Autonomous Vehicles: Resource Allocation, Security, and Data Privacy

Biraja Prasad Nayak, Lopamudra Hota, Arun Kumar, Ashok Kumar Turuk, *Member, IEEE*, and Peter H. J. Chong, *Senior Member, IEEE*

***Abstract*—Vehicular Ad-hoc Network (VANET) is a technology of importance for the Intelligent Transportation System, which provides safe and comfortable driving, infotainment, traffic management, route optimization, accident prevention, etc. Imparting suitable Quality of Service (QoS), high reliability, and low latency in VANET is a task that is challenging due to the presence of various constraints such as dynamic topology, an imperfection in hardware, congestion in the channel, fluctuation in vehicle density, etc. It is essential to allocate and utilize the resources effectively to maximize the benefit and enhance network performance. It is vital to use the available bandwidth, power, computing, and storage resources efficiently. Along with resource allocation, security and privacy challenges are of equal importance for VANET. One of the major concerns is to make the communication channel secure and prevent the network from attacks by malicious agents. Also, preserving the privacy of vehicles by hiding real identities to circumvent tracking is a challenging task. The authorized agents are allowed to know the actual identity of vehicles. This paper exhibits an in-depth survey of resource allocation schemes in different aspects of VANET. It analyzes the security and privacy of messages, vehicles, and the overall network. Also, the paper presents and discusses the open issues and future research areas in resource allocation, security, and privacy of VANET.**

***Index Terms*—Autonomous vehicle, privacy, resource allocation, security, vehicular ad-hoc network (VANET).**

I. Introduction

AN AUTONOMOUS Vehicle (AV) is a self-driving vehicle capable of sensing the environment and driving safely with little or no human intervention. The different applications of AV are highway autopilot, lane change assistance, adaptive cruise control, self-parking, etc. [1]–[4], for which it has gained momentum in the recent few years. The vehicle does the majority of the task, and the human driver becomes a mere assistant. According to statistics, in 2019, around 31 million AVs were there with some level of automation. It is expected to exceed 54 million in 2024 [5], which gives an idea about the demand for AVs in the future.

Manuscript received January 22, 2021; revised July 25, 2021; accepted September 2, 2021. Date of publication September 7, 2021; date of current version February 16, 2022. *(Corresponding author: Arun Kumar.)*

Biraja Prasad Nayak, Lopamudra Hota, Arun Kumar, and Ashok Kumar Turuk are with the Department of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela 769008, India (e-mail: kumararun@nitrkl.ac.in).

Peter H. J. Chong is with the Department of Electrical and Electronic Engineering, Auckland University of Technology, Auckland 1010, New Zealand.

Digital Object Identifier 10.1109/TGCN.2021.3110822

Vehicular Ad-hoc Network (VANET) plays a vital role to achieve autonomy of vehicles. With the coordination of resources in the network, VANET provides safety, comfort and improves driving conditions by providing traffic information in real-time. Many advancements are going on in this field to improve the VANET technology. In recent advances, while considering Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication to pass on information, Transport Protocol Experts Group (TPEG) is used instead of Traffic Message Channel (TMC). TPEG can handle 3000 messages a minute instead of TMC's 60 messages a minute. Datex II or Datex 2 is a data exchange standard developed by the European Committee for Standardization [6]. It provides information about traffic conditions between different traffic coordinating centers to update traffic status and road scenarios. To manage a network of such complexity, coordination among resources is necessary to provide adequate information in time.

Resource management plays a crucial role in AV communication. Different resources to be allocated include radio resources, transmission power, channel allocation, computation, and storage resources. One of the evolving research areas among industry and academia are Vehicle-to-Everything (V2X) communication using WLAN-based and cellular-based network [7], [8]. Other areas gaining interest are resource allocation using the vehicular cloud, edge computing, and machine learning. Optimal resource allocation enhances the performance of the network [9]. The type of service, i.e., safety and non-safety services, differs in how to allocate resources. Protection of life and property and avoidance of accidents are safety-related services that require reliability, short delay, and high security. Improvement in the quality of driving and the use of technology for entertainment are non-safety services. Safety services get high priority than non-safety services. However, resource allocation is challenging [10] due to dynamic topology and varying speed of vehicles.

Apart from resource allocation, security and privacy-preserving are some of the other concerns in AV [11]. A communication medium is always susceptible to various attacks. The network may encounter attacks such as impersonate attack, replay attack, Sybil attack, jamming, GPS spoofing attack, etc. [12]–[17]. Strict security measures have to be provided in AV to ensure safety from malicious agents. A good security solution provides confidentiality, integrity, and availability. Messages are authenticated by Trusted Authorities (TAs) to ensure their validity. While authenticating messages,

TABLE I
LIST OF COMMONLY USED ABBREVIATIONS

Abbreviation	Description
VANET	Vehicular Ad-hoc Network
QoS	Quality of Service
AV	Autonomous Vehicle
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
TA	Trusted Authorities
CSP	Cloud Service Providers
VC	Vehicular Cloud
SMDP	Semi-Markov Decision Process
NFV	Network Function Virtualization
SDN	Software Defined Network
CH	Cluster Head
C-V2X	Cellular-V2X
CSI	Channel State Information
CUE	Cellular User Equipment
VUE	Vehicular User Equipment
RB	Resource Block
SINR	Signal-to-Interference-plus-Noise Ratio
RSU	Road-Side Unit
PUE	Pedestrian User Equipment
D2D	Device-to-Device
BS	Base Station
DRL	Deep Reinforcement Learning
CC	Conventional Cloud
ECC	Elliptic Curve Cryptography

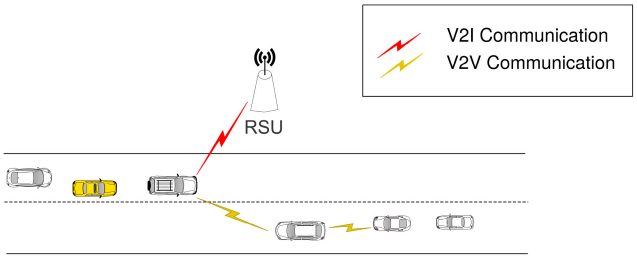

Fig. 1. A simple architecture of VANET.

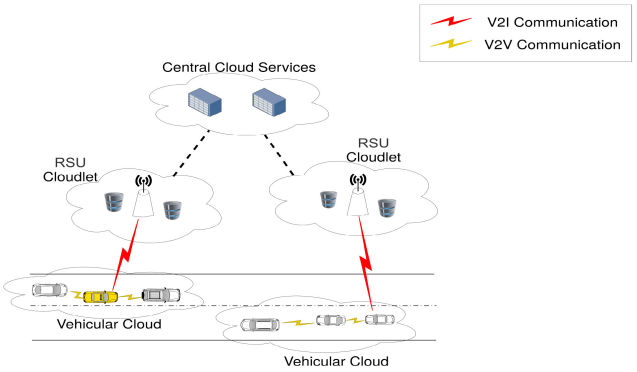

Fig. 2. Cloud and edge computing based communication in VANET [18].

vehicle face privacy issue which should be prevented. Privacy preservation helps in hiding the original identity of the vehicles, which prevents tracking [15]. In contrast, authorized agents are allowed to trace the identity of vehicles to find malicious agents.

This paper presents an extensive survey on resource allocation in VANET. It provides recent advancements in resource allocation. The paper also emphasizes the privacy and security issues of networks and the approaches adopted by researchers to overcome these issues. The commonly used abbreviations of this paper are presented in Table I.

The remaining part of this paper is structured as follows. Section II, presents the approaches for resource allocation in VANET and the open issues associated with it. The privacy and security issues, along with their open issues are presented and discussed in Section III. Finally, the paper is concluded in Section IV.

II. RESOURCE ALLOCATION

Resource allocation is the process of managing and reserving assets to achieve the network's goal. The restriction in size of equipment makes the vehicle limited in resources and, hence, reduces the system's processing power. Figure 1 illustrates a simple generalized view of the VANET architecture. Optimization of resources is vital to provide better services in terms of quick response, minimizing delay, and maximizing throughput. This work categorizes the allocation of resources in different scenarios as follows.

A. Resource Allocation in Cloud and Edge Computing

As an individual vehicle has limited storage and computational resource, there is always a need for sharing resources to enhance the capability of the network. VANETs are integrating with cloud and edge computing to achieve this. Figure 2 shows a general setup of VANET in cloud and edge computing scenario.

In [19], the authors concentrated on supporting mobile applications in cloud-assisted vehicular infrastructure. To share resources, Cloud Service Providers (CSP) form coalition in which they participate based on a two-sided matching theory. For coalition, a utility function is devised which depends on the willingness of service providers. Other factors affecting coalition are renting, leasing, and the service fee charged by network providers. In [20], Zheng *et al.* described the Computation-as-a-Service and proposed a model which includes Vehicular Cloud (VC) and Remote Cloud. Depending on the resource units available, the model uses Semi-Markov Decision Process (SMDP) to decide either to operate locally in VC or to transmit it to Remote Cloud. The state, action, and reward depends on the SMDP to get the optimal solution.

The authors in [21] proposed PEer-to-Peer protocol for Allocated REsources (PrEPARE) scheme. Resources are searched and allocated with the use of V2V communication only. Location of the requester or super-peer helps for routing. If the source vehicle is in direct contact with the destination, then information is sent to the target; otherwise, it uses an intermediate vehicle called super-peer, which is farthest from the source and within the communication range. In [22], an Availability-based Resource Allocation approach for vehicular Cloud (AVARAC) is proposed in which no infrastructure is involved. The cluster head manages the resource of the vehicular cloud. Based on the service provided, the system receives a reward. SMDP is responsible for the allocation of resources.

In [23], Collaborative Computation Offloading and Resource Allocation Optimization (CCORAO) approach is

proposed. The time for various offloading decision depends on the number of computational resources they provide to vehicles. A utility function aims to measure satisfaction level and identify vehicle's utility. It depends on delay in task processing, computational resource cost, and normalization factor. The problem of computational offloading decision is addressed with the help of Game Theory. The authors also proposed a Distributed Computation Offloading and Resource Allocation (DCORA) Algorithm to maximize the utility of the system.

In [24], the challenges of increasing computing and storage tasks, and the need for heterogeneous QoS is identified. Delay-sensitive applications are given priority and assigned resources of the multi-access edge computing server whereas, delay-tolerant applications are allocated resources of the cloud computing server. Cloud server, along with Network Function Virtualization (NFV) and Software Defined Network (SDN) [25] control modules, manages routing and resources. In contrast, the MEC server, along with NFV and SDN control modules, handles bandwidth resource integration. Bandwidth slicing is utilized, which maximizes network utility.

In [26], Sun *et al.* proposed a system architecture using MEC and Cluster Head (CH) vehicles. The CH acts as controller of computational offloading. The problem of computation offloading decision is transfigured into a knapsack problem. Bat algorithm is modified, and a multi-objective Vehicular Edge Computing task scheduling algorithm is proposed. Updating the position, improving the quality of the initial population, maintaining population diversity, and crowding distance are some modifications done.

Task assignment, along with resource allocation in vehicular fog computing, is discussed in [27]. The authors formulated the problem from a min-max perspective to reduce task latency. The whole problem is decomposed into two subproblems consisting of one-to-one matching and bandwidth allocation subproblem. Mobility prediction information is used for matching. In [28], the authors proposed a vehicular cloud system that uses SMDP. As per the request of the members, the leader of the vehicular cloud assigns resources. The proposed method maximizes reward using optimal resource allocation techniques.

Some advantages of resource allocation using cloud and edge computing are: 1) enhancing the storage and computation power of resource constraint vehicles; 2) underutilized resources of a vehicle are utilized by cloud infrastructure; and 3) pay-per-use facility reduces the cost. Disadvantages may include: 1) data loss while exchanging data between a server and vehicle; 2) risk of DoS attack; 3) due to dynamic network topology there is a risk of disruption of service; and 4) takes additional time to offload data to the cloud.

B. Resource Allocation in V2X Communication

V2X communication includes the interaction of vehicles with other vehicles (V2V), infrastructure (V2I), pedestrian (V2P), and network (V2N) [30]. Figure 3 illustrates V2X enabled vehicular communication. This section discusses various works on resource allocation in V2X communication.

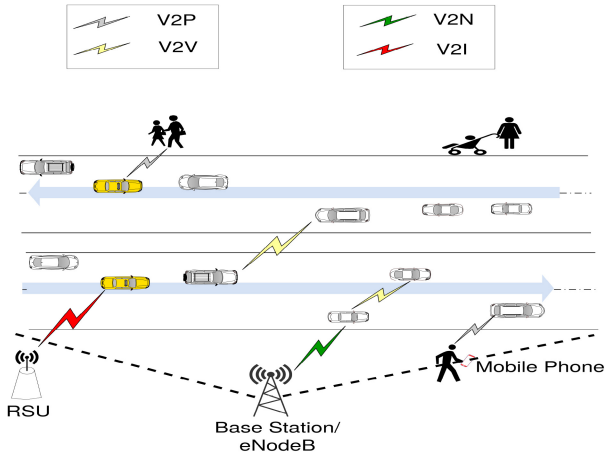

Fig. 3. A V2X enabled vehicular communication model [29].

Cellular-V2X (C-V2X) operates in a spectrum that has been licensed to mobile operators. It has a higher spectral efficiency. In [31], surrounding vehicles select resources autonomously satisfying periodicity, latency, and message size. For vehicles where LTE transmission is not accessible, vehicles can synchronize with Global Navigation Satellite System. Autonomous selection depends on latency period, time to process a message, sub-frame selection, and resource reservation period. It uses a loopback concept to select a sub-frame from a set based on extrapolation from earlier reception.

The authors in [29] allocated resources using a hybrid scheme. It uses both C-V2X and IEEE 802.11p communications. Cellular eNodeB selects an optimal receiver to find the D2D link and channel. Before establishing a link, each vehicle checks the packet's lifetime to ensure that packet will reach the receiver before the expiry of lifetime. In [32], resources are allocated based on the clustering mechanism. Intra-cell interference, reliability, and latency requirement are some of the challenges. Requirements are transfigured into constraints depending on slow varying Channel State Information (CSI). Sum rate maximization of Cellular User Equipment (CUE), reliability, and latency requirements of Vehicular User Equipments (VUEs) are the objectives of the proposed algorithm. VUEs share common Resource Blocks (RBs). A Cluster-based Resource block sharing and pOWer allocatioN (CROWN) scheme help to resolve the above issue.

The work in [33] utilizes scheduled resource allocation and autonomous resource selection modes. It is further divided into reuse mode and dedicated mode. ProSe Per-Packet Priority (PPPP) [34] is utilized to prioritize data transmission. Empty Resource Block Allocation (ERBA) algorithm is used for autonomous resource selection mode and dedicated mode in which empty unlicensed bands are allocated. Once unlicensed bands are finished or allocated, VUEs with the highest CSI are assigned to the licensed band. In Reuse Resource Block Allocation (RRBA) algorithm, only one V2V pair and one Pedestrian User Equipment (PUE) can reuse the same RB.

In [35], mode 3 and mode 4 communication modes [36] are used. Utilizing an optimal power approach, the authors recommended maximizing information value, with the requirement of minimum SINR and maximum transmit power limitation.

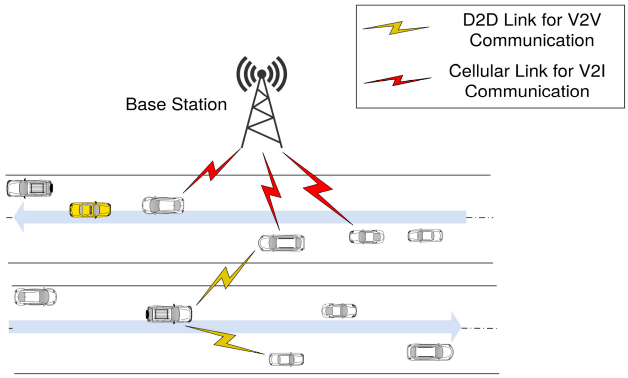

Fig. 4. A D2D-based communication architecture in VANET [38].

Mode and algorithm are used based on load of the network. If the load of the network is light (i.e., number of RBs which are vacant are more than the number of VUE), then it uses mode 4 or dedicated mode and Vacant Resource Blocks and Power Allocation (VRBPA) algorithm otherwise it uses both VRBPA and Occupied Resource Blocks and Power Allocation (ORBPA) algorithm. ORBPA algorithm uses reuse mode to allocate resources. It uses matching theory to match VUE with PUE and reuses its RB.

In real-time, CSI may not be perfect due to high mobility of vehicles. Resource allocation in a V2X environment with poor CSI is discussed in [37]. The authors aimed to achieve CUE's minimum SINR requirement and maximize the sum ergodic capacity of VUEs. Spectral resources of multiple CUEs are reused by one VUE at max with a constraint of the maximum transmission power of VUE. A lower bound-based power control approach fulfils this constraint.

It gives the advantage of: 1) receiving surrounding information from nearby resources such as other vehicles, infrastructure, pedestrian, network, etc.; 2) reliable; and 3) uses the resources of cellular network which is faster than V2X. There are also some disadvantages like: 1) difficult to manage the resources; 2) more risk of interference; and 3) VANETs will get less priority.

C. D2D Based Resource Allocation

Device-to-Device (D2D) communication includes V2V communication and the involvement of mobile user equipment. V2V communication utilizes the benefits of D2D communication. Figure 4 shows D2D-based communication in VANET.

In [39], VUEs used orthogonal RBs to communicate. VUEs and CUEs utilized the same RB. Due to the reliability and latency requirements of VUEs, vehicles are assigned RBs for a confined period. In CUEs, the focus is on maximizing the sum throughput. Resources are allocated to sub-CUEs and sub-VUEs. The authors proposed Separate resOurce bLock and powEr allocatioN (SOLEN) algorithm to allocate resource. The RB allocation problem is modified into a maximum weight matching problem and is solved by the Hungarian algorithm. The authors in [38] proposed a hybrid model consisting of IEEE 802.11p and D2D based communication [29]. The Base Station (BS) manages the selection of a D2D link. Weights are given to links depending on expected end-to-end delay and lifetime of the packet and are used to select a link. Only if the remaining lifetime of a packet is less than the threshold, request is sent to BS.

In [40], power and spectrum allocation for D2D enabled vehicular communications is discussed. It is based on slowly changing large-scale fading information [41]. For V2I and V2V links, the requirement is for high capacity and reliability respectively. Each vehicle can have V2V and V2I connections simultaneously. Only while reusing CUE (cellular user) - DUE (D2D user) pair interference is possible. The authors proposed sum CUE capacity maximization design ensuring high throughput. Again, a minimum CUE capacity maximization design is presented, to increase the minimum capacity for channels. The authors in [42] focused on the optimal selection of access mode. Vehicular receiver decides on access mode selection among cellular network and VANET network communication [43]. A transmission delay constraint is maintained depending on transmission distance. Dual decomposition method is proposed using the Lagrangian formula to obtain a sub-optimal solution iteratively. The BSs and vehicular transmitters that are idle can be switched off to get better performance.

In [44], the authors proposed a model to jointly optimize power allocation, radio resource, and modulation or coding in LTE V2V communication. The proposed algorithm escalates the information rate and reduces the interference of CUE. A constraint in latency is transfigured into constraint in data rate using the Poisson distribution model. Radio resource management is achieved using binary search and Lagrange dual decomposition method. The goal of the optimization problem is to maximize the minimum SINR of CUE. The authors in [45] proposed an algorithm to achieve network connectivity and minimize interference in VANETs. Connectivity is achieved using an approach derived from the minimum spanning tree. The interference graph's maximum degree is reduced to minimize the number of allocated resources.

In [46], transmission power minimization while satisfying reliability and queuing latency constraints is discussed. The problem is decomposed into RB allocation and power minimization problems using the Lyapunov framework. Vehicles are grouped into zones using a clustering mechanism to reduce message exchange between Road-Side Units (RSUs) and vehicles. The zones are formed based on the similarities of VUEs. In each zone, RBs and VUEs are matched using one-to-many matching. Ultimately, the power allocation approach is considered for all VUE pairs upon the matched RBs to meet the latency and reliability constraints.

In [47], the authors presented a model to optimize spectral efficiency and manage interference. Vehicles are grouped into clusters in which vehicle having speed near to the average cluster speed is considered as cluster head. To avoid intra-cluster interference, the number of vehicles in each cluster is limited to the number of available subcarriers. Cluster head can only communicate with the BS. Vehicles transmit information directly to the cluster head or use multi-hop mode. The authors introduced interference neutralization to avoid inter-cluster interference.

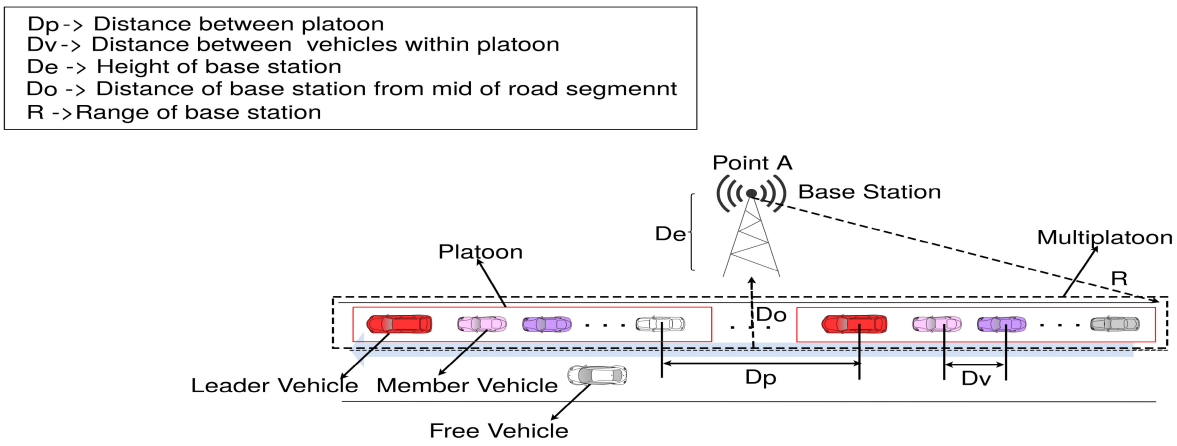

Fig. 5. Diagramatic representation of multiplatoon scenario in a road segment [50].

The authors in [48] allocated spectrum in cognitive vehicle network based on QoS. The CR-VANET is divided into High load CR-VANET (HCR-VANET) and Low load CR-VANET (LCR-VANET). While allocating spectrum in LCR-VANET, the proposed algorithm maximizes the throughput. In the case of HCR-VANET, SMDP based Channel Allocation Scheme (SMDP-CAS) is proposed to solve the problem of low acceptance probability for safe application service. In [49], the authors proposed an approach to maximize V2V communication using the D2D communication technique. Multiple VUEs use the RB of CUE. Serial Allocation Algorithm allocates RB for V2V communication. It uses Clustering Allocation Algorithm to form the same number of clusters as that of CUEs.

D2D based resource allocation gives faster access to information and is more reliable. Besides these advantages, interference and difficulty in pairing are some of the disadvantages.

D. Resource Allocation in Multiplatoon

A group of vehicles moving together maintaining a particular speed and distance between them is called a platoon. The challenges involved in moving vehicles in a platoon are: 1) maintaining a constant speed; 2) controlling the platoon; and 3) inter-vehicle spacing. In each platoon, there is a platoon head and member vehicles. Figure 5 shows a diagrammatic representation of a multiplatoon scenario in a road segment.

In [50], platoons share the velocity and acceleration information and braking and leaving information with other platoons. The proposed work is about allocation of sub-channel and power control [51]. Sub-channel allocation for leader vehicles is achieved using D2D-multicast and evolved Multimedia Broadcast Multicast Services (eMBMS) based model, and for member vehicles, scheme 1 and scheme 2 are used. In power control, the minimum received signal power threshold and SINR threshold are considered. Power control is achieved using eMBMS and D2D based models. In [52], to attain low delay in V2V communication, direct D2D communication is regarded as a crucial requirement. The vehicles share the communication spectrum channel with the user equipment of cellular users using D2D underlay scheme [53]. There is a signaling overhead due to frequent message exchange for resource reallocation, which deteriorates the delay performance. Hung *et al.* used the concept of a platoon, where the platoon leader decides if resources need to be reallocated or not. The authors used Lyapunov optimization to reduce resource reallocation rates and improve delay performance.

In [54], Liu *et al.* concentrated on resource allocation in intersection management [55]. The authors proposed two schemes. In scheme A, the central controller allocates resources available to convoy in a queue according to request arrival, and the convoy releases resources after their utilization. In scheme B, two queues are maintained to arrange the vehicles from two roads. If the maintenance time of one convoy exceeds the time constraint, then the resource is allocated to the other queue. The convoy with a higher number of vehicles is given priority to allocate resources. Convoy is removed from the queue once resources are allocated.

In [56], a Security-Aware Joint Channel and Power Allocation algorithm (SA-JCPA) is proposed to avoid eavesdropping [14] and achieve optimal resource allocation. To sustain multiplatoon and cellular communication the Orthogonal Frequency-Division Multiplexing technique is implemented. Cellular users share an orthogonal channel with only one multiplatoon V2V pair and vice versa. The goal is to maximize V2V achievable data rate, QoS, and link's secrecy rate. Channel sharing strategy is achieved using bipartite graph matching.

Advantages of resource allocation in multiplatoon are: 1) easy to handle the vehicles as the network is divided into small groups and 2) less traffic is sent to the BS as mostly platoon head is communicating with the BS. Some disadvantages include: 1) failure of platoon head leads to coordination failure of network; 2) increase in complexity when platoon head is leaving the platoon; and 3) security attack on the head node may lead to an accident.

E. Machine Learning Based Resource Allocation

A massive amount of data is generated from sensors and the surrounding vehicles to assist in smooth and safe driving. Applying traditional approaches to compute such massive data

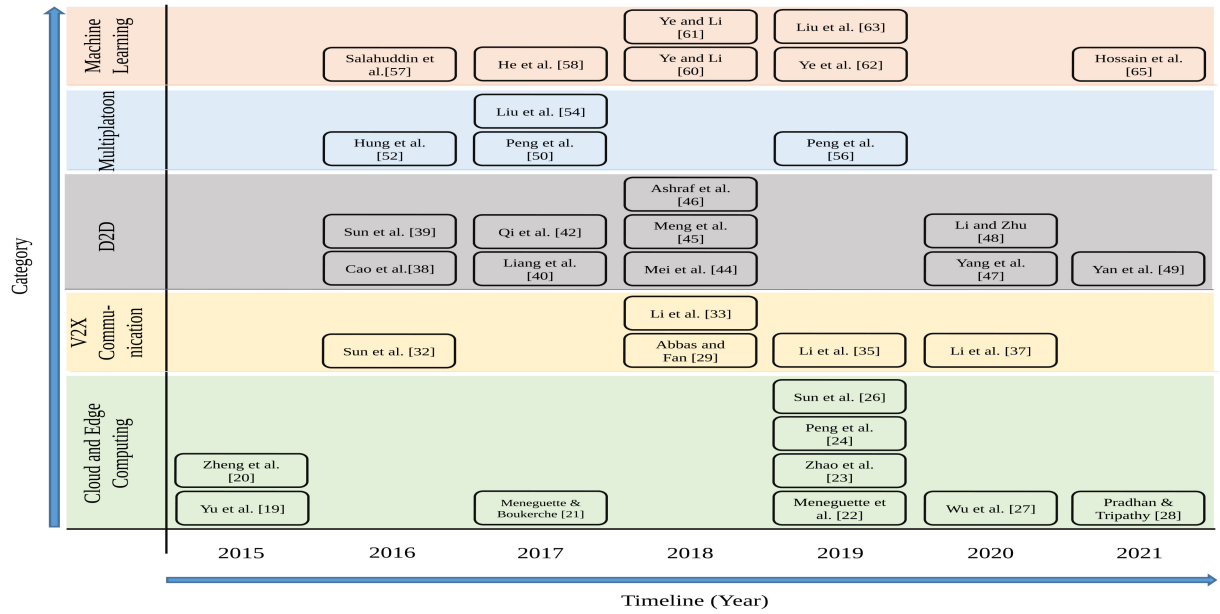

Fig. 6. Chronological graph of survey in resource allocation.

may not give a good performance. Machine learning acts as a powerful tool to analyze and make data-driven decisions strengthening VANETs performance.

The authors in [57] proposed an idea to extend traditional cloud to a VC along with the use of reinforcement learning to allocate resources. Salahuddin *et al.* proposed Markov Decision Process (MDP) over the Heuristic approach to reduce resource allocation cost and overhead, and enhance QoS for end-user perceived latency. Among various techniques to solve MDP, policy iteration technique is utilized to achieve optimal policy.

The authors in [58] focused on the management of resources in software-defined and virtualized VANETs using Deep Reinforcement Learning (DRL) approach. Here, resource allocation is done for the network, computing resources, and caching. This leads to an increase in complexity. The MEC servers, BS, and content caches are virtualized and managed by a Mobile Virtual Network Operator (MVNO) [59]. For arranging resources for a particular vehicle, the MVNO sends the combined collected status of resources to the deep Q-network and obtains a response of the optimal policy. MVNO's revenue is the system reward and is formulated as a function of received SNR.

In [60], the authors proposed a DRL approach to allocate sub-band channels and make decisions for the power level at which transmission is to be done. It is a decentralized method and does not need the whole network's information; hence, transmission overhead is minimized. The sum rate of V2I plays a role in the reward function. It focused on maintaining latency constraints and minimizing interference. MDP is used to make state transitions using the environment and action taken by the agent. Q-learning and deep Q-network are used to train and test the network. The authors again proposed a similar approach in [61] using V2V broadcasting. Each vehicle is treated as an agent. To avoid the broadcast storm problem, the selection of messages to be rebroadcasted is carefully inspected. The vehicles which are away have a higher chance to rebroadcast the message.

The authors in [62] focused on unicast and broadcast communication. SINR threshold and latency constraints are maintained to achieve the desired goal. The probability of transition from one state to another and rewards depends on the environment state and action taken by the agent. In a given state, a Q-value is used to measure the standard of action. The authors proposed two algorithms for the training stage and testing stage procedures of unicast and broadcast. Mobile edge servers provide a computation facility to vehicles to fulfill the computational requirements. In [63], the authors proposed two methods, Q-learning based and DRL based methods for offloading and resource allocation. The edge computing servers are categorized into vehicular edge servers and fixed edge servers. Q-value is either decided by old value or replaced by backed-up value. In DRL framework [64], the training data set is selected by DRL agent according to learning complexities instead of randomly. The authors in [65] proposed a spectrum sensing and road segmentation approach for better data transmission. The spectrum sensing technique uses a fuzzy algorithm in combination with a Naive Bayes algorithm. A tri-agent reinforcement learning algorithm used by Spectrum Sensing Agent to allocate spectrum. Figure 6 shows work done in different years on resource allocation.

Advantages of machine learning based resource allocation are: 1) ability to handle large datasets and 2) suitable for decision making while allocating resources. Some of the disadvantages include: 1) creation and training of dataset are complex and time taking; 2) developing a proper model is difficult; and 3) retraining of model due to the dynamic topology.

F. Open Issues of Resource Allocation in VANET

A significant amount of work is done on resource allocation in VANET. Various literature has discussed different

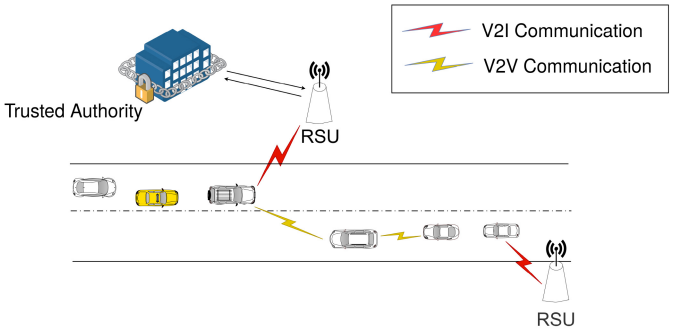

Fig. 7. A generalized VANET architecture while providing security.

limitations and requirements of the network during the allocation of resources. Only some resources are considered for allocation at a time, but none of the previous work focused on allocating all types of resources simultaneously. If all types of resources are assigned at once, the challenges involved, complexities and trade-offs associated with different resources, and effect on the network's performance have not been highlighted yet.

Different sensors of AV generate a massive amount of data. Also, an enormous amount of information is gathered from the surrounding network to get a smooth driving experience. It takes a lot of storage space in the resource-constrained network. For what period, these data are to be stored and then relinquished is a matter of concern for the effective management of resources. It can be a good area of research to handle the storage space effectively. This can be achieved by updating necessary new data along with retaining relevant old data. It also includes deleting outdated data and irrelevant new data by applying various data cleansing techniques. One can concentrate on handling storage space effectively to improve the efficiency of the network.

In the dynamic environment of VANETs, the scalability of network is an important aspect. The speed change of vehicles differs in a broad range. Along with that, VANET has a dynamic topology, and the network's density also varies according to time of the day or available situation. With such uncertainty, it is tough to attain scalability. So, scalability is a crucial area that needs to be taken care of.

III. Security and Privacy

Security is one of the most crucial issues that need to be addressed in AVs. Autonomous driving requires strict cybersecurity and safety measures to ensure safety to the driver, passenger, and surrounding objects [11], [66]. Security threats in VANET not only lead to property or financial loss but may also lead to life loss and privacy loss of an individual or sometimes a group of people.

Misbehavior of vehicles, particularly sensor nodes or false information passing, may steer to unnecessary delay while reaching the destination. Figure 7 shows a generalized architecture of VANET while providing security. Some of the security threats involved in VANET are:

- GPS Spoofing Attack [13]: The attacker of this attack broadcasts the fake location of GPS and misleads the receiver of the GPS.
- Denial of Service (DoS) Attack [15]: The attacker attacks the VANET system to prevent legitimate vehicles from accessing the network by jamming network channel.
- Sybil Attack [13]: The attacker replicates the identity of numerous vehicles. It may initiate a DoS attack.
- Man-in-the-middle Attack [12]: Here, the attacker stealthily relays the message to modify it, whereas the sender and receiver think they are communicating with each other.
- Impersonate Attack [15]: It is an attack in which the attacker resembles another valid vehicle's identity.
- Replay Attack [13]: In a replay attack, a valid message is dishonestly replicated or postponed.
- Eavesdropping [14]: This is an attack in which the attacker secretly listens to communicating devices.

A. Security

Securing communication channels in V2V and V2I communications is a core security problem. There is an equally likely probability of exhibiting malicious behavior by other nodes, which deteriorates network performance. However, it is essential to establish trust among vehicles in the network. A good security solution should provide confidentiality, integrity, and availability. Some of the literature which resolves the security issue are as follows.

The authors in [67] used a dual authentication and key management mechanism for the safe transmission of data. Dual authentication is achieved through offline registration using fingerprint of the user and provides a secret key for each vehicle through a smart card. The approach also includes group keys for primary and secondary users. With the assistance of vehicle's secret key, the vehicles give rise to hash code, which is verified to perform authentication. The group key is updated whenever a vehicle joins or leaves a group. In [68], Ho *et al.* focused on data security sensed by different sensors in an AV. The model concentrated on the exchange of certificates, authentication of devices, and transmission of data. For signature verification of the device, RSA is considered a better option than Elliptic Curve Digital Signature Algorithm (ECDSA), while ECDSA performs better in case of signature generation. Considering key size of the AES, 128-bit AES performs better compared to 192 and 256-bit keys.

An anonymous and lightweight Authentication based on Smart Card (ASC) scheme is proposed in [69]. It authenticates the vehicle and validates the message. The login ID is dynamically changed often by smart cards to hide the real identity and provide anonymity. It also offers dynamic password change, which helps in preventing a password guessing attack. A cybersecurity framework based on a hierarchical game is proposed in [70]. There are two types of players, namely a head agent and secondary agents. Agents coordinate among themselves to detect, predict, and react appropriately against attacks. Intrusion Decision Agent is considered head agent, and Intrusion Detection System, Intrusion Prediction System, and Intrusion Reaction System are regarded as secondary agents [71]. The proposed approach reduces false-negative and false-positive rates. It also keeps down the communication delay and overhead.

In [72], the authors integrated single-server 3-factor authentication and key agreement protocol for VCC. The user registers and authenticates to the Conventional Cloud (CC) using identity, password, and biometric. Then CC issues a smart card [73] to the user. The user and VC mutually authenticate each other and establishes a session key to communicate with each other. It helps in achieving single sign-on and relieves the user from public key management.

The authors in [74] proposed a secure and efficient sharing of content in a crowdsourced vehicular content-centric network. The requester sends its interest to participants for required content. Participants, with the help of content providers, check the authenticity of the requester. It uses Identity-Based Proxy Re-Encryption (IB-PRE) and Named Function Networking (NFN) techniques to provide security and privacy, respectively. In [75], Cui *et al.* considered a Semi-Trusted Authority (STA). It uses a self-healing key sharing mechanism integrated with a certificateless signature. To identify a malicious vehicle, both RSU and STA need to compute the identity of that vehicle. Elliptic Curve Cryptography (ECC) is used to provide security to the system.

While sharing messages, there can be attacks that will influence the correctness and integrity of the information. In [76], Rathore *et al.* proposed TangleCV policy, a decentralized approach for sharing messages in connected vehicles. It is a directed acyclic graph-based blockchain solution that provides improved scalability and efficiency against information integrity and information correctness attacks. The authors in [77] proposed security in online cab booking services. Vehicles are connected with IoT devices to store and send information. The information about pickup and drop points, pickup time, traffic congestion, and rating can be altered by an adversary. To safeguard this alteration, the proposed approach provides security through the use of blockchain.

In [78], the authors adopted Ciphertext-Policy Attribute-Based Encryption (CP-ABE) technique to obtain one-to-many data sharing in a vehicular social network. To record the access policy of data, they used blockchain, which also provides self-certification to users and dispenses cloud non-repudiation. The CSP is supervised by blockchain. Practical Byzantine Fault Tolerance (PBFT) [79] is used to avert a malicious attack. In [80], the authors proposed a secure content sharing scheme in a vehicular named data network using a double-layer blockchain. Because of the characteristics of grouped OBUs, a Private Blockchain for OBUs (PBO) is formed and data is made tamper-proof. Consortium Blockchain for RSUs is created to the stabilize demand and supply of PBOs. Data trading between PBOs is done using matching.

In [81], Tangade *et al.* proposed a Trust Management scheme based on Hybrid Cryptography (TMHC). The system architecture consists of an Agent of TA (ATA), RSUs, vehicles, and Regional Transport Office (RTO). RTO initializes the parameters of the system and ATA. RSUs and vehicles register in off-line mode with RTO. The trust value is evaluated by RSU and is computed by ATA based on reward points. Reward points depend on the type of safety alerts made by vehicle. A blockchain-based authentication and key agreement protocol is proposed in [82]. Multiple TAs are used to manage the vehicle-related information in the ledger. It uses RSUs for the computational task instead of TA, which reduces the overhead of the TA. In [83], the authors have proposed a new mining technique called Proof-of-Driving (PoD). It is similar to Proof-of-Work (PoW), except it requires fewer resources than PoW. Poor quality nodes or malicious nodes do not take part in consensus, thus optimizing the miner nodes.

B. Privacy

Privacy is a mechanism that hides the identity and location of a vehicle from unauthorized agents. It preserves the privacy of passenger. Safeguarding privacy avoids tracking of a vehicle and provides a robust network. However, privacy-preserving does not prevent authorized agents such as TAs from tracing the actual identity. Vehicles misbehaving are monitored by TA.

The authors in [84] proposed an identity-based Conditional Privacy-Preserving Authentication (CPPA) approach. ECC is used to reduce complexity and increase the efficiency of the system. Batch verification of multiple messages is achieved using small exponent test technology [85]. This approach improved the performance in terms of computation and communication costs. An identity-based signature approach is proposed in [86]. It preserves the privacy of the user by using Elliptic curve cryptosystem. The signature scheme utilizes a one-way hash function and ID-based batch verification to achieve faster authentication.

In [87], a Secure Privacy-preserving Authentication scheme for VANET with Cuckoo Filter (SPACF) is proposed. The cuckoo filter is a data structure utilized to verify if an item is present or not. It constructs a notification message to reduce message overhead. If a signature is invalid, the whole batch is not discarded, but valid signatures are extracted. A binary search technique is used to get a valid signature. An Efficient Anonymous Authentication and conditional Privacy-preserving (EAAP) scheme is proposed in [88]. User manually registers in TA. In return, TA gives an authentication key using a smart card. Signature and certificates are used along with other parameters to verify the vehicles and RSUs.

Providing security and privacy in the parking is an important issue. The authors [4] proposed a Privacy-preserving Automated Valet parking protocol (PrivAV) to provide anonymous authentication. It offers dual authentication using smartphone and one-time password. Automated Valet Parking (AVP) server with the assistance of local server prevents the risk of vehicle theft and privacy.

In [89], the proposed scheme utilizes Chinese Remainder Theorem while generating a new group key for vehicles. For identity verification, fingerprint is used as opposed to real identity and password. Elliptic curve mechanism is utilized for signature verification rather than bilinear pairing. It reduces the complexity of computation. The authors in [90] proposed a Privacy Preserving identity-based Broadcast proxy re-encryption (P2B) scheme. Message is sent to the receiver through cloud. The sender generates ciphertext using keys and then re-encrypts it to create re-ciphertext with a re-key. The re-ciphertext is then broadcasted to the receivers.

The authors in [91] described privacy protection using a multi-cloud environment. An authentication scheme is

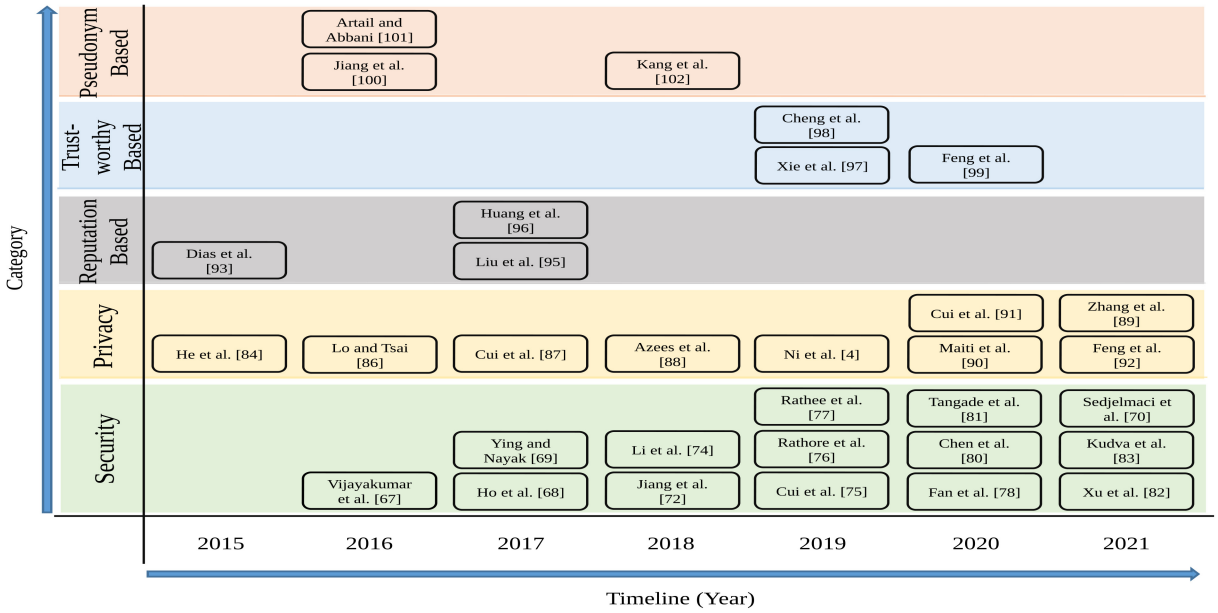

Fig. 8. Chronological graph of survey in security and privacy issues.

proposed in which TA registers vehicles and CSP to set up communication between multiple CSP and vehicles. CSPs are registered once to attain fast authentication. With the help of a cloud broker, TA manages the cloud services. The BS does not participate in the authentication process. The scheme uses ECC to provide security. Feng *et al.* [92] proposed an efficient privacy-preserving authentication model. The authors used blockchain to store vehicle certificates. Asynchronous accumulator extends the structure of blockchain by verifying the membership of vehicle with the help of a witness.

C. Reputation Based Security and Privacy

It is challenging to detect the misbehavior of nodes in VANETs. To achieve this, the authors in [93] proposed a cooperative watchdog system. The system operation depends on the reputation of the node [94]. It relies on the reputation score calculated by the node itself, neighboring node, and the value assigned by the watchdog. By detecting these misbehaving vehicles, the network can reduce the wastage of resources and enhance performance.

To provide security from attacks like trajectory tracking, intrusion, and unauthorized control in [95], a Privacy-Preserving Dual Authentication and key agreement Scheme (PPDAS) is proposed. It uses bilinear pairing for encryption and secures communication between RSU, OBU, and other vehicles with the help of TA. It provides dual authentication. First, authenticity is verified by TA with the assistance of OBUs anonymous identity and temporary encryption key. Second, authenticity is verified by the vehicle's reputation using the history of interaction behavior. Burrows-Abadi-Needham (BAN) logic is used to show the correctness of the scheme.

Along with reputation management for security, resource allocation is also achieved in [96]. The authors proposed a distributed approach to calculate the reputation of the vehicles based on similarity, familiarity, and timeliness. The reputation weight is collected by a local authority. It finds the last reputation value to get the final cost of reputation. Further, this value is used to allocate resources for VEC. Higher the value of reputation higher is the priority to get resources.

D. Trustworthy Based Security and Privacy

A semi-decentralized scheme to manage trust using blockchain is proposed in [97]. Information is gathered from all over the network with the assistance of SDN and 5G. Messages and videos collected from vehicles and RSUs near the accident site are uploaded to the cloud network after being encrypted. Score given by different vehicles to the tag of the message generating vehicle evaluates its trustworthiness.

Data sharing between vehicles are treated as social interaction in [98]. Based on the quantity and quality of interaction, the trustworthiness of the vehicle is evaluated. Direct interaction between vehicles gives direct trust, whereas vehicles not having direct interaction uses social interaction to deduce trust. It focused on the trustworthiness of vehicles based on three-valued subjective logic. Initially, the network is assumed to be static, and proposed OpinionWalk algorithm to deduce indirect trust. In dynamic trust assessment, the topology and weight of edge changes to get direct trust assessment and community-based trust assessment.

Transmitting messages during vehicular communication should be done with accuracy and trustworthiness. In [99], the authors proposed an approach called Blockchain-assisted Privacy-preserving Authentication System (BPAS), which is scalable and efficient. In this method, the vehicles do not need an online registration except for initialization of system and registration of vehicles. TA is responsible for initialization, and smart contract deployment.

E. Pseudonym Based Security and Privacy

Certificate Revocation List (CRL) takes a considerable amount of resources and time to check the list. To avoid

TABLE II
BRIEF OVERVIEW OF WORK DONE IN VANET

Sl no.	Algo./ Paper	Year	Category	Basic Concept	Performance Against	Evolution From/ Compared With	Restriction/ Requirement/Others
1	[19]	2015	Resource allocation in cloud & edge computing	Resource demands are combined with prices.	With and without service provider cooperation	-	Two sided matching theory
2	[20]	2015	Resource allocation in cloud & edge computing	Arrival and departure of request and vehicle follows Poisson distribution. Uses SMDP	Action probability and expected reward	Greedy Allocation & Simulated Annealing	Long-term expected reward maximized
3	PrEPARE [21]	2017	Resource allocation in cloud & edge computing	Location of the requester or superpeer is utilized for routing	Service time, service availability, service delay & search time	EMBLS, HLMS	QoS requirement, No external infrastructure
4	AVARAC [22]	2019	Resource allocation in cloud & edge computing	SMDP	Average reward while varying different parameters	ADVICe	No external infrastructure
5	CCORAO [23]	2019	Resource allocation in cloud & edge computing	Utilizes Distributed Computation Offloading and Resource Allocation (DCORA) Algorithm	System utility and average completion time	Local processing, cloud computing, entire MEC	Game Theory and Nash equilibrium
6	[24]	2019	Resource allocation in cloud & edge computing	NFV and SDN control modules are installed in both cloud and MEC servers	Bandwidth slicing, average no. of AVs in different utility gains	No bandwidth slicing	Minimum SINR and QoS requirement
7	Multi-objective VEC task scheduling [26]	2019	Resource allocation in cloud & edge computing	Transformation of problem to knapsack problem	Execution time, weight ratio, offloading ratio with different vehicle size, cluster radius	-	Bat algorithm
8	[27]	2020	Resource allocation in cloud & edge computing	To reduce task latency formulated problem from min-max perspective, mobility prediction	Time delay and different file size	Random task, computation size, without mobility prediction	One-to-one matching
9	[28]	2021	Resource allocation in cloud & edge computing	SMDP	Request and vehicle arrival rate, departure rate	Zheng et al., Liang et al.	Maximize reward
10	Greedy cellular based D2D Link Selection [29]	2018	Resource allocation in V2X communication	Assign appropriate channel from cellular based D2D link	Average latency and packet delivery ratio	Without D2D, with D2D (IEEE 802.11p and C-V2X)	SINR requirement and packet lifetime
11	CROWN [32]	2016	Resource allocation in V2X communication	Clustering mechanism is used to allocate resources	Cumulative distribution function, sum rate, availability	[103]-Ext, RBSPA	Maximize sum rate, minimize latency
12	[33]	2018	Resource allocation in V2X communication	Autonomous resource selection & scheduled resource allocation, dedicated & reuse mode	Information value & system throughput	Different algo. for V2X communication	QoS requirement
13	VRBPA and ORBPA [35]	2019	Resource allocation in V2X communication	Scheduled resource allocation & autonomous resource selection, matching VUE & PUE	Information value, spectral efficiency, access rate, vehicle speed	Optimal algorithm, [104], [33]	SINR, QoS requirement, reliability, latency
14	[37]	2020	Resource allocation in V2X communication	Spectral resources of CUEs reused, constraint of maximum transmission power of VUE	Sum ergodic capacity of VUEs	SA-O2M, pure cellular network, [105]	Minimum SINR requirement
15	SOLEN [39]	2016	D2D based resource allocation	VUEs and CUE can utilize the same RB	Sum rate and average power	SRBP, modified- [106] & modified- [103]	QoS, reliability and latency requirement
16	Greedy D2D link selection [38]	2016	D2D based resource allocation	Weights given to links used by algorithm to select a link	Packet delivery rate and average delay	Without & with D2D (D2D & IEEE 802.11p)	SINR requirement
17	[40]	2017	D2D based resource allocation	Different links for different requirements	Sum ergodic capacity of CUEs, SINR of an arbitrary DUE	SOLEN [39]	SINR & QoS requirement
18	[42]	2017	D2D based resource allocation	Vehicular receiver decides access mode selection among cellular network and VANET network communication	Throughput	No V2V, max power, resource partition, optimal, optimal+PR	SINR & QoS requirement, Lagrangian technique used
19	[44]	2018	D2D based resource allocation	Latency constraint transfigured into data rate constraint using Poisson distribution	SINR, packet latency, CDF, packet arrival rate	SOLEN [39]	Latency and reliability requirement
20	RAM algorithm [45]	2018	D2D based resource allocation	Resource allocation algorithm derived from minimum spanning tree	Connectivity index, arrival rate, FC component	Greedy coloring & random algorithm	Graph theory
21	[46]	2018	D2D based resource allocation	Vehicles are grouped into zones, Lyapunov framework used, One-to-many matching	CDF, queuing latency, SINR	3GPP baseline	QoS requirement
22	[47]	2020	D2D based resource allocation	Vehicles are grouped into clusters, Cluster head only communicated with the base station	Throughput gain	Without cooperative communication	Multi-hop mode
23	CASCA and SMDP-CAS [48]	2020	D2D based resource allocation	CR used, based on load CR-VANET divided into HCR-VANET & LCR-VANET	Reward and acceptance probability of SAS and UAS	Game Theory algorithm	QoS requirement of primary user
24	[49]	2021	D2D based resource allocation	Multiple VUEs use same RB of CUEs	No. & speed of VUEs, success- fully communicated vehicles	Random allocation	Used clustering algorithm
25	[50]	2017	Resource allocation in multiplatoon	Platoon shares VaA and BaL information	Transmission power and transmission delay	eMBMS & D2D-multicast model	SINR requirement
26	[52]	2016	Resource allocation in multiplatoon	Vehicles uses spectrum channel with cellular users, Lyapunov optimization is used	Delay and probability of reallocation	Distance to base station	SINR requirement

this, an efficient anonymous batch authentication scheme is proposed in [100]. CRL process is replaced with a Hash Message Authentication Code (HMAC). HMAC also checks message integrity before batch authentication. The area is divided into domains in which RSUs control the vehicles, and pseudonyms-based authentication is used to achieve privacy.

TABLE II
(Continued.) BRIEF OVERVIEW OF WORK DONE IN VANET

Sl no.	Algo./ Paper	Year	Category	Basic Concept	Performance Against	Evolution From/ Compared With	Restriction/ Requirement/Others
27	[54]	2017	Resource allocation in multiplatoon	Central controller allocates resources available to the convoy in a queue according to the request arrival, Intersection management	System throughput with respect to traffic volume	With respect to different schemes	Uses platooning concept
28	SA-JCPA [56]	2019	Resource allocation in multiplatoon	Cellular user shares orthogonal channel with only one multiplatooning V2V pairs	V2V sum rate with respect to V2V links and vehicle speed	Benchmark 1, 2, 3 and Greedy algorithm	Bipartite graph matching
29	[57]	2016	Machine learning based resource allocation	Uses MDP to reduce resource allocation cost and overhead, RL is used	Cumulative VM migration overhead with respect to time	Heuristic	QoS requirement
30	[58]	2017	Machine learning based resource allocation	Allocation of resources for computing and caching, managed by MVNO, DRL is used	Total utility with respect to changing price	Without edge caching, MEC and virtualization	Includes SDN, virtualization, MEC
31	[60]	2018	Machine learning based resource allocation	Decentralized approach, does not need information of whole network, RL is used	Sum rate and probability with respect to no. of vehicles	Random allocation and method by [107]	SINR and latency requirement
32	[61]	2018	Machine learning based resource allocation	Uses Q-Learning to make the system learn & decide, DRL used, V2V broadcasting	probability and sum capacity	Baseline method [107]	SINR and latency constraint
33	[62]	2019	Machine learning based resource allocation	DRL used, unicast & broadcast communication	Sum rate and probability	Random algorithm and [107] method	SINR and latency constraint
34	[63]	2019	Machine learning based resource allocation	DRL used, edge computing servers categorized into vehicular edge and fixed edge servers	Network utility and delay	Local, VES and FES method	Latency requirement
35	[65]	2021	Machine learning based resource allocation	Road Segmentation, Used Naive Bayes algorithm	No. of vehicle, throughput, delay, sensing time	Regional clustering, Binary decision making	No. of clusters equal to no. of CUEs
36	KCRT [67]	2016	Security	Dual authentication and key management, individual keys for each user & group keys	Key computational and recovery time	CRGK, FRGK, KCRT, NTRU, EGKM	Authentication by fingerprint scan and secret key
37	[68]	2017	Security	Exchange of certificates, authentication of device and transmission of data	Signature generation and verification	ECDSA, RSA varying key size in AES	Hybrid of different algorithms
38	[69]	2017	Security	Authentication based on smart card, login id is created and changed dynamically	Computational cost and overhead, packet delay	Mun's protocol, Zhao's protocol, He's protocol	Provides anonymity
39	Integrated AKA protocol [72]	2018	Security	Integrated Single-server 3-factor Authentication and Key Agreement protocol, single sign-on	Time cost, rounds in authentica- tion, binary length of messages	HW, HKWS and ODKHW	Mutual authentication
40	CVCCN [74]	2018	Security	IB-PRE technique to provide security and NFV to provide privacy	Requester utility, Cache hit ratio	Multicast, best-route	Used greedy online schedule algorithm
41	[75]	2019	Security	Both RSU and STA computes the identity of vehicle	Computational overhead, communication cost, packet loss, transmission delay	NECPPA, ABAH, ESCPKA	Used Elliptic Curve Cryptography
42	TangleCV policy [76]	2019	Security	Directed acyclic graph based blockchain solution, nodes authenticated by PKI	-	-	Improved efficiency & scalability
43	[77]	2019	Security	Use of blockchain to safeguard pickup and drop points, time of pickup, traffic congestion	Network congestion, attack possibility, user rating alteration	Existing approach [108]	Vehicles connected with IoT devices
44	[78]	2020	Security	CP-ABE technique, CSP is supervised by blockchain	Time for user encryption and decryption and data revocation	Chase's schemeFan's scheme	PBFT is used to avert malicious attack
45	[80]	2020	Security	Double layer blockchain, PBO, CBR	Cluster change, bargain times, welfare, requester utility	No. of vehicles, reque- ster, random matching	Data trading done using matching
46	TMHC [81]	2020	Security	Trust management, hybrid cryptography, symmetric hash message authentication & asymmetric identity-based digital signature	Communication, computation & storage overhead, end-to-end delay	ID-MAP, BLS, PKI-Certi, Xiaoyan's	Reward points are based on the type of safety alerts
47	CDG [70]	2021	Security	Agents cooperate among one another to detect, predict and react appropriately against attacks	False positive, false negative, overhead and delay	[109], [110], [111]	Based on hierarchical game
48	[82]	2021	Security	RSU used for authentication to reduce load on TA	Computational cost & time, communication cost	Xiong et al., He et al., Ying and Nayak [69]	Used blockchain
49	[83]	2021	Security	Construct new type of mining	Time interval, no. of nodes	Traditional PBFT, Service standard score	Used blockchain
50	CPPA scheme [84]	2015	Privacy	Batch verification of multiple message	Execution time, computation and communication cost	Shim's scheme, Zhang et al.'s scheme, Bayat et al.'s scheme	Used Elliptic Curve Cryptography

The authors in [101] managed pseudonyms of vehicles to achieve anonymity of the vehicle. The RSUs obtain pseudonyms generated by the TA and distributes with the vehicles. Once the pseudonyms are used, RSUs shuffle the pseudonyms among themselves to increase anonymity. One pseudonym is used by one vehicle at a particular time. A

TABLE II
(Continued.) BRIEF OVERVIEW OF WORK DONE IN VANET

Sl no.	Algo./ Paper	Year	Category	Basic Concept	Performance Against	Evolution From/ Compared With	Restriction/ Requirement/Others
51	[86]	2016	Privacy	One-way hash function and ID-based batch verification of signatures	Computational and communication cost	Yoon et al., EIBS, ZLLHS, KIBS (CAPS)	Used Elliptic Curve Cryptography
52	SPACF scheme [87]	2017	Privacy	Cuckoo filter, binary search technique to get a valid signature, batch verification	Lookup throughput, computation & communication cost, verificat- ion delay, transmission overhead	Chim et al. scheme, Horng et al. scheme, He et al. scheme	Used Elliptic Curve Cryptography
53	EAAP scheme [88]	2017	Privacy	Signature and certificates used along with other parameters to verify the vehicles and RSUs	Verification cost, RSU serving capability	BLS, ECPP, CAS, GSB, KPSD, TAA, IBCPPA	Used bilinear pairing technique
54	PrivAV protocol [4]	2019	Privacy	Two factor authentication, AVP server and local server to prevent theft and privacy	Time Cost, computational overhead	LI, HLKW, JLYM, VAKD, JKMS	Used bilinear pairing technique
55	P2B scheme [90]	2020	Privacy	Sender re-encrypts the ciphertext to generate re-ciphertext, it is then broadcasted to the receivers	Computation time, communication & storage overhead, transmission delay	Xu16 scheme, Sun18 scheme, Hur12 scheme	Used Lagrange interpolation and bilinear pairing
56	[91]	2020	Privacy	Appropriate CSPs for vehicles are selected by Cloud broker which is managed by TA	Computation & communication cost, packet loss, transmission delay	Liu's scheme, Ying's scheme, Jiang's scheme	Used Elliptic Curve Cryptography
57	PA-CRT protocol [89]	2021	Privacy	For generating new group key, the scheme uses Chinese Remainder Theorem	Computation and transmission cost, verification delay	Horng et al. scheme, Bayat et al. scheme, Shim et al. scheme, Malhi et al. scheme, He et al. scheme	Used Elliptic Curve Cryptography
58	[92]	2021	Privacy	Used blockchain along with asynchronous accumulator to verify membership	No. of certificates, average latency, No. of vehicles	CPAS, ABAKA, IBV	Used Merkel tree
59	CWS [93]	2015	Reputation based security and privacy	Reputation of the node based on score calculated by the node itself, neighbor of the node and the value assigned by the watchdog	Delivery probability, delay, overhead ratio, no. of dropped bundles	Varying selfish node percent and without CWS	Waste reduction, enhance performance
60	PPDAS [95]	2017	Reputation based security and privacy	Anonymous identity and temporary encryption key, vehicle's reputation using history of interaction behaviour	Computation cost, authentication time, message delay	CLAKA, VGKM, PPAS, VAAS	Used bilinear pairing
61	DREAMS [96]	2017	Reputation based security and privacy	Reputation of the vehicles calculated based on similarity, familiarity and timeliness	Reputation value, recognition rate, resource budget	MWSL, TSL	With higher reputa- tion higher priority to get resource
62	[97]	2019	Trustworthy based security and privacy	Security goals are achieved using blockchain, score given by different vehicles to message generating vehicle	Processing time, detection accuracy, transmission delay, encryption time	No. of vehicles, AES/ CBC, Twofish/CTR, Serpent/CTR	SDN enabled 5G-VANET
63	[98]	2019	Trustworthy based security and privacy	Uses social interaction and weight of edges to get community-based trust assessment	Error of accuracy, CDF, computing time	Global vehicular & local social network	Modeled as a directed graph
64	BPAS [99]	2020	Trustworthy based security and privacy	Integrates blockchain and cryptography, uses Attribute-Based Encryption	Time cost of operations	Basic, ABE & hyperledger operations	Used elliptic Curve Cryptography
65	ABAH scheme [100]	2016	Pseudonym Based security and privacy	CRL process replaced with HMAC, session key and group key are generated during batch verification	Broadcast, broadcast authentication & verification delay, packet loss ratio	ECDSA-AKA, BLS, IBV, ABAKA, CPAS, EMAP	Used bilinear pairing
66	[101]	2016	Pseudonym Based security and privacy	Once the pseudonyms are used, RSUs shuffle them among themselves	Anonymity set size, pseudonym distribution traffic per RSU	Network activity, transmission range	Used distributed optimization algo.
67	[102]	2018	Pseudonym Based security and privacy	Pseudonym is managed using a hierarchical architecture	Pseudonym requesting delay, communication overhead, pseudonym entropy	Existing scheme [112]	Context-aware pseudonym changing

vehicle can use multiple pseudonyms according to the number of activities it is involved.

In [102], a hierarchical approach is proposed in which new pseudonyms are distributed by local authorities when vehicles want to change pseudonyms. Changing a pseudonym is assisted by context information. Road intersection acts as a hotspot for the alteration of pseudonyms as the density of vehicles is high in intersections compared to lanes. The network

takes advantage of density, and malicious agents fail to recognize the vehicle whose pseudonym is changed. Figure 8 shows the work done in different years on security and privacy issues.

F. Open Issues in Security and Privacy in VANET

Maintaining safety and security in VANETs is a challenging task that requires a significant amount of computation for authenticating and validating messages. Along with this, the network has to allocate resources which also involves computation task. Controlling both the challenges cooperatively without hampering the performance is an issue of concern.

For authentication, security, and privacy, the network requires RSUs and TA. But in real-time, RSU may not be available in remote areas. The vehicles coordinate and communicate among themselves to pass information. In these situations, there arises a problem of authenticating and providing security and privacy services to vehicles.

In literature, vehicles change their pseudonyms in congested areas such as in road intersections or more traffic. But in case of vehicles traveling on highways, changing pseudonyms is challenging as there is not much road intersection and traffic availability.

IV. Conclusion

A brief overview of the allocation of the communication channel, radio resources, transmission power, computing, and storage resources is presented in this survey paper. While allocating resources, the network should take care of latency, reliability, and SINR requirements. Resource allocation mechanisms are different for delay-tolerant cases and non-delay tolerant circumstances. The paper has segregated resource allocation techniques into different categories. Along with resource allocation, the paper has also concentrated on privacy and security issues in the network. To attain anonymity, the network uses pseudonyms for hiding the real identity from a malicious agent. The role of TA is of great importance to provide security and privacy. At last, this work has presented and discussed the open issues associated with resource allocation, security, and privacy. Table II provides an overview of work done in different literature studied.

References

[1] B. Zhu, J. Han, J. Zhao, and H. Wang, "Combined hierarchical learning framework for personalized automatic lane-changing," *IEEE Trans. Intell. Transp. Syst.*, early access, May 8, 2020, doi: 10.1109/TITS.2020.2990787.

[2] J. Nie, J. Zhang, W. Ding, X. Wan, X. Chen, and B. Ran, "Decentralized cooperative lane-changing decision-making for connected autonomous vehicles," *IEEE Access*, vol. 4, pp. 9413–9420, 2016.

[3] Y. Lin and H. L. T. Nguyen, "Adaptive neuro-fuzzy predictor-based control for cooperative adaptive cruise control system," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1054–1063, Mar. 2020.

[4] J. Ni, X. Lin, and X. Shen, "Toward privacy-preserving valet parking in autonomous driving era," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2893–2905, Mar. 2019.

[5] *Autonomous Vehicles Worldwide—Statistics & Facts*. Accessed: Jul. 19, 2021. [Online]. Available: https://www.statista.com/topics/3573/autonomous-vehicle-technology/

[6] *DATEX II*. Accessed: Jul. 19, 2021. [Online]. Available: https://datex2.eu/datex2/about

[7] M. Noor-A-Rahim, Z. Liu, H. Lee, G. G. M. N. Ali, D. Pesch, and P. Xiao, "A survey on resource allocation in vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 4, 2020, doi: 10.1109/TITS.2020.3019322.

[8] A. Masmoudi, K. Mnif, and F. Zarai, "A survey on radio resource allocation for V2X communication," *Wireless Commun. Mobile Comput.*, vol. 2019, Oct. 2019, Art. no. 2430656.

[9] J. Liu, Y. Xu, and Z. Li, "Resource allocation for performance enhancement in mobile ad hoc networks," *IEEE Access*, vol. 7, pp. 73790–73803, 2019.

[10] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Challenges of future VANET and cloud-based approaches," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–15, May 2018.

[11] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[12] F. Ahmad, A. Adnane, V. N. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, pp. 1–19, 2018.

[13] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Veh. Commun.*, vol. 19, pp. 1–36, Oct. 2019.

[14] M. S. Sheikh and J. Liang, "A comprehensive survey on VANET security services in traffic management system," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–23, Sep. 2019.

[15] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[16] A. K. Mishra, A. K. Tripathy, D. Puthal, and L. T. Yang, "Analytical model for sybil attack phases in Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 379–387, Feb. 2019.

[17] A. K. Mishra and A. K. Turuk, "A comparative analysis of node replica detection schemes in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 61, pp. 21–32, Feb. 2016.

[18] A. Boukerche and R. I. Meneguette, "Vehicular cloud network: A new challenge for resource management based systems," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 159–164.

[19] R. Yu *et al.*, "Cooperative resource management in cloud-enabled vehicular networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7938–7951, Dec. 2015.

[20] K. Zheng, H. Meng, P. Chatzimisios, L. Lei, and X. Shen, "An SMDP-based resource allocation in vehicular cloud computing systems," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7920–7928, Dec. 2015.

[21] R. I. Meneguette and A. Boukerche, "Peer-to-peer protocol for allocated resources in vehicular cloud based on V2V communication," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, San Francisco, CA, USA, Mar. 2017, pp. 1–6.

[22] R. I. Meneguette, A. Boukerche, and A. H. M. Pimenta, "AVARAC: An availability-based resource allocation scheme for vehicular cloud," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 10, pp. 3688–3699, Oct. 2019.

[23] J. Zhao, Q. Li, Y. Gong, and K. Zhang, "Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7944–7956, Aug. 2019.

[24] H. Peng, Q. Ye, and X. S. Shen, "SDN-based resource management for autonomous vehicular networks: A multi-access edge computing approach," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 156–162, Aug. 2019.

[25] J. Bhatia, Y. Modi, S. Tanwar, and M. Bhavsar, "Software defined vehicular networks: A comprehensive review," *Int. J. Commun. Syst.*, vol. 32, no. 12, pp. 1–22, 2019.

[26] J. Sun, Q. Gu, T. Zheng, P. Dong, and Y. Qin, "Joint communication and computing resource allocation in vehicular edge computing," *Int. J. Distrib. Sens. Netw.*, vol. 15, no. 3, pp. 1–13, 2019.

[27] X. Wu, S. Zhao, R. Zhang, and L. Yang, "Mobility prediction-based joint task assignment and resource allocation in vehicular fog computing," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6.

[28] S. Pradhan and S. Tripathy, "FRAC: A flexible resource allocation for vehicular cloud system," *IET Intell. Transp. Syst.*, vol. 14, no. 14, pp. 2141–2150, 2021.

[29] F. Abbas and P. Fan, "A hybrid low-latency D2D resource allocation scheme based on cellular V2X networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Kansas City, MO, USA, May 2018, pp. 1–6.

[30] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1858–1877, 3rd Quart., 2018.

[31] S. Amberkar, "C-V2X autonomous resource selection explained," Bengaluru, India, Sasken Technol., White Paper, Jan. 2019.

[32] W. Sun, D. Yuan, E. G. Ström, and F. Brännström, "Cluster-based radio resource management for D2D-supported safety-critical V2X communications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2756–2769, Apr. 2016.

[33] X. Li, R. Shankaran, M. Orgun, L. Ma, and Y. Xu, "Joint autonomous resource selection and scheduled resource allocation for D2D-based V2X communication," in *Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring)*, Jun. 2018, pp. 1–5.

[34] *Proximity-Based Services (ProSe), Stage 2 (Release 13), V13.3.0*, 3GPP Standard TS 23.303, Mar. 2016.

[35] X. Li, L. Ma, R. Shankaran, Y. Xu, and M. A. Orgun, "Joint power control and resource allocation mode selection for safety-related V2X communication," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7970–7986, Aug. 2019.

[36] R. Molina-Masegosa and J. Gozalvez, "LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications," *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 30–39, Dec. 2017.

[37] X. Li, L. Ma, Y. Xu, and R. Shankaran, "Resource allocation for D2D-based V2X communication with imperfect CSI," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3545–3558, Apr. 2020.

[38] X. Cao, L. Liu, Y. Cheng, L. X. Cai, and C. Sun, "On optimal device-to-device resource allocation for minimizing end-to-end delay in VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7905–7916, Oct. 2016.

[39] W. Sun, E. G. Ström, F. Brännström, K. C. Sou, and Y. Sui, "Radio resource management for D2D-based V2V communication," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6636–6650, Aug. 2016.

[40] L. Liang, G. Y. Li, and W. Xu, "Resource allocation for D2D-enabled vehicular communications," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3186–3197, Jul. 2017.

[41] X. Liu, Q. He, Y. Li, and J. Wang, "Large-scale fading based power allocation for device-to-device underlay cellular communication," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, May 2015, pp. 1–5.

[42] Y. Qi, H. Wang, L. Zhang, and B. Wang, "Optimal access mode selection and resource allocation for cellular-VANET heterogeneous networks," *IET Commun.*, vol. 11, no. 13, pp. 2012–2019, 2017.

[43] S. A. Hussain *et al.*, "An efficient channel access scheme for vehicular ad hoc networks," *Mobile Inf. Syst.*, vol. 2017, pp. 1–10, Jun. 2017.

[44] J. Mei, K. Zheng, L. Zhao, Y. Teng, and X. Wang, "A latency and reliability guaranteed resource allocation scheme for LTE V2V communication systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3850–3860, Jun. 2018.

[45] Y. Meng, Y. Dong, X. Liu, and Y. Zhao, "An interference-aware resource allocation scheme for connectivity improvement in vehicular networks," *IEEE Access*, vol. 6, pp. 51319–51328, 2018.

[46] M. I. Ashraf, C. Liu, M. Bennis, W. Saad, and C. S. Hong, "Dynamic resource allocation for optimized latency and reliability in vehicular networks," *IEEE Access*, vol. 6, pp. 63843–63858, 2018.

[47] F. Yang, J. Han, X. Ding, Z. Wei, and X. Bi, "Spectral efficiency optimization and interference management for multi-hop D2D communications in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6422–6436, Jun. 2020.

[48] R. Li and P. Zhu, "Spectrum allocation strategies based on QoS in cognitive vehicle networks," *IEEE Access*, vol. 8, pp. 99922–99933, 2020.

[49] Q. Yan, B.-J. Hu, and Q. Wen, "Joint resource allocation and power control for V2V communication of high-density vehicle network," in *Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring)*, Apr. 2021, pp. 1–6.

[50] H. Peng *et al.*, "Resource allocation for cellular-based inter-vehicle communications in autonomous multiplatoons," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11249–11263, Dec. 2017.

[51] Z. Kuang, Z. Chen, J. Pan, and D. Sajjadi, "Joint optimization of spectrum access and power allocation in uplink OFDMA CR-VANETs," *Wireless Netw.*, vol. 25, no. 1, pp. 1–11, 2019.

[52] S. Hung, X. Zhang, A. Festag, K. Chen, and G. Fettweis, "An efficient radio resource re-allocation scheme for delay guaranteed vehicle-to-vehicle network," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Montreal, QC, Canada, Sep. 2016, pp. 1–6.

[53] X. Lin, J. G. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6727–6740, Dec. 2014.

[54] H. Liu, H. Yang, K. Zheng, and L. Lei, "Resource allocation schemes in multi-vehicle cooperation systems," *J. Commun. Inf. Netw.*, vol. 2, no. 2, pp. 113–125, 2017.

[55] Y. Li and Q. Liu, "Intersection management for autonomous vehicles with vehicle-to-infrastructure communication," *PLoS One*, vol. 15, no. 7, pp. 1–12, 2020.

[56] X. Peng, H. Zhou, B. Qian, K. Yu, N. Cheng, and X. Shen, "Security-aware resource sharing for D2D enabled multiplatooning vehicular communications," in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Honolulu, HI, USA, Sep. 2019, pp. 1–6.

[57] M. A. Salahuddin, A. Al-Fuqaha, and M. Guizani, "Reinforcement learning for resource provisioning in the vehicular cloud," *IEEE Wireless Commun.*, vol. 23, no. 4, pp. 128–135, Aug. 2016.

[58] Y. He, F. R. Yu, N. Zhao, H. Yin, and A. Boukerche, "Deep reinforcement learning (DRL)-based resource management in software-defined and virtualized vehicular ad hoc networks," in *Proc. 6th ACM Symp. Develop. Anal. Intell. Veh. Netw. Appl.*, Nov. 2017, pp. 47–54.

[59] D. Krishnaswamy, P. N. Lundqvist, R. S. Daley, and V. L. Bychkovsky, "Apparatus and method for mobile virtual network operator (MVNO) hosting and pricing," U.S. Patent 8 825 876, Sep. 2014.

[60] H. Ye and G. Y. Li, "Deep reinforcement learning for resource allocation in V2V communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1–6.

[61] H. Ye and G. Y. Li, "Deep reinforcement learning based distributed resource allocation for V2V broadcasting," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 440–445.

[62] H. Ye, G. Y. Li, and B.-F. Juang, "Deep reinforcement learning based resource allocation for V2V communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3163–3173, Apr. 2019.

[63] Y. Liu, H. Yu, S. Xie, and Y. Zhang, "Deep reinforcement learning for offloading and resource allocation in vehicle edge computing and networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11158–11168, Nov. 2019.

[64] S. S. Doddalinganavar, P. Tergundi, and R. S. Patil, "Survey on deep reinforcement learning protocol in VANET," in *Proc. 1st Int. Conf. Adv. Inf. Technol. (ICAIT)*, Chikmagalur, India, Jul. 2019, pp. 81–86.

[65] M. A. Hossain *et al.*, "Machine learning-based cooperative spectrum sensing in dynamic segmentation enabled cognitive radio vehicular network," *Energies*, vol. 14, no. 4, pp. 1–30, 2021.

[66] M. Obaidat, M. Khodjaeva, J. Holst, and M. B. Zid, *Security and Privacy Challenges in Vehicular Ad Hoc Networks*. Cham, Switzerland: Springer, 2020, pp. 223–251.

[67] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015–1028, Apr. 2016.

[68] J. Y. Ho, W. Y. Koh, B. Veeravalli, J. W. Wong, and H. Guo, "Secure sensing inputs for autonomous vehicles," in *Proc. IEEE Reg. 10 Conf.*, Nov. 2017, pp. 1978–1983.

[69] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, Dec. 2017.

[70] S. Sedjelmaci, I. H. Brahmi, N. Ansari, and M. H. Rehmani, "Cyber security framework for vehicular network based on a hierarchical game," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 1, pp. 429–440, Jan.–Mar. 2021.

[71] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for VANETs: A statistical approach to rogue node detection," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6703–6714, Aug. 2015.

[72] Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated authentication and key agreement framework for vehicular cloud computing," *IEEE Netw.*, vol. 32, no. 3, pp. 28–35, May/Jun. 2018.

[73] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward secrecy," *IEEE Trans. Consum. Electron.*, vol. 49, no. 4, pp. 1246–1248, Nov. 2003.

[74] C. Li, S. Gong, X. Wang, L. Wang, Q. Jiang, and K. Okamura, "Secure and efficient content distribution in crowdsourced vehicular content-centric networking," *IEEE Access*, vol. 6, pp. 5727–5739, 2018.

[75] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in VANETs," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2972–2986, Mar. 2019.

[76] H. Rathore, A. Samant, M. Jadliwala, and A. Mohamed, "TangleCV: Decentralized Technique for secure message sharing in connected vehicles," in *Proc. ACM Workshop Automot. Cybersecurity*, Mar. 2019, pp. 45–48.
[77] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, pp. 1–15, 2019.
[78] K. Fan *et al.*, "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5826–5835, Jun. 2020.
[79] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Oper. Syst. Design Implement.*, vol. 99, Feb. 1999, pp. 173–186.
[80] C. Chen, C. Wang, T. Qiu, N. Lv, and Q. Pei, "A secure content sharing scheme based on blockchain in vehicular named data networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3278–3289, May 2020.
[81] S. Tangade, S. S. Manvi, and P. Lorenz, "Trust management scheme based on hybrid cryptography for secure communications in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5232–5243, May 2020.
[82] Z. Xu, W. Liang, K.-C. Li, J. Xu, and H. Jin, "A blockchain-based Roadside Unit-assisted authentication and key agreement protocol for Internet of Vehicles," *J. Parallel Distrib. Comput.*, vol. 149, pp. 29–39, Mar. 2021.
[83] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," *Inf. Sci.*, vol. 545, pp. 170–187, Feb. 2021.
[84] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 2681–2691, 2015.
[85] S. Horng *et al.*, "b-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Security*, vol. 8, pp. 1860–1875, 2013.
[86] N. Lo and J. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.
[87] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017.
[88] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.
[89] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese Remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar./Apr. 2021.
[90] S. Maiti and S. Misra, "P2B: Privacy preserving identity-based broadcast proxy re-encryption," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5610–5617, May 2020.
[91] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1654–1667, 2020.
[92] X. Feng, Q. Shi, Q. Xie, and L. Liu, "An efficient privacy-preserving authentication model based on blockchain for VANETs," *J. Syst. Archit.*, vol. 117, pp. 1–10, Aug. 2021.
[93] J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7929–7937, Dec. 2015.
[94] C. H. Kim and I. H. Bae, *A Misbehavior-Based Reputation Management System for VANETs*. Dordrecht, Netherlands: Springer, 2012, pp. 441–450.
[95] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.
[96] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.
[97] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.
[98] T. Cheng, G. Liu, Q. Yang, and J. Sun, "Trust assessment in vehicular social network based on three-valued subjective logic," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 652–663, Mar. 2019.
[99] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.
[100] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.
[101] H. Artail and N. Abbani, "A pseudonym management system to achieve anonymity in vehicular ad hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 1, pp. 106–119, Jan./Feb. 2016.
[102] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2627–2637, Aug. 2018.
[103] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular networks," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3541–3551, Aug. 2013.
[104] Y. Gu, L. X. Cai, M. Pan, L. Song, and Z. Han, "Exploiting the stable fixture matching game for content sharing in D2D-based LTE-V2X communications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–6.
[105] L. Liang, J. Kim, S. C. Jha, K. Sivanesan, and G. Y. Li, "Spectrum and power allocation for vehicular communications with delayed CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 458–461, Aug. 2017.
[106] M. Zulhasnine, C. Huang, and A. Srinivasan, "Efficient resource allocation for device-to-device communication underlaying LTE network," in *Proc. IEEE 6th Int. Conf. Wireless Mobile Comput. Netw. Commun.*, Niagara Falls, ON, Canada, Oct. 2010, pp. 368–375.
[107] M. I. Ashraf, M. Bennis, C. Perfecto, and W. Saad, "Dynamic proximity-aware resource allocation in vehicle-to-vehicle (V2V) communications," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Washington, DC, USA, Dec. 2016, pp. 1–6.
[108] T. T. Dandala, V. Krishnamurthy, and R. Alwan, "Internet of Vehicles (IoV) for traffic management," in *Proc. Int. Conf. Comput. Commun. Signal Process. (ICCCSP)*, Chennai, India, Jan. 2017, pp. 1–4.
[109] A. Boudguiga, W. Klaudel, A. Boulanger, and P. Chiron, "A simple intrusion detection method for controller area network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–7.
[110] M. J. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PloS One*, vol. 11, no. 6, pp. 1–17, 2016.
[111] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 5, pp. 1143–1153, May 2017.
[112] Y. Park, C. Sur, and K. H. Rhee, "Pseudonymous authentication for secure V2I services in cloud-based vehicular networks," *J. Ambient Intell. Humanized Comput.*, vol. 7, pp. 661–671, Oct. 2016.