Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 1353290, 12 pages
http://dx.doi.org/10.1155/2016/1353290

Research Article

SmartCop: Enabling Smart Traffic Violations Ticketing in Vehicular Named Data Networks

Syed Hassan Ahmed, Muhammad Azfar Yaqub, Safdar Hussain Bouk, and Dongkyun Kim

School of Computer Science & Engineering, Kyungpook National University, Daegu 702-701, Republic of Korea

Correspondence should be addressed to Dongkyun Kim; dongkyun@knu.ac.kr

Received 30 March 2016; Accepted 29 May 2016

Academic Editor: Yeong M. Jang

Recently, various applications for Vehicular Ad hoc Networks (VANETs) have been proposed and smart traffic violation ticketing is one of them. On the other hand, the new Information-Centric Networking (ICN) architectures have emerged and been investigated into VANETs, such as Vehicular Named Data Networking (VNDN). However, the existing applications in VANETs are not suitable for VNDN paradigm due to the dependency on a *"named content"* instead of a current *"host-centric"* approach. Thus, we need to design the emerging and new architectures for VNDN applications. In this paper, we propose a smart traffic violation ticketing (TVT) system for VNDN, named as *SmartCop*, that enables a cop vehicle (CV) to issue tickets for traffic violation(s) to the offender(s) autonomously, once they are in the transmission range of that CV. The ticket issuing delay, messaging cost, and percentage of violations detected for varying number of vehicles, violators, CVs, and vehicles speeds are estimated through simulations. In addition, we provide a road map of future research directions for enabling safe driving experience in future cars aided with VNDN technology.

1. Introduction

For the past decades, VANETs have been extensively investigated by the researchers, academia, and industries. Although initially designed to improve the road safety, VANETs can additionally offer commercial, informational, and entertainment services to the drivers and passengers, thus also increasing the revenues to the car manufacturers and various service providers. To be precise, the safety applications are mostly supported by the on-board units (OBUs) that depend on a Dedicated Short Range Communication (DSRC) protocol between vehicles (V2V) and in some cases infrastructures (V2I) as well. On the other hand, the nonsafety applications depend on the various TCP/IP protocols that have been proposed to operate on top of the amended 802.11p/Wireless Access in Vehicular Environments (WAVE) in the VANETs [1]. Furthermore, the IEEE 1609.4 multichannel architecture has also been introduced to WAVE standard that allowed efficient use of available spectrum for vehicular communications both in Europe and in USA. According to the standard, there is a 10 MHz Control Channel (CCH) and six 10 MHz Service Channels (SCHs) for exchanging safety/control messages (i.e., Beacons) and nonsafety applications' data, respectively.

In short, such advancements in vehicular communications system pursue as a potential tool to tackle the increasing number of road accidents caused by various violations been made on the roads. In this era of automation, we expect that new cars will be smart enough to proactively detect emergency situations and avoid road accidents [2]. For instance, we have seen Google, Tesla, Hyundai, BMW, and so many manufactures moving towards the autonomous cars. Figure 1 reflects the future smart vehicle. In the context of this paper, our focus will be on automating the traffic police vehicles and law enforcement departments in order to assist cops on the roads.

Conventionally, a traffic cop needs to identify a vehicle violating any traffic rule either manually or by use of electronic devices such as speed sensors and cameras. Then a cop follows the said vehicle and instructs the driver to pull over. The same cop then has to alight from his/her patrol car to

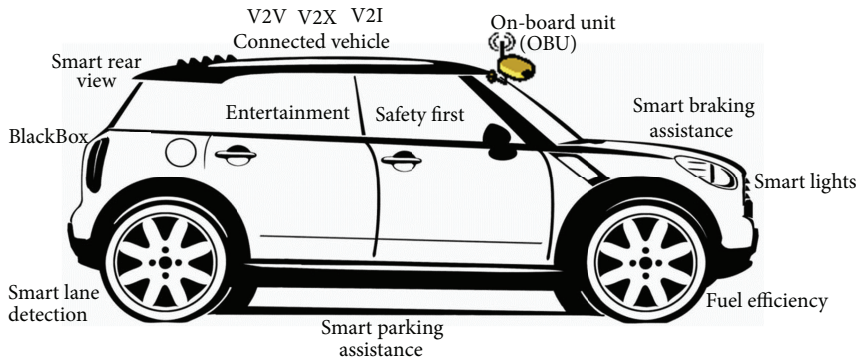


Figure 1: Components of a future smart vehicle.

manually inspect the vehicle to determine its identity and to manually inspect the offending driver's license to determine his/her identity. He/she then issues a violation ticket bearing the identity of the vehicle, the identity of the driver, nature of traffic violation, and the associated fine. The present system of issuing tickets for traffic violations has many shortcomings; for example,

(1) it is a time consuming and labor intensive process;

(2) sometimes the offending driver engages in a violent encounter with the traffic cop;

(3) in case of multiple violators, it is hard to follow up all at once;

(4) it is nearly impossible to cover all the road segments for sensing the traffic rules violations (by the means of camera, speed sensors, etc.).

The alternative way is to install speed cameras everywhere and monitor them all at once or partially while sitting back in the office. Once the installed camera detects any violator, it captures the video and image of the vehicle and later on the ticket is sent to the relevant owner by pulling out the relevant information against the number plate. However, it is impractical assumption to get all the streets and stop signs covered by the cameras. Moreover, on the long distance highways, also it would be an immature argument to install the speed cameras leaving no uncovered area behind. In addition, the maintenance cost of those cameras and sensors will compromise the cost effectiveness of the transportation departments and also the privacy concerns of the civilians will be disturbed.

Therefore, the researchers came up with an idea of equipping the vehicles with automatic traffic ticketing devices. Again, the main objective is to minimize the human errors and danger to the life of both the cop and the offender at the same time. For example, authors in [3] proposed to install a Radio Frequency Identification Device (RFID) that collects the data from in-vehicle sensors and delivers that data once the vehicle is crossing any tollbooth or cop vehicle (CV). This system aims to issue tickets autonomously in case of any violation within safe distance between cop and offender. However, the RFID systems lack meeting the current VANETs requirements, especially in terms of transmission ranges, speed variations, and authentication. Also, some additional hardware needs to be installed in vehicles other than OBUs, which are mostly used for V2V and V2I communications. One solution is to use the existing OBUs to enable the smarter ticket issuing mechanism for traffic violations given that the OBUs are equipped with the wireless communication technologies, for example, IEEE 802.11p/DSRC technologies. Although, we have a variety of solutions available for WAVE enabled OBUs in VANETs empowering the communication capabilities, all share the following common features:

(i) Each vehicle is assigned an IP address.

(ii) Specific destination addresses are used for applications to communicate.

(iii) Mostly, the candidate solutions aim to select one best path to reach the destination IP address.

However, assigning IP addresses to the mobile objects such as vehicles is not straight forward. The reason is simple; that is, IP address management requires infrastructure support, such as a central server (e.g., DHCP). Here it is worth mentioning that IP address concepts were originally introduced for wired technologies while mobility is an intrinsic feature of the VANETs, resulting in a highly dynamic network topology. Similarly, the best way to assign IPs to the mobile objects has been recognized as an open research issue [4].

Meanwhile, Named Data Network (NDN) [5] as an extension of Content-Centric Network (CCN) [6] has been applied in VANETs by several researchers, which is an emerging architecture of the future Internet projects [7]. NDN mainly shifts the communication concept from IP/host-based to the data centric in VANETs and can be referred to as Vehicular NDN (VNDN). In contrast to the IP based communications, in VNDN, a unique ID (called name) is assigned to the content instead of a host (i.e., end device), which attempts to relinquish the information from host's physical location and supports node mobility (i.e., vehicles in our case). NDN treats data or content as a first-class citizen of the network. In addition, VNDN uses simple request-reply based communication model, where a requesting node sends an "Interest" message and the provider sends back a response message with a requested data. Moreover, the recent literature

Table 1: Traffic violations in USA per year†.

Description	Value
Average number of people per day that receive a speeding ticket	112,000
Total annual number of people who receive speeding tickets	41,000,000
Total percentage of drivers that will get a speeding ticket this year	20.6%
Average cost of a speeding ticket (including fees)	$152
Total paid in speeding tickets per year	$6,232,000,000
Average annual speeding ticket revenue per US police officer	$300,000
Percent of speeding tickets that get contested in traffic court	5%
Total number of licensed drivers in America today	196,000,000

†Statistics source: http://www.statisticbrain.com/driving-citation-statistics.

shows that data in NDN is more secure than the IP based communications due to intrinsic security within the data rather than the secured communication session [8]. The fact of the matter is that including the future Internet technologies into the existing ad hoc infrastructures is a potential solution. It is obvious that VNDN tends to support various nonsafety applications such as video streaming. To the best of our knowledge, apart from the nonsafety applications, we proposed smart *traffic violation ticketing* (TVT) architecture as a first step towards the applied Vehicular CCN [9].

In this paper, we extend our work to apply the latest NDN architecture in VANETs and propose a complete system that tends to aid law enforcement agencies with safer and smarter TVT system. We name our proposed scheme as "*SmartCop.*" In SmartCop, we define several packet types and their roles to support traffic violation ticketing system. Moreover, it is able to detect the offenders and issue them tickets without human interference. Unlike the existing solutions, we only rely on OBU(s). Our main objective is to enable a CV to autonomously receive all violations' information from the neighboring OV(s). The major contributions of our SmartCop are (1) to detect the violator(s) from safe distance using future Internet, (2) to issue the tickets using wireless medium regardless of vehicles' speed and moving directions, (3) to collect ticket dues automatically, thus saving the time and efforts of both the offender and the cop at the same time, and (4) to tend to leave no unmonitored areas on the roads.

The rest of the paper is organized as follows. Section 2 summarizes the recent efforts being driven to automate the traffic violation ticketing system. Section 3 describes our proposed SmartCop system, while Section 4 provides simulation results and analysis. In Section 5, we briefly discuss the current issues and challenges in VNDN. Finally, Section 6 concludes the paper.

2. Related Work

The law enforcement agencies make a good amount of revenue each year by issuing road violation tickets. Table 1 shows that 20% of the total drivers in the United States receive tickets for overspeeding each year. More or less, the same statistics will be for other road violations globally. In this section, we overview the recent advancements being made to CVs and OVs to assist government officials (i.e., cops) on the roads and reduce the traffic violations, respectively.

In [10], the authors utilize GPS to get information about the vehicle state, that is, location and speed. The vehicle is equipped with a traffic violation warning and traffic violation storage device, which is used to store the map data, traffic regulations of the current road segment, and the traffic violations made by the driver. A controller is used to control and manage the different units of the device. The GPS data is matched with the map data and traffic regulations, stored previously in the device, to determine if a violation has been made. Based on the result, either the driver is issued a warning if a possible violation is calculated or a ticket is stored in the violation memory of the device if a violation has been committed. Furthermore, an encryption mechanism is also presented to store encrypted tickets in the memory. The issued tickets along with the violations details and personal information can be viewed later on the management display.

In [11], the authors utilize a radio frequency (RF) reader to determine the identity of a vehicle and conversely the identity of the driver and then issue traffic tickets according to the applicable traffic laws. The smart ticket device is controlled by a central processing unit and the device contains radio frequency reader, wireless transceiver, memory, and communication ports. RF tags are mounted on the number plate of the vehicles and in the driving license of the driver, which contain the vehicle and driver's identification information, respectively. The RF reader of the smart ticketing device is able to read the information from these RF tags from static and mobile vehicles. The information obtained is used to issue a traffic violation ticket, containing the vehicle and driver's information, time and nature of the violation, and the respective fine. Furthermore, an extension to this idea is to install speed sensors in the smart ticketing device with which overspeeding vehicles can also be caught easily.

In [12], the authors use a series of digital cameras, still and video, to monitor a traffic location. This system is coupled to a processing system, where image processors are used to compile vehicle and scene images produced by the digital camera system; furthermore, a verification system verifies the vehicle and driver's identity from the vehicle images. A notification system then notifies the potential violation information to the law enforcement agencies. The video camera records the footage both before and after the

Table 2: Former research efforts to reduce traffic violations.

Type	Year	Objectives	Technologies
US patent [10]	2004	Traffic violation warning & storage	GPS
US patent [11]	2006	Traffic violation identification & ticketing	Radio frequency reader
US patent [12]	2011	Traffic violation identification & ticketing	Digital still & video cameras
Research article [13]	2013	Traffic violation identification, ticketing & tracking	GPRS/GSM, Google Maps
US patent [14]	2014	Traffic violation detection device	Radio frequency reader
Research article [9]	2015	Traffic violation identification & ticketing	VCCN, DSRC, V2V, V2I

detection of the violation. A buffer is used to capture the footage before the violation is detected; it stores a nonstop video footage of the preceding few seconds. In case a violation is detected, the timer is started and when the timer expires the contents of the buffer are recorded and the resulting video clip is incorporated with the evidence from the digital still images of the violation of the identified violating car and the driver.

The authors propose a ticketing and tracking system in [13], by implementing a smart on-board GPS/GPRS system attached to the vehicle. Along with that, speed of the vehicle is monitored by the on-board system and in case of any speed violations, information about the vehicle, that is, location and maximum speed, is sent to the authorized office using a GPRS message which issues a violation ticket to the driver. The speed is monitored by GPS signal and accelerometer of the car. Moreover, the authors also propose a geocasting feature, that is, using Google Map to track the vehicles current location. The shock/vibrator sensors installed in the air bags are used to identify an accident, which leads to GSM/GPRS messages being sent to nearby vehicles, hospital, and other authorities.

An automated system is proposed in [14], where the police officers are given a handheld device which automatically detects traffic violations. The device is equipped with the traffic regulations and in case the vehicle driver is violating these regulations, an audio and visual system is installed to inform the driver and the authorities. The device is used to read the RF tags installed in the vehicles' number plates. The RF tag contains the vehicle ownership data which is used to issue ticket to the concerned driver. Furthermore, the device can also be connected to an on-site printer which prints the traffic violation ticket.

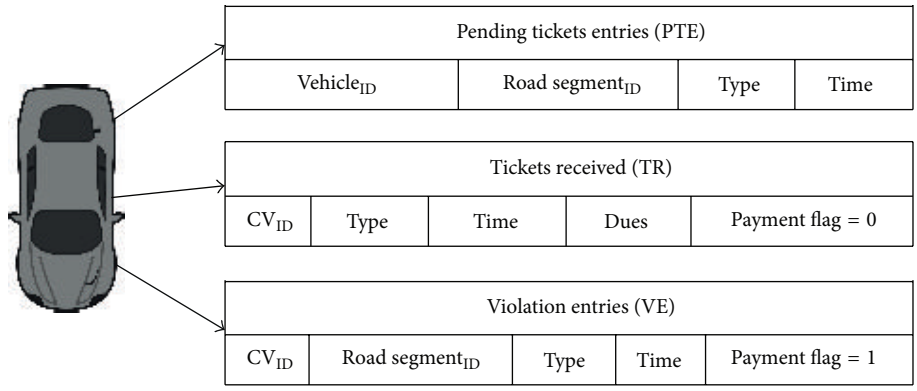
Furthermore, we proposed a unique traffic violation ticketing (TVT) system architecture in [9], where we considered the emergence of the content-centric and vehicular networking (VCCN). The main idea of the proposed architecture was to detect the offenders and issue them tickets without any human interference. However, we were precise and did not perform any experimentation. In this paper, we further extend our work and name it as a SmartCop, where extensive simulations have been performed and the architecture has been implemented over the IEEE 802.11p. Unlike the existing solutions, SmartCop only relies on on-board units (OBUs) with multiple interfaces. The proposed method contains different data structures; the ordinary vehicles (OV) contain three data structures, that is, Pending Tickets Entry (PTE), Tickets Received (TR), and Violation Entries (VE), whereas the cop vehicle (CV) contains two data structures, that is, Pending Tickets (PT) and Traffic Rules and Tickets (TRT). Also, it is able to cover the patrolled areas and more importantly the unpatrolled areas on the road where the violations by the ordinary vehicles (OV) go unnoticed. The violations by an OV in these areas are stored in the PTE. Since VNDN is a pull based communication paradigm, therefore in our architecture a CV periodically broadcasts an Interest message to have PTE(s) from its immediate neighbors. This allows the CV to issue ticket(s) in run time and avoid any manual contact with the driver. The tickets received by an OV are stored in the TR structure and upon contact with the RSU or tollbooth, the ticket's amount is deducted from the driver's bank account. For ticket payment the banking information of the drivers is accessible to the tollbooth and RSUs. Thus, the offenders are fined and charged autonomously. The record of payed tickets is stored in the VE structure of the OV.

Unfortunately, the automation of ticketing has not been investigated much as it argues to be and it can be seen from the summary depicted in Table 2.

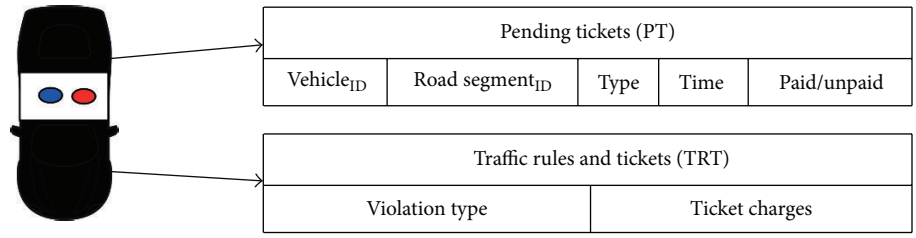
3. SmartCop: Smart Traffic Ticketing in Vehicular NDN

3.1. VNDN: Communication Background. In VNDN, communication is a receiver-driven process based on two types of packets: the Interest, which carries the request for a content unit identified by its name. Each vehicle propagating an Interest is named a *consumer* and similarly a vehicle providing that content is called a *provider*. Conventionally, each vehicle in VNDN maintains three data structures: (i) a Content Store (CS) storing the produced and incoming contents; (ii) a routing table named Forwarding Information Base (FIB), which stores the outgoing interface(s) (in VNDN, each vehicle is expected to be equipped with multiple interfaces for communication such as 802.11, LTE, and WiMax) to forward the Interests; (iii) a Pending Interest Table (PIT), which keeps track of forwarded Interests so that received content can be stored in the CS or sent back to the consumer(s) accordingly.

3.2. Proposed SmartCop System Architecture. Along with an assumption of dividing roads into segments, we bring homogeneity in all public and private vehicles and named them as ordinary vehicles (OVs). Moreover, we named the traffic monitoring vehicles as cop vehicles (CVs). As we mentioned before, there are unmonitored areas on highway



(a) Ordinary vehicle (OV): data structures



(b) Cop vehicle (CV): data structures

Figure 2: New data structures for SmartCop.

and also in an urban environment, which are collectively referred to here as an *"unpatrolled area."* It is expected that if any rule gets violated in an unpatrolled area it never gets noticed. Those violations can be of various types such as overspeeding, avoiding STOP signs, wrong lane, and parking in a no-parking zone. To cope with this, our proposed architecture enables OVs and CVs to maintain additional data structures as shown in Figures 2(a) and 2(b). Here it is worth mentioning that currently the OBUs and sensors installed in vehicles are capable of sensing violation(s) depleted by the driver. However, there might be a case where an OV violates a traffic rule and there is no nearby camera or CV to pursuit accordingly (refer to Figure 6). Therefore, we intend to manage those recorded violations in Pending Tickets Entry (PTE) table at each OV. Since, VNDN is a pull based communication paradigm, therefore in our architecture a CV periodically broadcasts an Interest message to have PTE(s) from its immediate neighbors (i.e., one-hop neighbors). This exchange of PTE enables each CV to issue ticket(s) at run time while avoiding the existing manual operations. More specifically, PTEs are shared using the same interfaces, from where the Interest was received, and upon receiving PTEs from neighboring OVs, a CV checks its Traffic Rules and Tickets (TRT) database (each CV is equipped with updated traffic rules and ticket prices table similar to Content Store in conventional CCN). Once the type of violation is matched, a corresponding CV sends back a ticket and dues to the relevant OV. Afterward, an OV stores this ticket information in its Tickets Received (TR) table. Here we assume that each driver has one central bank account or payment card registered with the department of transportation used for the payment of toll and other charges. While crossing any upcoming tollbooth, the automatic payment of the issued tickets is completed and the entry from TR moves to Violation Entries (VE) for the purpose of keeping records. Basic operations of the proposed SmartCop system and its behavior in the urban and highway environments are discussed in the following text.

3.3. Violator Detection and Ticket Issuing Process. In a SmartCop system, all OVs maintain PTE structure in its untampered blackbox. An OV becomes a violator when it has committed violations and has entry(ies) in its PTE. Cop vehicles periodically send the Interest messages to detect the violators and this Interest message is similar to the default NDN Interest message with additional PTE option (I_{PTE}). The CV stores I_{PTE} information in its PIT, which also includes the NONCE value. The NONCE value is a 32-bit long integer that is randomly generated by the originator of the Interest message. Along with that the same NONCE value is present in the Data message that is received in response, to recognize that the Data message is a response of the particular Interest.

When an OV receives I_{PTE}, it first searches its PTE. In case of no entry in PTE, it discards the Interest message. On the other hand, if the PTE is not empty, then OV sends all the PTE information in the Data message (D_{PTE}). D_{PTE} contains all the PTE information, the vehicle's ID, and the same NONCE from the Interest message. When the CV receives the D_{PTE}, it searches its PIT and if the entry is found, then it stores the PTE data in the PT. The overall flow of this process is shown in Figure 3.

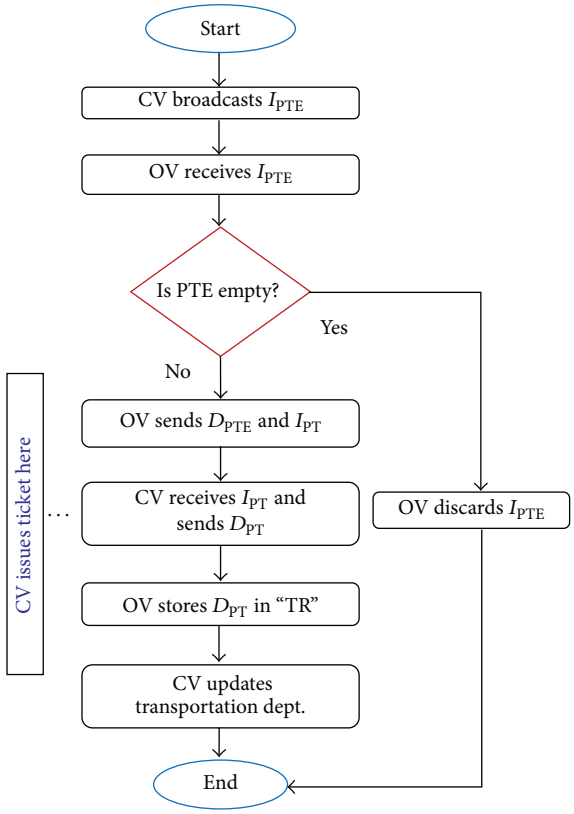


Figure 3: Violator detection and ticket issuing process.

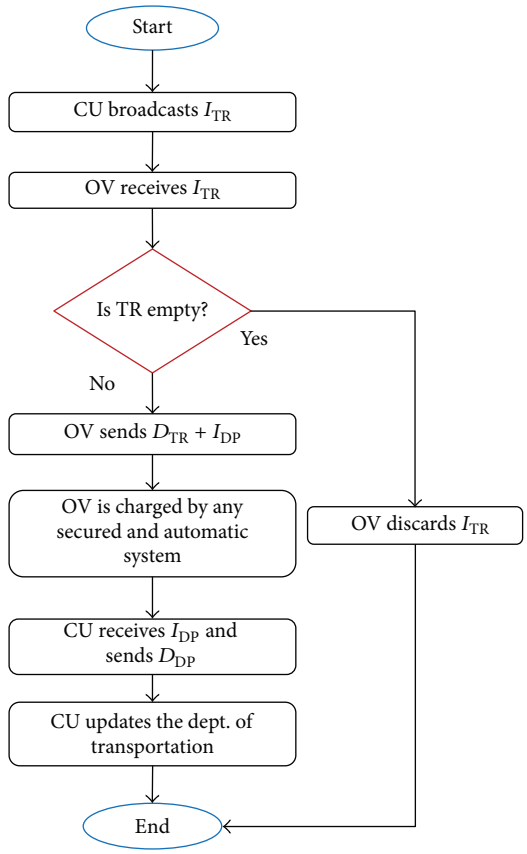


Figure 4: Violation of fine collection process.

Immediately after sending D_{PTE}, the OV also generates the Interest message (I_{PT}) including its own ID, NONCE, and the "PT" header to request the ticket from the cop vehicle and the OV creates an entry within its PIT. On reception of I_{PT}, the CV matches the OV's ID in its PT and if CV finds entries, it sends D_{PT} containing all entries along with the violation charges that are fixed for each violation. These violation charges are referenced by the CV from the standard TRT, which is available to all the CVs in the region, and the amount is fixed by the department of transportation or law enforcement agency, which is out of the scope of our paper. When D_{PT} is received at the OV, it finds the PIT and then creates the record in its TR with *payment* flag 0. In addition to that, the same entries are discarded from the PTE. Here it is worth mentioning that the CV also sets the *paid/unpaid* flag to 0 to highlight that the fines are still pending. We name this whole message exchange between the CV and OV as a *session*. In a single session there may be possible that an OV receives multiple tickets. The rationale behind this is that the OV made multiple violations and did not come in close proximity of the CV. Therefore, the *session* is one of the SmartCop evaluation parameters in simulations that is discussed in the next section.

3.4. Fine Collection Process. The fine collection process is almost similar to the ticket issuing process; however, it involves the collection unit (CU) instead of the CV to collect fines from the OVs. The CU can be the equipment installed at the tollgate on a highway or highway exit, or it may be installed at RSU installed at any dedicated location, for example, highway and bank. Figure 4 shows the flow diagram of this step.

The CU periodically sends the Interest with TR header/option (I_{TR}). Upon reception of I_{TR}, the OV finds the entries in its TR. In case of no entries, I_{TR} is discarded. On the other hand, if there is/are entry(ies) in the TR, the OV sends D_{TR} along with its ID. When the CU receives D_{TR}, then it deducts the charges from the account or any payment card type associated with that OV ID. After successful payment of the fines, this information is sent to the CVs in the region to mark their respective entries in their PT as 1/paid (the dues payment method as well as the information dissemination to all CVs in the region is out of the scope of this work). Immediately after sending D_{TR}, the OV sends I_{DP} to receive the confirmation that whether the fine is paid or not. In case of successful payment, the CU sends D_{DP}, which indicates that the fine of the said violations fine has been successfully collected. Afterwards, the OV removes all the matching entries with those in D_{DP} from the TR and stores them in the violations record, the Violation Entries (VE) table.

3.5. SmartCop in Urban Environment. In case of urban region, we witness a lot of Road Side Units (RSUs) deployed,

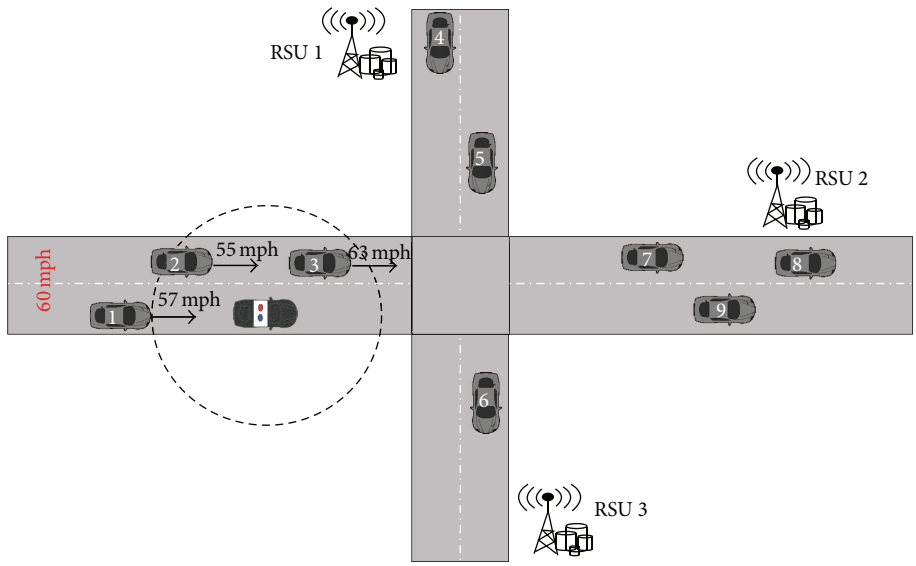


Figure 5: SmartCop: urban environment.

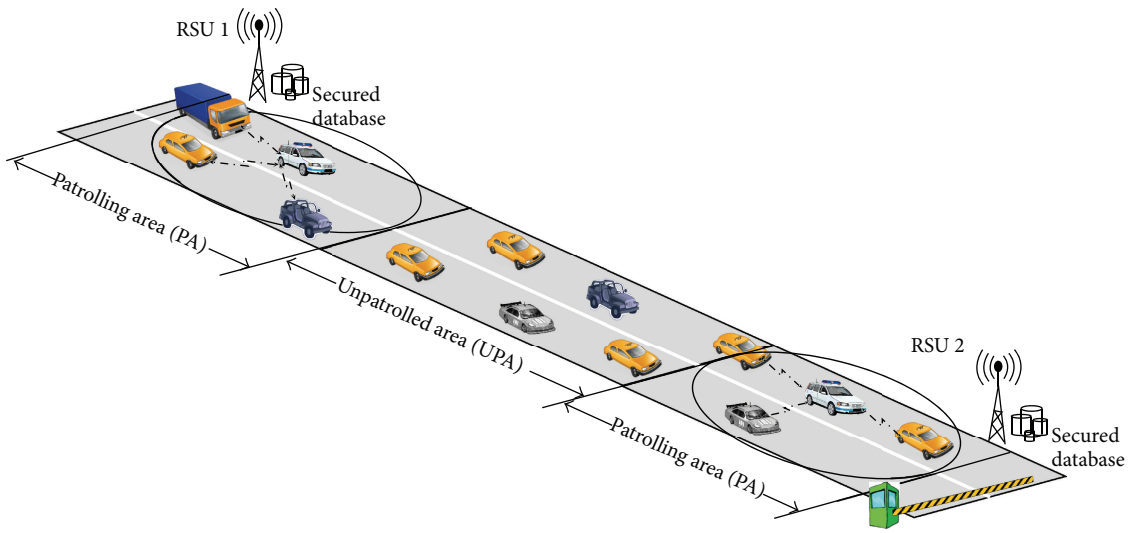


Figure 6: SmartCop: highway environment.

apparently supporting various applications. We expect those RSUs to work as ticket dues collectors due to their strong backbone connections to the wired networks. Figure 5 shows an urban scenario where an OV_3 is overspeeding and hence needs to be ticketed. Our smart traffic violation ticketing system enables the forthcoming CV to issue a relevant ticket to the vehicle OV_3 by sending an Interest packet for PTE, receiving PTE in return and updating the local law enforcement database through any available interface such as LTE or 3G (in VNDN, each vehicle is expected to be equipped with multiple interfaces for communication such as 802.11, LTE, and WiMax). For instance, the selection of the most reliable interface is out of the scope of this work. In SmartCop system, eventually an OV_3 pays the ticket dues while crossing the next RSU.

3.6. SmartCop in Highway Environment. On highways, mostly we have tollbooths as illustrated in Figure 6. Each tollbooth is equipped with at least one RSU and thus can attempt to charge the pending tickets stored in TR. However, there might be a case when a violating OV is not charged due to insufficient amount in the bank account and so on. In that case, we incorporate a binary flag in TR (i.e., 0 and 1) in the case of unpaid and paid tickets, respectively. In the former case, the transport department follows the conventional procedure that is mailing a ticket

Table 3: Simulation parameters.

Parameter	Value
MAC/PHY	IEEE 802.11p
Frequency band	5.9 GHz
Simulation duration	200 s
CVs	1–5
OVs	30–80
Violators	5–25
Number of violations/violators	Random (1–5)
Average vehicle speed	50–100 km/h

manually. In the latter case, the entry is moved to VE with a flag value of 1, thus ensuring that the payment has been completed.

4. Simulation Results and Analysis

In this section, we briefly discuss the simulation environment, the parameters, and the results of the proposed SmartCop scheme.

4.1. Simulation Environment. To evaluate the proposed SmartCop scheme, the NDN forwarding daemon architecture and IEEE 802.11p are implemented over each vehicle and simulated in the Network Simulator (NS2). Each vehicle in the simulation has the capability to communicate at the transmission range of 300 meters. Along with the default NDN structures (CS, PIT, and FIB), the structures supported by SmartCop, that is, PTE, TR, VE, PT, and TRT, are also implemented to properly evaluate its functionality. NDN's default Interest and data messages are modified to support violation ticketing operations. The highway mobility model along with the varying number of vehicles is simulated, which move at the average speed of 50 to 100 km/h. The total number of vehicles (N) is the sum of CV, OV, and the violators. Violator vehicles randomly make violations between 1 and 5 randomly during the simulation time of 200 s. Each CV sends the periodic Interest message after every 1 s to find the violators. The rest of the simulation parameters are shown in Table 3.

The SmartCop performance is the average of twenty simulation runs for each point in graphs with the confidence interval of 10%. Following is the description of the performance metrics that have been analyzed.

(i) Average cost is the total number of messages (Interest and data) that have been exchanged between the CV and the violators to successfully issue the violation ticket.

(ii) Satisfied delay is the amount of time between the Interest and the data messages received by a violator from the CV to successfully get the ticket(s) for violation(s).

(iii) Total delay is the amount of time when a violator committed the violation and received the ticket for that violation.

(iv) Number of sessions is the message exchange between a CV and the violator to get the violation ticket.

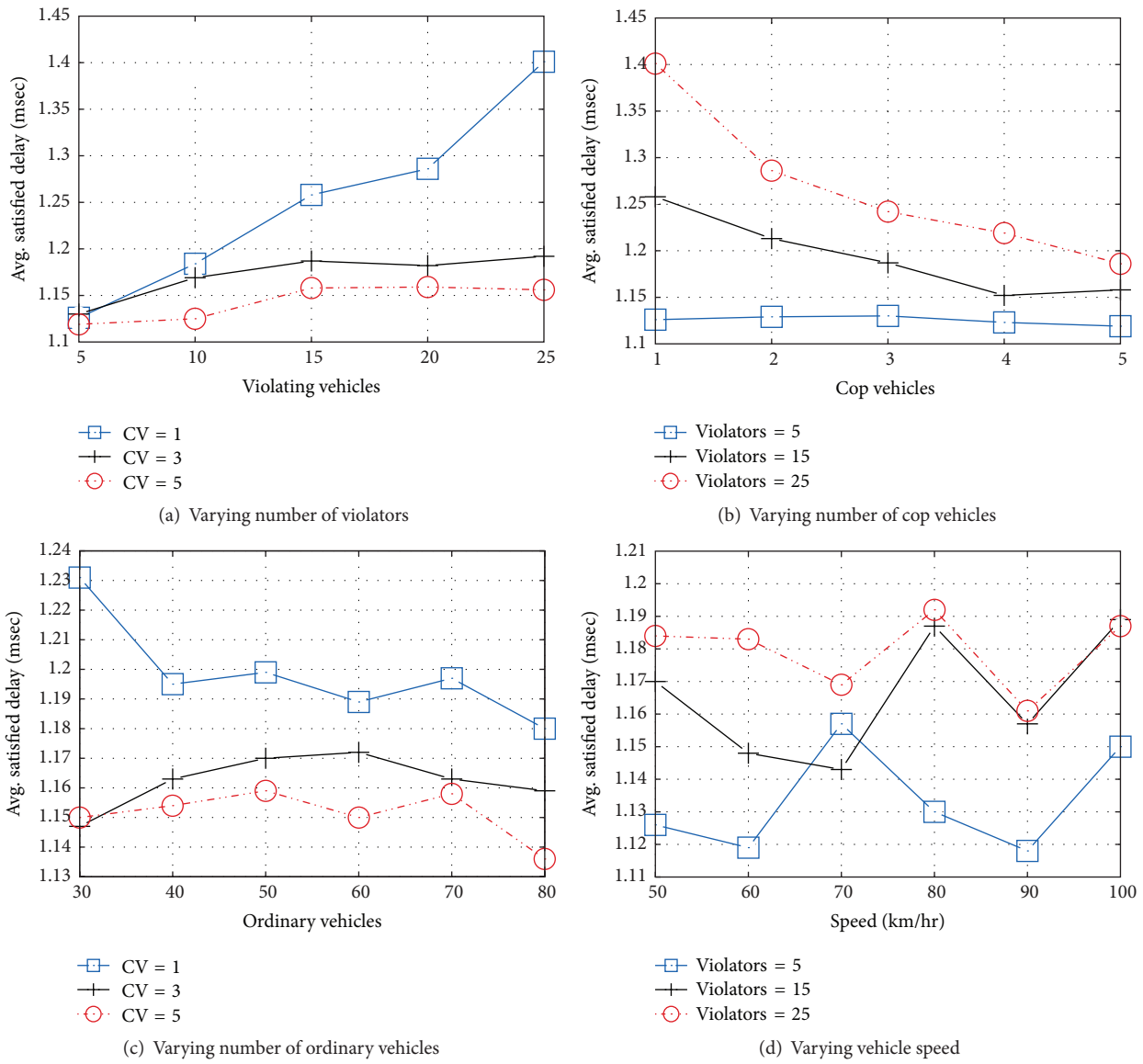
(v) Tickets satisfied is the ratio of tickets received and the total number of violations during the simulation period.

4.2. Results and Analysis. In this section, we briefly discuss the simulation results of the proposed SmartCop scheme.

Figure 7 shows the average satisfied delay for varying number of violators (Figure 7(a)), CVs (Figure 7(b)), OVs (Figure 7(c)), and the vehicle's speed (Figure 7(d)). The average satisfied delay is the duration between the I_{PTE} and D_{PT} received by a violator to successfully get the ticket for a traffic violation. To simply state, it is the violation ticket *session* delay during which the CV and the violator exchange messages for the violation ticket. It is evident from the figure that the higher the number of violators, the longer the delay. The rationale of this phenomenon is that, in the presence of a large number of violators, the message exchange will increase the traffic and the PTE, PT, TR, and other structures' search delay will be larger than results in a large violation satisfaction delay. The opposite is the case with the number of CVs. In case of more CVs, the violation ticket messaging overhead is distributed among the CVs that issue tickets with less delay; refer to Figures 7(a) and 7(b). On the other hand, the number of ordinary vehicles and the speed of the vehicle have not that much impact on the average satisfied delay because the NDN traffic on the ordinary vehicles does not access the PTE, PT, TR, and SmartCop related data structures. Therefore, the maximum difference in the satisfied delay is 0.03 ms for varying number of OVs and CV = 1 in Figure 7(c) and less than 0.035 ms for varying speed as evident from Figure 7(d). This concludes that the number of CVs and the violators in the area have the major impact on the satisfied delay.

Next, we analyzed the average total delay, which is the total time between the instance when a violation was committed (or entry was created in the PTE) and the ticket that was issued to the vehicle (or the entry was created in the TR for the respective PTE entry). It is obvious from Figures 8(a), 8(b), and 8(c) that average total delay is indirectly proportional to the number of cop vehicles because the tickets are only issued by the CVs. In case of less number of CVs, the violations will be pending the PTE for a longer time until the violator enters the communication range of the CV. The opposite is the case for the large number of the CVs in the area. Another factor that has the huge effect on the average total delay is the node's speed; refer to Figure 8(d). A vehicle that drives at a faster speed may quickly come in the communication range of the ticket issuing point and happens to have a short delay.

The other parameter that we analyzed through simulations is the messaging cost to satisfy all the violations during a simulation run. Messaging cost is the total number of messages (Interest and data) exchanged between the violator and the CV to issue the ticket. Figure 9 shows the average cost for varying the above discussed parameters. It is obvious that the cost is directly proportional to the number of



(a) Varying number of violators

(b) Varying number of cop vehicles

(c) Varying number of ordinary vehicles

(d) Varying vehicle speed

FIGURE 7: Average satisfied delay.

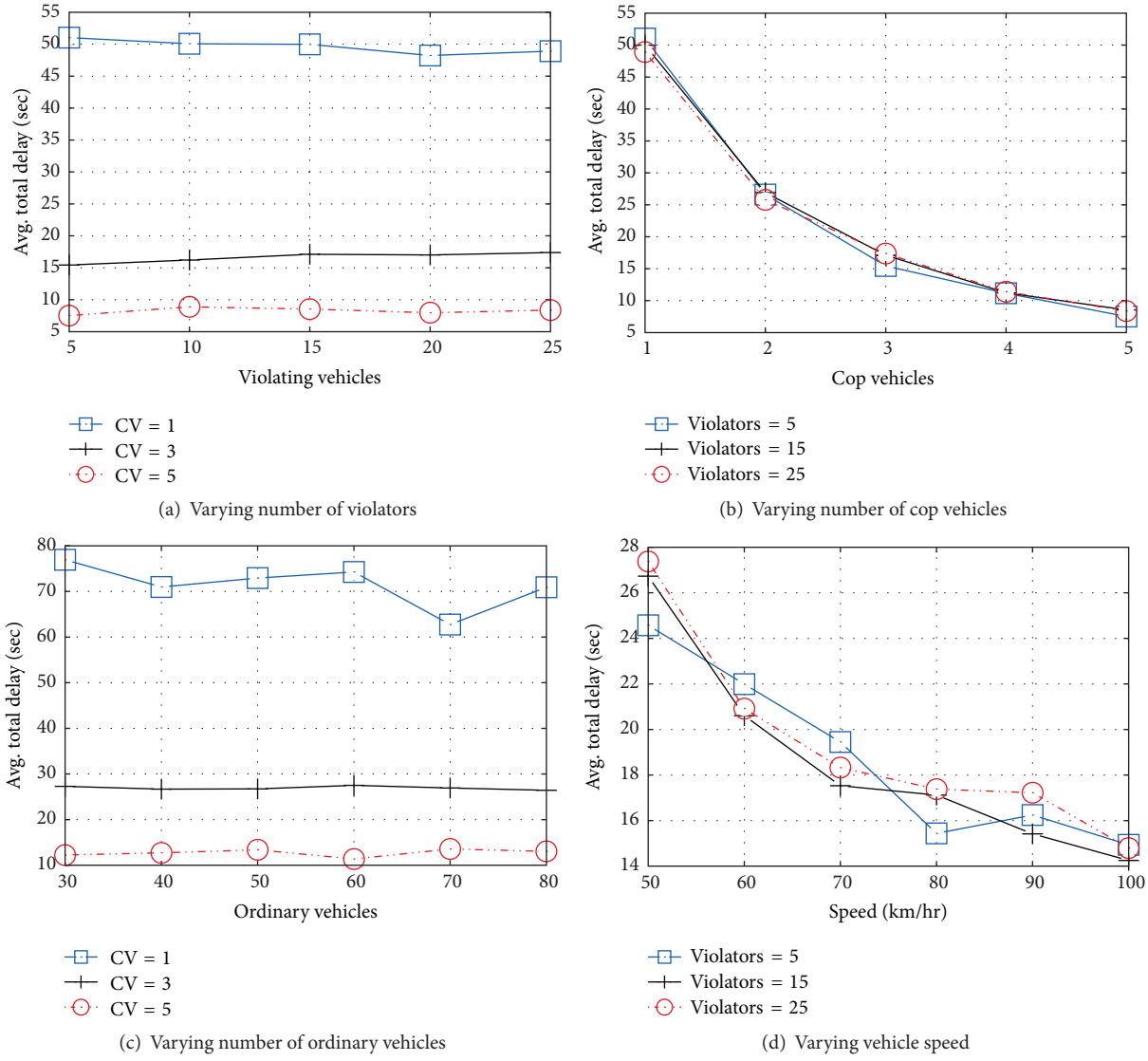
violators and the number of CVs. If the number of violators increases, then it requires more numbers of messages to issue tickets. Similarly, the larger the number of CVs in the area, the more tickets are issued to the violators that increases the messaging cost and it is obvious from the figure. Additionally, it can easily be analyzed from the results that the number of ordinary vehicles and the vehicle's speed have no significant effect on the messaging cost; refer to Figures 9(c) and 9(d).

5. Open Issues in VNDN and SmartCop System

In this section, we provide readers with the open issues connected to SmartCop system and VNDN, needing the attention from researchers working for a secure driving experience and other application domains in VANETs.

5.1. Naming in VNDN and SmartCop. Content naming is the most important issue in future networks where the focus of communication is *content* but not the IP/TCP based device addresses. Therefore, we have various naming schemes for conventional CCN, NDN, and VNDN. Some of them are categorized as hierarchical, flat, human readable, hash-based, attribute-based, and so on [15]. However, it is difficult to determine the best suitable scheme for VNDN, especially when we are trying to communicate a highly sensitive data between vehicles on roads such as in SmartCop system. Similarly, we need to design a hybrid naming scheme for different violation types and their relevant entries to be included in an *"Interest"* packet, which will be broadcast by a CV to each OV in its transmission range.

5.2. Content Distribution. For instance, we have assumed that every road segment will be covered with one CV or none.



(a) Varying number of violators

(b) Varying number of cop vehicles

(c) Varying number of ordinary vehicles

(d) Varying vehicle speed

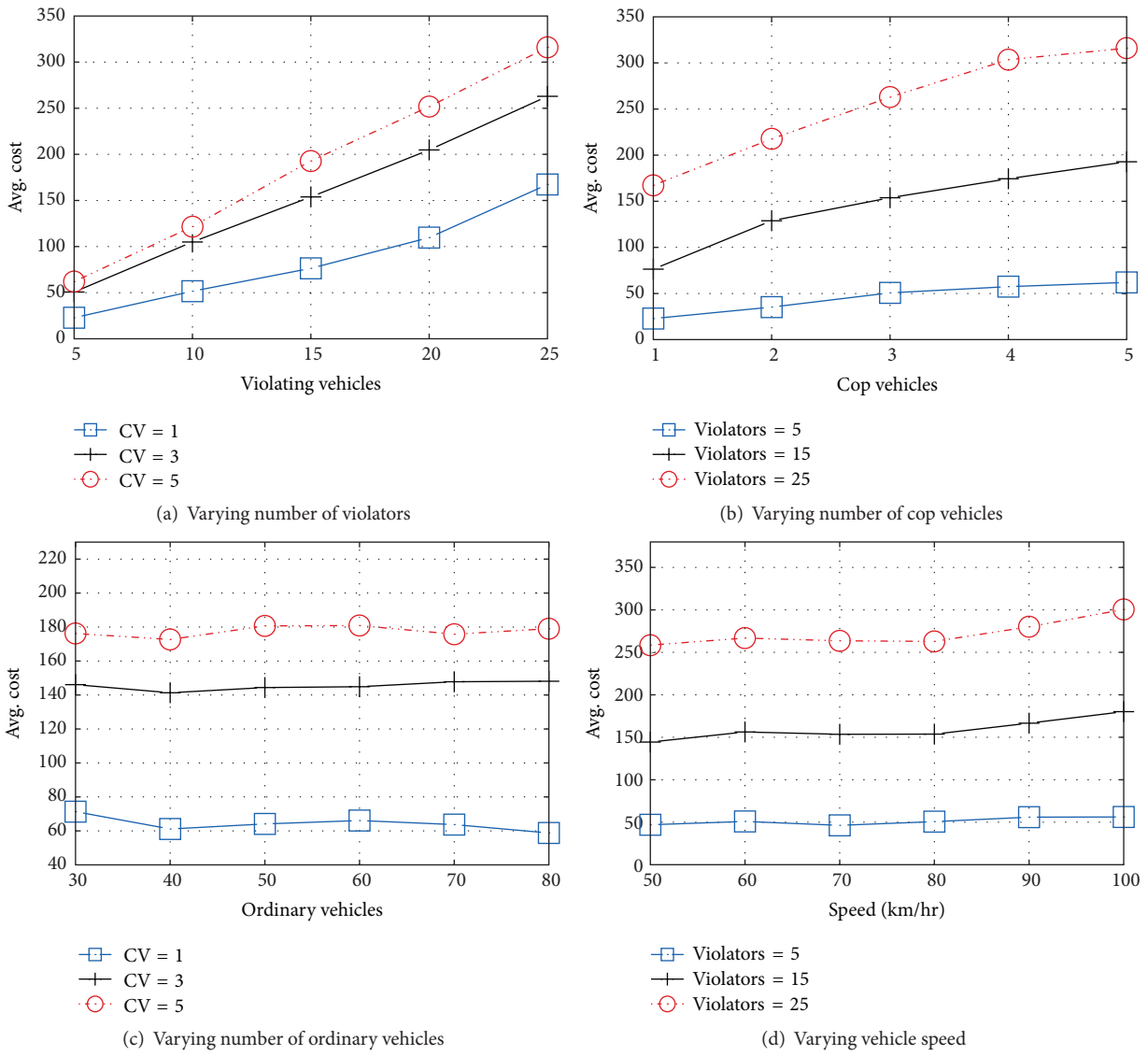
FIGURE 8: Average total delay.

However, there may be a case where two or more CVs come across; in that case we need to address the selection process of a CV for exchanging PTE by any OV. On the other hand, the identification of redundant data of PTE received by any CV is a significant challenge to be addressed.

5.3. Autonomous Ticket Issuance. Using our SmartCop system in a highly dynamic environment such as VANETs in urban scenario is a challenging task. There is the possibility of multiple offenders/violators in the immediate transmission range of a CV. Therefore, issuing a violation ticket to multiple OVs requires a highly cooperative and fast synchronization mechanism. Moreover, managing the PT entries in the CV's local memory should be addressed, respectively.

5.4. Interest Packets Flooding. Due to the broadcast nature of the wireless medium, conventionally, Interest packets are flooded within the network. Since SmartCop system applies only to the immediate neighbors of any CV, while preparing the test-bed or experimental environment, a controlled Interest flooding technique needs to be implemented. For instance, one can use the hop count flag to limit the Interest flooding.

5.5. Security and Privacy Issues. Although our SmartCop is an initial step towards the smart ticketing in future vehicles. It is also very important to address the security issues at the different levels of communications, especially in the presence of the wireless medium. Those include the authenticity of the *content* being sent to any CV and also of any *Interest* packet sent by a CV itself. Furthermore, issuing a ticket is very sensitive and private step, so it is required to make sure that no other vehicle can access and open the history of neighbor vehicle.



(a) Varying number of violators

(b) Varying number of cop vehicles

(c) Varying number of ordinary vehicles

(d) Varying vehicle speed

FIGURE 9: Average Interest-Data messaging cost to successfully issue violation tickets during simulation.

6. Conclusion

In this paper, we present an architecture for a smart and efficient traffic violation ticketing system for vehicles with future Internet technologies such as NDN. Our architecture will enable traffic law officials to identify drivers and violating vehicles without chasing and putting lives in danger. In order to achieve this, we apply basic VNDN operations into our SmartCop system, where a cop vehicle periodically broadcasts an Interest packet for violation entries saved by every ordinary vehicle in its local memory (PTE). This exchange of PTE enables a cop vehicle to issue a relevant ticket to the offender. Later on, the offenders' vehicle, when connected to any road side unit, pays the charged ticket autonomously. As a result, all the manual operations and delays caused by human errors are skipped. In the end, we also enlist the future work directions for improving and implementing our proposed SmartCop system into real test-bed environments and simulations. The simulations show that the ticket issuing delay and its messaging cost depend upon the number of violators, vehicles, and speed of the vehicles on the road.

Competing Interests

There are no competing interests regarding the publication of this paper.

Acknowledgments

This research was supported by Kyungpook National University Bokhyeon Research Fund, 2015.

References

[1] X. Liu, Z. Li, P. Yang, and Y. Dong, "Information-centric mobile ad hoc networks and content routing: a survey," *Ad Hoc Networks*, 2016.

[2] B. Das, S. Misra, and U. Roy, "Coalition formation for cooperative service-based message sharing in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 144–156, 2016.

[3] N. Ratnakar, "Smart Traffic Ticket Device," U.S. Patent Application 10/907, 271, filed March, 2005.

[4] N. Vaidya, "Open problems in mobile ad hoc networking," in *IEEE Local Area Networks*, p. 516, 2001.

[5] M. Amadeo, C. Campolo, and A. Molinaro, "Information-centric networking for connected vehicles: a survey and future perspectives," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 98–104, 2016.

[6] S. H. Ahmed, S. H. Bouk, and D. Kim, "RUFS: RobUst forwarder selection in vehicular content-centric networks," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1616–1619, 2015.

[7] M. Amadeo, C. Campolo, and A. Molinaro, "Enhancing content-centric networking for vehicular environments," *The Elsevier Journal of Computer Networks*, no. 16, pp. 3222–3234, 2013.

[8] Z. Yan, S. Zeadally, S. Zhang, R. Guo, and Y.-J. Park, "Distributed mobility management in named data networking," *Wireless Communications and Mobile Computing*, 2015.

[9] S. H. Ahmed, M. A. Yaqub, S. H. Bouk, and D. Kim, "Towards content-centric traffic ticketing in VANETs: an application perspective," in *Proceedings of the 7th International Conference on Ubiquitous and Future Networks (ICUFN '15)*, pp. 237–239, Sapporo, Japan, July 2015.

[10] T. Yamaki and T. Nishizaka, "Traffic violation warning and traffic violation storage equipment," U.S. Patent No. 6,720,889, April 2004.

[11] N. Ratnakar, "Smart traffic ticket device," US Patent Application 20060214783 A1, 2006.

[12] B. E. Higgins, "Automated traffic violation monitoring and reporting system with combined video and still-image data," U.S. Patent No. 7,986,339. 26 Jul. 2011.

[13] S. Tarapiah, S. Atalla, and R. AbuHania, "Smart on-board transportation management system using GPS/GSM/GPRS technologies to reduce traffic violation in developing countries," *International Journal of Digital Information and Wireless Communications*, vol. 3, no. 4, pp. 430–439, 2013.

[14] A. Harbi, S. H. S. Harmad, and D. A. M. Al-Fayez, "System for detecting and identifying traffic law violators and issuing citations," U.S. Patent No. 8,633,815. 21 Jan. 2014.

[15] S. H. Bouk, S. H. Ahmed, and D. Kim, "Hierarchical and hash based naming with Compact Trie name management scheme for Vehicular Content Centric Networks," *Computer Communications*, vol. 71, pp. 73–83, 2015.