Hindawi
Journal of Advanced Transportation
Volume 2021, Article ID 9888789, 15 pages
https://doi.org/10.1155/2021/9888789

Research Article

Autonomous Real-Time Speed-Limit Violation Detection and Reporting Systems Based on the Internet of Vehicles (IoV)

Samir A. Elsagheer Mohamed,[1,2,3] **Mohammad T. Parvez**,[1] **Khaled A. AlShalfan**,[4] **Mahmoud Y. Alaidy**,[1] **Mohammed A. Al-Hagery**,[5,6] **and Mohamed T. Ben Othman**[5,6]

[1]*Computer Engineering Department, College of Computer, Qassim University, Buraydah, Qassim, Saudi Arabia*
[2]*Computer Science and Engineering Department, Egypt-Japan University of Science and Technology (E-JUST), New Borg-El-Arab City, Alexandria, Egypt*
[3]*Faculty of Engineering, Aswan University, Aswan, Egypt*
[4]*College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia*
[5]*BIND Research Group, College of Computer, Qassim University, Buraydah, Qassim, Saudi Arabia*
[6]*Department of Computer Science, College of Computer, Qassim University, Buraydah, Qassim, Saudi Arabia*

Correspondence should be addressed to Samir A. Elsagheer Mohamed; samir.elsagheer@ejust.edu.eg

Received 8 August 2021; Accepted 16 August 2021; Published 24 September 2021

Academic Editor: Elżbieta Macioszek

Over-/underspeeding is one of the leading causes of road accidents. Traditional systems of detecting and reporting speed-limit violations are not suitable for smart cities. Even the sophisticated conventional systems that use cameras or RFIDs for automating speed-limit violations have several drawbacks, including cost, complexity, reliability, and maintenance. In this paper, we present two systems based on the Internet of Vehicles (IoV) to automatically detect speed-limit violations and autonomously report the committed violations to the authorities. Our systems require no extra hardware or equipment: only the On-Board Unit (OBU), the Road Side Unit (RSU), and the Cloud Server software have to be updated to have a fully functioning system as long as the IoV infrastructure is deployed. One of the systems will be installed on the OBU. A second alternative system design is to use Cloud Servers (CSs) and the IoV beacons that are sent from the vehicles. Additionally, unlike the existing systems installed in specific locations, all roads in the smart cities and highways will be fully monitored. Adaptive fine calculation according to new dynamic policies can be easily integrated into the proposed system. Furthermore, the proposed system can accurately operate in all weather conditions. Moreover, it allows the dynamic adjustment of the speed limits according to the current weather conditions. We have validated the proposed system by building a prototype system that effectively and accurately detects and reports over-/underspeed traffic violations alongside any road.

1. Introduction

Traffic rule violation is a major problem that affects society and the economy. Most road accidents are due to traffic rules' violations. These accidents cause death, physical disabilities, and psychological disorders for people. The World Health Organization (WHO) reports that approximately 1.35 million people die every year due to road crashes. The actual figures are much higher because accidents are not reported to the authorities in several developing countries.

Moreover, according to the WHO's statistical reports, 54% of people who die from road accidents are vulnerable road users. In addition, the WHO has set a target to reduce road causalities to half by 2030 according to the Agenda for Sustainable Development [1]. It is obvious that limiting or reducing traffic accidents can be achieved by minimizing or eliminating traffic violations. Although there are different types of traffic violations, one of the most dangerous violations is overspeeding (driving at a speed more than the maximum legal speed limits). In some situations, driving on highways at a too slow speed, underspeeding, can also cause severe accidents. This paper focuses on over-/underspeeding (speed limit) traffic violation types only.

The problem of speed-limit violation detection has been studied intensively for several decades. Traditional means are by using traffic patrols and speed radars. Radar signals can be jammed or detected by radar detectors, and thus, they are not effective. Traditional sophisticated systems include cameras and speed detector radars to automatically identify the vehicle plate numbers and send information to the traffic authority to collect fines. More advanced traditional methods are by using RFID tags on each vehicle and using several RFID readers to estimate the speed of each vehicle. The camera-based approach suffers from the same problems as the radar-based system. In addition, they are very complex (involving Computer Vision), expensive, and inaccurate.

The traditional systems suffer from one serious problem, in addition to the cost, reliability, and flexibility. These traditional systems are usually installed in fixed locations. It is impossible to install a speed-limit detector every few meters to cover all roads. Therefore, they can only detect the speed-limit violations in a tiny fraction of the whole roads. Drivers can know the locations of these detectors and can slow down at these locations to avoid detection; then, the drivers can overspeed in the other segments (not covered). Social apps are widely developed and used to warn drivers about the location of speed cameras.

Almost all existing speed-limit violation detection systems require the development and deployment of costly dedicated equipment. Internet of Vehicles (IoV) [2], which is a subset of Intelligent Transportation Systems (ITSs), enables plenty of auspicious smart transportation applications that can be deployed in smart cities and highways. Thus, instead of building and deploying dedicated systems for detecting speed-limit violations, we propose the use of IoV infrastructure to automatically detect speed-limit violations and to automatically report them to the traffic authorities to collect fines from the owner of the vehicles without any human intervention in the process.

In this paper, we propose the use of Intelligent Transportation Systems (ITSs) and the Internet of Vehicles (IoV) to develop two smart, accurate, and efficient speed-limit violation detection systems. In addition, we present an automatic and autonomous reporting system of the committed speed-limit violations. These systems could be used in smart cities and highways to minimize speed-limit violations and to support the WHO's Sustainable Development targets.

IoV, once deployed, would enable the development of many useful applications related to safety [3–5], traffic management and optimization [6–8], road lighting control and monitoring [9], and infotainment [2]. The essential component of IoV is the smart vehicle that contains an On-Board Unit (OBU). OBU can be viewed as a vehicle computer with added IoV functionality and features (software and hardware). The legacy vehicle can be easily upgraded to be IoV capable by building the OBU and installing it in the vehicle. Vehicles can communicate with each other while moving on the road using Vehicle-to-Vehicle (V2V) communication. In addition, in IoV, the vehicles must communicate with an infrastructure that consists of interconnected Road Side Units (RSUs) installed alongside the road. Vehicles communicate with the infrastructure using V2I through the RSUs. A vehicle can communicate with the Cloud using V2C. Vehicles can communicate with pedestrians using V2P. There are many other communication types in IoV, such as V2G (grid), V2H (home), V2D (device), and V2R (road traffic sign). For more details, please refer to [3, 10, 11].

The proposed systems in this paper are based on IoV technology. Few components and communication protocols will be used from IoV. The proposed systems will not require any extra hardware components to operate effectively. Only software update to the existing IoV stack is needed to implement speed-limit violation detection and reporting. In addition, an essential feature of the proposed technique is that it monitors all roads for any speed-limit violation. This means that any speed-limit violation committed on any location of the road will be detected.

This paper presents two different systems to automatically and efficiently detect speed-limit violations based on IoV. In addition, we present a traffic violation reporting system to the traffic authorities. We present a new dynamic and adaptive fine calculation policy framework for the committed violations.

The rest of this paper is organized as follows: in Section 2, the related techniques and technologies are presented. The overall system architecture of speed-limit violation detection and reporting based on IoV is presented in Section 3. We present the two proposed speed-limit violation detection systems in Section 4. Speed-limit adaptive fine calculation framework is presented in Section 5. A prototype system developed for the validation of the proposed systems is outlined in Section 6. Finally, the conclusions and future directions are given in Section 7.

2. Related Techniques and Technologies

The following topics are relevant to this article: the advance in the positioning techniques, the traffic violation detection techniques, the ad hoc networking, the Vehicular Ad Hoc Network, and the security techniques to secure all communications.

2.1. Existing Speed-Limit Traffic Violation Recording Systems. The discussions here focus on two key issues: detecting the vehicle's speed and extracting the official speed-limit information at the current location of the vehicle.

Several works for detecting automatic traffic violations use different ways to estimate the speed of the vehicle. In [12], the vehicle speed is estimated using a motion plane-based approach considering the projection displacement difference (PDD). Here, the vehicle reference point is the same as the center of a vehicle license plate and is used to estimate the motion plane. Then, the displacement is estimated by mapping the plate position to the motion plane. Another work that uses customized hardware to estimate the speed is [13], where an array of active infrared sensors is used to report violation-related data to the data center. The work in [14] also uses customized hardware to estimate the speed of the vehicle. In [15], a speedometer using XBee is used to record the vehicle's speed to compare with the network of Master XBees.

The method in [16] uses Road Side Units (RSUs) in a Vehicular Ad Hoc Network (VANET) for estimating vehicular speed. Using information from nearby several RSUs, the speed of the vehicle can be estimated. A similar research proposal for detecting the speed-limit violation using VANET is presented in [17].

The work in [18] uses a different approach for detecting traffic violations based on the real-time video feedback of CCTV cameras. The real-time video footage is analyzed to detect traffic violations, including speed-limit violations. Similar work is reported in [19] where IP (Internet Protocol)-enabled cameras are used to monitor the roads to monitor traffic violations. Another work that uses real-time video feedback for traffic monitoring is reported in [20]. In a similar approach, works in [13, 21, 22] explore the use of Unmanned Aerial Vehicle (UAV) for road safety, traffic, and highway infrastructure management.

As for the second issue, different traffic violation recording systems use different approaches to extract the speed-limit information at the vehicle's current location. The work in [23] attempts to detect the roadside signboards for speed-limit information using image processing and then notify the driver about the extracted information. In [15], a network of Master XBees is installed in every locality that can broadcast information about the speed limit of the locality.

Different researchers used techniques for the notification and recording of traffic violations. The work in [23] uses Arduino and GPRS to send traffic violation data to the Cloud for processing. In [16], the traffic violation is computed and recorded in the Cloud from the data sent by Road Side Units. In [15], when speed-limit violation is detected (even after warning), the information regarding the vehicle registration number is transmitted to the master XBee installed specifically for the task. This master XBee is connected to the Cloud Server, and traffic data can be accessed from anywhere.

2.2. Internet of Vehicles (IoV). Since this work utilizes the Internet of Vehicles (IoV) (a typical architecture of IoV is given in Figure 1), a brief discussion of the key issues in IoV research is presented here. The use of IoV and VANET for Intelligent Transportation Systems has increased a lot in recent years [2, 24]. Due to the nature of its domain, IoV applications need greater data throughput, lower latency, higher security, and massive connectivity [24]. Emerging new applications in IoV requires seamless connectivity, edge, fog, software-defined, and named data network [25]. When deployed in smart cities, IoV applications need large-scale data sensing, collection, information processing, and storage [3].

A key concern in IoV and VANET is the security issue in the communicated data to/from vehicles. Using conventional cryptographic techniques may affect the performance of delay-sensitive networks such as IoV and VANETs. To overcome this issue, some researchers have proposed RFID (Radio-Frequency Identification) device-based authentication scheme for IoV [2].

Another issue is the radio access technologies that are used in IoV applications. The work in [10] discusses reliable and scalable wireless transmissions for the Internet of Vehicles (IoV). With the massive amount of data transmitted in IoV applications, the work in [10] analyzed the performance of Vehicle-to-Vehicle (V2V) beacon broadcasting using random access-based (IEEE 802.11p). The work in [3] proposed a new architecture for the IoV applications in smart cities.

The work in [26] studies the applications of machine learning (ML) to handle IoV requirements of ultralow latency, high reliability, high security, and massive connections of the next-generation (6G) network. The goal here is to assist in the evolution of intelligent radio (IR), and self-learning with proactive exploration.

2.3. Positioning Techniques. To locate mobile users techniques such as Time Difference of Arrival (TDOA), Enhanced Observed Time Difference of Arrival (E-OTD), Angle of Arrival (AOA), Time of Arrival (TOA), Received Signal Strength (RSS) indication [27], and GPS systems are used [28, 29]. Many of these methods suffer from issues such as security, the need for special types of antennas, highly complex design algorithms, high estimation time, and high cost. Several research attempts are conducted to provide secure location services and location verification to be sure that the vehicle is not cheating its current location [30–32].

There are many other methods proposed for estimating the location of vehicles. Visible light-based positioning for IoV is discussed in [33]. The work in [34] proposed the use of nanointegrated devices to provide accurate distance estimation for VANET. The ego-positioning algorithm based on camera for IoV is presented in [35]. Moreover, Doppler-shifted signals to localize a vehicle by using two RSUs are proposed in [28].

Several works focus on the relative locations between vehicles. The relative position between vehicles as well as between a vehicle and Road Side Unit (RSU) is studied in [36]. The authors attempted to optimize the nonranging technology such as DVHop algorithm (with chemical reaction optimization) to reduce the error of localization. Similarly, the authors in [37] propose a method to study the behavioral correlation between vehicles to cluster them. Then, deep learning is used to predict the vehicles' future location distribution. The work in [38] also deals with the noisy observation of the pairwise distance and the angle between vehicles and considers this as a nonlinear optimization problem, which is solved by deep learning models. Another word for relative localization for ground vehicles is [39], where UAV is used for ranging measurements with ground base stations and other UAVs in the round-trip time mode.

In [40], the authors take a different approach for correcting the location estimation by a technique called

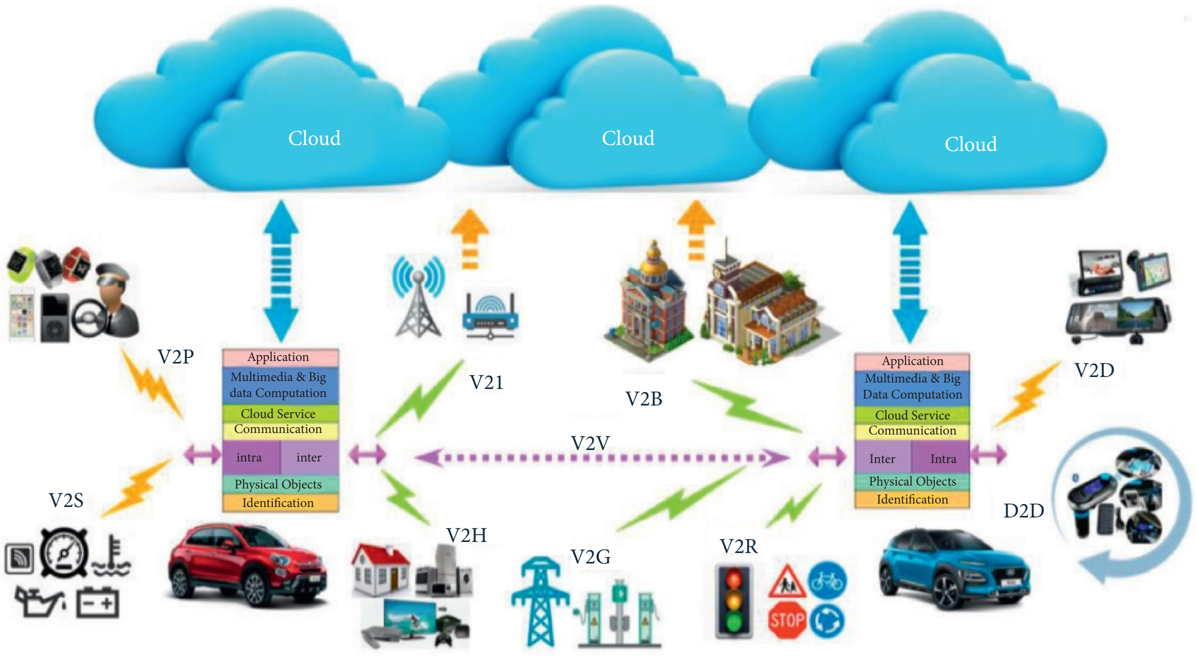

Figure 1: A universal Internet of Vehicles architecture for smart cities [3].

collaborative driving. They try to correct GPS errors of a legacy car if that car encounters a sensor-rich car in a downtown scenario where GPS accuracies can be bad. The authors in [40] report that GPS error for legacy vehicles is reduced from 90% to 30% for sensor-rich vehicles. Another work that deals with correcting the GPS locations is [41]. Here, the authors propose an assistant vehicle localization method based on direction-of-arrival (DOA) estimation to improve the accuracy of vehicle localization. The proposed system is very complex, consisting of a minimum of three multiple-input-multiple-output (MIMO) base stations (BSs). The positions of the three BSs and the DOAs of vehicles estimated by the BSs are used to estimate the locations of the vehicles.

The work in [42] deals with users' location privacy: designing a realistic, privacy-preserving positioning system based on fingerprinting. The work in [27] studies the effect of the Received Signal Strength (RSS) on positioning performance. Another work that uses RSS is [30] for wireless localization that can be used in applications where the information whether an object is inside or outside of a specific area is needed only. For more details on localization techniques in IoV and VANET, please refer to the surveys in [43, 44].

3. Overall System Architecture of the Speed-Limit Violation Detection and Reporting Based on IoV

In this section, we present the overall system architecture of the proposed systems for detecting the speed-limit violation and reporting the violations to the authorities using IoV technology. The architecture consists of the basic functional layers of IoV. However, the On-Board Unit (OBU), the Road Side Unit (RSU), and the Cloud Servers (CSs) are to be upgraded (software only). In the next sections, we explain each of the components of the system. We show in Figure 2 the abstract IoV architecture focusing on the essential components that will be used in the two systems (presented in the next section) for automatically detecting and reporting the speed-limit violations without any extra hardware.

3.1. *The On-Board Unit of the Vehicle.*

The most elementary module of IoV is the On-Board Unit (OBU) that has to be installed inside each vehicle. The OBU allows the vehicle to communicate with the other components of IoV and to perform IoV operations in the vehicle. We depict in Figure 2 the basic OBU as well as the extra modules that are essential to perform the autonomous and automatic speed-limit violation detection and reporting. Each of the modules/units of OBU is described as follows:

(a) *Internet of Vehicles (IoV) protocol stack* allows the vehicle to communicate securely with other entities and implements all the essential IoV layers.

(b) *V2I and V2C communication unit* for the Vehicle-to-Infrastructure (RSU) and Vehicle-to-Cloud communication. The communication is bidirectional. Committed traffic violations will be sent to RSU (using V2I), and then RSU will send them to Cloud Servers.

(c) *GNSS and location service unit* enables the vehicle to obtain in real-time its location, its speed, and its direction in degrees. More details are given in Section 3.5.

(d) *Speed-limit violation detection unit* implements the algorithm for speed-limit violation detection in the case when OBU is responsible for the detection as described in Section 4.1.

(e) *Speed-limit evaluation reporting unit* sends committed speed-limit violations to CSs through RSUs.

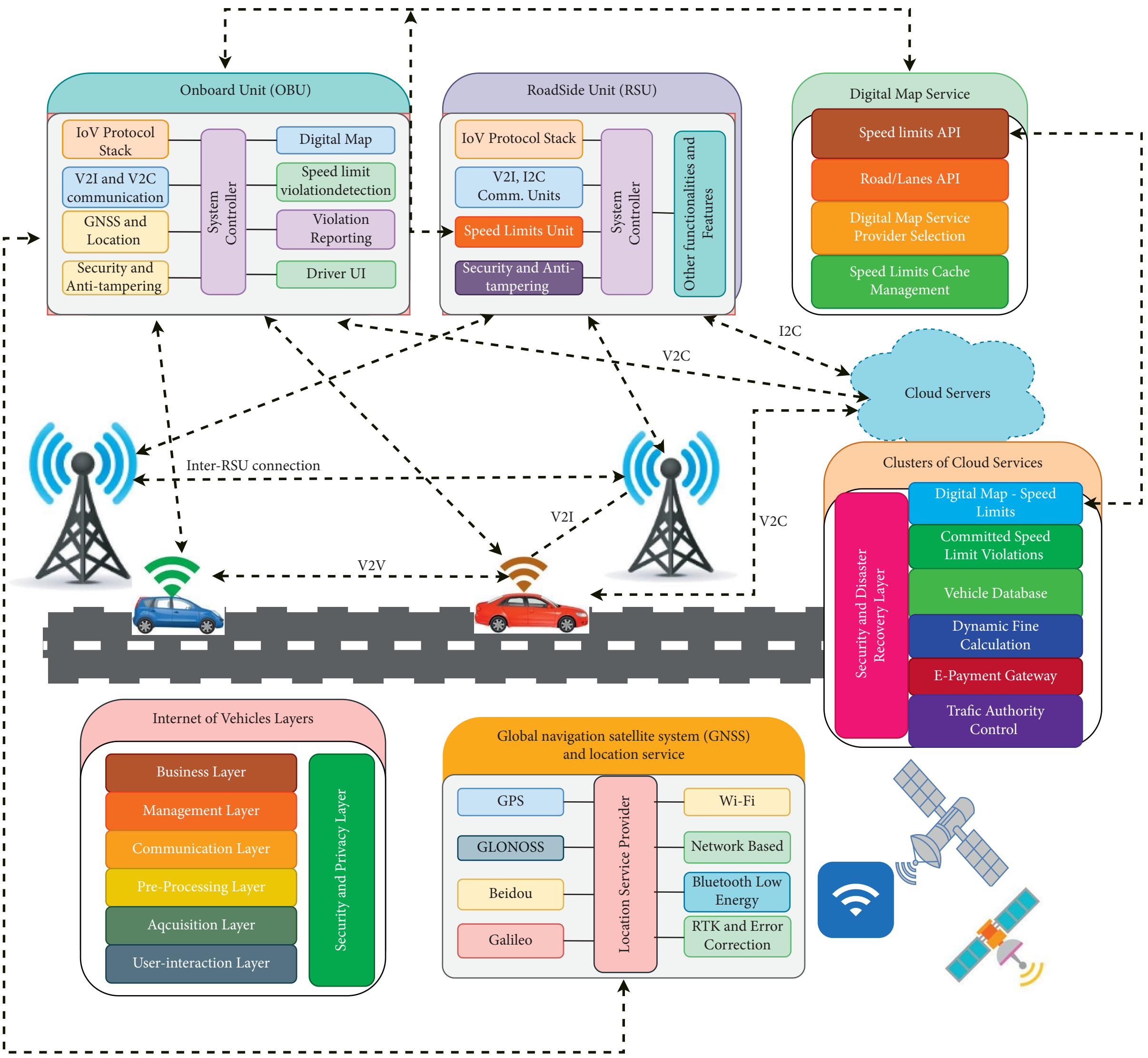

Figure 2: Overall over-/underspeed limit violation detection and reporting system based on the Internet of Vehicles.

(f) *Driver UI* provides visual and vocal messages and directions to drivers. It consists of an interactive touchscreen, microphone, speech recognition engine, and speakers. It produces warning messages and instructions to drivers.

(g) *Security and antitampering unit* provides the security layers of the components of the OBU. In addition, it provides the privacy of the information of the driver (to avoid tracking the vehicle for example). PKI integrated with the CSs' Certificate Authority (CA) specialized for IoV is implemented in this unit. It guarantees secure communication with the other entities. In addition, this unit protects OBU from being tampered with or bypassed. For more details about security issues in IoV, please refer to [26, 31, 45–53].

3.2. Interconnected Road Side Units (RSUs). An essential component of IoV is the infrastructure, which consists of Road Side Units (RSUs) that are connected to a dedicated network. This network is connected to CSs and Traffic Management. RSUs are installed alongside roads. In this way, vehicles can communicate with RSU's using V2I communication. In addition, vehicles can communicate with CSs using RSU as the gateway. As shown in Figure 2, an RSU has the following components:

(a) *Internet of Vehicles (IoV) protocol stack* is required for RSU's essential functionality. It is different from the stack on an RSU. RSU stack provides functionalities such as V2I, I2C, and RSU to RSU communication.

(b) *V2I and I2C communication unit* to allow the communication between an RSU and nearby vehicles on a road and to receive the messages from the vehicles and send them to CSs. This unit is essential for the functionality of the "Traffic Violation Detection and Reporting using the RSU," as described in Section 1.

(c) *Speed-limit unit* caches the allowed speed limits for each vehicle type. It obtains the speed-limit values from Digital Map Service that runs in CSs. This minimizes the requests to CSs and avoids excessive costs for fetching these values from the Digital Map Service Provider unit. Details about this are given in Section 3.4.

(d) *Security and antitampering unit* implements the necessary level of security for RSU to allow secure and private communication with all other entities. For more details, please refer to the equivalent unit in the OBU, in Section 3.1.

3.3. Cloud Servers (CSs). One essential component in IoV, which does not exist in VANET, is the Cloud. It consists of several clustered servers running in the Cloud that provide the required services to IoV. The CSs may provide the following services:

(a) *Digital Map-Speed Limits*. This is the most important service in this paper. More details are given in Section 3.4.

(b) *Committed Speed-Limit Violations*. This service acts as the database of the committed speed-limit violations for each vehicle. It receives the committed violations from the OBU or calculates them from the data received from RSU (as described in Section 1). For each committed violation, the start time and date of the violation, its duration, the maximum reached value of overspeeding or underspeeding, the location (coordinates, road name, city, and country), the vehicle electronic unique ID, etc. will be saved.

(c) *Vehicle Database*. It contains all vehicle data, such as electronic ID, driver name, and driver ID. In addition, digital certificates of each vehicle and any other information about the vehicle could be saved in this back-end database.

(d) *Dynamic Fine Calculation*. This service calculates the violation fines dynamically according to a dynamic policy that can be changed by the traffic authority. It could not be implemented by the existing techniques. Details about this are given in Section 5.

(e) *E-Payment Gateway*. This service integrates the e-payment methods to allow the automatic payment of the committed fines.

(f) *Traffic Authority Control*. This service allows the traffic authorities to control and monitor the system, for example, disabling the traffic violation on a specific period of time on a specific road or zone.

(g) *Security and Disaster Recovery Layer*. It includes all the security measures to secure the services from cybersecurity attacks. It involves backups and disaster recovery as well.

3.4. Digital Map Service and the Speed Limits. Another essential component of the proposed systems is the Digital Map Service and Speed-Limit Service providers. This enables the systems and the drivers to know the allowed speed ranges at each location and lane on the road. The speed limits vary according to the vehicle type. Speed limits can also be globally adjusted according to specific conditions, such as weather conditions. For example, RSU can broadcast to all vehicles to reduce the maximum speed limit for small cars to 60 km/hr for a specific road segment, because the IoV infrastructure has detected that it is currently foggy. This component consists of the following units:

(a) *Speed limits API*. It retrieves the speed-limit information as a function of a coordinate or a road segment. The retrieved data could vary according to the vehicle type, the lane, the time of the day, the weather condition, etc. Upon request from any other component on the system (OBU, RSU, or CSs), the API obtains the data from the Digital Map Service Provider. Details about this are given in Section 3.6.

(b) *Road/Lanes API*. It provides the lane and road information.

(c) *Digital Map Service Provider Selection*. It selects the suitable Digital Map Service Provider, if there are more than one. This depends on the policy, the cost, and service agreement.

(d) *Speed-Limit Cache Management*. Usually, if a third party provides the speed-limit information through their digital maps, the requests are not free, and this costs money. If each vehicle requests a speed-limit query every second while on the road, this means that a large number of requests will be sent to the Digital Map Service Providers. This will cause several problems and can cost too much. To make the system effective and efficient, this module will cache every new response from the service provider. Future requests from the OBU or RSU will be sent directly from the cached information. In addition, when a vehicle queries the system for the speed limits at a location, the OBU of the vehicle saves the returned information in its local storage for future uses. Furthermore, RSUs cache speed limits in their covered areas and broadcast this information to the vehicles. Thus, new requests to the service provider will be minimized. Care must be taken to set a suitable cache duration and to delete outdated cached items. In addition, for specific events, when the authority would like to change the speed limits for a specific time in road segments, then the old entries must be updated by the new one. The Cache Management unit handles all these actions.

3.5. Global Navigation Satellite System (GNSS) and Location Service. In IoV, the vehicle must know its current all the time. In addition, the vehicle's speed is calculated from the temporal change of the vehicle's location, if access to the CAN bus is not possible. Furthermore, the vehicle's moving direction (bearing angle) can be calculated from the change of location. Thus, location service is a must for the proper operation of IoV. As stated in Section 2.3, there are several location services for IoV. In this section, we will explain the most common ones. The most common one is GPS; however, its accuracy is not enough to allow the vehicle to know on which lane it is moving. As shown in Table 1, GPS provides an accuracy between 2 and 5 meters.

Currently, there are many GNSS [54] constellations such as GPS [55], BeiDou [56], Galileo [57], and GLONASS [58]. Each satellite system operates on different frequencies, as shown in Figure 3. To improve the accuracy of the location service, the GNSS receiver must receive from two or more satellite systems. This significantly improves the accuracy that can be in the range of 0.7–1.5 meters. For more details on the accuracy of combining two or more different systems, please refer to [60–62].

DGPS (Differential GPS) provides an accuracy of about 1–2 meters. It consists of installing a ground station that can calculate the real-time errors in the signals and broadcasts them to the surrounding vehicles. Similar to DGPS, RTK (Real-Time Kinematic) relays on a ground station to calculate the GNSS errors at its surrounding, as shown in Figure 4. One great advantage of RTK is that it can provide an accuracy of few centimeters (2–5 cm). Table 1 shows a comparison of the accuracy of the different positioning systems that can be used in IoV.

3.6. On the Digital Map Service Provider and the Speed-Limit Retrieval. Digital maps are essential components of the system. We need them to determine many parameters: the location of the committed violation and the allowed speed limit, etc. In the following, we discuss several digital map services available for research and development.

3.6.1. OpenStreetMaps. OpenStreetMap data can be used to extract the maximum speed limits and the number of lanes, etc. However, these map data are not available for all the countries.

3.6.2. Google Maps. Google Maps is a web mapping service developed by Google and launched in February 2005.

"The Roads API" returns the maximum speed limit for a given road coordinate on a road. However, the reported speed limits are not accurate, and the service is not available in many countries.

3.6.3. Sygic Digital Maps. Sygic navigation provides real-time traffic information based on TomTom Traffic. Sygic has a "Road info" API which is a Cloud-based service that can return the speed limits about the selected road or road segments.

However, we tested this service while driving on many roads in Saudi Arabia. However, the returned speed limits were not accurate and were outdated.

3.6.4. TomTom Digital Maps. This service is similar to Sygic; however, the service cost is high. For more information, please refer to the site: https://developer.tomtom.com/store/maps-api.

3.6.5. MS Bing Digital Maps. Microsoft Bing Maps is a web application with custom maps. There is a fee for providing the speed limit.

The Snap-to-Road API is a convenient REST service for this research work. Bing Maps Snap-to-Road API needs GPS points (latitude and longitude coordinates) in a URL and returns a corresponding set of data with the points that snap to the most likely roads and corresponding road names and the speed limits. This service provides accurate and updated information about the speed limit in many different countries. It is one of the best available speed-limit services suitable to our proposed systems.

3.6.6. HERE Technologies. HERE Technologies (here.com) is one of the leaders in location technologies. They have the most accurate and updated database and the most extensive coverage of the speed-limit information. The cost of the service is cheap, and they provide free monthly service access that is enough for testing and validation. We have integrated this service into our developed software and systems.

3.7. Security Considerations. An important concern about the applicability of the proposed systems is the security issues that may include hardware tampering, software tampering, and information security. IoV security issues are extensively studied in the literature. Our proposed systems use the same IoV security approaches. We will focus here on the security issues related to the functionality of the speed-limit violation detection and reporting application only. The Root of Trust is a very effective approach for securing the hardware of all the components of the system. Thus, it can be used to effectively secure OBU from any hardware tampering and program the vehicle system to not start if any violation of the hardware or software integrity is detected. Secure software development is a must for such systems, and it must be done by a trusted authority with software signing by their digital certificate. Thus, any tampering of the software can be detected and hence stop the engine of the vehicle. Only these software authorities can update or upgrade the OBU, RSU, and CS software. The users/drivers cannot have access to update the software on RSU and thus cannot stop the traffic violation detection or reporting when the violation detection and reporting are done by OBU. For the case when RSU and CS are used to detect and report speed-limit traffic violations, there is no security issue, as they will be maintained only by the traffic authority. A lot of research works deal with the issue to ensure that a vehicle is broadcasting its real location and speed information.

4. Proposed Systems for Speed-Limit Violation Detection and Reporting Using IoV

In this section, we present two smart systems that can effectively detect the speed-limit (overspeeding or underspeeding) violation and automatically report them based on IoV technology. The first one will be using the OBU of the vehicle itself. The second one is a centralized system that uses broadcast messages from vehicles and involves the use of

Table 1: Accuracy of the common location service types.

Location service type	Average accuracy	Remarks
Standard GPS	2–5 m	Not suitable for critical IoV applications, such as collision warning
Global navigation satellite system (GNSS)	1–2 m	Must receive from more than one satellite system and frequencies
Differential GPS (DGPS)	0.3–0.8 m	Correcting base station must be installed and sends real-time error information to surrounding GPS receivers. NTRIP protocol can be used with a subscription through the internet
RTK	0.01–0.05 m	Like DGPS, but using different algorithms, thus providing cm-accuracy, especially when a vehicle is close to a base station

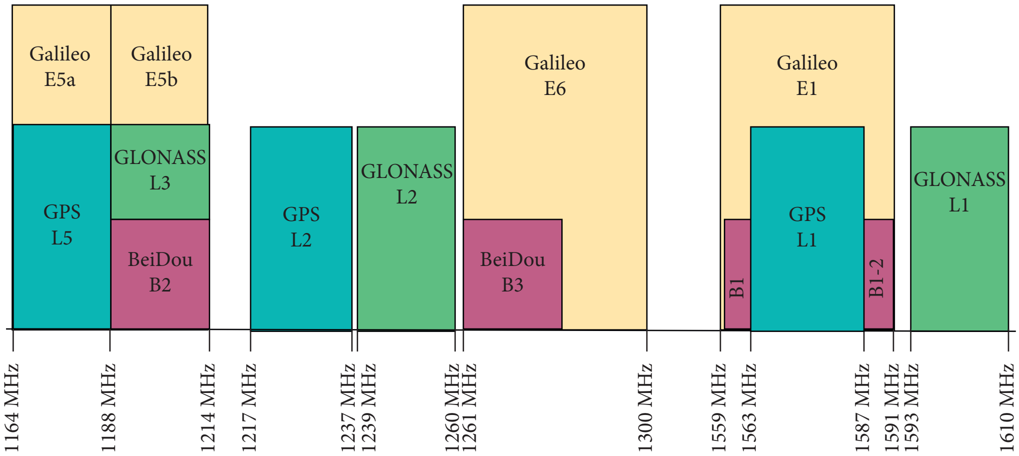

Figure 3: GNSS satellite systems and their frequencies [59].

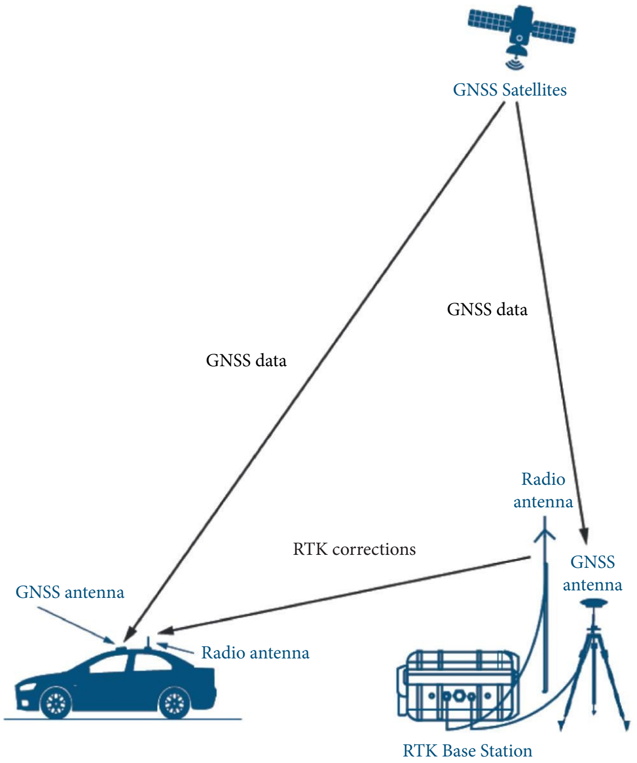

Figure 4: RTK (Real-Time Kinematic) for providing accurate positioning system and correcting the GNSS errors [63].

RSU and CSs to be able to determine the violation of any vehicle anywhere in the city. In addition, a dynamic and adaptive traffic fine calculation policy is proposed.

4.1. OBU-Only System for Violation Detection and Reporting. The vehicle is the first object that knows its speed in real-time at any time. It can know its speed from the CAN bus. In addition, the OBU of the vehicle can know the temporal change of the location of the vehicle from the GNSS or any other reliable location service. Thus, the vehicle's OBU can calculate the speed of the vehicle in real-time. In addition, as described in Section 3.4, the vehicle according to its current location, its type, and the lane on the road can know the allowed speed limits from the "Digital Map Service and the Speed Limits" component of IoV. These are the only needed information to be able to detect if the vehicle is moving within the allowed limits or violating the speed limits. Thus, why not updating the OBU software of the vehicle in order to detect any speed-limit violation anytime, anywhere without adding any extra hardware to the IoV architecture? Additionally, why not reporting these committed speed-limit violations by the vehicle's OBU to the traffic authority for collecting fines or taking legal actions according to the traffic rules and regulations. Traditionally, it is not logical that the vehicle detects and reports the violations it commits, but using IoV, this could be possible and this would provide many advantages compared to the existing techniques.

One challenge of this system is because the OBU is installed on the vehicle; thus, it could be tampered to disable the reporting feature. However, there are intensive research efforts in securing both the hardware and the software of IoV components (all the building blocks). Thus, any tampering of any components, including the OBU, can be easily detected, and the vehicle will stop and not start. For more details, please refer to Section 3.7.

In this section, we present how the OBU of the vehicle can detect and report the speed-limit violations in the context of IoV. The algorithm is presented in detail in listing Algorithm 1. A simplified flowchart for this algorithm is shown in Figure 5. In brief, the overall algorithm can be summarized as follows: the OBU obtains its current location, then it obtains or calculates its current speed, next it obtains the allowed speed limits, then it compares the current speed with the allowed one, then it records the violation if occurred, and finally, it reports the violations.

In some countries, if a vehicle is moving at a very low speed beyond the minimum allowed speed limit, it is considered as another kind of traffic violation. This is because underspeeding can also cause accidents and traffic congestions. The previous algorithm can be slightly modified to detect and report this kind of violation, as explained in Algorithm 2. A simplified flowchart for this algorithm is shown in Figure 6.

4.2. Speed-Limit Violation Detection and Reporting Using the RSU and the CSs. In this section, we present a different system that detects and reports speed-limit violations. In the previous section, we presented a system that uses only the OBU of the vehicle to autonomously detect and report the speed limit violations without support from the RSU or the CSs. In this section, another system is proposed. In this system, the detection and reporting are carried out by the OBU of the vehicle, the road-side units (RSUs), and the cloud servers (CSs). The rationales behind this approach are as follows. Each vehicle periodically broadcasts its current location to the infrastructure using Vehicle-to-Infrastructure (V2I) messages. These messages are received by nearby RSU(s). These messages contain the timestamp, the vehicle's current location, and other information that is used for other purposes. In the case when the detection and reporting are to be done on CSs, but not by the vehicle only, we have two cases.

4.2.1. When Vehicles Broadcast Their Real-Time Speed. If a vehicle is broadcasting its real-time speed, then RSUs will receive these messages. Each RSU will encapsulate the received messages and sends them to CSs. The encapsulated messages contain the RSU ID. Thus, CSs can know the rated speed limits for the area covered by that RSU. The CSs will have for each vehicle the vehicle speed and the allowed speed limits as a function of time (the timestamp of each V2I message). CSs compare the allowed speed limits with each vehicle to know if the vehicle is violating the speed limit or not. The challenge here is to obtain the duration of the over-/underspeeding and the maximum/minimum reached speeds. CSs can easily determine if a vehicle is violating or not. In the case of a violation, CSs can obtain all the details of the violation (start time, duration, peak speed, location, etc.) from the available data. This can be done by slightly modifying Algorithm 1, as given in the previous section.

4.2.2. When Vehicles Broadcast Their Temporal Locations Only. The minimum information to be sent from a vehicle to RSU is the vehicle's temporal location. If a vehicle is not broadcasting its real-time speed, then the vehicle's temporal location is enough to calculate the speed as a function of time. Similar to what is described in Section 4.2.1, an RSU receives messages broadcasted from vehicles and encapsulates the messages and resends them to CSs. CSs calculate the temporal speed for a vehicle from temporal locations of the vehicle, then continue the processing following the same way as described in Section 4.2.1.

To calculate the temporal speed from the temporal location, the following approach is used.

For a given vehicle, for two consecutive broadcast messages m_{i-1}, m_i, the vehicle at time t_{i-1} where at location R_{i-1}, then at time t_i, it moved to location $\mathscr{P}_i$, where $\mathscr{P}_i$ and R_{i-1} are represented by latitude α and the longitude β in degrees. The distance between the two locations $d\left(\mathscr{P}_i, \mathscr{P}_{i-1}\right)$ can be obtained by Haversine's formula [64]. It is used to obtain the shortest distance between two points over the Earth's surface as follows:

$$d\left(\mathrm{R}_i, \mathrm{R}_{i-1}\right) = \mathscr{R}^* c, \qquad (1)$$

where $\mathscr{R}$ is the radius of the Earth (mean radius = 6,371 km), where $c = 2^* a \tan 2\left(\sqrt{a}, \sqrt{1-a}\right)$, where $a = \sin^2 (\pi(\alpha_i - \alpha_{i-1})/360) + \cos\ (\pi\alpha_i/180)\ ^* \cos\ (\pi\alpha_{i-1}/180)\ ^* \sin^2\ (\pi (\beta_i - \beta_{i-1})/360)$.

```
(1) Obtain the current speed, Current_Speed, of the vehicle depending on the following methods.
    (a) If there is access to the internal computer of the vehicle using CAN bus protocol, then obtain the current speed of the vehicle using the CAN bus decoding hardware. This is the most accurate and preferable method as the speed is available all the time even if the GNSS signal cannot be received from any satellite constellation.
    (b) Else if GNSS signal can be received from at least one satellite constellation system, use the GNSS receiver of the OBU to calculate the current speed.
        (i) If no error-correcting service is available, then decrease the value of the current speed by a safety value to compensate for the errors in the GNSS accuracy, for example, 5 km/s.
    (c) Else If the GNSS signal is very week and the GNSS receiver cannot receive from at least one satellite system, then the current speed is invalid and the traffic violation cannot be obtained, and skip the remaining steps.
(2) Obtain the current location coordinate, Current_Location, of the vehicle using the GNSS module in the On-Board Unit (OBU). For more details, please refer to Section 3.5.
(3) Obtain the maximum allowed speed limit, Maximum_Allowed_Speed_Limit for this Current_Location on the road, the Vehicle_Type, the Current_Lane, and the Weather_Condition as follows.
    (a) If the information is cached in the internal memory of the OBU (requested previously or received from any Road Side Unit or CSs), then use the maximum allowed speed limit saved previously.
    (b) Else if there is a nearby Road Side Unit, request the maximum allowed speed limit from it and save it in the internal memory.
    (c) Otherwise, use the Internet access to reach directly the CSs to request the Maximum_Allowed_Speed_Limit and save it in the internal memory. The "Digital Map-Speed Limit" service executes the following:
        (i) If the location is stored in the System Database, respond with the maximum speed limit for this location.
        (ii) Otherwise, do a REST request to "Digital Map Service Provider" to obtain the maximum speed limit for this location, save it in the System Database, and respond back to the requesting vehicle. This is the only payable request. All the other requests are free as they are all saved inside the different modules of the entire system. For more details, please refer to Section 3.4.
(4) If the Current_Speed > Maximum_Allowed_Speed_Limit, then an overspeed limit violation occurred, do the following:
    (a) Warn (vocally and visually) the driver that he/she is committing a speed-limit violation. According to the traffic authority regulations, it could be allowed to overspeed for few seconds without recording a violation (for example, to overtake a slow vehicle). This is completely possible with our approach.
    (b) Record in the internal memory of the OBU an Over_Speed_Limit violation event. Record also the current time as the start time.
    (c) Record the Current_Location, the road information from the digital map, Maximum_Allowed_Speed_Limit (important in a case of future modification of this value by the traffic authority).
    (d) Calculate the maximum reached speed and the duration of the overspeeding as follows:
        (i) Set the Maximum_Excess_Speed = Current_Speed-Maximum_Allowed_Speed_Limit.
        (ii) While Maximum_Allowed_Speed_Limit < Current_Speed.
            (1) Wait for a specific time, for example, 20 seconds
            (2) Recalculate the Current_Speed from step 1
            (3) If (Current_Speed-Maximum_Allowed_Speed_Limit) > Maximum_Excess_Speed, then set Maximum_Excess_Speed = Current_Speed-Maximum_Allowed_Speed_Limit
        (iii) Now, the speed violation ends, thus, record the current time as the violation end time and the Maximum_Excess_Speed in that violation. This is essential as the fines depend mainly on this value.
    (e) Report the committed violation as follows:
        (i) If there is connectivity to a nearby RSU, then send the violation details to it. The RSU then sends the violation details to the CSs.
        (ii) Else if there is Internet access to the CSs, then send the violation details directly to them.
        (ii) Otherwise, wait until any available connectivity is available and sends the violation.
        (iii) An "Acknowledgment message" must be sent back from the Cloud Server to the OBU that the violation is successfully reported in order to flag the violation as reported.
(5) Wait for a predefined time (set globally in the whole system, e.g., 20 seconds) and then repeat the whole process to periodically check if the vehicle is overspeeding.
```

Algorithm 1: Overspeed limit violation detection and reporting using the On-Board Unit (OBU) of the vehicle.

We can obtain the temporal speed of the vehicle as follows:

$$v_i = \frac{d\left(\mathrm{R}_i, \mathrm{R}_{i-1}\right)}{t_i - t_{i-1}}. \tag{2}$$

The CS can determine the start, duration, maximum/minimum speed, and location of any speed-limit violation committed by any vehicle from the temporal speed information according to Algorithm 1.

5. Dynamic and Adaptive Speed-Limit Violation Fine Calculation Policy

All the existing methods of speed-limit fine calculation are based on a single value (usually the detected vehicle speed) using the camera systems or the speed radars. One very promising contribution of this work is that using our proposed systems, much more information about the violation can be obtained as our system knows the real-time

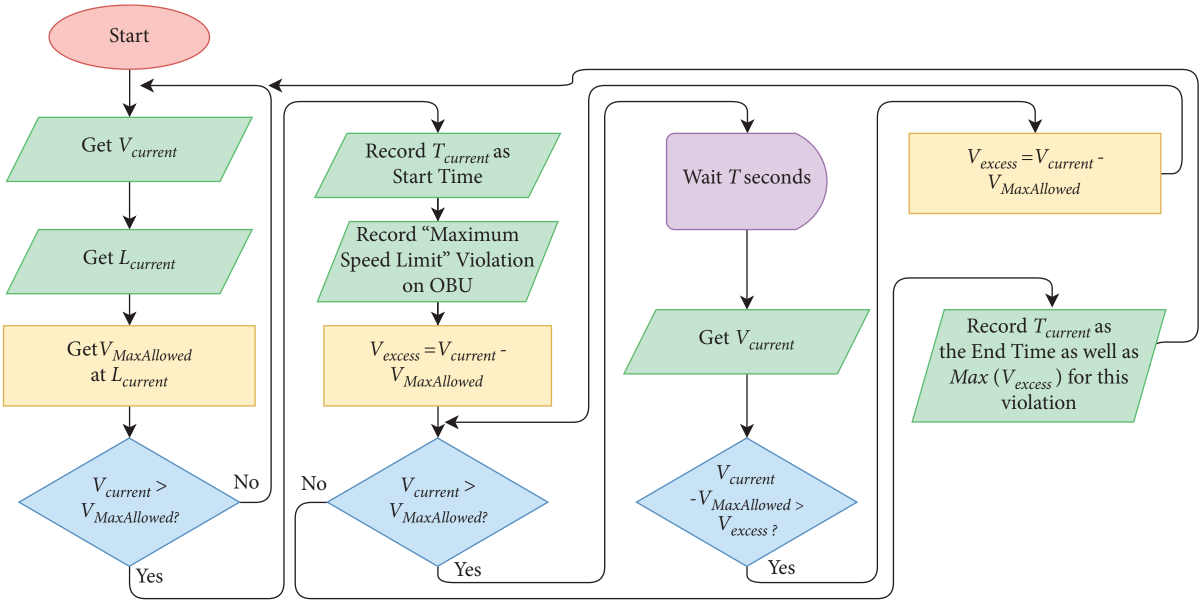
Start
Get $V_{current}$
Get $L_{current}$
Get $V_{MaxAllowed}$ at $L_{current}$
$V_{current} > V_{MaxAllowed}$?
No
Yes
Record $T_{current}$ as Start Time
Record “Maximum Speed Limit” Violation on OBU
$V_{excess} = V_{current}$ - $V_{MaxAllowed}$
No
$V_{current} > V_{MaxAllowed}$?
Yes
Wait T seconds
Get $V_{current}$
$V_{current}$ -$V_{MaxAllowed} > V_{excess}$?
Yes
$V_{excess} = V_{current}$ - $V_{MaxAllowed}$
Record $T_{current}$ as the End Time as well as $Max\ (V_{excess})$ for this violation

FIGURE 5: Flowchart of overspeeding violation detection using the OBU (simplified flowchart of Algorithm 1).

```
(1) Obtain the current speed, Current_Speed, of the vehicle depending on the following methods as in step #1 of Algorithm 1, except in step 1b).
    (i) If no error-correcting service is available, then increase the value of the current speed by a safety value to compensate for the errors in the GNSS accuracy, for example, 5 km/s.
(2) Obtain the current location coordinate, Current_Location as step #2 of Algorithm 1.
(3) Obtain the minimum allowed speed limit, Minimum_Allowed_Speed_Limit for this Current_Location on the road, the Vehicle_Type, the Current_Lane, and the Weather_Condition as given in step #3 of Algorithm 1.
(4) If the Current_Speed < Minimum_Allowed_Speed_Limit, then an underspeed limit violation occurred, do the following:
  (a) Record in the internal memory of the OBU an Under_Speed_Limit violation event. Record also the current time as the start time.
  (b) Record the Current_Location, the road information from the digital map, Minimum_Allowed_Speed_Limit (important in a case of future modification of this value by the traffic authority).
  (c) Calculate the maximum underspeeding value and the duration of the underspeeding as follows:
    (i) Set the Maximum_Under_Speed = Minimum_Allowed_Speed_Limit-Current_Speed.
    (ii) While Current_Speed < Minimum_Allowed_Speed_Limit.
      (1) Wait for a specific time, for example, 20 seconds
      (2) Recalculate the Current_Speed from step 1
      (3) If (Minimum_Allowed_Speed_Limit - Current_Speed) > Maximum_Under_Speed, then set Maximum_Under_Speed = Minimum_Allowed_Speed_Limit-Current_Speed
    (iii) Now, the speed violation ends, and thus, record the current time as the violation end time and the Maximum_Under_Speed in that violation. This is essential as the fines depend mainly on this value.
  (e) Report the committed violation as step #4d in Algorithm 1.
(5) Wait for a predefined time as in Algorithm 1.
```

ALGORITHM 2: Underspeed limit violation detection and reporting using the On-Board Unit (OBU) of the vehicle.

speed of the vehicle as well as the allowed speed limits in addition to the current weather conditions. Thus, our proposed systems can allow the collection and/or the knowledge of the following parameters:

(i) Start time of the speed-limit violation.

(ii) End time of the speed-limit violation. Thus, the duration of the violation can be calculated.

(iii) The maximum reached overspeeding or the minimum underspeeding, as well as the average violating speed.

(iv) The lane number during the violation.

(v) The vehicle types.

(vi) The location of the violation. Effects of over-/underspeeding differ from lane to lane.

(vii) History of the speed-limit violations of each vehicle. Drivers who are committing frequent speed-limit violations can be identified. The systems can know the number of violations in the same trip, day, week, or month.

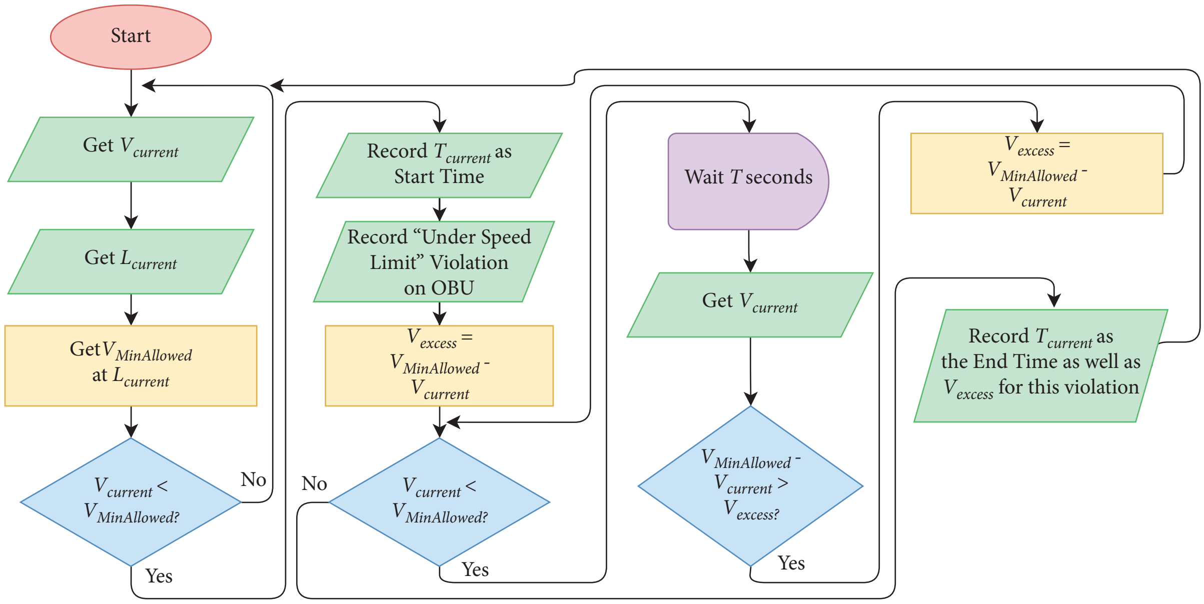
Start
Get $V_{current}$
Get $L_{current}$
Get $V_{MinAllowed}$ at $L_{current}$
$V_{current} <$ $V_{MinAllowed?}$
No
Yes
Record $T_{current}$ as Start Time
Record "Under Speed Limit" Violation on OBU
$V_{excess} =$ $V_{MinAllowed} -$ $V_{current}$
No
$V_{current} <$ $V_{MinAllowed?}$
Yes
Wait T seconds
Get $V_{current}$
$V_{MinAllowed} -$ $V_{current} >$ $V_{excess?}$
Yes
$V_{excess} =$ $V_{MinAllowed} -$ $V_{current}$
Record $T_{current}$ as the End Time as well as V_{excess} for this violation

FIGURE 6: Flowchart of underspeeding violation detection using the OBU (simplified flowchart of Algorithm 2).

(viii) The time of the day: for example, speed limits can be adjusted differently according to specific hours.

(ix) The weather condition. IoV infrastructure is connected with weather measurement sensors (that measure the current weather condition). This allows the real-time adjustment of the allowed speeds according to current weather conditions. For example, if the maximum allowed speed in normal weather conditions (as reported by the speed-limit service provider) for a sedan vehicle is 120 km/h, then the allowed speed can be 100 km/h in rainy conditions, 70 km/h in snowy condition, and 40 km/h in foggy condition. The RSU broadcasts the real-time speed limits according to the weather condition, and thus, the proposed system detects and reports the violations accordingly. Almost all the existing systems cannot detect the violations in bad weather conditions (for example, camera systems cannot detect violations in foggy conditions). Our proposed systems are immune to weather conditions and can detect any violation using dynamic real-time speed limits.

All this collected information about the violation can enable the traffic authorities to implement dynamic fine calculation policies for speed-limit violations. For example, the fine can be $10 if the duration of a violation is one minute, and it can be $300 if a violation lasts for 20 minutes. Furthermore, the fine can be $500 if the vehicle speed is 120 km/h and the weather condition is foggy. Another example, if the average overspeeding is 20 km/h, the fine can be $200, but it could be $700 if the average overspeeding during the violation is 80 km/h.

One other feature of the system is that a driver can be warned (vocally and visually) by OBU if he/she is about to violate the allowed speed. This warning can significantly reduce the number of speed-limit violations.

6. Development of Working Prototype System

To validate the proposed systems, we have implemented them on a prototype system. We have implemented a simplified IoV testbed that consists of Raspberry Pi 4, GNSS receivers, Internet Connectivity, Speakers, LCDs, and other equipment, as shown in Figure 7. We have developed the IoV essential working stack on Raspberry Pi 4, and we have set up the ad hoc network and both V2V and V2I communication. In addition, we have developed the Cloud Server essential services hosted and secured in a secure data center with 500 Mbps Internet dedicated connection and operated by VMWare vSphere. For the digital maps and the speed-limit service, we have used two subscriptions for two different service providers: MS Bing and HERE technologies. We have implemented Algorithm 1 (Section 4.1) and then tested and validated the prototype. We have conducted several tests on different road types: side roads, local roads, and highways. The prototype could effectively detect and report all the speed-limit violations committed by the vehicle to the CS. The applications of the CS were developed in Django. The reported speed-limit violation information can effectively be used by the traffic authorities to implement dynamic traffic fine calculation policies because of the different important information that is collected about the committed violations.

Several real-time validations of the system are conducted in different cities. The system is very accurate in detecting the speed-limit violation, under the condition that the speed-limit service provider (MS Bing in the prototype) is reporting correct values of the speed limits. In this case, the accuracy is 100%. In

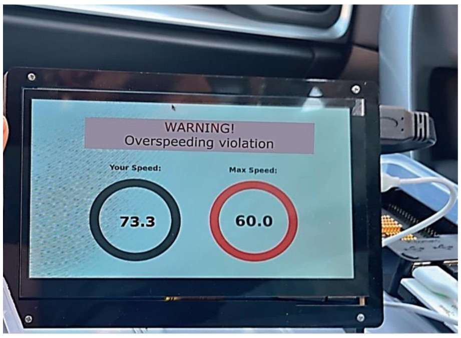

Figure 7: Developed prototype in action.

the production system to be deployed in the smart cities and the Intelligent Transportation Systems (ITSs), the authorities must be sure of the accuracy of the speed-limit service provider(s) to be used in the proposed systems.

7. Conclusions and Future Directions

In this paper, two different systems are proposed to automatically detect and report speed-limit violations using IoV technology without involving any extra hardware. The proposed systems extend the existing Internet of Vehicles (IoV) by only updating the firmware/software of the On-Board Unit (OBU) of the vehicle, the Road Side Unit (RSU), and the Cloud Servers (CSs). In the first proposed system, the OBU of the vehicle itself detects if the vehicle is violating the allowed speed limits and, in such a case, several useful information about the committed violation such as the start time, the duration of the same violation, the peak speed during the violation, the lane, and the road information. This enables modern dynamic and adaptive fine calculation policies that were not possible using the existing techniques. In addition, the violations will be detected and reported anywhere on the road anytime. This means that all the roads will be fully monitored, unlike the exiting techniques that are installed in a few fixed locations on the roads (thus monitoring only these few fixed areas). The proposed systems are very accurate and reliable. The deployment of such systems could effectively reduce/minimize road accidents and causalities. We have validated the proposed system by building a hardware prototype of IoV and developed the speed-limit violation detection and reporting system on top of that prototype. The developed prototype effectively and accurately detects any speed-limit violation on the road.

Future research work may include developing a real system in practice for the IoV protocol stack. In addition, standardizing the speed-limit violation based on IoV is an essential perspective. Furthermore, automating the detection of other traffic violations such as tailgating is another important future work. Although this work relies on the security layer of IoV, which has been studied intensively in the literature and can be considered secure enough to avoid reporting bogus (tampered) location or speed information, it is important to consider the security aspects of such systems in the future work.

Data Availability

The source code of the developed prototype used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was funded by the National Plan for Science, Technology, and Innovation (MAARIFAH), King Abdulaziz City for Science and Technology (KACST), Kingdom of Saudi Arabia. Award number: 13-INF2456-08-R.

References

[1] WHO, “Road traffic injuries,” *Fact Sheets*, WHO, 2021, https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries.

[2] S. Sharma and B. Kaushik, “A survey on internet of vehicles: applications, security issues & solutions,” *Vehicular Communications*, vol. 20, Article ID 100182, 2019.

[3] L.-M. Ang, K. P. Seng, G. K. Ijemaru, and A. M. Zungeru, “Deployment of IoV for smart cities: applications, architecture, and challenges,” *IEEE Access*, vol. 7, pp. 6473–6492, 2019.

[4] I. Santos-González, P. Caballero-Gil, A. Rivero-García, and C. Caballero-Gil, “Priority and collision avoidance system for traffic lights,” *Ad Hoc Networks*, vol. 94, Article ID 101931, 2019.

[5] L.-W. Chen and Y.-F. Ho, “Centimeter-grade metropolitan positioning for lane-level intelligent transportation systems based on the internet of vehicles,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1474–1485, 2019.

[6] M. Kerimov, S. Evtiukov, and A. Marusin, “Model of multilevel system managing automated traffic enforcement facilities recording traffic violations,” *Transportation Research Procedia*, vol. 50, pp. 242–252, 2020.

[7] M. Radivojević, M. Tanasković, and Z. Stević, “The adaptive algorithm of a four way intersection regulated by traffic lights with four phases within a cycle,” *Expert Systems with Applications*, vol. 166, Article ID 114073, 2021.

[8] S. A. Elsagheer Mohamed and K. A. AlShalfan, “Intelligent traffic management system based on the internet of vehicles (IoV),” *Journal of Advanced Transportation*, vol. 2021, Article ID 4037533, 23 pages, 2021.

[9] S. A. E. Mohamed, “Smart street lighting control and monitoring system for electrical power saving by using VANET,” *International Journal of Communications, Network and System Sciences*, vol. 6, no. 8, pp. 351–360, 2013.

[10] Y. Ni, L. Cai, J. He et al., “Toward reliable and scalable internet of vehicles: performance analysis and resource management,” *Proceedings of the IEEE*, vol. 108, no. 2, pp. 324–340, 2020.

[11] N. Gupta, A. Prakash, and R. Tripathi, *Internet of Vehicles and its Applications in Autonomous Driving*, Springer, Berlin, Germany, 2021.

[12] M. Famouri, Z. Azimifar, and A. Wong, “A novel motion plane-based approach to vehicle speed estimation,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 4, pp. 1237–1246, 2019.

[13] B. J. Damascene and R. Okuda, “Low-cost speed limit monitoring system for developing countries using a series of

active infrared sensors," in *Proceedings of the 2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, pp. 740–744, Kanazawa, Japan, September 2017.

[14] P. R. Kambadkone, G. P. Hancke, and T. D. Ramotsoela, "Real time speed detection and ticketing system," in *Proceedings of the 2017 IEEE AFRICON*, pp. 1593–1598, Cape Town, South Africa, September 2017.

[15] J. Goswami, S. Ghosh, S. Katiyar, and A. Majumder, "Development of a prototype to detect speed limit violation for better traffic management," in *Proceedings of the 2015 Eighth International Conference On Contemporary Computing (IC3)*, pp. 449–454, Noida, India, August 2015.

[16] R. P. Nayak, D. S. Sethi, and D. S. K. Bhoi, "PHVA: a position based high speed vehicle detection algorithm for detecting high speed vehicles using vehicular cloud," in *Proceedings of the 2018 International Conference on Information Technology (ICIT)*, pp. 227–232, Bhubaneswar, India, Decemer 2018.

[17] S. A. Elsagheer Mohamed, "Automatic traffic violation recording and reporting system to limit traffic accidents: based on vehicular ad-hoc networks (VANET)," in *Proceedings of the 2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*, Aswan, Egypt, February 2019.

[18] G. Desai, V. Ambre, S. Jakharia, and S. Sherkhane, "Smart road surveillance using image processing," in *Proceedings of the 2018 International Conference on Smart City and Emerging Technology (ICSCET)*, pp. 1–5, Mumbai, India, January 2018.

[19] Y. Denis, Z. Ruslan, R. Andrey, K. Volodymyr, and M. Oleksandr, "Intelligent system for reliable monitoring and controlling of automobile traffic," in *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pp. 637–640, Kyiv, Ukraine, May 2018.

[20] A. Sentas, S. Kul, and A. Sayar, "Real-time traffic rules infringing determination over the video stream: wrong way and clearway violation detection," in *Proceedings of the 2019 International Artificial Intelligence and Data Processing Symposium (IDAP)*, pp. 1–4, Malatya, Turkey, September 2019.

[21] F. Outay, H. A. Mengash, and M. Adnan, "Applications of unmanned aerial vehicle (UAV) in road safety, traffic and highway infrastructure management: recent advances and challenges," *Transportation Research Part A: Policy and Practice*, vol. 141, no. September, pp. 116–129, 2020.

[22] A. D. Boursianis, M. S. Papadopoulou, P. Diamantoulakis et al., "Internet of things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: a comprehensive review," *Internet of Things*, Article ID 100187, 2020.

[23] A. Reddy, S. Patel, K. P. Bharath, and R. Kumar, "Embedded vehicle speed control and over-speed violation alert using IoT," in *Proceedings of the 2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*, vol. 1, pp. 1–5, Vellore, India, March 2019.

[24] B. Ji, X. Zhang, S. Mumtaz et al., "Survey on the internet of vehicles: network architectures and applications," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 34–41, 2020.

[25] P. K. Singh, S. K. Nandi, and S. Nandi, "A tutorial survey on vehicular communication state of the art, and future research directions," *Vehicular Communications*, vol. 18, Article ID 100164, 2019.

[26] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: machine-learning approaches," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 292–307, 2020.

[27] S. A. Elsagheer Mohamed, "Why the accuracy of the received signal strengths as A positioning technique was not accurate?" *International Journal of Wireless & Mobile Networks*, vol. 3, no. 3, pp. 69–82, 2011.

[28] K. Suresh Kumar Reddy, D. Rajaveerappa, and S. Khadeeja Banu, "Two base station method for finding location of mobile vehicles based on Doppler shifted signals," in *Proceedings of the 2013 International Conference on Emerging Trends in Communication, Control, Signal Processing and Computing Applications (C2SPCA)*, Bangalore, India, October 2013.

[29] S. Tomic, M. Beko, L. M. Camarinha-Matos, and L. B. Oliveira, "Distributed localization with complemented RSS and AOA measurements: theory and methods," *Applied Sciences*, vol. 10, no. 1, p. 272, 2020.

[30] C. L. Nguyen and A. Khan, "WiLAD: wireless localisation through anomaly detection," in *Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference*, Singapore, December 2017.

[31] S. A. E. Mohamed, "Secure position verification approach for wireless ad-hoc networks," *International Journal on Network Security*, vol. 15, no. 4, pp. 248–255, 2013.

[32] Y. Li, Y. Hu, R. Zhang, Y. Zhang, and T. Hedgpeth, "Secure indoor positioning against signal strength attacks via optimized multi-voting," in *Proceedings of the International Symposium on Quality of Service*, Phoenix, AZ, USA, June 2019.

[33] B. Zhou, A. Liu, V. Lau et al., "Performance limits of visible light-based positioning for internet-of-vehicles: time-domain localization cooperation gain," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5374–5388, 2021.

[34] A. Nasr and S. A. E. Mohamed, "Accurate distance estimation for VANET using nanointegrated devices," *Optics and Photonics Journal*, vol. 2, pp. 113–118, 2012.

[35] K.-W. Chen, C.-H. Wang, X. Wei et al., "Vision-based positioning for internet-of-vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 2, pp. 364–376, 2017.

[36] M.-S. Gu, F. Miao, C.-B. Gao, Z.-S. He, W.-J. Fan, and L. Li, "Research of localization algorithm of internet of vehicles based on intelligent transportation," in *Proceedings of the 2018 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR)*, Chengdu, China, July 2018.

[37] K. Lin, Y. Li, J. Deng, P. Pace, and G. Fortino, "Clustering-learning-based long-term predictive localization in 5G-envisioned internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5232–5246, 2021.

[38] J. Eom, H. Kim, S. H. Lee, and S. Kim, "DNN-assisted cooperative localization in vehicular networks," *Energies*, vol. 12, no. 14, pp. 2758–14, 2019.

[39] Y. Liu and Y. Shen, "UAV-Aided high-accuracy relative localization of ground vehicles," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, May 2018.

[40] S. Demetriou, P. Jain, and K.-H. Kim, "CoDrive: improving automobile positioning via collaborative driving," in *Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pp. 72–80, Honolulu, HI, USA, April 2018.

[41] H. Wang, L. Wan, M. Dong, K. Ota, and X. Wang, "Assistant vehicle localization based on three collaborative base stations via SBL-based robust DOA estimation," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5766–5777, 2019.

[42] P. Richter, H. Leppakoski, E. S. Lohan et al., "Received signal strength quantization for secure indoor positioning via fingerprinting," in *Proceedings of the 2018 8th International Conference on Localization and GNSS (ICL-GNSS)*, p. 26, Guimaraes, Portugal, June 2018.

[43] S. Kuutti, S. Fallah, K. Katsaros, M. Dianati, F. Mccullough, and A. Mouzakitis, "A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 829–846, 2018.

[44] F. B. Günay, E. Öztürk, T. Çavdar, Y. S. Hanay, and A. u. R. Khan, "Vehicular ad hoc network (VANET) localization techniques: a survey," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3001–3033, 2020.

[45] F. Ahmad, C. A. Kerrache, F. Kurugollu, and R. Hussain, "Realization of blockchain in named data networking-based internet-of-vehicles," *IT Professional*, vol. 21, no. 4, pp. 41–47, 2019.

[46] M. A. Habib, M. Ahmad, S. Jabbar et al., "Security and privacy based access control model for internet of connected vehicles," *Future Generation Computer Systems*, vol. 97, pp. 687–696, 2019.

[47] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, "A survey on security and privacy issues in IoV," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, p. 5409, 2020.

[48] A. Castiglione, F. Palmieri, F. Colace, M. Lombardi, D. Santaniello, and G. D'Aniello, "Securing the internet of vehicles through lightweight block ciphers," *Pattern Recognition Letters*, vol. 135, pp. 264–270, 2020.

[49] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of vehicles: architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2018.

[50] A. Elkhalil, J. zhang, R. Elhabob, and N. Eltayieb, "An efficient signcryption of heterogeneous systems for Internet of Vehicles," *Journal of Systems Architecture*, vol. 113, Article ID 101885, 2020.

[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 Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2391–2406, 2018.

[52] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, Article ID 100214, 2020.

[53] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: communication, applications and challenges," *Vehicular Communications*, vol. 19, Article ID 100179, 2019.

[54] GNSS-Global Navigation Satellite Systems, 2008.

[55] J. L. Awange, "The global positioning system," in *Environmental Science And Engineering*Springer, Berlin, Germany, 2012.

[56] Q. Zhao, C. Wang, J. Guo, B. Wang, and J. Liu, "Precise orbit and clock determination for BeiDou-3 experimental satellites with yaw attitude analysis," *GPS Solutions*, vol. 22, no. 1, 2018.

[57] M. Falcone, J. Hahn, and T. Burger, *Galileo*Springer, Berlin, Germany, 2017.

[58] S. Revnivykh, *GLONASS Status and Modernization*, International GNSS Committee, Beijing, China, 2012.

[59] Novatel.com, "Automotive: high precision GNSS," 2020, https://novatel.com/industries/autonomous-vehicles#overview.

[60] H. C. Chen, Y. S. Huang, K. W. Chiang, M. Yang, and R. J. Rau, "The performance comparison between GPs and BeiDou-2/compass: a perspective from Asia," *Journal of the Chinese Institute of Engineers*, vol. 32, no. 5, pp. 679–689, 2009.

[61] I. Khomsin, I. Mutiara Anjasmara, D. Guruh Pratomo, and W. Ristanto, "Accuracy analysis of GNSS (GPS, GLONASS and BEIDOU) obsevation for positioning," *E3S Web of Conferences*, vol. 94, 2019.

[62] X. Li, M. Ge, X. Dai et al., "Accuracy and reliability of multi-GNSS real-time precise positioning: GPS, GLONASS, BeiDou, and Galileo," *Journal of Geodesy*, vol. 89, no. 6, pp. 607–635, 2015.

[63] "VBOX automotive-how does it work?-RTK," 2021, https://www.vboxautomotive.co.uk/index.php/en/how-does-it-work-rtk.

[64] "Calculate distance and bearing between two latitude/longitude points," 2021, https://www.movable-type.co.uk/scripts/latlong.html.