IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 30, 2020, accepted July 8, 2020, date of publication July 14, 2020, date of current version July 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3009336

Why is Internet of Autonomous Vehicles not as Plug and Play as We Think ? Lessons to Be Learnt From Present Internet and Future Directions

SAMEER QAZI[1], (Member, IEEE), FARAH SABIR[1], BILAL A. KHAWAJA[2,3], (Senior Member, IEEE), SYED MUHAMMAD ATIF[1], AND MUHAMMAD MUSTAQIM[3]

[1]College of Engineering, PAF Karachi Institute of Economics and Technology, Karachi 75190, Pakistan
[2]Department of Electrical Engineering, Faculty of Engineering, Islamic University of Madinah, Madinah 41411, Saudi Arabia
[3]Department of Electronic and Power Engineering (EPE), PN-Engineering College (PNEC), National University of Sciences and Technology (NUST), Karachi 75104, Pakistan

Corresponding authors: Sameer Qazi (sameer.qazi@pafkiet.edu.pk) and Bilal A. Khawaja (7166@iu.edu.sa)

ABSTRACT The recent race for autonomous or 'driverless' vehicles, has spawned a lot of research in the area of Internet of Autonomous Vehicles (IAVs). With the advent of the latest technology fueled by Artificial Intelligence and Machine Learning, Autonomous Vehicles (AVs) can now determine the best possible route to a destination based on the current traffic situation and take dynamic driving decisions accordingly, while preventing accidents. Field trials for single autonomous vehicles have been largely successful. However, as more autonomous vehicles will be added to the intelligent transport networks, current research is now centered around their synergistic coexistence in the offering of network-centric and user-centric services. This development is governed by borrowing several concepts from the legacy Internet to address the problems of IAVs. In this paper, we present an extensive overview of the research challenges in the IAVs. Moreover, our contributions in this paper are that (i) We show how the network-oriented cooperative client-server model will give way to a more unorthodox and 'selfish' decentralized and peer-to-peer (P2P) model, for example in the offering of navigation services on the IAV. (ii) We discuss how centralized architecture will give way to more distributed architectures for real-time information propagation over the IAV. (iii) We discuss how network-centric policies will begin to shift to user-centric under more beneficial revenue models by offering network-assisted quality of service (QoS) provisioning. (iv) We discuss in detail how vehicle traffic grooming in the IAV would present as much of a challenge as in the legacy Internet. (v) We discuss the disruptive role of value-added services on the IAV, and (iv) Finally, we discuss the problem of cyber threats in the IAV just as in the legacy Internet.

INDEX TERMS Internet of Autonomous Vehicles, network-centric services, user-centric services, vehicular ad-hoc networks (VANETs), wireless communications.

ACRONYMS

(See table 1.)

I. INTRODUCTION

Traffic congestion and the increasing number of traffic accidents has fueled billions of dollars' worth of research into intelligent traffic control systems and autonomous ''driverless'' vehicles technology, respectively. Through the Internet of Autonomous Vehicles (IAVs) [1], [2] technology, the live and current road traffic conditions can be transmitted to the central command and control system in the form of floating vehicle data, as shown in Fig. 1. The central command and control system can crunch the numbers received into complex optimization routines to come with the best traffic management plans that aim to ease traffic congestion and pollution. Autonomous Vehicles (AVs) receive these network-assisted

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau.

TABLE 1. List of acronyms and abbreviations used in the paper.

Internet of Autonomous Vehicles	IAVs
Autonomous Vehicles	AVs
Peer-to-Peer	P2P
Quality of Service	QoS
Internet of Things	IoT
Dedicated Short-Range Communications	DSRC
Wireless Access in Vehicular Environments	WAVE
Radio Detection and Ranging	RADAR
Light Detection and Ranging	LIDAR
Vehicle-to-Vehicle	V2V
Vehicle-to-Roadside Unit	V2R
Roadside Unit-to-Roadside Unit	R2R
Vehicle-to-Infrastructure	V2I
Roadside Unit-to-Infrastructure	R2I
Roadside Unit	RSU
Supervisory Control and Data Acquisition	SCADA
Amplitude Shift Keying	ASK
Quadrature Phase Shift Keying	QPSK
National Information and Communications Technology Australia	NICTA
Wireless Fidelity	Wi-Fi
Split Cycle Offset Optimization Technique	SCOOT
Electronic Control Unit	ECUs
Connected and Autonomous Vehicle	CAV
Intrusion Detection System	IDS
Controller Area Network	CAN
Feed Forward Neural Network	FFNN
Support Vector Machine	SVM

navigation directions and contribute in assisting the network to be congestion and accident-free. The current model for this service is user-requested along the lines of a server-client model.

Such communication between Traffic Network Infrastructure and AVs is beneficial from both network-centric and user-centric point of views. Traffic authorities want to leverage the information gathered about the network traffic conditions made possible through huge leaps in video and image processing algorithms [3], [4], as well as floating vehicle data [5], [6] and Big Data Processing to be able to optimize the traffic signal timing plans, ramp metering, congestion charging systems on highways, etc. based on real-time traffic density estimates. However, unbeknownst to the traffic authorities, the users may themselves be making several decisions on their own 'benefitting' from their perception of the network based on other users. This is not unlike the situation when peer-to-peer (P2P) content sharing and overlay routing services on the internet began to offer a better quality of service (QoS) to the user based on the selfish decisions [7]. However, such user-centric autonomy on the network created network management issues on the part of ISPs [8]–[11]. In this article, we review what benefits such IAVs can provide through value-added services associated with it from a network-centric and user-centric point of view.

Our contribution in this article is as follows: Recent research literature [5], [12], [13] has identified motivation, architectures, policy decisions, and protocol layers for connected vehicles technology. Although, they have failed to address at depth the network-centric service model and the user-centric service model and the pertinent issue of the synergy between network-selfish and user-selfish behavior when a futuristic IAVs will take over. The service model over the IAV will then be not much, unlike the current service model on the internet. Our main aim in this paper is to discuss the synergy between network-selfish and user-selfish behavior learning from past experiences in the internet. This may give future directions to engineers working on improving the capabilities of future IAVs. As compared to the research studies presented by other researchers, our contributions in this paper are further highlighted in Table 2.

The rest of the article is organized as follows: Section II presents a detailed background and overview of IAVs and its relationship with the Internet of Things (IoT) technology, prospects, projects, and active research trends. Section III gives an overview of the architecture and communications standards related to the IAVs. It also covers the frequency bands, infrastructure, and devices used in different countries for the IAVs system. Sections IV, V, and VI present the challenges related to the information propagation models, navigation models, traffic grooming problems, respectively. These sections target the main questions related to the theme of the paper that is it really possible to offer disruption free services over a cooperative IAV network in the presence of several competing variables. Sections VII and VIII cover the futuristic challenges of the P2P value-added services over such IAVs and the security and vulnerability issues, respectively, and finally, Section IX concludes the paper. The organization of the paper is illustrated in Fig. 2.

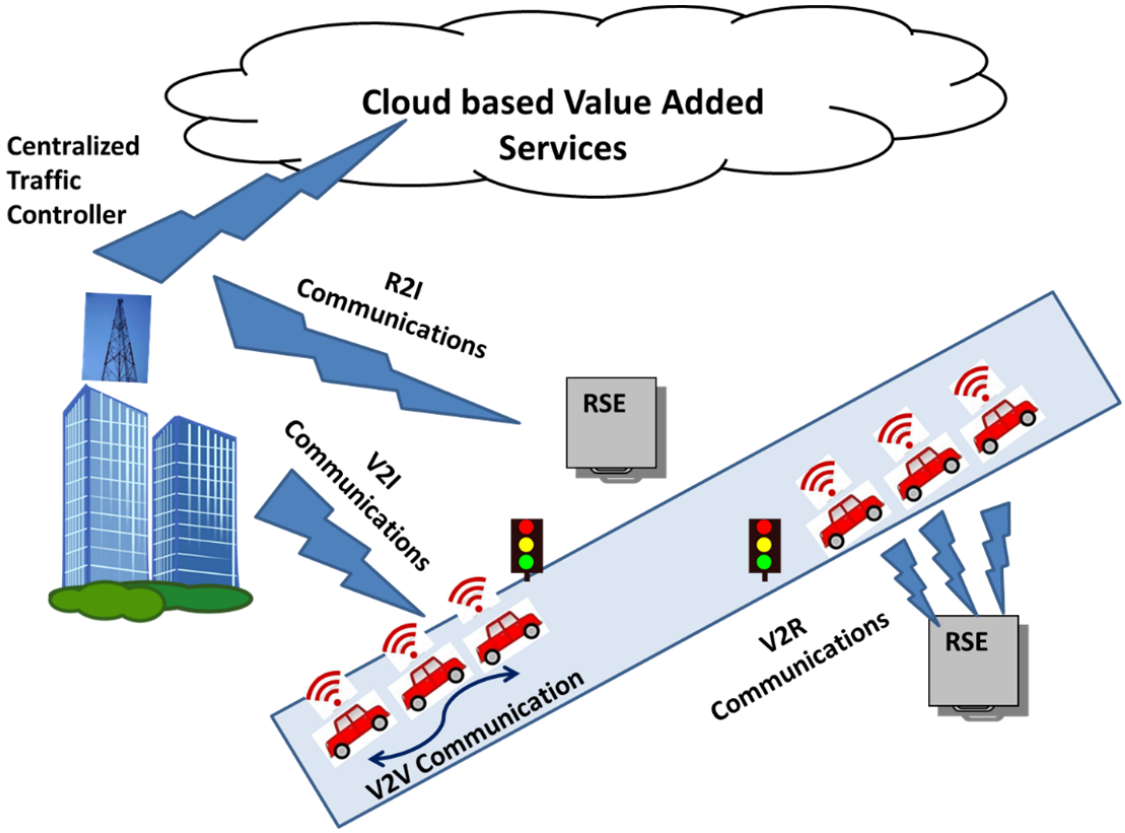

FIGURE 1. Centralized Architecture of an IAV System.

TABLE 2. Comparison of research work presented in this paper with the work presented by other researchers.

References / Year	Layered Architecture Design in IAV	Physical Layer Communications in IAV	Traffic Control in IAV	Coordination Algorithms for Connected Vehicles Technology in IAV	User-Centric and Network-Centric Challenges in IAV	Centralized, P2P and other Value Added Services over IAV	Security and Privacy Aspects of IAV
[6] / 2017	√						
[25] / 2007		√					
[30] / 2003			√				
[31] / 2019			√				
[32] / 2018			√				
[34] / 2019				√			
[35] / 2019				√			
[36] / 2019				√			
[37] / 2018				√			
[38] / 2018			√				
[39] / 2018			√				
[47] / 2014							√
[5] / 2018	√						
[52] / 2018		√					
[53] / 2019		√					
[48] / 2015		√					
[56] / 2010							√
[57] / 2014							√
[58] / 2017							√
[85] / 2018						√	
[49] / 2018		√					
[This Work] / 2020	√	√	√	√	√	√	√

II. RELATED WORK

Since, the last two decades, active research has been carried out in the domain of IoT [14], [15] and IAVs [13], [16], [17], researchers have focused their energies in the development of artificially intelligent algorithms and systems that can work without any intervention of humans [18]–[21].

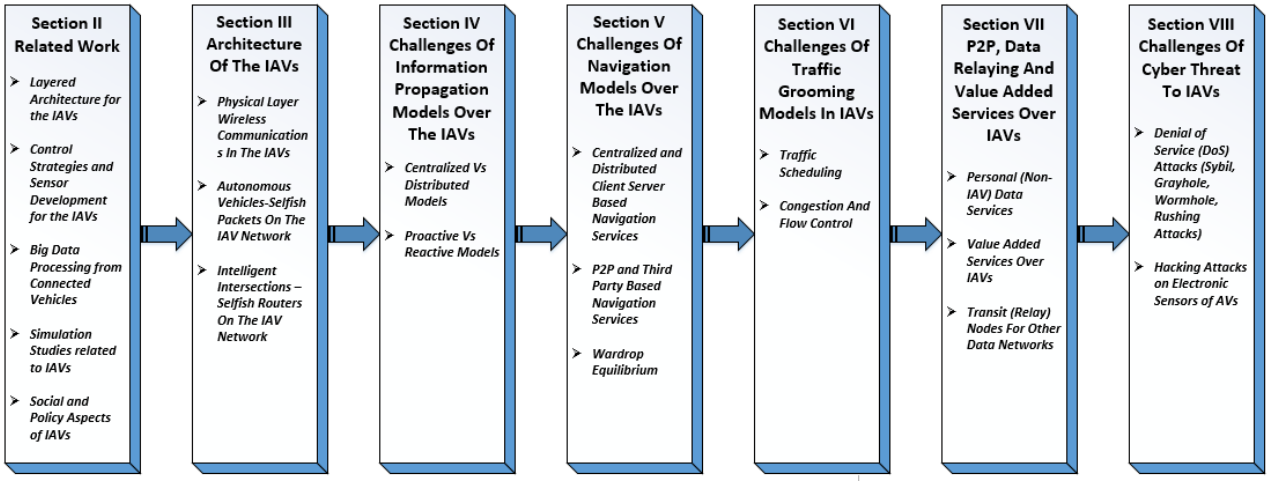

FIGURE 2. Taxonomy and pictorial view of the paper organization.

A. LAYERED ARCHITECTURE MODELS FOR THE IAVs

Contreras-Castillo *et al.* [6] have presented a 7-layered architecture for the IAVs by drawing analogies with the legacy Internets TCP/IP protocol stack that help in coordinating the different functions of complex interconnected systems and devices. Similarly, Kaiwartya *et al.* [5] have presented a more practical layered architecture to keep different layers working independently, yet coexisting.

The work aptly names the layers as perception, coordination, artificial intelligence, application, and business layers, respectively. Any massively networked IoT based systems will rely on the efficient means of data communications, IAV is the same; different physical layer technologies have been studied for communication of the networked vehicles in close proximity to each other and other roadside units. The technologies studied include Dedicated Short Range Communications (DSRC) and Wireless Access in Vehicular Environments (WAVE) [22]–[24] for intercommunications and ZigBee, Bluetooth for intra communications between the sensors of AVs [25].

B. CONTROL STRATEGIES AND SENSOR DEVELOPMENT FOR THE IAVs

Efficient sensor development relying on ultrasonic technology [26], Radio Detection and Ranging (RADARs) [27], Light Detection and Ranging (LIDARs) [28], [29] and complex image processing algorithms [4] as well as control systems and algorithms [30], [31], have been developed. This enables the vehicles within the near field IAV, to announce and plan their trajectory in coordination with other cars [32], [33] and coordinate their collective motion [27], [34], [35] with other cars while traveling the form of platoons [36], [37] with efficient self-driving algorithms; such as Robust Cruise Control [38], [39].

C. BIG DATA PROCESSING FROM CONNECTED VEHICLES

Making use of the connected vehicle data will also be leveraged by the traffic authorities for the implementation of better vehicular traffic control and coordination. Different solutions have been considered by researchers, such as making use of floating vehicle data [40] and efficient closed-loop control system strategies [30], and adaptive fuzzy control [41] to make dynamic traffic coordination plans possible based on the current-most traffic situation.

D. SIMULATION STUDIES RELATED TO IAVs

As the IAV concept continues to dominate the thoughts of researchers, several simulation-based studies [42], [43], as well as test rigs have been used to study the dynamic evolutionary behavior of such systems so that they can be better designed.

Other researchers focused their attention to situations where IAV has achieved partial penetration in the market, and they exist with unconnected vehicles [44].

These studies concentrate on the safety and societal impact of the IAVs. Safety studies carried out include studying the situational behavior [45] where distributed control algorithms for self-driving connected vehicles could potentially fail, e.g., at complicated intersections requiring efficient algorithms to arbitrate access [34], [46]. Closely related to safety are the security aspects of such IAVs; detailed studies have been carried out by the researcher to study the impact of cyber threats [47].

E. SOCIAL AND POLICY ASPECTS OF IAVs

Social and policy aspects of such IAVs have also been studied by the researchers and analysts [13]. Since the idea of IAV was floated, the researchers have been questioning the moral aspects of decision-making by self-driving cars. Who would be blamed if such cars were involved in accidents resulting in loss of lives? Similarly, the social fabric of the society may change altogether as people may prefer to avail the services of self-driving cars on-the-go instead of choosing to 'own' them. The above mentioned related research work have been summarized in Table 3 for the benefit of the readers.

TABLE 3. Active research areas in the IAV technology.

S. No	Research Challenges in IAV	References
1.	Layered Architecture Design in the IAV	[5], [6]
2.	Physical Layer Communications and Data Transmission Requirements of the IAV	[25], [48], [52], [53]
3.	Social Aspects of the IAV	[13], [51]
4.	Simulations and Test Platform for IAV	[40], [42], [43], [54], [55]
5.	Control Systems Hardware Design for Autonomous Driving and Traffic Control in IAV	[30],[31], [32], [38], [39]
6.	Coordination Algorithms for Connected Vehicles Technology in IAV	[17], [27], [34], [35], [36], [37], [46]
7.	Interaction of IAV with unconnected vehicles	[44]
8.	Advanced LIDAR, RADAR and Image Processing technology for Autonomous Driving and Platoon Formations in IAV	[4], [27], [28], [29]
9.	Deep Learning and Artificial Intelligences Algorithms for IAV	[20], [21]
10.	Security and Privacy Aspects of the IAV	[47], [56], [57], [58]

III. ARCHITECTURE OF THE IAVS - WHO COMMUNICATES AND WITH WHOM IN THE IAVs?

Research literature typically depicts an Internet of Vehicles network, as shown in Fig. 1. The three main ingredients are the AVs, intelligent traffic intersections, and the physical communications layer bringing about a co-operation between the two, possibly being global optimization to this system. It is interesting to note that the development of AVs and intelligent traffic intersections came way before the concept of IAV. AVs are capable of making intelligent driving decisions by observing their environment and taking appropriate steps to avoid any traffic accidents while reducing their traveling delays. Similarly, intelligent traffic intersections are capable of implementing intelligent traffic control based on assessing the traffic situation in real-time to improve their Grade of Service.

A. PHYSICAL LAYER WIRELESS COMMUNICATIONS IN THE IAVs

The physical layer communications in an Internet of Vehicle predominantly occur between Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside Unit (V2R), Roadside Unit-to-Roadside Unit (R2R), Vehicle-to-Infrastructure (V2I) and Roadside Unit-to-Infrastructure (R2I), respectively. In this paper, we do not address the communication between the personal devices/sensors and vehicles for which established technologies, e.g., ZigBee, Bluetooth, Wi-Fi HALOW, and supervisory control and data acquisition (SCADA) based protocols are already established and mature since these communications do not play any part in the synergy of network and user-based services over an IAVs. For more knowledge, the user is referred to a variety of good research literature with an in-depth discussion of these technologies [25], [48], [49].

The concept of V2V and V2R is not new and has been around for over 4 decades. Developments related to DSRC have a long history in Japan, having begun in the 1980's with the RACS [50]. In 2001, the first DSRC standard for Electronic Tolling application was used in Japan at 5.8 GHz frequency band, carrier frequency interval of 5 MHz, and modulation techniques of amplitude shift keying (ASK) and quadrature phase-shift keying (QPSK) [50].

The modern needs of vehicle and roadside equipment communication aim to benefit both the traffic management authorities as well as the commuters. In 2016, the U.S. Department of Transport (DOT) began the connected vehicle research program, which is a multimodal initiative that aims to enable safe, interoperable networked wireless communications among vehicles, infrastructure, and personal communications devices. U.S DOT has dedicated a licensed spectrum in the 5.9 GHz band for communications over the Internet of Vehicles [22], [24]. Several wireless standards have been developed or in the process of developing, such as WAVE, IEEE 802.11p, and IEEE 1609.x standard termed as WAVE-DSRC teamed with the new SAE J2735 message dictionary standard.

The DSRC standard [23] is an exhaustive protocol to deal with the V2V and V2R communication requirements. In WAVE based Wi-Fi-driven architecture, RSUs alongside roads are used as wireless access points, which provide communication coverage to the vehicles inside its coverage area. In ad-hoc architecture, a group of on-road vehicles forms ad-hoc networks using WAVE [5]. Although, many recent advances over the last decade have made autonomous driving capabilities close to human drivers. Challenges of high data-rates due to a large number of sensors in AVs over an unreliable channel such as over the internet of moving vehicles sparked a large volume of research [59], [60]. The communications have to be managed between vehicles traveling at high speeds as well as between moving vehicles and roadside equipment [24]. While two or more 'connected' moving vehicles moving as platoons with the same velocity may appear stationary to each other, often the connected vehicle's communications may be impeded due to the presence of large trucks or buses. The problem of reliable communications between vehicles not in direct line of sight was thoroughly investigated in several research studies [61], [62], where the physical layer considered is 5.9GHz DSRC. The paper further considers a hybrid architecture for providing continuous vehicular links to the internet using cellular-WLAN roaming.

For R2R, R2I, and V2I communications, several researchers have come up with their unique and intelligent proposals. NICTA has recently worked on the STaRComm project, which set the goal of designing a wireless mesh

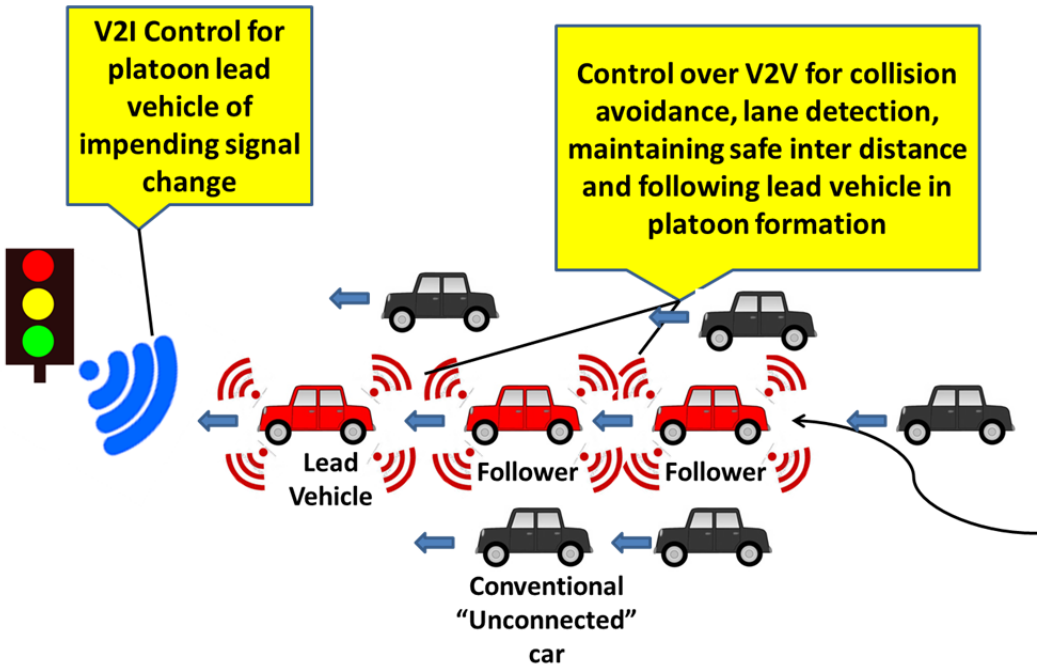

FIGURE 3. Platoon formation by autonomous vehicles.

network (WMN) architecture to solve the communication needs of the traffic control system in Sydney, Australia. The research team used WMN as a physical layer network between signal controllers on 7 busy intersections with distances ranging between 200-500m and cover real propagation environments with high rise buildings, foliage, and a lot of traffic [63], [64].

The predominantly available technology for communications of vehicles and roadside units with infrastructure is through 2G/3G/4G/LTE. These networks are already well established with data transfer rates that vary with user mobility levels. Currently, value-added services in the form of navigation help and driving directions are available over Google Maps.

B. AUTONOMOUS VEHICLES - SELFISH PACKETS ON THE IAV NETWORK

Intelligent vehicles capable of making fully autonomous driving decisions [65] such as adaptive cruise control, electronic stability control, automatic navigation, lane-keeping, and forward collision avoidance have already been around for some time [66]. This is analogous to user-centric selfish behavior on the internet, where all users may demand more bandwidth, reduced latency, and packet losses for the connection. Similarly, the vehicles in an IAV rely on several sensors and real-time communication with other vehicles to get the maximum performance benefit in terms of reduced traveling delays and optimal fuel costs. The vehicles rely on several sensors to accomplish these tasks such as appropriately calibrated cameras [67] for detection of traffic lights and other moving objects (vehicles, pedestrians), ultrasonic sensors [26] and RADARs [27] for distance measurement to objects and obstacles adjacent to the vehicle as shown in Fig. 3. Recent advances in the LIDAR technologies enable near-perfect 3D image generation around the vehicle for autonomous driving decisions [28], [29]. Google's driverless vehicle gave huge publicity to AVs and attracted a pool of talent from several disciplines [68]. Vehicles might communicate with roadside equipment and other vehicles to produce better-coordinated flows [69]. These edge level communications may sometimes be extended to infrastructure level communications, V2I and R2I. This happens when it is necessary to share network measurements, or a requested service can be fulfilled by a central entity having a broader perspective of the network, such as the best possible route based on current traffic conditions. New information and control systems are paving the way to novel traffic management approaches. Furthermore, autonomous driving is starting to enable the careful control of vehicle trajectories and the synchronization of their arrival times at the intersections [70], as shown in Fig. 4; thus, AVs may speed up or slow down to minimize their waiting times at an intersection.

Future capabilities of AVs under the IAV framework will include autonomous decision-making skills for optimized navigation to optimize parameters such as reduced journey time, fuel usage, minimize road tolls. However, while AVs will be fully empowered for self-driving, their arbitration at an intersection may be fully controlled by the smart traffic intersection. Several types of research and algorithms are also being proposed to improve the efficiency of IAV by reducing traffic density, e.g., a multi-lane formation control method is proposed for connected IAV to facilitate a tight

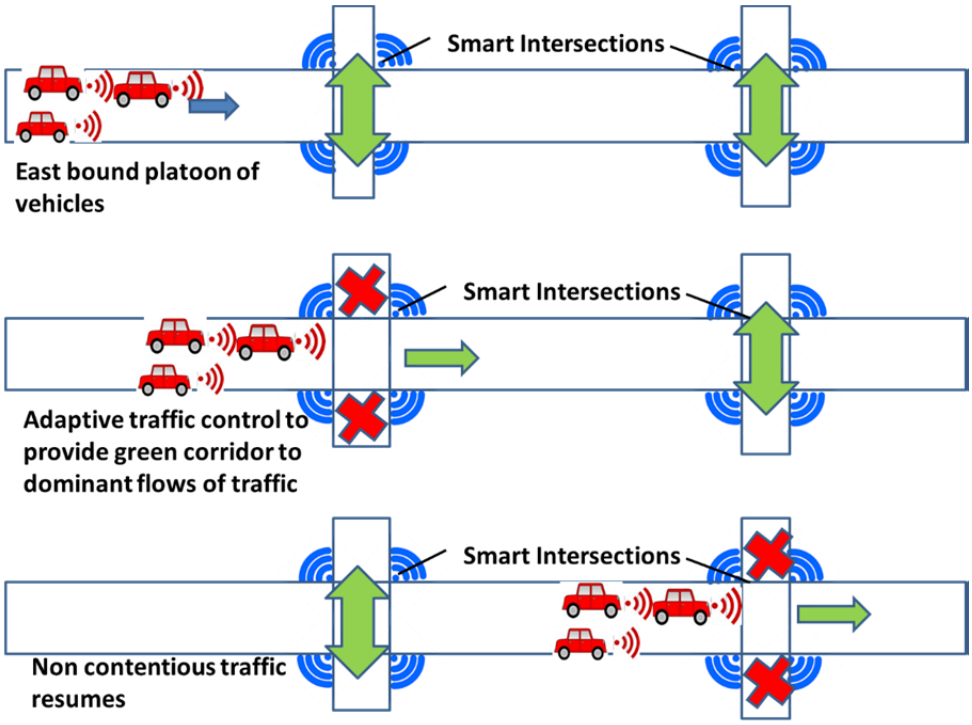

FIGURE 4. Adaptive "Actuated" Traffic control to give 'green' corridors to dominant traffic flows.

and flexible formation where designated positions are sent to IAV, and each vehicle performs their trajectory planning by themselves. The interlaced formation is used to provide lane changing efficiency, at the same time making full use of lane capacity. A recently proposed, Hungarian algorithm can help in getting the minimum amount of the lanes changed, which in return helps in reducing the load of the overall system [36].

Driver's safety is one of the main concerns in IAV, projected trajectories of the vehicle are desired to avoid collisions and make decisions in a timely manner. Gaussian Process Regression (GPR) model can be used, which models past trajectory data and distributes to learned models between the nearby vehicles via the V2I communication method. This technique makes use of clustering for extracting better models from the available data. Hence the more accurate location of a vehicle can be identified to avoid accidents [32]. Another method to optimize the IAV control can be to merge IAV at the roundabouts using predictive control to reduce traffic congestions. This can be achieved by putting collision avoidance as a hard constraint [46]. The platoon control system is also used for IAV, as shown in Fig. 4 with the constraint of lane discipline, making use of V2V and V2I communication.

This type of control not only provides better fuel conservation and safety but also improves traffic efficiency. Platoon driving techniques ensure that the traffic will always be organized, and the risk of collision will be minimal. Platoon control aims all vehicles to have the same velocity and gap [37].

C. INTELLIGENT INTERSECTIONS – SELFISH ROUTERS ON THE IAV NETWORK

Intelligent Traffic Intersections based on newer proposed designs exercise as much control in 'forwarding' autonomous cars towards next-hop as a traditional router has over the packets on the internet. Like an Internet router, it can determine forwarding delays based on the traffic situation and use pre-determined algorithms for best arbitration by contending vehicles. Here, we present a brief history of the development of Intelligent Intersection technologies and how they will play a role in future IAV.

Interest in adaptive technologies for road traffic control was developed as early as towards the turn of the 21st century [30], [71], [72]. Among the various available traffic density sensing technologies, video sensors stand out due to their several advantages. Few of them are ease of installation, availability of sensors, moderate cost, traffic detail, spatial coverage, automated analysis, as well as manual verification. Among the various traffic density sensing technologies available, video sensors have several advantages including relative ease of installation, availability of sensors already installed by road management organizations, moderate cost, the possibility of the detailed description of traffic, e.g., private vehicles vs. public transport; spatial coverage, automated analysis using computer vision techniques and the ability to verify the data manually. Video data has first been and is still often manually analyzed, but can also be processed automatically using methods from the field of computer vision. Various types of transportation data can be extracted from traffic video data

through traditional traffic sensors at a specific location to the detection and identification of all objects in the scene and their tracking from one image to the next to reconstitute trajectories, all the way to the higher semantic interpretation of activities occurring in the video. Solutions have been available for about two decades for the simplest types of data (classified counts and speeds) for simple environments, e.g., highways. However, complete and generic solutions for higher-level interpretations of video data, starting with all the road users' trajectories, still elude researchers for complex environments such as urban intersections with mixed traffic of medium to high density. Video processing based traffic density estimation for smart traffic signal applications has been recently investigated by researchers [3], [67].

Video-based surveillance is the most cost-effective solution as it does not require any expensive infrastructure upgrades, e.g., in the installation of loop detectors and CCTV equipment is mostly available at all major traffic intersection points from a security perspective. Such techniques may also be used for incident detection, e.g., accidents or wrong side drivers.

The first generation of adaptive traffic control systems includes Split Cycle Offset Optimization Technique (SCOOT) [73] and Sydney Coordinated Adaptive Traffic Systems (SCATS) [74]. SCOOT is an adaptive UTC system which is continually assessing the traffic flow data obtained from the use of on-street detectors embedded in the road or video-based detection to monitor queue conditions in real-time at each signaling junction. It can be used to optimize the performance at a single or at most adjacent signaling junctions to optimize the green splits, offsets, and cycle time to try to keep congestion to a minimum. Congestion is managed by the system making small, but unnoticeable changes to the green split and cycle time in each cycle. This is not possible using fixed time plans as each plan change can take several cycles to stabilize and start working as intended. In addition to the congestion management benefits of SCOOT, real-time traffic data can be obtained, which provides information on congestion levels and can assist with incident management, e.g., accidents.

SCATS is one of the pioneer adaptive traffic control systems which is being currently used in 42,000 intersections in over 154 cities in 25 countries. Although this system is automated, it still lacks the coordination between different signaling junctions required to optimize the parameters globally.

InSync Adaptive Traffic Control System[1] developed by Rhythm Engineering is an intelligent transportation system also based on video-based detection that enables traffic signals to adapt to actual traffic demand. As of November 2015, InSync is operational in 2,300 traffic signals in 31 states and 160 municipalities in the U.S.

Carnegie Mellon University has implemented a smart traffic management system called Scalable Urban Traffic Control (SURTRAC)[2] in Pittsburgh boasting reductions of 40 percent in the vehicle wait time, nearly 26 percent in travel time and 21 percent in projected vehicle emissions. This system relies on advanced algorithms based on traffic theory and artificial intelligence [75]. This system manages urban (grid-like) road networks, where there are multiple (typically competing) dominant flows that shift dynamically through the day, and where specific dominant flows cannot be pre-determined (as in arterial or major crossroad applications). Urban networks also often have closely spaced intersections requiring tight coordination of the intersection controllers. The combination of competing for dominant flows and densely spaced intersections presents a challenge for all adaptive traffic control systems. SURTRAC determines dominant flows dynamically by continually communicating projected outflows to adjacent downstream neighbors. This information gives each intersection controller a more informed basis for locally balancing competing inflows while simultaneously promoting the establishment of larger ''green corridors'' when traffic flow circumstances warrant. Some researchers have compared different adaptive traffic controlling schemes by showing similarity of concepts from the domain of control systems [76]. Similarly, others have proposed Fuzzy logic based adaptive traffic control system [41]. One research group is particularly interested in making adaptive traffic controlling strategies relying solely on floating vehicle data [40].

The University of Florida has a sponsored project Autonomous Vehicles at Intelligent Intersections and Advanced Networks (AVIAN) which is a multidisciplinary research project aimed at developing and testing the necessary software and hardware for enhancing traffic signal control operations simultaneously with vehicle trajectories, when the traffic stream consists of connected vehicles, AVs, as well as conventional vehicles. Companies involved in developing similar smart traffic management systems include BMW and Siemens addressing V2I communication. We review a few techniques below where traffic arbitration of AVs is governed by the smart traffic intersection with the coordination of the AV.

In the following sections, we highlight why we think that IAV is not as 'plug and play' as we think learning from the selfish service model in the legacy Internet [80]. In the remainder of this article, we consider an AV as a selfish packet being routed in an IAV composed of distributed selfish intersections providing arbitration and routing mechanisms, as was discussed in the preceding sections of this article. We show that the network-centric objective of selfishly optimizing network parameters will be defeated by user-centric selfish goals of reduction of traveling delays, fuel costs and road tolls etc.

[1]https://rhythmtraffic.com/

[2]https://www.surtrac.net/

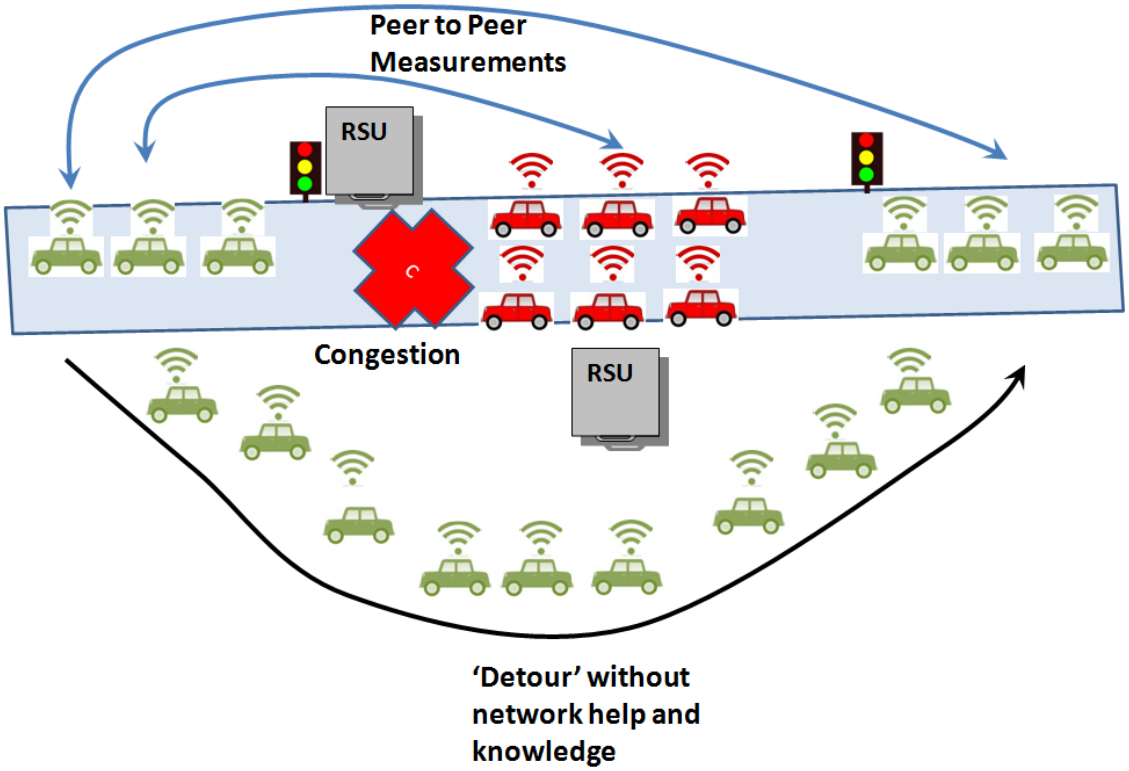

FIGURE 5. Potential of Selfish Behaviour on the IAV: 'Detour' taken by AVs as a reactive measure to imminent Traffic Hotspot by P2P measurements.

IV. CHALLENGES OF INFORMATION PROPAGATION MODELS OVER THE IAVs

A. CENTRALIZED VS DISTRIBUTED MODELS

Current models envision that traffic information over the IAV will be communicated to a central server to manage the resources for the AVs on the traffic network. However, as traffic conditions vary quickly over the network, the fastest possible mechanism for sharing such development will not be through centralized schemes but through gossiping between distributed domains. The routers in the internet learn of important developments on the network by gossiping with immediate peers, for example, when some part of the network they were able to reach is no longer reachable or is reachable with a new cost. Similar architecture may be used over IAV for scalable and fast dissemination of traffic information over the network. While the network will aim to aggregate such information for global optimization often taking much time, selfish AVs may query other AVs for their view of the traffic situation without reliance on the network view and try to take navigation decisions themselves without the involvement of the network as shown in Fig. 5. Although, 5th generation (5G) wireless technologies can provide us with an uninterrupted connected world, but it comes with its own problems that require sophisticated resource management and isolation techniques. Some research has been in progress to combine Multi-access Edge Computing (MEC) and Radio Access Network (RAN) to allow modification of specific network slices for latency-sensitive and bitrate demanding tasks [53]. Thus we argue, that while information may be propagated to centralized servers, the real-time decision in the IAV may be through distributed information exchanges.

B. PROACTIVE VS REACTIVE MODELS

Information exchanges at the physical layer of the IAV, such as V2R, V2V, and V2I, will use the popular technologies as mentioned before, e.g., DSRC and WAVE. However, while the primary mode is proactive whereby vehicles continuously exchange information with each other to make real-time driving decisions such as maintaining inter car safe distance for platoon formation and indicating other vehicles about the next driving decision so that they can plan their trajectory accordingly. Reactive mode of communication will be used for value-added services such as navigation services for finding the most efficient route to a destination (as discussed in the next section) by gossiping amongst nearby AVs.

V. CHALLENGES OF NAVIGATION MODELS OVER THE IAVs

The navigation model in the IAV resembles closely to the problem of path discovery in the legacy Internet, which is discussed further in the following sub-sections.

A. CENTRALIZED AND DISTRIBUTED CLIENT SERVER BASED NAVIGATION SERVICES

In the centralized model distributed AVs share their measurements (traveling delays, surrounding traffic density etc.) both in real-time and non-real-time which are then used by one or

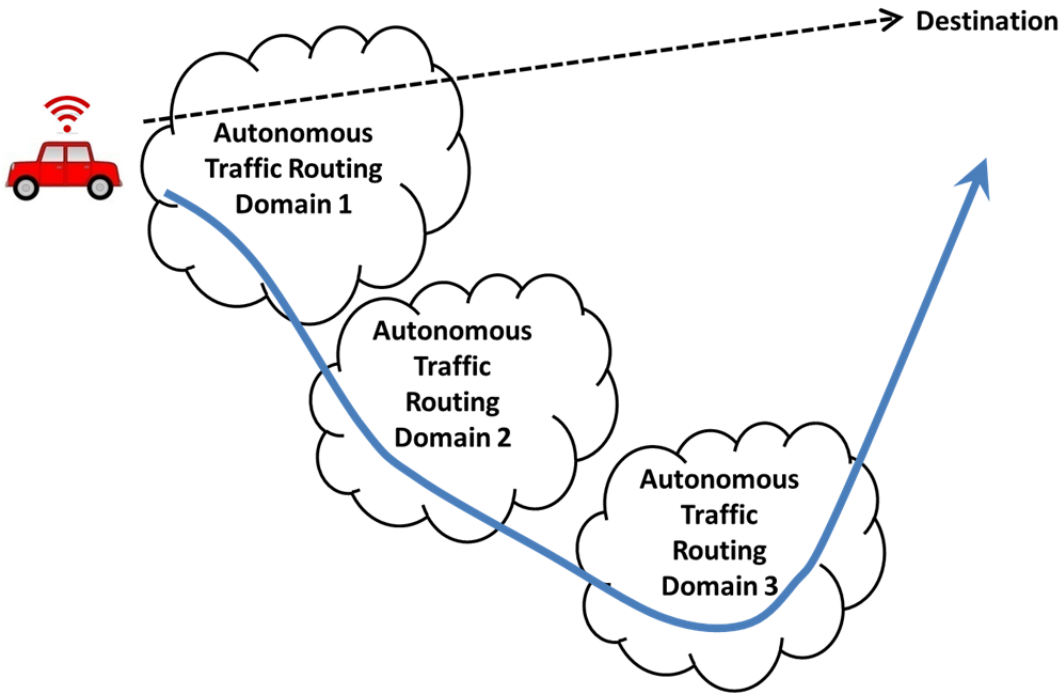

FIGURE 6. Implications of Hot Potato Routing in the IAV like the Legacy Internet.

more central network entities to guide them when requested by an AV (possibly indicating service level expected), about the best possible route. This model is loosely equivalent to the network-assisted source-based routing model in the legacy internet [81]. However, as more and more autonomous cars are added to the system, there are bound to be: (i) Scalability issues with this centralized route computation model. (ii) Traffic conditions on the roads may be varying quickly with the emergence of routes reducing the efficiency of one-time end-to-end path computation. (iii) Problems of selfish peers (AVs) not sharing their measurements timely, truthfully, or at all. Thus, network-based navigation services may be based on distributed traffic routing domains as in the internet for scalability. An AV approaching a new routing domain may request navigation help in reaching the intended destination and is guided with next-hop navigation to the next routing domain while taking the AV one step closer to the destination.

This new model may resolve scalability issues, but selfish decisions by the autonomous traffic domains may lead to inferior paths. A classic example from the internet is 'Hot Potato' routing [82], which is a well-known concept in the internet whereby an ISP does not let packets transit through its network that are not destined for it.

Similarly, individual IAV traffic routing domains will make selfish decisions to improve their level of service for customers that must use its resources to reach intended destination degrading the service of autonomous cars 'only' wishing to transit through it to get to their intended destination as depicted in Fig. 6. Autonomous cars diverted to other Autonomous Traffic domains continue to be offered the same treatment until it finally does reach its destination with sub-optimal travel metrics.

B. P2P AND THIRD-PARTY BASED NAVIGATION SERVICES

An easy way to defeat the above model is that autonomous peers share their views of the network with each other and decide upon the best possible path themselves selfishly, as shown in Fig. 5. Peers participating in a P2P network query each other for navigation services and autonomous cars may be directed to use this route instead of one indicated by traffic network.

Researchers envision that a central or several distributed traffic management authorities will collect real-time road traffic conditions from connected vehicles network and crunch the numbers in their computing facilities to develop the eco traffic plans. However, over time, more and more third parties will be coming up with their own algorithms, and subscription plans for ease of commuters often benefitting with user shared real-time measurements.

C. WARDROP EQUILIBRIUM

Network assisted navigation services will equip the users back again with the liberty to make selfish decisions. Researchers have interestingly come up with a game theory-based approach to understand the behavior of selfish drivers on the network, each choosing the best or shortest time duration path on the network [83]. Each driver will try to use whatever route is quickest, but this may make other routes

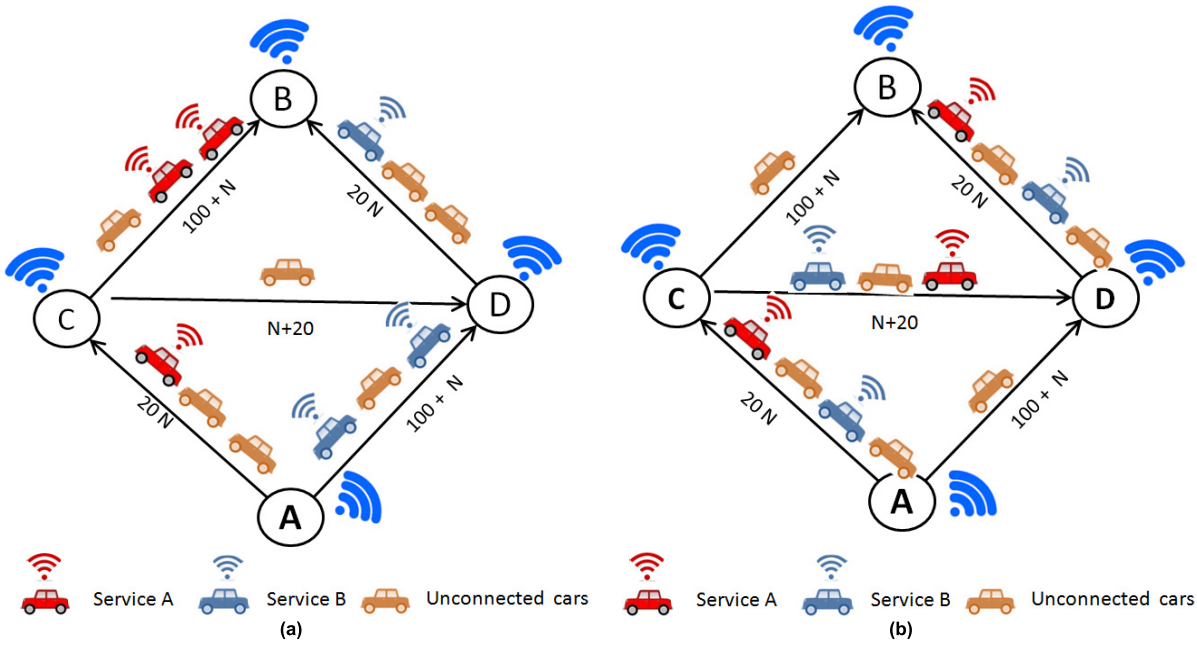

FIGURE 7. (a) (Right) Traffic along original paths ACB and ADB. Link Delays mentioned alongside as a function of the number of vehicles' N' (b) (Left) Demonstration of Braess's paradox. Selfish decision by some motorists to reduce their delay lead to the use of two parallel paths ACB and ACDB, causing everyone's delay to increase in spite of the addition of more resources on the network.

quicker or slower and cause other drivers to change their routes. The network only attains equilibrium, referred to as Wardrop Equilibrium, when each driver cannot reduce his delay by switching his path. Such selfish behavior is made more convenient through the availability of traffic congestion information through the Internet of Vehicles framework. We demonstrate this effect through a toy example. Fig. 7(a) shows the original two paths between the nodes A and B via nodes C and D. We expect the level of congestion at a link to depend on the total flow through the link. Thus, each link delay is a function of the number of vehicles present, and is indicated along with each link. Here, it is assumed that waiting times at traffic signals are considered negligible for these dominant modes of traffic, so traveling times are predominantly just a function of traveling delays dependent on levels of congestion. Initially, each path ACB and ADB has a path delay of $(20 \times 3) + (100 + 3) = 163$ time units. We assume AVs take suggestions from two different but equally popular organizations (Service A and Service B) employing different algorithms of suggesting the best possible path with the least traveling times. Due to some minor differences in algorithms, Service A suggests path ACB as the optimal path, and Service B suggests path ADB as the optimal path, both having the same delays of 163-time units. Services A and B, however, continually look for lower delay paths, and they simultaneously consider path ACDB with expected lower time delay of $(20 \times 3) \times 2 + (20 + 1) = 141$-time units. Both services suggest this new path to their customers, and traffic is switched to this new path. The addition of this link CD should have relieved congestion, but ironically the addition of a link causes the journey time of Service A and Service B subscribers to lengthen to $(20 \times 4) \times 2 + (20 + 3) = 183$-time units as well as the original paths to $(20 \times 4) + (100 + 1) = 181$-time units as shown in Fig. 7(b). Due to the decision being taken selfishly by users of Service Providers A and B, they will again converge to one of the original paths, in turn, congesting them again and selecting others just like in this case, causing the process of oscillations to continue until Wardrop equilibrium is established.

Surprisingly identification of unused or underused network resources by drivers for redistribution of traffic can worsen overall QoS for all users, as was shown in the preceding example; this phenomenon is identified as the Braess's paradox [83]. It is not possible for the Traffic Authorities to adapt their signal timing plans to manage traffic fluctuations at such short time scales due to these route oscillations.

VI. CHALLENGES OF TRAFFIC GROOMING IN IAVs

Just in the legacy internet controlling traffic is of vital importance for fair service to all users. Traffic Grooming refers to several facets of traffic control. For example, traffic scheduling covers the problem of traffic arbitration at convergence points such as traffic intersection points, which creates minimum queueing and waiting delays. Similarly, congestion control and flow control refer to controlling the volume of ingress traffic at specified points in the network so as not to create hot spots in the network and enable fair resource sharing by all users.

A. TRAFFIC SCHEDULING

Traffic Scheduling refers to that aspect of the IAV where contention-free arbitration would have to be provided to

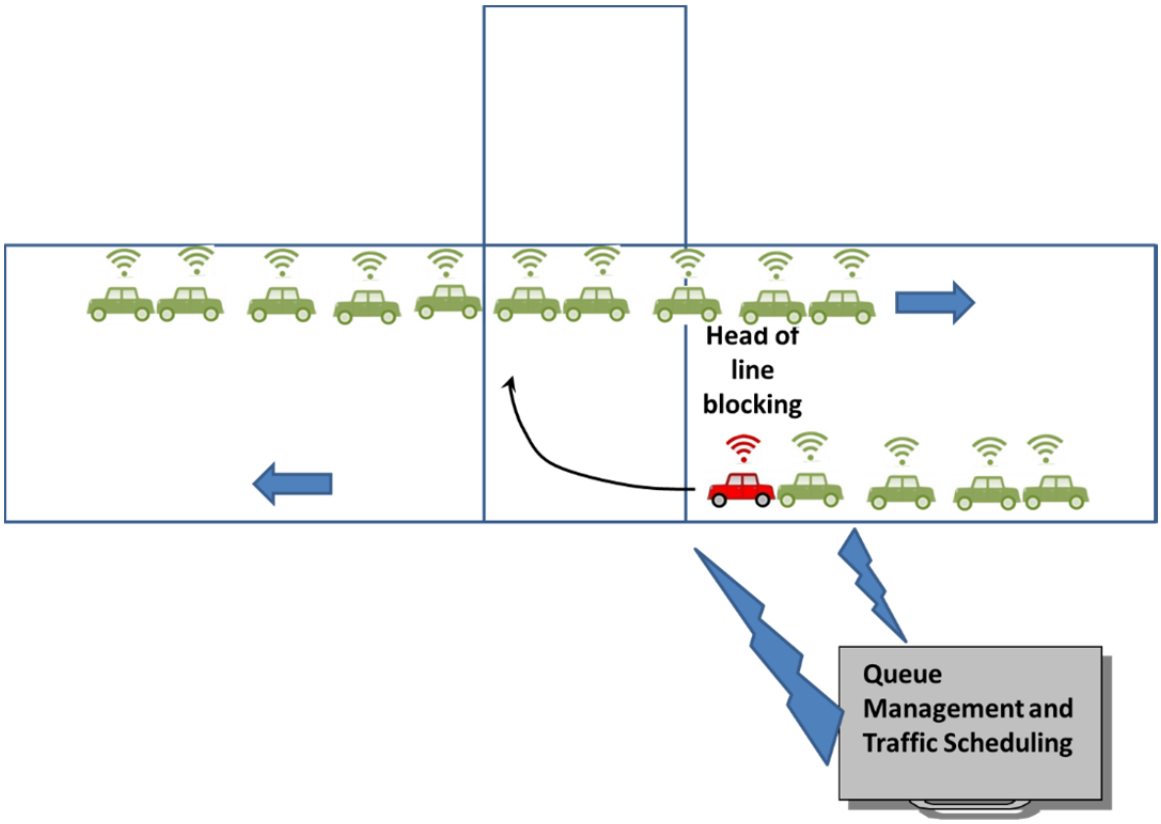

FIGURE 8. Like a conventional Internet Router, a possible scenario of Head-of-Line blocking in an IAV.

vehicles are convergence points such as intersections and roundabouts. Traffic Authorities would aim to optimize the global parameters of the network rather than benefit only a subset of users. On the other hand, all commuters in an IAV would make selfish driving decisions to reduce their traveling delays. However, at such intersection points, the arbitration would have to be provided by the central or distributed traffic controller after the reception of connected vehicle data. It is envisioned that in the future, in a well behaved connected vehicle model, AVs especially will be availing navigation directions from well-regulated traffic plans by traffic authorities and arbitrate contention-free access at traffic intersections through mutual intelligent coordination.

These models would require very sophisticated algorithms, such as those based on efficient control system algorithms [30], [41]. The latest ideas could be borrowed from the state-of-the-art queueing algorithms being proposed for data center networks as in the legacy Internet, enabling zero queues [77].

Two research groups at MIT have independently come up with the very radical idea of implementing software-defined arbitration at points of intersection in coordination with Traffic sources in any network, be it a Datacenter [77], [78] or a Road Traffic network [79]. The idea revolves around a centralized arbiter deciding upon the transmission time and the path through the network. The arbiter makes sure that situations like Head of Line Blocking, as shown in Fig. 8 does not occur where an entire traffic queue at intersections cannot make progress due to the progress of ahead of the queue, which cannot be immediately serviced blocking them. In slot based intersection arbitration, AVs can be instructed by smart traffic intersections to speed up or slow down for collision-free access to the traffic intersection. The reservation-based access made by future autonomous cars will be managed by the traffic controller of the intersection in real-time allocating time slots to AVs. This is not much unlike the service architecture of the routes in the legacy Internet.

B. CONGESTION AND FLOW CONTROL

Traffic in the internet has to be regulated to prevent choking network bandwidth. The first and foremost algorithm to regulate traffic volumes is using the closed-loop TCP flow control and congestion control algorithm. In this algorithm, the sender keeps track of the amount of traffic injected in the network, reducing the flow as congestion or impending congestion is detected. Recent work [78] has discussed in length the application of communication network-related concepts of Random Early Detection in Intelligent Transport Networks. The idea comes from the internet; in Random Early Detection, packets are dropped by Internet Routers even before congestion has happened to warn senders to reduce their sending rate due to imminent congestion, thus predicting and preventing congestion [84]. This approach can be modified in transportation networks to increase the green phase times of the traffic flows that may soon be the cause

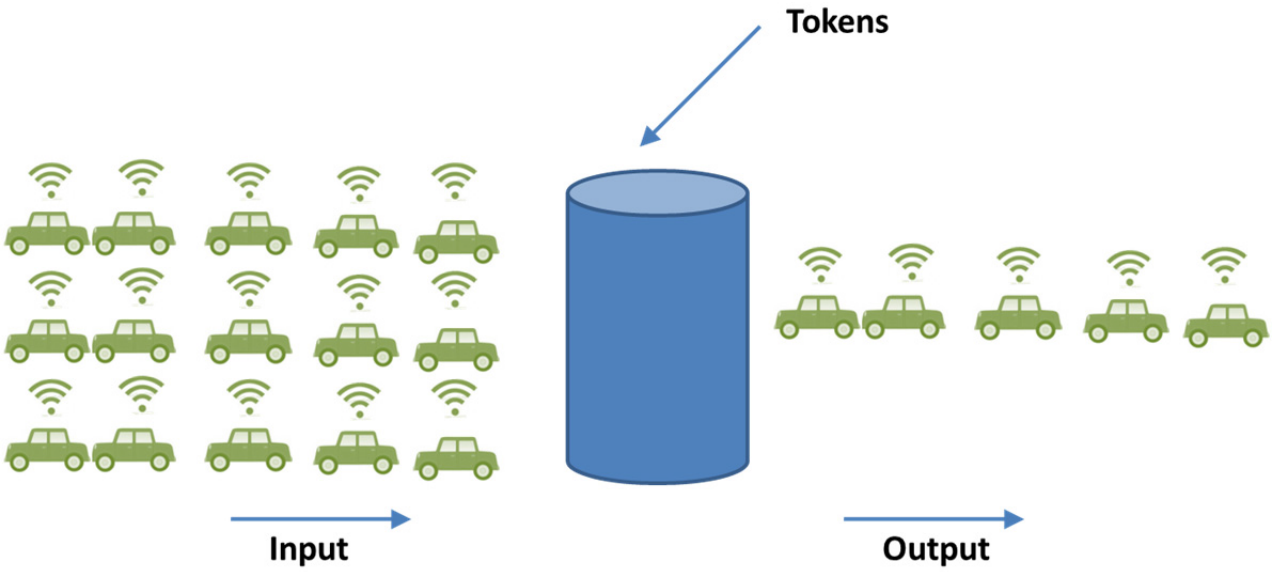

FIGURE 9. Token Bucket Regulator for Traffic Shaping in an IAV as used in the legacy Internet.

of congestion in the network while not starving other traffic. In the IAV, the notion of a flow can be visualized as Origin-Destination Flows, where origin and destinations are defined at a course level of sub-urban areas connected through a dense and congested core of the main central business districts (CBDs). We foresee that in order to regulate traffic on the IAV, we will need similar closed-loop flow and congestion control mechanisms such as the TCP/IP protocol stack of the internet, which will mainly be incorporated at the ingress and egress points of these sub-urban areas. AVs in transit with similar origin-destination identifiers will be treated as one flow and will regularly communicate their trip progress with the roadside equipment. The roadside units will continuously exchange this information with the corresponding sub-urban egress points of these vehicles.

AVs will be discharged into the network based on existing levels of congestion in the network as well as ingress points of their intended destinations. Such traffic schedulers to regulate discharge will be based on similar concepts of Token Bucket Regulators, as depicted in Fig. 9.

In this approach, a conceptual 'bucket' is filled with tokens at a constant rate dictated by the rate at which traffic should be discharged from that point.

Each token makes a certain amount of traffic at the input to be transferred to the output. This keeps flash crowds in check.

VII. PEER-TO-PEER (P2P), DATA RELAYING AND VALUE-ADDED SERVICES OVER IAVs?

A. PERSONAL (NON-IAV) DATA SERVICES

While the initial plan is that the Internet of Vehicles will only exchange information related to efficient traffic management. The rise in the internet of vehicles over the next decade will spark an unprecedented increase in the use of data service even when people are not the move, facilitated with the recent advancement of driver assistance features in AVs. Internet of vehicles may amongst themselves form an ad-hoc P2P network, and people may find themselves downloading the latest movies and songs from other peers' collections and uploading theirs [85]. This peer association may develop through trustworthiness established between commuters with similar transport routines, e.g., traveling to/from office at similar times. Similarly, another service peers may request over the Internet of Vehicles peers not having back end internet connectivity may request 'access point' request from other peers.

B. VALUE ADDED SERVICES OVER IAVs

As more and more users will be able to give up their privacy in exchange for value-added service over the internet of vehicles, they will become targets for electronic marketing firms to promote their services and businesses [85] and cyber threats as discussed in the next section.

C. TRANSIT (RELAY) NODES FOR OTHER DATA NETWORKS

The advent and deployment of 5G wireless technologies are bringing a paradigm shift in the way users currently communicate by providing data-rates of up to 10Gbps, 1-ms latency, and reduced power consumption, etc. [86], [87]. Moreover, extensive research efforts are already underway for the future Beyond 5G (B5G) and 6^{th} generation (6G) [88], [89] wireless technologies operating at very high frequencies, i.e., terahertz (THz) frequency bands. One of the critical problems that exist at these frequency bands is the high propagation path loss, which leads to lower transmission distances [88].

In these new (5G) and upcoming (B5G and 6G) wireless technologies, if the IAV nodes could be used as relays for data

transit, then there would have to be a balance in data priorities for signal transmissions. It is very critical for the IAV nodes because any latency in data transmission could have a disastrous impact on the IAVs, such as causing accidents through a domino effect.

VIII. CHALLENGES OF CYBER THREAT TO IAVs

Just like the conventional internet, users of IAV are prone to network disruptions or theft of personal information. In this section, we highlight some of these issues. The intensification in the requirement of connected applications like connected vehicles, is also giving rise to challenges related to privacy, authentication, and security. Security is pretty much related to the reliability factor as one single incident due to the security breach can lead to the loss of consumer's trust in the latest technology [90]. The repercussion of vulnerabilities to end-users of IAVs includes property and data theft, physical harm, and compromise of privacy [91].

A modern Connected and Autonomous Vehicle (CAV) consists of several tens of ECUs coordinated to each other with hundreds of millions of code to operate effectively [92]–[94]. This brings vulnerabilities that can be exploited to generate a cyber-attacks. One can imagine the adversities of CAV cyber-attacks by keeping in mind that Windows Vista has tens of million lines of code and has about thousand known vulnerabilities that were successfully exploited to generate huge scale attacks like WannaCry and NotPeyta [95].

A. DENIAL OF SERVICE (DOS) ATTACKS (SYBIL, GRAYHOLE, WORMHOLE, RUSHING ATTACKS)

Another potential attack surface of CAV is DSRC that is used for V2V and V2I communications. IEEE 802.11p WAVE is the primary DSRC communication standard is found to be vulnerable against jamming denial of service (DoS) attack [98]. Other possible attacks through DSRC are global positioning system (GPS) spoofing, location tracking, and masquerading, etc.

In recent years, several researchers have proposed different strategies and frameworks to mitigate the effect of cyber-attacks. In [99], the authors discuss a three-prong strategy based on OTA, Cloud-based, and layered based solutions for protecting against cyber threats. In [100], Khan *et al.* proposed LSTM-NN based false information attack detection framework for the SDN in-vehicle Ethernet network. The advantage SDN in terms of security management is that the network is easily programmable and less error-prone compare to the traditional network due to centralized control overflow. Hence, the security policy can be updated easily.

The number of advanced IDS has been proposed by Alheeti *et al.* for CAV that are not based on the data field of the CAV frame [101]–[104]. In [101], the authors proposed a novel IDS based on Integrated Circuit Metric technology. It uses the bias values of magnetometer sensors and simulated vehicle network traffic. A hierarchical IDS based on clustering and log data was proposed in [102]. It is designed explicitly for Sybil and Wormhole attacks. In [104], the authors proposed an IDS to detect anomaly exhibited by external communication of CAVs due to gray hole and rushing attacks, which primarily disturb communication between roadside equipment and vehicles. It extracts features of attacks from trace files and consists of a feed-forward neural network (FFNN) and a support vector machine (SVM).

Driverless taxis services are already exiting in the market (e.g., Waymo). This new sort of concept, thanks to IAVs, brings challenges in terms of security. In paper [105], the authors proposed a behavioral-biometric-based authentication scheme for riders. The papers [106], [107] highlights the impact and adversity of hacking a single driverless car on traffic congestion. In a nutshell, we believe that cybersecurity in term of IAVs is still an open research domain, and we require a more innovative and out-of-box solution to address this new sort of security threats and challenges.

B. HACKING ATTACKS ON ELECTRONIC SENSORS OF AVs

Vehicles consist of various electronic subsystems. Every subsystem includes ECU for managing various modules like airbags in case of any emergency, braking system, and Engine control. These subsystems execute on their own allocated communication modules like DSRC radios for V2V safety communications and embedded cellular module that is an essential component of the telematics system. The interface of distinctly allocated communication modules with the surroundings is to be protected individually [57].

For the physical interactions among the various sensors and ECUs, manufacturers standardized on specific buses, like the Controller Area Network (CAN), which serves as a bridge among layers of data protocol; hence it became the primary network for communication of intra-vehicle networks. Due to the physical and rational transmission of CAN packets to nodes, any malefic element could effortlessly interfere with the network communications or send packets to other nodes [56].

OBD ports that are mandatory in modern vehicles are also potential attack surface for CAV. In a survey [96], it is claimed that 50% of OBD ports are highly vulnerable to hacking. In [97], authors successfully crafts as cyber-attacks through OBD port and trigger a specific message on the bus.

GPS is utilized to localize and position on the unified map. GPS spoofing or jamming is performed to duplicate the signals and introduce incorrect locations [47].

The infrastructure of connectivity for IAVs involves V2V, V2I, V2R, and the ''cloud''. The integration of IAVs with various communication infrastructures will necessarily cause it to be accessible through the internet, making them vulnerable to damaging attacks. Generally, this security breach involves password and key attacks. They are categorized as a dictionary attack, rainbow table attack, and brute force attack. Another type is DoS, in which attacks are targeted on the system's normal service. It is disrupted either by an individual or various targeting systems. Other attacks include Phishing, Network protocol attacks, and Rogue updates [58].

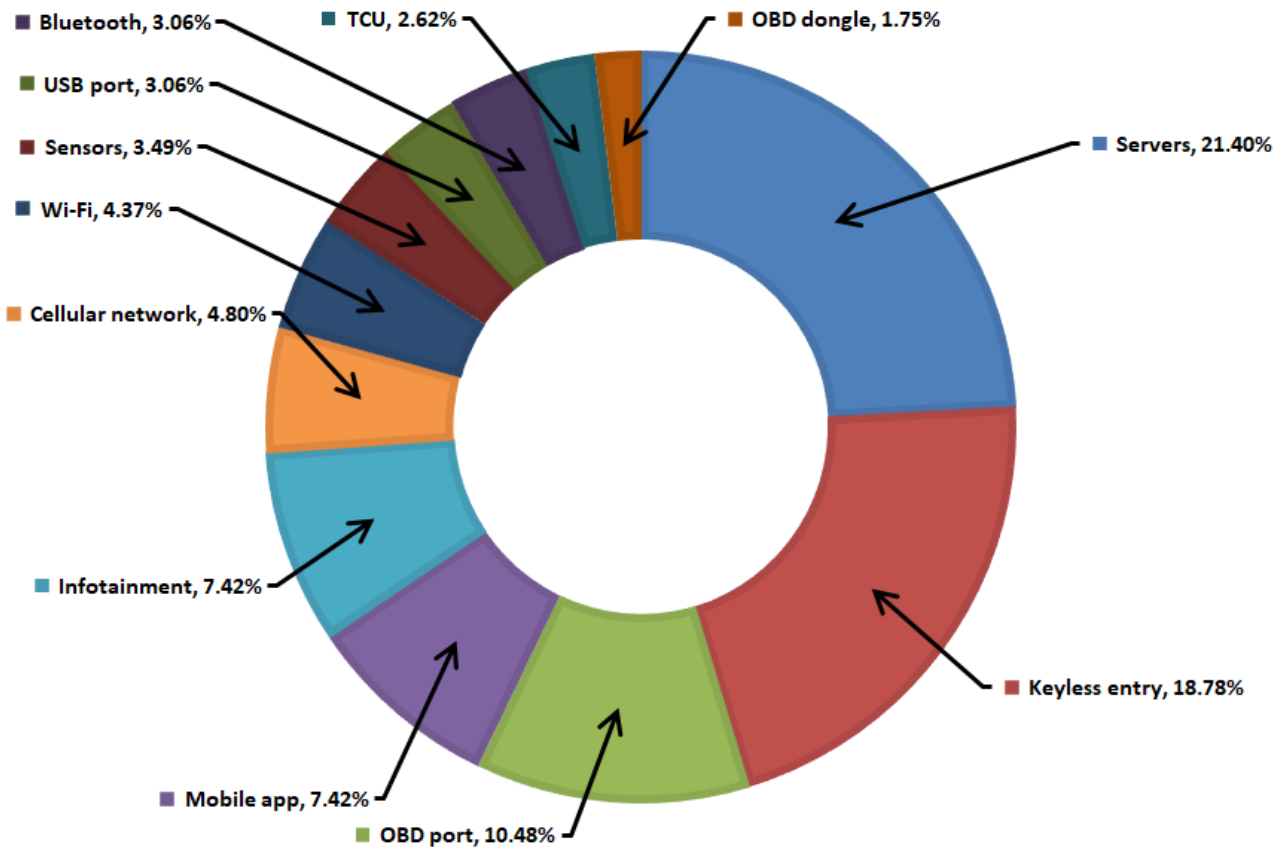

FIGURE 10. Attack Probability On Different Attack Surfaces.

The communication among primary and secondary sensors of IAV and their underlying connections might permit an unauthorized entry to let undesired data into the system of IAV by identifying the weakest spot. Furthermore, LIDARs features of the IAV can be easily tricked into making incorrect decisions by saturation and spoofing techniques leading towards accidents and thefts [91].

Different types of mediums are used to attack IAVs. Fig. 10 represents the likelihood of their occurrence with respect to each medium [108].

IX. CONCLUSION/FUTURE WORK

In this paper, the authors presented an exhaustive review of the Internet of Autonomous Vehicles (IAVs), which are drawing a lot of attention due to the widespread deployment of the IoT technology worldwide. The main aim of this paper was to discuss the synergy between network-selfish and user-selfish behavior learning from previous experiences in internet technology.

The survey paper presented a review of the layered architecture proposed and used by the IAVs systems. The physical layer communications standards like Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside unit (V2R) and Vehicle-to-Infrastructure (V2I), etc., frequency bands, modulation type and devices used are also discussed. The behavior of autonomous vehicles (AVs) in the IAV system is also discussed in detail with special emphasis on the key technologies like control over V2V for collision avoidance, lane detection, maintaining a safe distance between vehicles etc. Moreover, the impact of Intelligent Intersections in the IAV network is discussed by taking examples from the first generation of deployed intelligent systems like SCOOT and SCATS systems from Australia. Then, more recent examples are also discussed, like InSync, SURTRAC, and AVIAN systems from the USA.

The paper also discusses in great depth the challenges of information propagation models, navigation models, traffic scheduling and congestion, and flow control in the IAVs system. The most critical challenge discussed in this paper is related to the cybersecurity threat and their related vulnerabilities to the IAV network. This is the most important and challenging factor for the AVs in the IAV system because it is directly related to the reliability of the IAV system. One security breach can lead to the loss of human life and consumer trust from this technology. These challenges and how to mitigate them are discussed.

As mentioned throughout in this paper, future research in the area of IAV will definitely face challenges in finding the correct equilibrium of network-centric and user-centric behavior patterns aimed to benefit both selfishly. Another critical challenge will be to design efficient architectures for scalable distributed information exchange in the network

domain to compete with possible P2P associations between the IAV nodes bypassing the network service provisioning completely for navigation and other services. Traffic Grooming is a service that is inherently network-centric; selfish users present a direct challenge to this problem. Similarly, Value-Added Services over IAV networks or IAV nodes behaving as relay nodes for other non-IAV related data services will pose a threat to timely exchanges of real-time, mission-critical data over IAVs. Lastly, the threat of cyber-attacks on such IAVs is as much of a real challenge as in the legacy Internet.

The comprehensive review presented in this paper will help in more coordinated efforts from both the industry and the academic researchers for bringing about improvements in the IAV technologies. This may give future directions to designers/engineers/researchers working on improving the capabilities of future IAVs.

REFERENCES

[1] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 241–246, doi: 10.1109/WF-IoT.2014.6803166.

[2] T. Koslowski. (Apr. 2013). *Forget the Internet of Things: Here Comes the Internet of Cars*. [Online]. Available: https://www.wired.com/2013/01/forget-the-internet-of-things-here-comes-the-internet-of-cars/

[3] B. Nemade, "Automatic traffic surveillance using video tracking," *Procedia Comput. Sci.*, vol. 79, pp. 402–409, Jan. 2016, doi: 10.1016/j.procs.2016.03.052.

[4] Z. Wang, W. Huo, P. Yu, L. Qi, and N. Cao, "Research on vehicle taillight detection and semantic recognition based on Internet of vehicle," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Zhengzhou, China, Oct. 2018, pp. 147–1473, doi: 10.1109/CyberC.2018.00038.

[5] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016, doi: 10.1109/ACCESS.2016.2603219.

[6] J. Contreras-Castillo, S. Zeadally, and J. A. G. Ibáñez, "A seven-layered model architecture for Internet of vehicles," *J. Inf. Telecommun.*, vol. 1, no. 1, pp. 4–22, Jan. 2017, doi: 10.1080/24751839.2017.1295601.

[7] T. Roughgarden and É. Tardos, "How bad is selfish routing?" *J. ACM*, vol. 49, no. 2, pp. 236–259, Mar. 2002, doi: 10.1145/506147.506153.

[8] A.-J. Su, D. R. Choffnes, A. Kuzmanovic, and F. E. Bustamante, "Drafting behind Akamai: Inferring network conditions based on CDN redirections," *IEEE/ACM Trans. Netw.*, vol. 17, no. 6, pp. 1752–1765, Dec. 2009, doi: 10.1109/TNET.2009.2022157.

[9] R. Keralapura, C.-N. Chuah, N. Taft, and G. Iannaccone, "Race conditions in coexisting overlay networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 1, pp. 1–14, Feb. 2008, doi: 10.1109/TNET.2007.897959.

[10] V. Aggarwal, A. Feldmann, and C. Scheideler, "Can ISPS and P2P users cooperate for improved performance?" *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 3, p. 29, Jul. 2007, doi: 10.1145/1273445.1273449.

[11] V. Pandey, "Towards widespread SDN adoption: Need for synergy between photonics and SDN within the data center," in *Proc. IEEE Photon. Soc. Summer Top. Meeting Ser.*, Jul. 2013, pp. 227–228, doi: 10.1109/PHOSST.2013.6614478.

[12] J. M. Anderson, K. Nidhi, K. Stanley, P. Sorensen, C. Samaras, and O. Oluwatola, "Autonomous vehicle technology: A guide for policymakers," Rand Corp., Santa Monica, CA, USA, Tech. Rep., 2016, doi: 10.7249/RR443-2.

[13] S. A. Bagloee, M. Tavana, M. Asadi, and T. Oliver, "Autonomous vehicles: Challenges, opportunities, and future implications for transportation policies," *J. Mod. Transp.*, vol. 24, no. 4, pp. 284–303, Dec. 2016, doi: 10.1007/s40534-016-0117-3.

[14] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[15] K. Shafique, B. A. Khawaja, M. D. Khurram, S. M. Sibtain, Y. Siddiqui, M. Mustaqim, H. T. Chattha, and X. Yang, "Energy harvesting using a low-cost rectenna for Internet of Things (IoT) applications," *IEEE Access*, vol. 6, pp. 30932–30941, 2018, doi: 10.1109/ACCESS.2018.2834392.

[16] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of Internet of vehicles," *China Commun.*, vol. 11, no. 10, pp. 1–15, Oct. 2014, doi: 10.1109/CC.2014.6969789.

[17] E. Uhlemann, "Time for autonomous vehicles to connect [connected vehicles]," *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 10–13, Sep. 2018, doi: 10.1109/MVT.2018.2848342.

[18] M. Song, K. Zhong, J. Zhang, Y. Hu, D. Liu, W. Zhang, J. Wang, and T. Li, "*In-situ* AI: Towards autonomous and incremental deep learning for IoT systems," in *Proc. IEEE Int. Symp. High Perform. Comput. Archit. (HPCA)*, Vienna, Austria, Feb. 2018, pp. 92–103, doi: 10.1109/HPCA.2018.00018.

[19] J. Guo, Z. Wang, X. Shi, X. Yang, P. Yu, L. Feng, and W. Li, "A deep reinforcement learning based mechanism for cell outage compensation in massive IoT environments," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Tangier, Morocco, Jun. 2019, pp. 284–289, doi: 10.1109/IWCMC.2019.8766654.

[20] A. Carrio, C. Sampedro, A. Rodriguez-Ramos, and P. Campoy, "A review of deep learning methods and applications for unmanned aerial vehicles," *J. Sensors*, vol. 2017, pp. 1–13, Aug. 2017, doi: 10.1155/2017/3296874.

[21] S. Grigorescu, B. Trasnea, T. Cocias, and G. Macesanu, "A survey of deep learning techniques for autonomous driving," *J. Field Robot.*, vol. 37, no. 3, pp. 362–386, Apr. 2020, doi: 10.1002/rob.21918.

[22] Y. Li, "An overview of the DSRC/WAVE technology," in *Quality, Reliability, Security and Robustness in Heterogeneous Networks*, vol. 74. Berlin, Germany: Springer, 2012, pp. 544–558.

[23] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the united states," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011, doi: 10.1109/JPROC.2011.2132790.

[24] X. Wu, S. Subramanian, R. Guha, R. G. White, J. Li, K. W. Lu, A. Bucceri, and T. Zhang, "Vehicular communications using DSRC: Challenges, enhancements, and evolution," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 399–408, Sep. 2013, doi: 10.1109/JSAC.2013.SUP.0513036.

[25] H.-M. Tsai, O. K. Tonguz, C. Saraydar, T. Talty, M. Ames, and A. Macdonald, "ZigBee-based intra-car wireless sensor networks: A case study," *IEEE Wireless Commun.*, vol. 14, no. 6, pp. 67–77, Dec. 2007, doi: 10.1109/MWC.2007.4407229.

[26] L. Alonso, V. Milanés, C. Torre-Ferrero, J. Godoy, J. P. Oria, and T. De Pedro, "Ultrasonic sensors in urban traffic driving-aid systems," *Sensors*, vol. 11, no. 1, pp. 661–673, Jan. 2011, doi: 10.3390/s110100661.

[27] S. Wei, Y. Zou, X. Zhang, T. Zhang, and X. Li, "An integrated longitudinal and lateral vehicle following control system with radar and vehicle-to-vehicle communication," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1116–1127, Feb. 2019, doi: 10.1109/TVT.2018.2890418.

[28] H. Alismail and B. Browning, "Automatic calibration of spinning actuated LiDAR internal parameters: Automatic calibration of spinning actuated LiDAR," *J. Field Robot.*, vol. 32, no. 5, pp. 723–747, Aug. 2015, doi: 10.1002/rob.21543.

[29] E. Shang, X. An, T. Wu, T. Hu, Q. Yuan, and H. He, "LiDAR based negative obstacle detection for field autonomous land vehicles," *J. Field Robot.*, vol. 33, no. 5, pp. 591–617, Aug. 2016, doi: 10.1002/rob.21609.

[30] F. Luyanda, D. Gettman, L. Head, S. Shelby, D. Bullock, and P. Mirchandani, "ACS-lite algorithmic architecture: Applying adaptive control system technology to closed-loop traffic signal control systems," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1856, no. 1, pp. 175–184, Jan. 2003, doi: 10.3141/1856-19.

[31] S. Nonaka and T. Sakakibara, "Two-step control using invariant manifold on connected vehicle model," in *Proc. 58th Annu. Conf. Soc. Instrum. Control Eng. Jpn. (SICE)*, Hiroshima, Japan, Sep. 2019, pp. 319–324, doi: 10.23919/SICE.2019.8859745.

[32] S. A. Goli, B. H. Far, and A. O. Fapojuwo, "Vehicle trajectory prediction with Gaussian process regression in connected vehicle environment⋆," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Changshu, China, Jun. 2018, pp. 550–555, doi: 10.1109/IVS.2018.8500614.

[33] S. Yuan, P. Zhao, Q. Zhang, and X. Hu, "Research on model predictive control-based trajectory tracking for unmanned vehicles," in *Proc. 4th Int. Conf. Control Robot. Eng. (ICCRE)*, Nanjing, China, Apr. 2019, pp. 79–86, doi: 10.1109/ICCRE.2019.8724158.

[34] Y. Chen, J. Zha, and J. Wang, "An autonomous T-intersection driving strategy considering oncoming vehicles based on connected vehicle technology," *IEEE/ASME Trans. Mechatronics*, vol. 24, no. 6, pp. 2779–2790, Dec. 2019, doi: 10.1109/TMECH.2019.2942769.

[35] D. D. Yoon, G. G. M. N. Ali, and B. Ayalew, "Cooperative perception in connected vehicle traffic under field-of-view and participation variations," in *Proc. IEEE 2nd Connected Automated Vehicles Symp. (CAVS)*, Honolulu, HI, USA, Sep. 2019, pp. 1–6, doi: 10.1109/CAVS.2019.8887832.

[36] M. Cai, Q. Xu, K. Li, and J. Wang, "Multi-lane formation assignment and control for connected vehicles," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Paris, France, Jun. 2019, pp. 1968–1973, doi: 10.1109/IVS.2019.8813792.

[37] Y. Li and C. He, "Connected autonomous vehicle platoon control considering vehicle dynamic information," in *Proc. 37th Chin. Control Conf. (CCC)*, Wuhan, China, Jul. 2018, pp. 7834–7839, doi: 10.23919/ChiCC.2018.8483514.

[38] R. A. Dollar and A. Vahidi, "Efficient and collision-free anticipative cruise control in randomly mixed strings," *IEEE Trans. Intell. Vehicles*, vol. 3, no. 4, pp. 439–452, Dec. 2018, doi: 10.1109/TIV.2018.2873895.

[39] C. Han, J. Yang, M. Li, and L. Wu, "Robust cruise control of heterogeneous connected vehicle systems," in *Proc. Chin. Control Decis. Conf. (CCDC)*, Shenyang, China, Jun. 2018, pp. 6516–6520, doi: 10.1109/CCDC.2018.8408275.

[40] V. Astarita, V. P. Giofrè, G. Guido, and A. Vitale, "The use of adaptive traffic signal systems based on floating car data," *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–13, May s2017, doi: 10.1155/2017/4617451.

[41] J. Favilla, A. Machion, and F. Gomide, "Fuzzy traffic control: Adaptive strategies," in *Proc. 2nd IEEE Int. Conf. Fuzzy Syst.*, San Francisco, CA, USA, Mar./Apr. 1993, pp. 506–511, doi: 10.1109/FUZZY.1993.327519.

[42] S. Liu, W. Zhang, X. Wu, S. Feng, X. Pei, and D. Yao, "A simulation system and speed guidance algorithms for intersection traffic control using connected vehicle technology," *Tsinghua Sci. Technol.*, vol. 24, no. 2, pp. 160–170, Apr. 2019, doi: 10.26599/TST.2018.9010073.

[43] G. Shah, R. Valiente, N. Gupta, S. M. O. Gani, B. Toghi, Y. P. Fallah, and S. D. Gupta, "Real-time hardware-in-the-loop emulation framework for DSRC-based connected vehicle applications," in *Proc. IEEE 2nd Connected Automated Vehicles Symp. (CAVS)*, Honolulu, HI, USA, Sep. 2019, pp. 1–6, doi: 10.1109/CAVS.2019.8887797.

[44] J. Rios-Torres and A. A. Malikopoulos, "Impact of partial penetrations of connected and automated vehicles on fuel consumption and traffic flow," *IEEE Trans. Intell. Vehicles*, vol. 3, no. 4, pp. 453–462, Dec. 2018, doi: 10.1109/TIV.2018.2873899.

[45] J. Han, A. Sciarretta, L. L. Ojeda, G. De Nunzio, and L. Thibault, "Safe- and eco-driving control for connected and automated electric vehicles using analytical state-constrained optimal solution," *IEEE Trans. Intell. Vehicles*, vol. 3, no. 2, pp. 163–172, Jun. 2018, doi: 10.1109/TIV.2018.2804162.

[46] M. H. B. M. Nor and T. Namerikawa, "Merging of connected and automated vehicles at roundabout using model predictive control," in *Proc. 57th Annu. Conf. Soc. Instrum. Control Eng. Jpn. (SICE)*, Nara, Japan, Sep. 2018, pp. 272–277, doi: 10.23919/SICE.2018.8492635.

[47] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2014, doi: 10.1109/TITS.2014.2342271.

[48] E. Khorov, A. Lyakhov, A. Krotov, and A. Guschin, "A survey on IEEE 802.11ah: An enabling networking technology for smart cities," *Comput. Commun.*, vol. 58, pp. 53–69, Mar. 2015, doi: 10.1016/j.comcom.2014.08.008.

[49] L. Zhang, W. Cao, X. Zhang, and H. Xu, "MAC2: Enabling multicasting and congestion control with multichannel transmission for intelligent vehicle terminal in Internet of vehicles," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 8, pp. 1–20, Aug. 2018, doi: 10.1177/1550147718793586.

[50] K. Tachikawa. (2001). *Dedicated Short-Range Communications for ITS—Trends in Research, Development and Standardization*. [Online]. Available: http://www.oki.com/en/otr/downloads/otr-187-08.pdf

[51] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle landscape—Architectures, enabling technologies, applications, and development areas," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2391–2406, Aug. 2018, doi: 10.1109/TITS.2017.2749459.

[52] A. Bujari, C. E. Palazzi, and A. Vitella, "Broadcasting messages in the Internet of vehicles," in *Proc. IEEE 29th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Bologna, Italy, Sep. 2018, pp. 58–62, doi: 10.1109/PIMRC.2018.8580751.

[53] E. Coronado, G. Cebrian-Marquez, G. Baggio, and R. Riggio, "Addressing bitrate and latency requirements for connected and autonomous vehicles," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Paris, France, Apr. 2019, pp. 961–962, doi: 10.1109/INFCOMW.2019.8845099.

[54] Y. Wang, Y. Li, D. Tian, J. Wang, and J. Wang, "A method of visual management platform for connected vehicles data," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Shenzhen, China, Oct. 2015, pp. 175–179, doi: 10.1109/ICCVE.2015.89.

[55] O. Masutani, S. Nemoto, and Y. Hideshima, "Toward a better IPA experience for a connected vehicle by means of usage prediction," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Kyoto, Japan, Mar. 2019, pp. 681–686, doi: 10.1109/PERCOMW.2019.8730679.

[56] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, 2010, pp. 447–462, doi: 10.1109/SP.2010.34.

[57] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014, doi: 10.1109/JIOT.2014.2302386.

[58] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.

[59] X. Yang, J. Liu, F. Zhao, and N. H. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Proc. MOBIQUITOUS*, 2004, pp. 114–123, doi: 10.1109/MOBIQ.2004.1331717.

[60] J. Gozalvez, M. Sepulcre, and R. Bauza, "IEEE 802.11p vehicle to infrastructure communications in urban environments," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 176–183, May 2012, doi: 10.1109/MCOM.2012.6194400.

[61] B. Gallagher, H. Akatsuka, and H. Suzuki, "Wireless communications for vehicle safety: Radio link performance and wireless connectivity methods," *IEEE Veh. Technol. Mag.*, vol. 1, no. 4, pp. 4–24, Dec. 2006, doi: 10.1109/MVT.2006.343641.

[62] P. Alexander, D. Haley, and A. Grant, "Cooperative intelligent transport systems: 5.9-GHz field trials," *Proc. IEEE*, vol. 99, no. 7, pp. 1213–1235, Jul. 2011, doi: 10.1109/JPROC.2011.2105230.

[63] K.-C. Lan, Z. Wang, M. Hassan, T. Moors, R. Berriman, L. Libman, M. Ott, B. Landfeldt, and Z. Zaidi "Experiences in deploying a wireless mesh network testbed for traffic control," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 5, p. 17, Oct. 2007, doi: 10.1145/1290168.1290171.

[64] K.-C. Lan, A. Seneviratne, Z. Wang, R. Berriman, T. Moors, M. Hassan, L. Libman, M. Ott, B. Landfeldt, and Z. Zaidi, "Implementation of a wireless mesh network testbed for traffic control," in *Proc. 16th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2007, pp. 1022–1027, doi: 10.1109/ICCCN.2007.4317952.

[65] K. Bengler, K. Dietmayer, B. Farber, M. Maurer, C. Stiller, and H. Winner, "Three decades of driver assistance systems: Review and future perspectives," *IEEE Intell. Transp. Syst. Mag.*, vol. 6, no. 4, pp. 6–22, Oct. 2014, doi: 10.1109/MITS.2014.2336271.

[66] W. Knight. (2013). *Driverless Cars are Further Away than you Think*. [Online]. Available: https://www.technologyreview.com/s/520431/driverless-cars-are-further-away-than-you-think/

[67] Y. Wan, Y. Huang, and B. Buckles, "Camera calibration and vehicle tracking: Highway traffic video analytics," *Transp. Res. C, Emerg. Technol.*, vol. 44, pp. 202–213, Jul. 2014, doi: 10.1016/j.trc.2014.02.018.

[68] Google. (2015). *Google Self-Driving Car Project*. [Online]. Available: http://static. googleusercontent.com/media/www.google.com/en//selfdriving car/files/reports/report-0615.pdf

[69] J. Lee and B. Park, "Development and evaluation of a cooperative vehicle intersection control algorithm under the connected vehicles environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 81–90, Mar. 2012, doi: 10.1109/TITS.2011.2178836.

[70] K. Dresner and P. Stone, "A multiagent approach to autonomous intersection management," *J. Artif. Intell. Res.*, vol. 31, pp. 591–656, Mar. 2008.
[71] M. Papageorgiou, C. Kiakaki, V. Dinopoulou, A. Kotsialos, and Y. Wang, "Review of road traffic control strategies," *Proc. IEEE*, vol. 91, no. 12, pp. 2043–2067, Dec. 2003, doi: 10.1109/JPROC.2003.819610.
[72] T. L. Thorpe, "Vehicle traffic light control using SARSA," Dept. Comput. Sci., Colorado State Univ., Fort Collins, CO, USA, Masters Project Rep., Apr. 1997. Accessed: May 12, 2020. [Online]. Available: https://www.semanticscholar.org/paper/Vehicle-Traffic-Light-Control-Using-SARSA-Thorpe/b3cc49265733a355789696bab3f246578b1d2ca4
[73] D. I. Robertson and R. D. Bretherton, "Optimizing networks of traffic signals in real time-the SCOOT method," *IEEE Trans. Veh. Technol.*, vol. 40, no. 1, pp. 11–15, Feb. 1991, doi: 10.1109/25.69966.
[74] P. R. Lowrie, "SCATS: The Sydney coordinated adaptive traffic system-principles, methodology, algorithms," presented at the IEE Int. Conf. Road Traffic Signalling, London U.K., Apr. 1982, pp. 67–70.
[75] X.-F. Xie, S. F. Smith, L. Lu, and G. J. Barlow, "Schedule-driven intersection control," *Transp. Res. C, Emerg. Technol.*, vol. 24, pp. 168–189, Oct. 2012, doi: 10.1016/j.trc.2012.03.004.
[76] C. M. Day, D. M. Bullock, A. P. Nichols, T. M. Brennan, and C.-S. Chou, "Integrating adaptive and traffic responsive algorithms," *Procedia-Social Behav. Sci.*, vol. 48, pp. 3451–3460, Jan. 2012, doi: 10.1016/j.sbspro.2012.06.1309.
[77] J. Perry, A. Ousterhout, H. Balakrishnan, D. Shah, and H. Fugal, "Fastpass: A centralized 'zero-queue' datacenter network," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 307–318, Feb. 2015, doi: 10.1145/2740070.2626309.
[78] R. Sanchez-Iborra and M.-D. Cano, "On the similarities between urban traffic management and communication networks: Application of the random early detection algorithm for self-regulating intersections," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 4, pp. 48–61, 2017, doi: 10.1109/MITS.2017.2743202.
[79] R. Tachet, P. Santi, S. Sobolevsky, L. I. Reyes-Castro, E. Frazzoli, D. Helbing, and C. Ratti, "Revisiting street intersections using slot-based systems," *PLoS ONE*, vol. 11, no. 3, Mar. 2016, Art. no. e0149607, doi: 10.1371/journal.pone.0149607.
[80] L. Qiu, Y. R. Yang, Y. Zhang, and S. Shenker, "On selfish routing in Internet-like environments," *IEEE/ACM Trans. Netw.*, vol. 14, no. 4, pp. 725–738, Aug. 2006, doi: 10.1109/TNET.2006.880179.
[81] X. Yang and D. Wetherall, "Source selectable path diversity via routing deflections," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 36, no. 4, p. 159, Aug. 2006, doi: 10.1145/1151659.1159933.
[82] R. Teixeira, A. Shaikh, T. Griffin, and J. Rexford, "Dynamics of hot-potato routing in IP networks," in *Proc. Joint Int. Conf. Meas. Modeling Comput. Syst. (SIGMETRICS /PERFORMANCE)*, New York, NY, USA, 2004, p. 307, doi: 10.1145/1005686.1005723.
[83] F. Kelly, "The mathematics of traffic in networks," Princeton Companion Math., Princeton Univ. Press, Princeton, NJ, USA, Tech. Rep., 2008, pp. 862–870, vol. 1, no. 1. Accessed: May 20, 2020. [Online]. Available: http://www.statslab.cam.ac.uk/~frank/PAPERS/PRINCETON/pcm0052.pdf
[84] G. Varghese, *Network Algorithmics: An Interdisciplinary Approach to Designing Fast Networked Devices*. Boston, MA, USA: Elsevier, 2005.
[85] L. Zhang, Z. Zhao, Q. Wu, H. Zhao, H. Xu, and X. Wu, "Energy-aware dynamic resource allocation in UAV assisted mobile edge computing over social Internet of vehicles," *IEEE Access*, vol. 6, pp. 56700–56715, 2018, doi: 10.1109/ACCESS.2018.2872753.
[86] A. K. Vallappil, M. K. A. Rahim, B. A. Khawaja, and M. N. Iqbal, "Compact metamaterial based 4×4 butler matrix with improved bandwidth for 5G applications," *IEEE Access*, vol. 8, pp. 13573–13583, 2020.
[87] M. K. Ishfaq, T. A. Rahman, M. Himdi, H. T. Chattha, Y. Saleem, B. A. Khawaja, and F. Masud, "Compact four-element phased antenna array for 5G applications," *IEEE Access*, vol. 7, pp. 161103–161111, 2019.
[88] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019.
[89] I. Akyildiz, J. Jornet, and C. Han, "TeraNets: Ultra-broadband communication networks in the terahertz band," *IEEE Wireless Commun.*, vol. 21, no. 4, pp. 130–135, Aug. 2014.
[90] P. Papadimitratos, "On the road: Reflections on the security of vehicular communication systems," in *Proc. IEEE Int. Conf. Veh. Electron. Saf.*, Columbus, OH, USA, Sep. 2008, pp. 359–363, doi: 10.1109/ICVES.2008.4640913.
[91] AVIN APMA. (Sep. 2019). *Cybersecurity for Connected and Autonomous Vehicles: Considerations and Opportunities for Growth*. [Online]. Available: https://www.oce-ontario.org/docs/default-source/publications/oce-apma-deloitte_cav-cybersecurity-report_sept-2019.pdf?sfvrsn=2
[92] D. J. Glancy, "Privacy in autonomous vehicles," *Santa Clara L. Rev.*, vol. 52, no. 4, p. 1171, 2012.
[93] R. N. Charette, "This car runs on code," *IEEE Spectr.*, vol. 46, no. 3, p. 3, Feb. 2009.
[94] D. Klinedinst and C. King, "On board diagnostics: Risks and vulnerabilities of the connected vehicle," Softw. Eng. Inst., Carnegie Mellon Univ., CERT Coordination Center, Pittsburgh, PA, USA, Tech. Rep., Mar. 2016. Accessed: May 18, 2020. [Online]. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pdf
[95] N. Perlroth, M. Scott, and S. Frenkel, "Cyberattack hits Ukraine then spreads internationally," New York Times, vol. 27, 2017.
[96] W. Yan, "A two-year survey on security challenges in automotive threat landscape," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Oct. 2015, pp. 185–189.
[97] D. K. Nilsson and U. E. Larson, "Simulated attacks on CAN buses: Vehicle virus," in *Proc. IASTED Int. Conf. Commun. Syst. Netw. (AsiaCSN)*, 2008, pp. 66–72.
[98] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.
[99] M. H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 45–51, Jun. 2017, doi: 10.1109/MVT.2017.2669348.
[100] Z. Khan, M. Chowdhury, M. Islam, C.-Y. Huang, and M. Rahman, "Long short-term memory neural networks for false information attack detection in software-defined in-vehicle network," 2019, *arXiv:1906.10203*. [Online]. Available: http://arxiv.org/abs/1906.10203
[101] K. M. A. Alheeti and K. McDonald-Maier, "An intelligent intrusion detection scheme for self-driving vehicles based on magnetometer sensors," in *Proc. Int. Conf. Students Appl. Eng. (ISCAE)*, Newcastle upon Tyne, U.K., Oct. 2016, pp. 75–78, doi: 10.1109/ICSAE.2016.7810164.
[102] K. M. A. Alheeti, M. S. Al-Ani, and K. McDonald-Maier, "A hierarchical detection method in external communication for self-driving vehicles based on TDMA," *PLoS ONE*, vol. 13, no. 1, Jan. 2018, Art. no. e0188760, doi: 10.1371/journal.pone.0188760.
[103] K. M. A. Alheeti, R. Al-Zaidi, J. Woods, and K. McDonald-Maier, "An intrusion detection scheme for driverless vehicles based gyroscope sensor profiling," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, 2017, pp. 448–449, doi: 10.1109/ICCE.2017.7889391.
[104] K. A. Alheeti, A. Gruebler, and K. McDonald-Maier, "Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks," *Computers*, vol. 5, no. 3, p. 16, Jul. 2016, doi: 10.3390/computers5030016.
[105] S. Gupta and B. Crispo, "A perspective study towards biometric-based rider authentication schemes for driverless taxis," in *Proc. Int. Conf. Innov. Intell. Informat., Comput., Technol. (ICT)*, Sakhier, Bahrain, Sep. 2019, pp. 1–6, doi: 10.1109/3ICT.2019.8910310.
[106] S. Vivek, D. Yanni, P. J. Yunker, and J. L. Silverberg, "Cyberphysical risks of hacked Internet-connected vehicles," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 100, no. 1, Jul. 2019, Art. no. 012316, doi: 10.1103/PhysRevE.100.012316.
[107] M. Waniek, G. Raman, B. AlShebli, J. C.-H. Peng, and T. Rahwan, "Traffic networks are vulnerable to disinformation attacks," 2020, *arXiv:2003.03723*. [Online]. Available: http://arxiv.org/abs/2003.03723
[108] (2019). *Global Automotive Cybersecurity Report*. [Online]. Available: https://industrytoday.com/wp-content/uploads/2018/12/Upstream-Security-Global-Automotive-Cybersecurity-Report-2019.pdf

SAMEER QAZI (Member, IEEE) received the B.E. degree from the National University of Sciences and Technology (NUST), Pakistan, in 2001, and the M.S. and Ph.D. degrees from the University of New South Wales, Australia, in 2004 and 2009, respectively. He has worked as an Assistant Professor with the Department of Electronics and Power Engineering, NUST-PNEC, Pakistan, and an Assistant Professor and the Head of the Electrical Engineering Department, DHA Suffa University, Pakistan. He is currently working as an Associate Professor and the Head of the Electrical Engineering Department, College of Engineering, Karachi Institute of Economics and Technology, Pakistan. His research interests include network traffic matrix estimation, non-negative matrix factorization architectures and applications, UAV-based video surveillance applications, and the Internet of Things (IoT).

FARAH SABIR received the B.E. degree in electrical engineering from DHA SUFFA University, Karachi, Pakistan, in 2017, and the M.S. degree in electrical power systems from the NED University of Engineering and Technology, Karachi, in 2019. Since February 2017, she has been working as a Lecturer with the Electrical Engineering Department, PAF-KIET University, Karachi. Her research interests include electrical power systems and smart metering systems. She is also involved in the research related to modeling and analysis of distance relays in FACTs compensated transmission lines and the Internet-of-Things (IoT) devices.

BILAL A. KHAWAJA (Senior Member, IEEE) received the B.S. degree in computer engineering from the Sir Syed University of Engineering and Technology, Karachi, Pakistan, in 2002, the M.Sc. degree in communication engineering and signal processing from the University of Plymouth, Plymouth, U.K., in 2005, and the Ph.D. degree in electrical engineering from the University of Bristol, Bristol, U.K., in 2010. From 2003 to 2004, he was a Software Engineer with Simcon International (Pvt.) Ltd., Pakistan. From 2010 to 2016, he was an Assistant Professor with the Electronics and Power Engineering Department, PN-Engineering College, National University of Science and Technology (NUST), Karachi. In 2015, he was a Visiting Postdoctoral Researcher with the Lightwave Systems Research Laboratory, Queens University, Kingston, Canada, involved in the Natural Sciences and Engineering Research Council (NSERC), Canada, CREATE Next Generation Optical Network (NGON) project on the characterization and measurements of 25-GHz RF signal generation optical comb sources. He is currently an Associate Professor with the Department of Electrical Engineering, Faculty of Engineering, Islamic University of Madinah, Medina, Saudi Arabia. He has authored or coauthored several journals and IEEE proceeding publications. His current research interests include next-generation of millimeter-wave (mm-wave) radio-over-fiber and optical communication systems, mm-wave and THz signal generation mode-locked lasers and RF transceiver design and antennas design/characterization for the Wi-Fi/IoT/UAVs/FANETs/5G systems/UWB wireless body area networks, wireless sensor networks, and millimeter-wave frequency bands. He is an Active Reviewer for many reputed IEEE journals and letters.

SYED MUHAMMAD ATIF graduated in computer engineering from the Sir Syed University of Engineering and Technology and the M.S. degree in computer networks from the Usman Institute of Technology. He is currently pursuing the Ph.D. degree in computer science with PAF-KIET under the HEC Indigenous Fellowship Program. His current research interests include network tomography, green routing, and non-negative matrix factorization.

MUHAMMAD MUSTAQIM received the B.S. degree from the University of Central Florida (UCF), Florida, USA, in 2007, and the M.S. degree in electrical engineering from PAF-KIET, Karachi, Pakistan, in 2012. He is currently pursuing the Ph.D. degree. Since 2010, he has been working as a Lecturer with the Electronics and Power Engineering Department, PN-Engineering College, National University of Science and Technology (NUST), Karachi. His research interests include software defined radios (SDRs), wireless networks, and RF and microwave systems.