. Hubaux, The security of vehicular ad hoc networks, in: 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN, 2005, pp. 11–21.
[62] J.P. Jeong, T.T. Oh, Survey on protocols and applications for vehicular sensor networks, Int. J. Distrib. Sens. Netw. 12 (8) (2016) 1550147716662948, https://doi.org/10.1177/1550147716662948.
[63] G. Samara, W.A.H. Al-Salihy, R. Sures, Security issues and challenges of vehicular ad hoc networks (VANET), in: 4th International Conference on New Trends in Information Science and Service Science, 2010, pp. 393–398.
[64] L. Bariah, D. Shehada, E. Salahat, C.Y. Yeun, Recent advances in VANET security: a survey, in: 2015 IEEE 82nd Vehicular Technology Conference, VTC2015-Fall, 2015, pp. 1–7.
[65] J.R. Douceur, The Sybil Attack, Springer, Berlin, Heidelberg, 2002.
[66] J. Sun, C. Zhang, Y. Zhang, Y. Fang, An identity-based security system for user privacy in vehicular ad hoc networks, IEEE Trans. Parallel Distrib. Syst. 21 (9) (2010) 1227–1239, https://doi.org/10.1109/TPDS.2010.14.
[67] A.A. Wagan, L.T. Jung, Security framework for low latency VANET applications, in: 2014 International Conference on Computer and Information Sciences, ICCOINS, 2014, pp. 1–6.
[68] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, J. Comput. Secur. 15 (1) (2007) 39–68.
[69] S. Kent, IP encapsulating security payload (ESP), RFC 4303, https://doi.org/10.17487/RFC4303, https://rfc-editor.org/rfc/rfc4303.txt, 2005.
[70] S. Kent, IP authentication header, RFC 4302, https://doi.org/10.17487/RFC4302, https://rfc-editor.org/rfc/rfc4302.txt, 2005.
[71] J.P. Jeong, IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases, Internet-draft draft-ietf-ipwave-vehicular-networking-20, Internet Engineering Task Force, https://datatracker.ietf.org/doc/draft-ietf-ipwave-vehicular-networking/, 2021.
[72] H.J. Jo, I.S. Kim, D.H. Lee, Reliable cooperative authentication for vehicular networks, IEEE Trans. Intell. Transp. Syst. 19 (4) (2018) 1065–1079, https://doi.org/10.1109/TITS.2017.2712772.
[73] W. Li, H. Song, ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (4) (2015) 960–969, https://doi.org/10.1109/TITS.2015.2494017.
[74] S.K. Bhoi, P.M. Khilar, A secure routing protocol for vehicular ad hoc network to provide ITS services, in: 2013 International Conference on Communication and Signal Processing, 2013, pp. 1170–1174.
[75] R.S. Raw, D.K. Lobiyal, B-MFR routing protocol for vehicular ad hoc networks, in: 2010 International Conference on Networking and Information Technology, 2010, pp. 420–423.
[76] C. Langley, R. Lucas, H. Fu, Key management in vehicular ad-hoc networks, in: 2008 IEEE International Conference on Electro/Information Technology, 2008, pp. 223–226.
[77] M. Burmester, E. Magkos, V. Chrissikopoulos, Strengthening privacy protection in VANETs, in: 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2008, pp. 508–513.
[78] B.A. Forouzan, Cryptography & Network Security (Sie) 2E, McGraw-Hill Education (India) Pvt Limited, 2011.
[79] S.K. Bhoi, P.M. Khilar, SST: a secure fault-tolerant smart transportation system for vehicular ad hoc network, in: 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012, pp. 545–550.
[80] P.J. Fernández, J. Santa, F. Bernal, A.F. Skarmeta, Securing vehicular IPv6 communications, IEEE Trans. Dependable Secure Comput. 13 (1) (2016) 46–58, https://doi.org/10.1109/TDSC.2015.2399300.
[81] S. Frankel, S. Krishnan, IP security (IPsec) and Internet key exchange (IKE) document roadmap, RFC 6071 (2011), https://doi.org/10.17487/RFC6071, https://rfc-editor.org/rfc/rfc6071.txt.
[82] K. Seo, S. Kent, Security architecture for the Internet protocol, RFC 4301, https://doi.org/10.17487/RFC4301, https://rfc-editor.org/rfc/rfc4301.txt, 2005.
[83] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, Internet key exchange protocol version 2 (IKEv2), RFC 7296 (2014), https://doi.org/10.17487/RFC7296, https://rfc-editor.org/rfc/rfc7296.txt.
[84] H. Moustafa, G. Bourdon, Y. Gourhant, Providing Authentication and Access Control in Vehicular Network Environment, Springer, US, Boston, MA, 2006.
[85] A.F. Santamaria, P. Fazio, P. Raimondo, M. Tropea, F. De Rango, A new distributed predictive congestion aware re-routing algorithm for CO_2 emissions

reduction, IEEE Trans. Veh. Technol. 68 (5) (2019) 4419–4433, https://doi.org/10.1109/TVT.2019.2905753.
[86] A. Santamaria, M. Tropea, P. Fazio, F. De Rango, Managing emergency situations in VANET through heterogeneous technologies cooperation, Sensors (2018) 1461–1478.
[87] A.L. Peppino Fazio, Floriano de Rango, Vehicular networks and road safety: an application for emergency/danger situations management using the WAVE/802.11p standard, Inf. Commun. Technol. Serv. 11 (5) (2013) 357–364.
[88] R.Z.J.H. BARR, R.V. RENESSE, JiST: an efficient approach to simulation using virtual machines, in: Software: Practice and Experience, vol. 35, 2005, pp. 539–576.
[89] B. Schunemann, K. Massow, I. Radusch, A novel approach for realistic emulation of vehicle-2-x communication applications, in: VTC Spring 2008 – IEEE Vehicular Technology Conference, 2008, pp. 2709–2713.
[90] L.A.L.F. da Costa, E.K. Duarte, M. Erneberg, E.P. de Freitas, A. Vinel, Poster: Safe Smart – a VANET system for efficient communication for emergency vehicles, in: 2020 IFIP Networking Conference (Networking), 2020, pp. 643–645.
[91] K.A. Hafeez, L. Zhao, B. Ma, J.W. Mark, Performance analysis and enhancement of the DSRC for VANET's safety applications, IEEE Trans. Veh. Technol. 62 (7) (2013) 3069–3083, https://doi.org/10.1109/TVT.2013.2251374.
[92] W. Liu, X. Tang, S. Jia, J. Pu, Safety message dissemination using edge computing in heterogeneous VANETs, in: 2018 IEEE 27th International Symposium on Industrial Electronics, ISIE, 2018, pp. 1276–1281.
[93] S. Jat, R.S. Tomar, M. Satya Prakash Sharma, Traffic analysis for accidents reduction in VANETs, in: 2019 International Conference on Computational Intelligence and Knowledge Economy, ICCIKE, 2019, pp. 115–118.
[94] A. Rahman, P. Gburzynski, Hidden problems with the hidden node problem, in: 23rd Biennial Symposium on Communications, 2006, pp. 270–273.
[95] I. Yaqoob, L.U. Khan, S.M.A. Kazmi, M. Imran, N. Guizani, C.S. Hong, Autonomous driving cars in smart cities: recent advances, requirements, and challenges, IEEE Netw. 34 (1) (2020) 174–181, https://doi.org/10.1109/MNET.2019.1900120.