An Intelligent Secure and Privacy-Preserving Parking Scheme Through Vehicular Communications

Rongxing Lu, *Student Member, IEEE*, Xiaodong Lin, *Member, IEEE*,
Haojin Zhu, *Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—There are always frustrations for drivers in finding parking spaces and being protected from auto theft. In this paper, to minimize the drivers' hassle and inconvenience, we propose a new intelligent secure privacy-preserving parking scheme through vehicular communications. The proposed scheme is characterized by employing parking lot RSUs to surveil and manage the whole parking lot and is enabled by communication between vehicles and the RSUs. Once vehicles that are equipped with wireless communication devices, which are also known as onboard units, enter the parking lot, the RSUs communicate with them and provide the drivers with real-time parking navigation service, secure intelligent antitheft protection, and friendly parking information dissemination. In addition, the drivers' privacy is not violated. Performance analysis through extensive simulations demonstrates the efficiency and practicality of the proposed scheme.**

***Index Terms*—Antitheft, information dissemination, navigation, security and privacy, smart parking, vehicular ad hoc networks (VANETs).**

I. Introduction

FINDING A vacant parking space in a congested area or a large parking lot, particularly during peak hours, is always time consuming and frustrating for drivers. It is common for drivers to keep circling within a parking lot for a parking space. To minimize hassle and inconvenience to drivers, many parking guidance systems have been developed over the last decade [2]–[4] to provide accurate real-time parking space availability to drivers by dynamically updated guide signs. Currently, most parking guidance systems obtain the availability of parking spaces by using the sensors installed across the whole parking lot. However, deploying sensors in a large parking lot can be very expensive. In addition, the drivers still need to circle to find a parking space. Therefore, it is highly desireable to have a quick and cost-effective way to track and guide drivers to available parking spaces. Aside from searching for available parking spaces, vehicle theft in large parking lots has become a serious concern. For example, statistics show that there are more than 170 000 vehicles stolen each year in Canada.

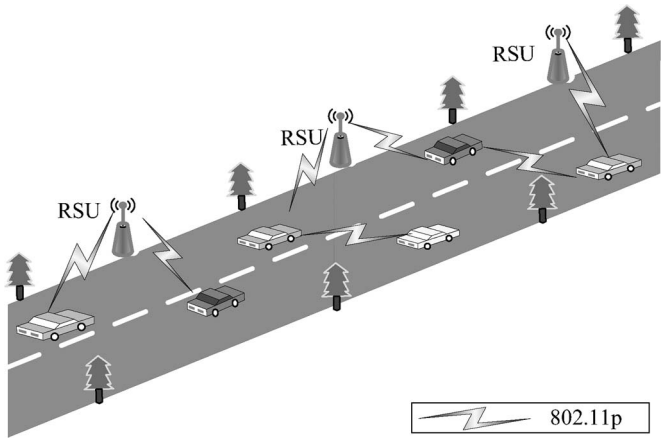


Fig. 1. VANET.

Recently, vehicular ad hoc networks (VANETs), as shown in Fig. 1, have received particular attention both in the industry and academia [5]–[8]. With the advance and wide deployment of wireless communication technologies, many major car manufactories and telecommunication industries have been gearing up to equip each car with the onboard unit (OBU) communication device, which allows different cars to communicate with each other and for roadside infrastructure, i.e., roadside units (RSUs), to improve not only road safety but to also provide a better driving experience [9], [10]. Therefore, it becomes possible for parking guidance systems to track parking space occupancy, guide drivers to empty parking spaces, and provide antitheft protection in large parking lots through vehicular communications.

In this paper, we develop an intelligent secure privacy-preserving parking scheme based on VANETs to provide drivers with convenient parking services in large parking lots. The proposed scheme is characterized by employing parking lot RSUs to surveil and manage the whole parking lot through vehicular communications. The main contributions of this paper are fourfold.

- First, the proposed scheme can support real-time parking navigation service to drivers in large parking lots. With the real-time parking navigation, drivers can quickly find a vacant parking space. Therefore, gasoline and the time wasted in searching for the vacant parking space can

Manuscript received June 24, 2009; revised October 17, 2009, December 14, 2009, February 10, 2010, and March 29, 2010; accepted April 16, 2010. Date of publication April 29, 2010; date of current version July 16, 2010. Part of this paper was presented at the 28th IEEE International Conference on Computer Communications. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada. The review of this paper was coordinated by Prof. L. Chen.

R. Lu and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: rxlu@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada (e-mail: xiaodong.lin@uoit.ca).

H. Zhu is with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: zhu-hj@cs.sjtu.edu.cn).

Digital Object Identifier 10.1109/TVT.2010.2049390

be reduced. We have developed a custom simulator to show the substantial improvement of the proposed intelligent parking lot in terms of the searching time delay (STD) compared with the current ordinary parking lot without navigation. Simulation results show that the real-time parking navigation service supported by the proposed scheme is effective. To the best of our knowledge, this work is the first such effort in the context of VANET-based real-time parking navigation.

- Second, the proposed scheme provides VANET-based intelligent antitheft protection services. With these services, all vehicles that are parked at the intelligent parking lot are guarded by the parking lot RSUs. Once a vehicle illegally leaves the parking lot, the RSUs can quickly detect the anomaly.
- Third, the proposed scheme can provide friendly parking information dissemination services to the moving vehicles. With this friendly parking information, the drivers can conveniently and quickly choose their preferred parking lots close to their destinations. We have also developed another custom simulator to demonstrate that the friendly parking information can quickly be disseminated by vehicular communication.
- Finally, the proposed scheme can also ensure the conditional privacy preservation of the OBUs (or drivers), which is regarded as the basic security requirement in VANET communications [10]–[18].

The remainder of this paper is organized as follows. In Section II, we introduce the system model and design goal. In Section III, we present the intelligent parking scheme, followed by the security and performance analyses through simulations in Sections IV and V, respectively. We discuss the related work in Section VI. Finally, we draw our conclusions in Section VII.

II. System Model and Design Goal

In this section, we characterize the intelligent parking lot by modeling the system and identifying the design goal.

A. System Model

We consider the flourish stage of VANETs, where each vehicle is equipped with an OBU device, and RSUs are also widely deployed. In particular, the system model of the intelligent parking lot consists of a trusted authority (TA), OBUs equipped on the vehicles, stationary parking lot RSUs, and a large number of parking spaces.

- TA is a trusted and powerful entity, which is responsible for the registration of both OBUs and the parking lot RSUs.
- OBUs are installed on the vehicles, which can communicate with each other and with RSUs to obtain useful information, including traffic information and parking lot information. Each OBU has a unique identifier ID_i. To protect the privacy of the OBU, when an OBU with ID_i registers itself to TA, TA first converts the real identifier ID_i into a pseudo-ID PID_i and generates a private key sk_i that corresponds to the pseudo-ID of the OBU. When an OBU enters an intelligent parking lot, it will receive a pair of ticket IDs and the corresponding ticket key, which is only known to the driver.
- RSUs are important components for intelligent parking lots. As shown in Fig. 2,[1] three RSUs, i.e., RSU_0 at position (0, 0), RSU_a at position (x_a, y_a), and RSU_b at position (x_b, y_b), are erected in the parking lot. With this deployment, the whole parking lot (including the parking spaces and vehicles) can be under the surveillance of the three RSUs. After the intelligent parking lot with identifier ID_j is inspected by TA, TA will generate a private key sk_j that corresponds to the identifier ID_j and distribute the private key sk_j to these parking lot RSUs.

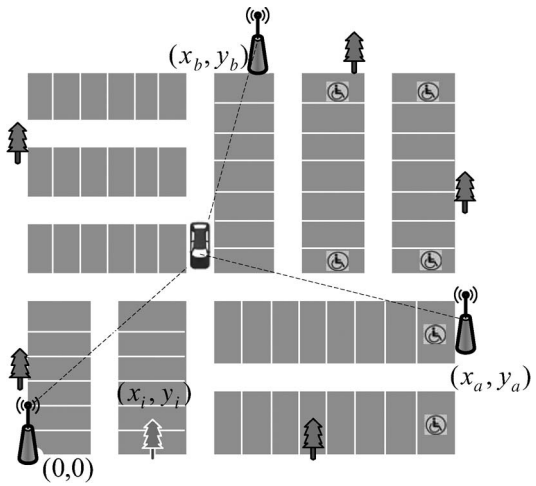


Fig. 2. Parking lot model under consideration.

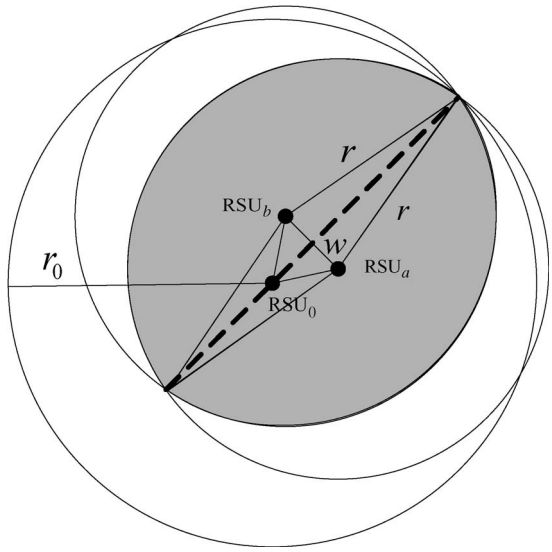


Fig. 3. Overlapped surveillance region $\mathbb{S}$ of three parking lot RSUs.

Fig. 3 shows one placement of RSUs in an intelligent parking lot, where the distance between RSU_a and RSU_b is w, and the transmission ranges of RSU_a, RSU_b, and RSU_0 are r, r, and $r_0 = \sqrt{r^2 - (w/2)^2} + w$,

[1] In reality, there may exist more than three RSUs in a parking lot to coordinate the tracking of the vehicle if the parking lot is extremely large or has some large structure in the middle.

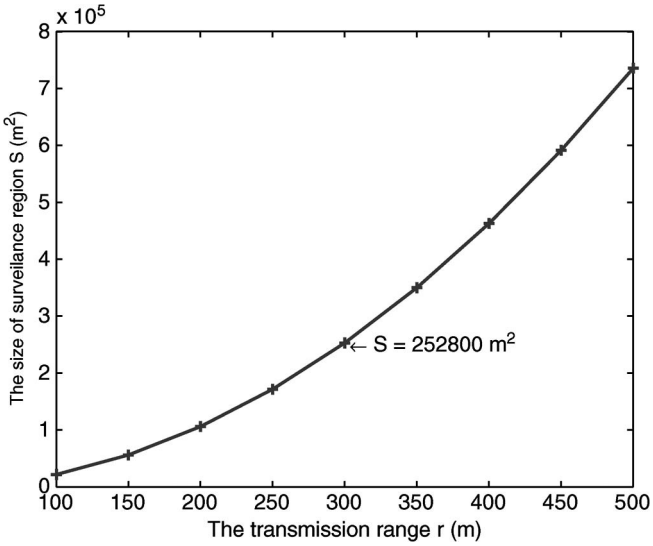


Fig. 4. Size of surveillance region versus different transmission range.

TABLE I
PARKING SPACE RECORD

POS	RES	OCC	PID	TID	TKEY	ST	LUT

respectively. Then, the size of the overlapped surveillance region is

$$\mathbb{S} = 2r^2 \cdot \arccos\left(\frac{w}{2r}\right) - w \cdot \sqrt{r^2 - \left(\frac{w}{2}\right)^2}. \qquad (1)$$

When the distance $w = 50$ m, as shown in Fig. 4, the surveillance region $\mathbb{S}$ varies with the transmission range r, where $100 \leq r \leq 500$ m, which belongs to the transmission range that is recommended in the IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) standard [19]. When the transmission range r expands, the surveillance region $\mathbb{S}$ will quickly increase. For example, when the transmission range $r = 300$ m, $\mathbb{S}$ can reach 252 800 m^2, which is large enough to surveil the practical parking lots.

- The parking space is a spatiotemporal resource recorded by the RSUs in an intelligent parking lot. Each parking space record, as shown in Table I, has the following attributes.
  - *Position* (POS). Each parking space can derive its position (x_i, y_i) on the unique Euclidean plane determined by the three parking lot RSUs, as shown in Fig. 2.
  - *Reservation* (RES). This field denotes the reservation status of the parking space. If the parking space is reserved, RES $= 1$; otherwise, RES $= 0$.
  - *Occupancy* (OCC). This field denotes the occupancy status of the parking space. If the parking space is occupied, OCC $= 1$. Otherwise, if the parking space is vacant, OCC $= 0$.
  - *Pseduo-ID* (PID). If the parking space is occupied by an OBU, this field records the OBU's pseduo-ID.
  - *Ticket ID* (TID). If the parking space is occupied by an OBU, this field records the OBU's ticket ID.
  - *Ticket key* (TKEY). If the parking space is occupied by an OBU, this field records the OBU's ticket key.
  - *Start time* (ST). This field records the OBU's start parking time at the parking space.
  - *Last update time* (LUT). This field records the timestamp at which the OBU sends the latest message.

For an intelligent parking lot, all parking space records are stored at the parking lot RSUs, which conveniently manage the whole parking lot by using these records.

B. Design Goal

Before describing our design goal for the intelligent parking scheme, we first make necessary assumptions in our system model.

- *Assumption 1*. TA is fully trusted by all OBUs and RSUs.
- *Assumption 2*. Each OBU is a customized tamper-proof device that is fixed on the vehicle, which can provide all the necessary functionalities for secure vehicular communication and, at the same time, can be produced in a large quantity at sufficient low costs [20], [21]. Before drivers operate the OBUs, they must provide a key sk_i, which is shared between them and the OBUs, for authenticating themselves. A driver first computes $\delta = h(sk_i \| T)$ and provides δ to an OBU, where $h()$ is a secure hash function, and T is the current timestamp. The OBU then checks the validity of the timestamp T, computes $\delta' = h(sk_i \| T)$, and compares it with δ. If $\delta = \delta'$, the driver is authenticated, and the OBU can be operated. Therefore, it is reasonable to assume that an adversary cannot compromise the inner data stored in the OBU or detach the OBU from the vehicle in a short period. When an OBU is switched on by the driver, it has two modes: 1) *active* and 2) *sleep*. In the *active* mode, the OBU consumes the vehicle power and unceasingly receives/sends the messages, whereas in the *sleep* mode, the OBU's energy consumption is low, and the OBU can only use its inner battery to send beacon messages for a long period.
- *Assumption 3*. There are at least three RSUs in the parking lot, which are actively powered and will not be compromised by the adversary. Each RSU has the ability to accurately measure the distance to each vehicle within the parking lot through a certain ranging method, e.g., time of arrival (TOA), time differences of arrival (TDOA), or another more accurate measurement technology [22]. In addition, the three RSUs cooperatively and synchronically cover the whole parking lot.

Our design goal is to develop an intelligent parking scheme for large parking lots, which can achieve the following desirable requirements: 1) real-time parking navigation; 2) intelligent antitheft protection; 3) friendly parking information dissemination; and 4) conditional privacy preservation.

- *Real-time parking navigation*. In the intelligent parking scheme, the three parking lot RSUs should provide the

navigation function so that, with the guidance of the RSUs, a vehicle can conveniently find a vacant parking space in a large parking lot.

- *Intelligent antitheft protection*. In the intelligent parking scheme, the three parking lot RSUs should also provide the guard function after the driver parks the vehicle and leaves for shopping or others. Once a vehicle theft occurs, the RSUs will send the warning alarms. Meanwhile, if the stolen vehicle is illegally driven away or towed away from the parking lot, vehicular communications should provide a tracking mechanism to track the stolen vehicle.
- *Friendly parking information dissemination*. In the intelligent parking scheme, the parking lot RSUs should disseminate the friendly parking information to the running vehicles. Then, before the drivers reach their destinations, they can choose their preferred parking lots in advance.
- *Conditional privacy preservation*. When a vehicle enters an intelligent parking lot, its real identifier ID_i should be kept secret. However, once an exceptional event occurs, the RSUs can learn the OBU's real identifier ID_i with the help of TA.

III. Proposed Intelligent Parking Scheme

In this section, we present the VANET-based intelligent parking scheme, which consists of four parts: 1) system setting; 2) real-time parking navigation; 3) intelligent antitheft protection; and 4) friendly parking information dissemination. Before describing them, we first review the bilinear pairing technique [23], which serves as the basis of the proposed intelligent parking scheme.

A. Bilinear Pairing Technique

Let $\mathbb{G}$, $\mathbb{G}_T$ be two cyclic groups of the same prime order q. Let e be a computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, which satisfies the following three properties.

1) *Bilinear*. For this property, $e(aP, bP) = e(P, P)^{ab}$, where $P, Q \in \mathbb{G}$, and $a, b \in \mathbb{Z}_q^*$.
2) *Nondegenerate*. There exist $P, Q \in \mathbb{G}$ such that $e(P, Q) \neq 1_{\mathbb{G}_T}$.
3) *Computability*. There exists an efficient algorithm for computing $e(P, Q)$ for all $P, Q \in \mathbb{G}$.

We call such a bilinear map e as an admissible bilinear pairing, and the modified Weil or Tate pairing in an elliptic curve can give a good implementation of the admissible bilinear pairing [23]. A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter k as input and outputs a 6-tuple $(q, \mathbb{G}, \mathbb{G}_T, e, P, Q)$ as the bilinear parameters, including a prime number q, with $|q| = k$, two cyclic groups $\mathbb{G}$, $\mathbb{G}_T$ of the same order q, an admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, and two random generators P, Q of $\mathbb{G}$.

B. System Setting

To set up the system, TA first initializes all required system parameters as follows. Given the security parameter k, TA generates a 6-tuple $(q, \mathbb{G}, \mathbb{G}_T, e, P, Q)$ by running $\mathcal{G}en(k)$. Let h be a secure cryptographic hash function, where $h : \{0,1\}^* \to \mathbb{Z}_q^*$, and $\mathbf{Enc}()$ is a secure symmetric encryption algorithm, e.g., AES [24]. TA defines a key derivation function (KDF) built on the hash function h. Then, TA chooses a random number $s \in \mathbb{Z}_q^*$ as a *master key* and generates an asymmetric identity-based master key $s_0 = \mathbf{KDF}(s\|0)$ and a symmetric encryption/decryption key $s_1 = \mathbf{KDF}(s\|1)$, respectively. In addition, TA computes the corresponding system public key $P_{pub} = s_0 P$. Finally, the system parameters *params* are established, which include $\{q, \mathbb{G}, \mathbb{G}_T, e, P, Q, P_{pub}, h, \mathbf{Enc}(), \mathbf{KDF}\}$.

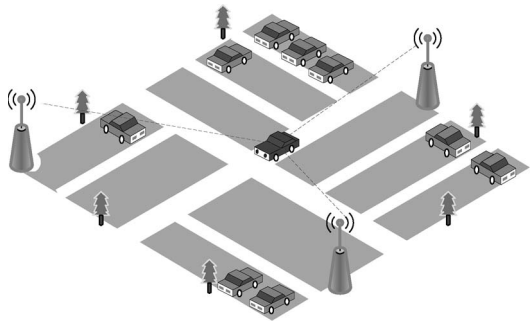


Fig. 5. Typical smart parking lot.

When an OBU with identifier ID_i registers itself to the system, TA first checks its validity. If the identifier ID_i passes the check, TA executes the following two steps.

Step 1. Use the secret key s_1 to encrypt the real identifier ID_i into a pseudo-ID $\mathrm{PID}_i = \mathbf{Enc}_{s_1}(\mathrm{ID}_i \| r_i)$, where the nonce r_i is randomly chosen from $\mathbb{Z}_q^*$. In processing the pseudo-ID PID_i, the OBU can hide its real identity ID_i to achieve identity privacy.

Step 2. Use the secret key s_2 to generate the private key of the OBU as $sk_i = (1/s_0 + \mathrm{PID}_i)Q$ and send (PID_i, sk_i) back to the OBU through a secure channel.

When a large parking lot with identifier ID_j is set up, each parking space is designated a location (x_i, y_i), and three parking lot RSUs of the same height $\mathtt{h}$ are erected at the locations (0, 0), (x_a, y_a), and (x_b, y_b), respectively. Then, the whole parking lot will be under the surveillance of these three RSUs, as shown in Fig. 5. After TA inspects the parking lot, TA generates the private key $sk_j = (1/s_0 + \mathrm{ID}_j)Q$ and stores the same private keys sk_j into the three RSUs. With these settings, a large intelligent parking lot is established.

C. Real-Time Parking Navigation

When a vehicle that is equipped with an OBU ID_i is ready to enter an intelligent parking lot with identifier ID_j, it first communicates with the parking lot RSUs to gain the ticket ID and ticket key for the parking navigation. The detailed protocol steps are described as follows.

Step 1. The OBU first chooses a random number $r \in \mathbb{Z}_q^*$ and computes $c = r \cdot (P_{pub} + \mathrm{ID}_j \cdot P) \in \mathbb{G}$, the verification information $V_O = r \cdot sk_i = (r/s_0 + \mathrm{PID}_i)Q$, and the ephemeral key $\mathtt{k} = \mathbf{KDF}(k)$, where $k = e(Q, P)^r \in \mathbb{G}_T$.

Step 2. The OBU gains the current timestamp T, formats the information PID_i, T, V_O as the message $M_O = \text{PID}_i \| T \| V_o$, and encrypts M_O as $C_O = \mathbf{Enc}_{\mathsf{k}}(M_O)$. After that, the OBU sends $C = (c \| C_O)$ to the RSUs.

Step 3. Upon receiving $C = (c \| C_O)$ at timestamp T', one RSU first computes $k' = e(sk_j, c)$ and decrypts C_O with the ephemeral key $\mathsf{k}' = \mathbf{KDF}(k')$; then, it parses the result M_O into $\text{PID}_i \| T \| V_O$. Because

$$k' = e(sk_j, c) = e\left(\frac{1}{s + \text{ID}_j} Q, r \cdot (P_{pub} + \text{ID}_j \cdot P)\right) = e(Q, P)^r = k \quad \Longrightarrow \mathsf{k}' = \mathsf{k} \tag{2}$$

the correction of the decrypted results follows.

Step 4. The RSU checks $|T' - T| \leq \Delta T$, where ΔT is the expected valid time interval for transmission delay. If it holds, the RSU proceeds to the next operation; otherwise, it stops (because it can be a replaying attack[2]). The RSU also verifies the identity PID_i by checking $e(V_O, P_{pub} + \text{PID}_i \cdot P) \stackrel{?}{=} k'$. If it holds, PID_i is authenticated, because only PID_i can compute the verification information V_O in this session such that

$$e(V_O, P_{pub} + \text{PID}_i \cdot P) = e\left(\frac{r}{s_0 + \text{PID}_i} Q, P_{pub} + \text{PID}_j \cdot P\right) = e(Q, P)^r = k'. \tag{3}$$

Step 5. Once C is accepted, the RSU chooses a random ticket key $\text{ticketKey} \in \mathbb{Z}_q^*$ and uses the one-way hash function $h()$ to compute the corresponding ticket ID as

$$\text{ticketID} = h(\text{ticketKey}) \tag{4}$$

for the OBU. The RSU then gains the current timestamp T, formats the information ticketID, ticketKey, ID_j, and T as the message $M_R = \text{ticketID} \| \text{ticketKey} \| \text{ID}_j \| T$, uses the ephemeral key k' to encrypt it into $C' = \mathbf{Enc}_{\mathsf{k}'}(M_R)$, and sends C' back to the OBU. In addition, the RSU synchronizes the information $\langle \text{PID}_i, \text{ticketID}, \text{ticketKey} \rangle$ with the other two RSUs.

Step 6. Upon receiving C' at timestamp T', the OBU decrypts C' with the ephemeral key k and parses the result M_R into ticketID, ticketKey, ID_j, and T. After checking $|T' - T| \leq \Delta T$ and $\text{ticketID} \stackrel{?}{=} h(\text{ticketKey})$, the OBU accepts the pair of $\langle \text{ticketID}, \text{ticketKey} \rangle$, which will be served to achieve navigation and guarding from the RSUs.

Real-Time Parking Navigation: After the vehicle enters a large parking lot, based on the driver's preferences, the RSUs first choose a proper vacant parking space, i.e., at location (x_i, y_i). Then, the three RSUs cooperatively and synchronically measure the distances from the vehicle to themselves, i.e., d_0, d_a, and d_b in Fig. 5. With the input of (d_0, d_a, d_b), the RSUs invoke Algorithm 1 to get the position (x_v, y_v) of the vehicle.

Algorithm 1: PositionVehicle()

Data: distances (d_0, d_a, d_b) measured by $(\text{RSU}_0, \text{RSU}_a, \text{RSU}_b)$, the height $\mathtt{h}$ of RSUs, and a threshold value ε that is contingent upon the noise in the ranging measurement.

Result: Vehicle's current position (x_v, y_v).

1. **begin**
2. Convert (d_0, d_a, d_b) to the plane distances (D_0, D_a, D_b), where

$$D_0 = \sqrt{d_0^2 - \mathtt{h}^2} \quad D_a = \sqrt{d_a^2 - \mathtt{h}^2} \quad D_b = \sqrt{d_b^2 - \mathtt{h}^2}. \tag{5}$$

3. Solve out two possible positions (x_{v_1}, y_{v_1}) and (x_{v_2}, y_{v_2}) from

$$\begin{cases} \sqrt{(x - x_a)^2 + (y - y_a)^2} = D_a \\ \sqrt{(x - x_b)^2 + (y - y_b)^2} = D_b. \end{cases} \tag{6}$$

4. **If** $|\sqrt{x_{v_1}^2 + y_{v_1}^2} - D_0| \leq \varepsilon$, **then**
5. **return** (x_{v_1}, y_{v_1})
6. **else, if** $|\sqrt{x_{v_2}^2 + y_{v_2}^2} - D_0| \leq \varepsilon$ **then**
7. **return** (x_{v_2}, y_{v_2})
8. **end**
9. **end**

With the positions (x_i, y_i) and (x_v, y_v), the RSUs can choose the shortest path for the vehicle and navigate the vehicle to the vacant parking space by the following steps.

Step 1. The RSUs generate the real-time navigation information NavInfo based on the position (x_v, y_v).

Step 2. The RSUs encrypt NavInfo into $C = \mathbf{Enc}_{\text{ticketKey}}(\text{NavInfo})$ and send the message $\text{ticketID} \| C$ to the OBU. After receiving $\text{ticketID} \| C$, the OBU can recover NavInfo. Then, the driver can follow the real-time navigation information NavInfo. Note that the reason for encrypting NavInfo here is to prevent other vehicles from eavesdropping and using the same navigation information that will cause a collision in searching for the parking space.

Step 3. The RSUs again invoke Algorithm 1 to get the vehicle's current position (x_v, y_v). If

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2} \leq \varepsilon' \tag{7}$$

where ε' is a threshold value that is contingent upon the noise in the ranging measurement, the RSUs believe that the vehicle arrives at the appointed parking space (x_i, y_i) and wait for the vehicle's feedback. If the vehicle confirms that the parking space is empty, it sends a positive feedback to the RSUs. Then, the RSUs stop the navigation. However, if the vehicle sends an exception information back to

[2]Note that, to prevent replaying attacks, both OBUs and RSUs should achieve the geosynchronized time that was obtained from the GPS in advance.

TABLE II
UPDATE A PARKING SPACE RECORD

POS	RES	OCC	PID	TID	TKEY	ST	LUT
(x_i, y_i)	0	1	PID_i	ticketID	ticketKey	T_S	T_L

the RSUs and continuously moves, the parking lot RSUs choose a new vacant parking space (x_i, y_i) and go back to Step 1. Note that, to save the bandwidth, the RSUs do not need to repeat information to a vehicle as to where the empty spot is. However, considering that there exist drivers who are unfamiliar with a given parking lot, the RSUs may still guide how they can get to the assigned parking space when the vehicles are at some intersections in a large parking lot.

Discussion: The availability of the Global Position System (GPS) has widely been used in land vehicle navigation applications. However, the positioning systems based on the GPS may not be suitable for real-time parking navigation. The reason is that the precision of many commonly used GPSs may not precisely position each parking space, and more importantly, the status of an empty parking space is dynamic. A parking space that is vacant at the current time can be occupied in the next time. Therefore, in the proposed intelligent parking scheme, the three parking lot RSUs can use TDOA or TDA [22] to cooperatively position the vehicle and achieve the real-time parking navigation.

D. Intelligent Antitheft Protection in Large Parking Lots

One of the major concerns to the public is vehicle theft, particularly at unattended parking lots. In the following discussion, we will illustrate how the proposed scheme can be used to protect from vehicle theft.

When a vehicle parks at the parking space (x_i, y_i), the parking lot RSUs obtain the current timestamps T_S, set the last update time $T_L = T_S$, and update the parking space record, as shown in Table II. Meanwhile, the driver locks and sets the OBU to *sleep* mode before leaving the vehicle. In the *sleep* mode, the OBU begins to periodically send beacon status information that is formatted as

$$\text{beaconInfo} = \text{ID}_j \| \text{ticketID} \| on \| T_L \| \Theta$$

to the RSUs, where ID_j is the parking lot's identifier, "on" is the status, T_L is the current timestamp, and $\Theta = h(\text{ticketKey} \| \text{"}on\text{"} \| T_L)$. When the driver comes back to the parking lot, he/she enters his/her authentication key to unlock the OBU and adjusts the OBU to the *active* mode. Then, the OBU will send

$$\text{beaconInfo} = \text{ID}_j \| \text{ticketID} \| off \| T_L \| \Theta$$

to the RSUs, where $\Theta = h(\text{ticketKey} \| off \| T_L)$, and finally leaves the parking lot.

Intelligent Antitheft Protection: Based on the beacon status information sent by the OBU, the parking lot RSUs can guard the vehicle. Concretely, for a parking space record with position (x_i, y_i), as shown in Table II, the RSUs can periodically invoke Algorithm 2 to detect whether there is an exception that takes place on the vehicle that parks at position (x_i, y_i).

Algorithm 2: DetectVehicleException()
Data: An occupied parking space record as shown in Table II
Result: An exception or $\perp$

```
1. begin
2.   if RSUs receive an updated beaconInfo with the same
     ticketID from the OBU within a predefined period, then
3.     parse it as [ID_j||ticketID||status||T_L||Θ] and check
       the validity of T_L to resist the replaying attack
4.     compute Θ' = h(ticketKey||status||T_L)
5.     if status == "on", then
6.       relocate the position (x_v, y_v) of the vehicle and
         compare it with the recorded (x_i, y_i)
7.       If sqrt((x_v - x_i)^2 + (y_v - y_i)^2) ≤ ε then
8.         update the field LUT with T_L
9.         return ⊥
10.      else if sqrt((x_v - x_i)^2 + (y_v - y_i)^2) > ε then
11.        detect an exception event
12.        update the field LUT with T_L
13.        return Exception-I
14.      end
15.    else, if status == off, then
16.      if Θ' == Θ, then
17.        update the field LUT with T_L, copy the
           record into a history table, and reset the
           record to its initial status.
18.        return ⊥
19.      else, if Θ' ≠ Θ, then
20.        detect an exception event
21.        return Exception-II
22.      end
23.    end
24.  else, if RSUs do not receive an update beaconInfo within
     a predefined period, then
25.    detect an exception event
26.    return Exception-III
27.  end
28. end
```

If the returned value of Algorithm 2 is "$\perp$" and the *status* is "on," the vehicle is stationary, and no vehicle thief has touched the vehicle. If the returned value is "$\perp$" and the *status* is "off," the vehicle goes to leave the parking lot. Because only the driver knows the authentication key and can unlock the OBU to change the *status* to "off," the RSUs believe that the vehicle is legally leaving. However, when the returned value is an exception, the RSUs can detect the vehicle theft.

- Exception I means that the current position (x_v, y_v) of the vehicle is different from the position (x_i, y_i). When Exception I occurs, the RSUs can detect that the vehicle is

illegally moving, e.g., illegal towing. Thus, the RSUs will broadcast a warning alarm.

- Exception II shows that a vehicle thief wants to drive a vehicle and leave the parking lot at time T_L. However, without knowing the ticketKey, he/she cannot forge a valid authentication message $\Theta = h(\text{ticketKey}\|off\|T_L)$ to pass the RSUs' authentication. Therefore, the RSUs can detect this kind of exception and broadcast a warning alarm.
- Exception III implies that a vehicle thief has stolen a vehicle and left the parking lot. The reason for this exception occurrence is that the detection period of RSUs is very long. To avoid this exception to some extent, the optimal detection period should be determined as follows. Consider that the speed limit in the parking lot is 10 km/h ($\approx$2.7 m/s) and that the distance of the parking space that is closest to the entrance is 10 m. Then, the maximum detection period for a vehicle can roughly be calculated as $10/2.7 = 3.7$ s. The calculation shows that the optimal detection period should be less than 3.7 s.

Tracking of the Stolen Vehicle: Aside from choosing the optimal detection period, an anticipated tracking-stolen-vehicle mechanism should be provided by vehicular communications. Fortunately, because the OBU is a tamper-proof device and is equipped with the inner backup battery, although the vehicle power is cut off by the thief, the OBU can still periodically send beaconInfo $= \text{ID}_j\|\text{ticketID}\|on\|T_L\|\Theta$ for a long time period until all battery energy is used up. In this long period, when the thief drives the stolen vehicle along a road, all pass-by RSUs and OBUs can detect the exceptional beacon status information beaconInfo $= \text{ID}_j\|\text{ticketID}\|on\|T_L\|\Theta$ sent from a running vehicle, as shown in Fig. 1. Then, according to the parking lot's identifier ID_j, all pass-by RSUs and OBUs can report the location of the stolen vehicle to the parking lot. This way, the tracking of the stolen vehicle is achieved.

E. Friendly Parking Information Dissemination

When a driver arrives at a parking lot, if the parking lot has some vacant parking spaces, the driver will immediately enter the parking lot. However, if the parking lot is full, the driver will leave the current parking lot and look for another parking lot. Therefore, it is of special interest if the parking lot can provide friendly parking information to the running vehicles.

Because the field OCC of one parking space record can identify the current space status, the parking lot RSUs can easily calculate the total number of unoccupied parking spaces N_{uoc}. Therefore, before a vehicle enters the parking lot, the RSUs can provide N_{uoc} to facilitate the decision of the driver. Although the statistic N_{uoc} is accurate, it changes with time. Therefore, it is not suitable to simply disseminate N_{uoc} to running vehicles. Instead, the blocking probability $\mathbb{B}$ is a stable statistic, which denotes the probability that a vehicle could be blocked, i.e., the parking lot is full when the vehicle arrives. Therefore, the parking lot's capacity and blocking probability can be disseminated to the vehicles that run on the road by using Algorithm 3 [25].

Algorithm 3: ParkingLotInformationDissemination()

Data: Parking lot information, including the parking lot's capacity and $\mathbb{B}$

Result: Disseminate the parking lot information to the running vehicles as fast as possible

1. **begin**
2. RSUs periodically broadcast the parking lot information to the passing-by vehicles
3. Every time two running vehicles encounter, they exchange the parking lot information that they buffered to provide the minimum message delivery delay
4. **end**

In the following discussion, we describe how the parking lot RSUs calculate the blocking probability $\mathbb{B}$. Based on the past records in the record table, RSUs can get the vehicle-arrival rate by the statistic of T_s and obtain the mean parking time by the statistic of $T_L - T_S$. Assume that an intelligent parking lot near a shopping mall can offer the total c parking spaces. By statistics, the arrival of vehicles follows a Poisson process with a rate of λ vehicles per minute, and the mean parking time is $E(t)$ h. In the following discussion, under the $M/G/c/c$ queue model, we estimate the blocking probability $\mathbb{B}$. Assuming that the probability p_n denotes that there are n vehicles in the parking lot, then the probability p_c that all parking spaces are occupied is of special interest, because the blocking probability $\mathbb{B}$ is equal to p_c. According to the $M/G/c/c$ queue model [26], we can derive that

$$p_n = \frac{\rho^n}{n!} \cdot \left[\sum_{i=0}^{c} \frac{\rho^i}{i!}\right]^{-1}, \qquad \text{for } n = 0, 1, 2, \ldots, c \tag{8}$$

where $\rho = \lambda \cdot E(t)$. Therefore, the blocking probability $\mathbb{B}(c, \rho)$ is given by

$$\mathbb{B}(c, \rho) = p_c = \frac{\rho^c}{c!} \cdot \left[\sum_{i=0}^{c} \frac{\rho^i}{i!}\right]^{-1}. \tag{9}$$

Note that the computation of $\mathbb{B}(c, \rho)$ can become a serious problem when $c!$ is huge. Thus, an efficient recursion algorithm for computing $\mathbb{B}(c, \rho)$ is provided in the Appendix.

Fig. 6 shows that the blocking probability $\mathbb{B}(c, \rho)$ varies with the capability of the parking lot c under the different parameters $(\lambda, E(t))$. In the figure, we can see that the higher $\lambda \cdot E(t)$ is, the higher the blocking probability $\mathbb{B}(c, \rho)$ becomes, and with the increase in the parking lot's capacity c, the blocking probability will decrease. For example, when $\lambda = 6/\text{min}$ and $E(t) = 2.5$ hours, only if the parking lot's capacity $c \geq 900$, the blocking probability is 0. Therefore, with this friendly parking information $(c, \mathbb{B})$, the drivers can conveniently choose their preferred parking lots close to their destinations.

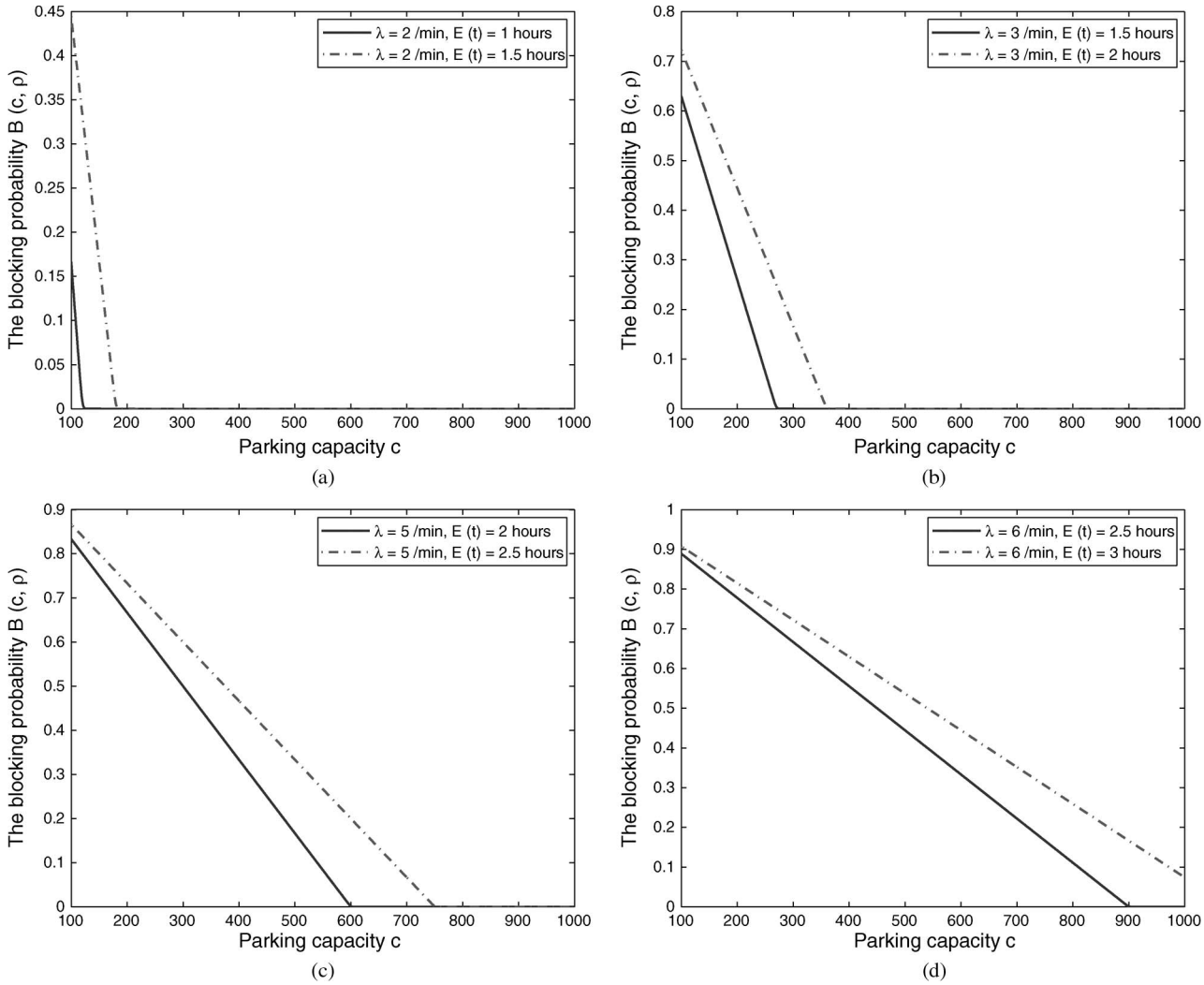


Fig. 6. Blocking probability $\mathbb{B}(c, \rho)$ versus the capability of the parking lot c. (a) Weekday. (b) Weekend. (c) Holiday. (d) Boxing day.

IV. Security Analyses

In this section, we discuss security issues of the proposed intelligent parking scheme, i.e., the security of the ticketKey, conditional privacy preservation of the OBU, and the selfishness issues at the parking lot.

- *Security of the ticketKey*. The security of ticketKey is extremely important for the intelligent parking lot. If the ticketKey could be compromised, then the intelligent antitheft protection does not work. In the proposed scheme, because the ticketKey is encrypted with the ephemeral key $\mathsf{k} = \mathbf{KDF}(k)$, where $k = e(Q, P)^r$, i.e., $C' = \mathbf{Enc}_{\mathsf{k}}(\text{ticketID} \| \text{ticketKey} \| \text{ID}_j \| T)$, only the OBU, with the same ephemeral key k, can recover it. As a result, the ticketKey is privacy preserving.
- *Conditional privacy preservation of the OBU*. Because the OBU uses the pseduo-ID PID_i during its communication with parking lot RSUs, the real identity ID_i is protected. At the same time, with the help of TA, the parking lot RSUs can reveal the real identity ID_i from PID_i, because TA has the ability to decrypt $\text{PID}_i = \mathbf{Enc}_{s_1}(\text{ID}_i \| r_i)$ by using the secret key s_1. Therefore, the conditional privacy preservation of the OBU is achieved. Note that, if the OBU only holds one pseduo-ID PID_i, the privacy preservation is weak. The reason is that, although the OBU's real identity is not exposed, an adversary can reveal the OBU's location privacy by linking different parking lots with the same pseduo-ID PID_i. Therefore, to achieve the location privacy, the OBU should request many pseduo-IDs from TA and use different pseduo-IDs at different parking lots [9]. Although multiple valid pseudo-IDs could incur the Sybil attack [27], i.e., a vehicle claims three spots next to each other using three different pseudo-IDs if the ε value is large enough, due to the conditional privacy preservation, the TA can reveal the real identity from the pseudo-ID, and thus, the Sybil attack can be postdetected.
- *Selfishness issues*. In a free parking lot, when some drivers look for parking spaces, they may behave selfishly. For example, for their own sakes, they may claim that some vacant parking spaces are occupied or some occupied parking spaces are open to lure other drivers there [28]. However, in the proposed intelligent parking scheme, because the whole parking lot is under the surveillance of the three parking lot RSUs, once the selfish behaviors take place, the RSUs can immediately detect them. Therefore,

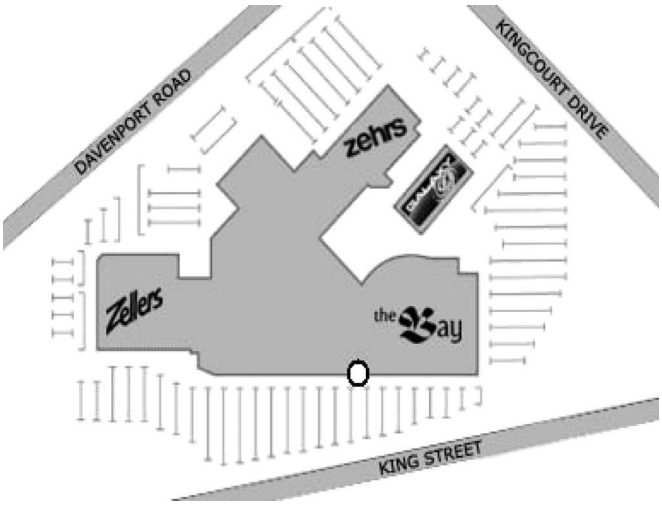


Fig. 7. Conestoga Mall parking lot.

the selfishness issues do not exist in the proposed intelligent parking scheme.

V. Performance Evaluation

In this section, we study the performance of the proposed intelligent parking scheme, including real-time parking navigation and friendly parking information dissemination, by using two custom simulators built in Java.

A. Simulations on Real-Time Parking Navigation

In this section, the first custom simulator is conducted to verify the efficiency of the real-time parking navigation, where the comparison is made with an ordinary parking lot with no parking guidance system in the aspect of the STD for an available parking space, which can be defined as the time period between the instant when a driver enters a parking lot and the instant when he/she finds a desired parking space.

1) Simulation Environment: The large parking lot adopted throughout our simulation is the parking lot at the Conestoga Mall, as shown in Fig. 7, which is a major shopping mall in Waterloo, ON, Canada [29]. The place marked with a white circle "○" is the main entrance of the mall. Conestoga Mall has plenty of available spaces along the perimeter with more than 1000 parking stalls, and there are three different entrances to the parking lot. For simplicity, we do not consider special services for the parking lot, e.g., handicapped parking, reserved parking, and reserved bus lanes.

In the parking lot, there are two types of drivers: 1) drivers who are always looking for a parking space close to the main entrance of a shopping mall or other amenities, i.e., prime parking spaces in the parking lot, and 2) drivers who are looking for any available parking and park in the first empty space that they see in the lot. The mobility model throughout our simulation is explained as follows. When a driver enters the parking lot, with a probability of p, the driver is a type-1 driver. Otherwise, the driver is a type-2 driver, with a probability of $1-p$. Each vehicle is driven with a randomly fluctuated speed in a range of 10% centered at the parking lot speed limit. As a type-1 driver, the driver will look for a parking spot close to the main entrance of the mall and keep circling around until he/she finds the nearest legal parking space to park. For a type-2 driver, instead, he/she just parks anywhere he/she can. When the driver enters an intersection within the parking lot, he/she will equally proceed with a random direction, except the incoming direction. The simulation configurations are listed in Table III.

TABLE III
Simulation Configuration

Parameter	Value
Parking spaces	1000
Parking lot entrances	3
The probability of type 1 driver	$p = [10\%, 30\%, 50\%, 80\%]$
The probability of type 2 driver	$1-p$
Speed limit in parking lot	10 km/h
Vehicle arrival rate at each entrance	6 vehicles/minutes

2) Simulation Results: First, we investigate the impact of the occupancy factor of the parking lot on the STD. We test, respectively, in a parking lot with intelligent navigation, without intelligent navigation in a sunny or foggy day, where the sunny day represents good visibility (i.e., a driver can see any parking spot within a 20-m radius) and reflects earlier discovery of an available parking space, and the foggy day represents bad visibility (i.e., a driver can only observe the parking spots within a 5-m radius). For each case, we test ten times, and the average STD over all these experiments is reported. As shown in Fig. 8, for a parking lot without an intelligent navigation system in a sunny or foggy day, with the increase in the occupancy factor, the STD for an available parking space significantly increases after the occupancy factor reaches 50%. In particular, on a foggy day, when the occupancy factor is above 80%, the time that a driver spends to find an available parking space is very long, (i.e., $>$ 2 min), and it becomes intolerable to most of drivers. However, with the help of the proposed intelligent parking system, the STD for an available parking space becomes low. Furthermore, the weather condition has no impact on the intelligent parking.

Another interesting observation, as shown in Fig. 9, is that, when the parameter $p = 80\%$, the increase in parking space does not improve the STD very much, particularly after the occupancy factor of parking lot becomes large. The possible reason is that 80% of the drivers still prefer to choose a parking spot close to the main entrance, even with the high occupancy factor, and this preference will cause the long STD for these drivers. Comparing the STDs in Fig. 8(a)–(d), this interesting observation can be also confirmed, i.e., the more the type-1 drivers (a larger p), the longer the search time.

Furthermore, due to the friendly parking information dissemination, another benefit can be gained from the proposed intelligent parking scheme. When the parking lot is full, any approaching driver can be notified in time and then go to find alternative parking. However, for a traditional parking lot, it may take a while for the driver to figure out that the parking lot is full, which results in wasting gasoline and time.

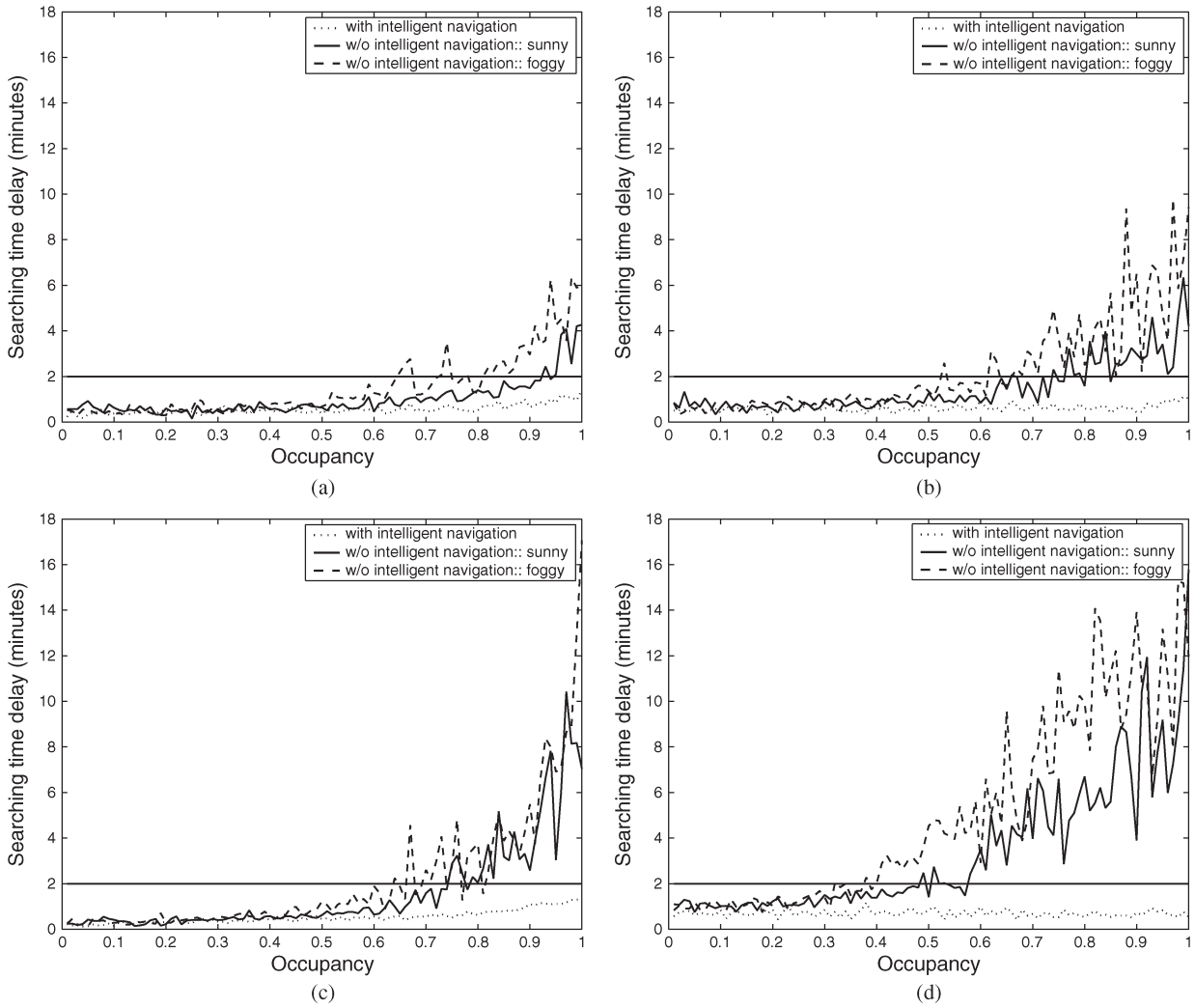


Fig. 8. Occupancy factor of parking lot versus the STD. (a) $p = 10\%$. (b) $p = 30\%$. (c) $p = 50\%$. (d) $p = 80\%$.

B. Simulations on Parking Information Dissemination

In this section, we use the second custom simulator to evaluate the performance of the friendly parking information dissemination.

1) Simulation Settings: In the simulations, we assume that an efficient collision-avoidance MAC protocol is employed in the lower layer, and a total of n vehicles with a transmission radius of R_v m are first uniformly deployed in an area of 3000 m $\times$ 3000 m, as shown in Fig. 10. Each vehicle follows the *shortest path map based movement* routing and moves around within the area with the average velocity v. Concretely, each vehicle first randomly chooses a destination in the area and gets there using the shortest route. After reaching the destination, with zero pause time, the vehicle randomly chooses a new destination, and so on. In the area, there are two smart parking lots A and B, where A is located at the center, and B is at the corner. Every 5 min, A and B will broadcast their parking information to vehicles that are passing by.

In the simulations, the performance metric is coverage ratio, which is the fraction of vehicles that have received the parking information within a given time period. This metric shows the ability of a strategy to disseminate the parking information to the running vehicles within a specified period of time. We list the detailed simulation parameter settings in Table IV and test the experiments with different numbers of vehicles, different velocity levels, and different transmission ranges. For each case, 50 networks are randomly generated, and the average coverage ratio is reported.

2) Simulation Results: In Fig. 11, we compare the coverage ratio versus a specified time period under different numbers of vehicles, with $\mathrm{R}_r = 500$ m and $\mathrm{R}_v = 100$ m. In the figure, we can see that, with the increase in the time period, the coverage ratio increases. For the same number of vehicles, the higher the velocity v is, the higher the coverage ratio in the same time period becomes. Comparing the coverage ratios in Fig. 8(a)–(d), we can also observe that the high number of vehicles can achieve higher coverage ratio. The reason is that, when the velocity and/or the number of vehicles increase, a vehicle can meet more vehicles at the same time period. Then, the coverage ratio increases. In addition, we can observe that the coverage ratio of parking lot A at the center is higher than that of parking lot B at the corner. The reason is that, when parking information

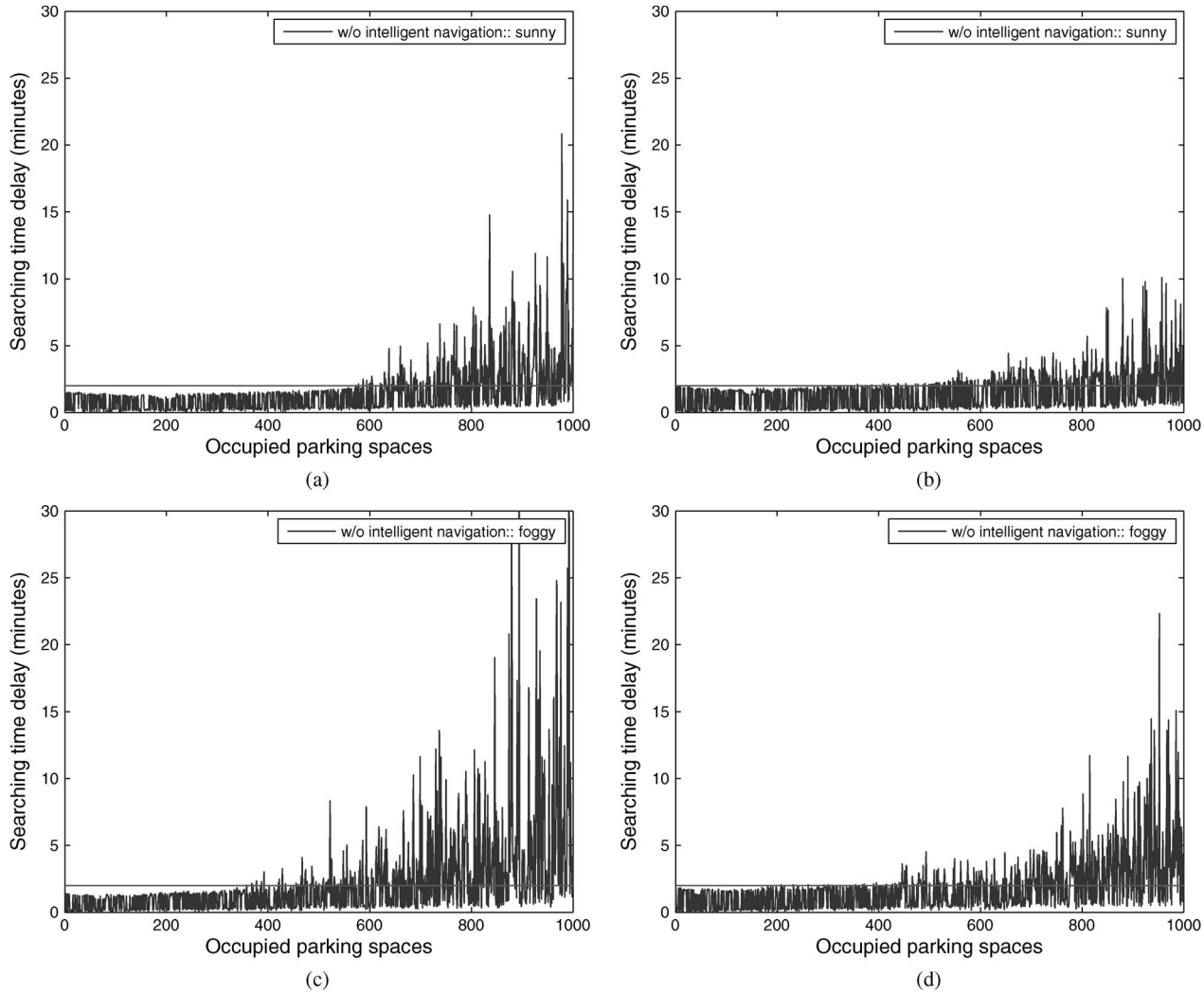


Fig. 9. Comparison of the STD with different parking capacity levels when $p = 80\%$. (a) Parking capacity with 1000. (b) Parking capacity with 1500. (c) Parking capacity with 1000. (d) Parking capacity with 1500.

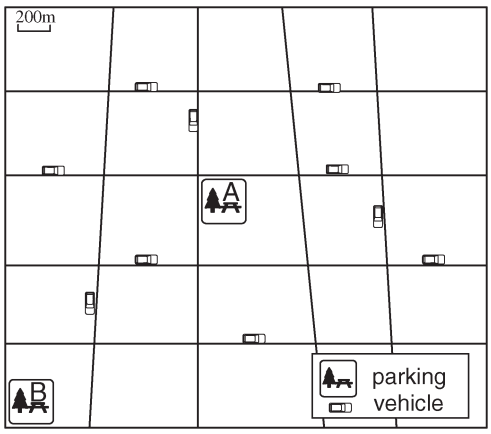


Fig. 10. Area considered in the simulation.

is broadcast by parking lot A at the center of the area, it can be received by more running vehicles and then quickly disseminated by these running vehicles.

We also show the coverage ratio with the transmission ranges $\mathrm{R}_r = 1000$ m and $\mathrm{R}_v = 300$ m in Fig. 12. Comparing the coverage ratios in Figs. 11 and 12, the coverage ratios in Fig. 12 are obviously higher than those in Fig. 11. The reason is that the larger the transmission ranges R_r, R_v, the more likely that the parking information could be disseminated to more vehicles in the same time period. As a result, the coverage ratio is high.

TABLE IV
SIMULATION SETTINGS

Parameter	Value
Area	3000 m $\times$ 3000 m
Location of A / B	at the center / at the corner
Transmission range of RSUs	$\mathrm{R}_r = [500\text{ m}, 1000\text{ m}]$
Number of vehicles	$n = [20, 40, 80, 120]$
Velocity of vehicles	$v = [40\text{ km/h}, 60\text{ km/h}]$
Transmission range of vehicle	$\mathrm{R}_v = [100\text{ m}, 300\text{ m}]$

VI. RELATED WORK

Recently, several works related to the parking lots have appeared in [25], [28], [30], and [31].

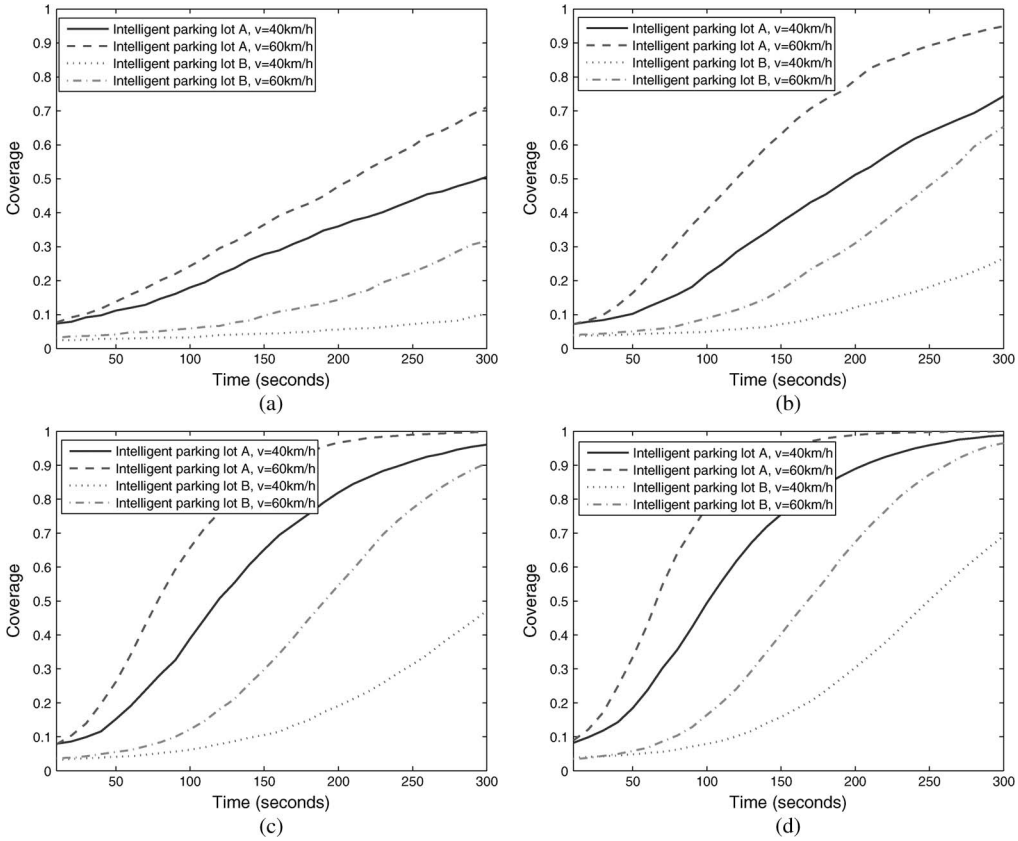


Fig. 11. Coverage ratio versus specified time period under different numbers of vehicles, with $\mathrm{R}_r = 500$ m and $\mathrm{R}_v = 100$ m. (a) $n = 20$. (b) $n = 40$. (c) $n = 80$. (d) $n = 120$.

In [28], Panayappan *et al.* provide a VANET-based approach for parking-space availability. In the approach, the parking lots are managed by RSUs, and these RSUs can provide open parking-space information to the drivers, which is very similar to the proposed intelligent parking scheme. In addition, the approach also provides security architecture to solve possible security vulnerabilities. However, the approach does not provide real-time parking navigation in large parking lots or any antitheft protection function [28]. In [31], Song *et al.* present a sensor-network-based vehicle antitheft system. In the system, sensors in the vehicles that are parked at the same parking lot first form a sensor network and then monitor and identify possible vehicle thefts by detecting unauthorized vehicle movements. However, the security and privacy issues in the system should be further explored [31]. In [25], based on the VANET techniques, Caliskan *et al.* propose a topology-independent scalable information-dissemination algorithm to discover free parking places spaces. With the friendly parking lot information disseminated by the parking automats and intervehicle broadcast, the drivers can conveniently find their preferred free parking lot.

Table V compares the achieved goals of the aforementioned three schemes and the proposed intelligent parking scheme. Although the proposed intelligent parking scheme requires three or more RSUs for a given parking lot with tight time synchronization to all radio-based triangulation, in the table, we can see that it is more practical when the VANET reaches its flourish stage.

VII. Conclusion

In this paper, we have proposed a new VANET-based intelligent parking scheme for large parking lots. With the proposed scheme, RSUs that are installed across a parking lot can surveil the whole parking lot and provide the following three convenient services to drivers: 1) real-time parking navigation; 2) intelligent antitheft protection; and 3) friendly parking information dissemination. In addition, the proposed scheme provides conditional privacy preservation for OBUs (drivers). Extensive simulations have also been conducted to demonstrate that the proposed scheme can efficiently reduce the STD for an available parking space and subsequently save fuel and the driver's time. Because the VANET technology will incrementally be deployed, it is expected that the application of the intelligent parking will also be incrementally implemented. In our future work, we will develop such a prototype system to further evaluate its effectiveness and workability and explore more practical issues related to the intelligent parking lots.

Appendix

We will show how we can compute $\mathbb{B}(c, \rho)$ for large c!. According to (9), we have

$$\mathbb{B}(c, \rho) = \frac{\rho^c / c!}{\rho^c / c! + \sum_{i=0}^{c-1} \rho^i / i!} \tag{10}$$

$$\mathbb{B}(c-1, \rho) = \frac{\rho^{c-1} / (c-1)!}{\sum_{i=0}^{c-1} \rho^i / i!}. \tag{11}$$

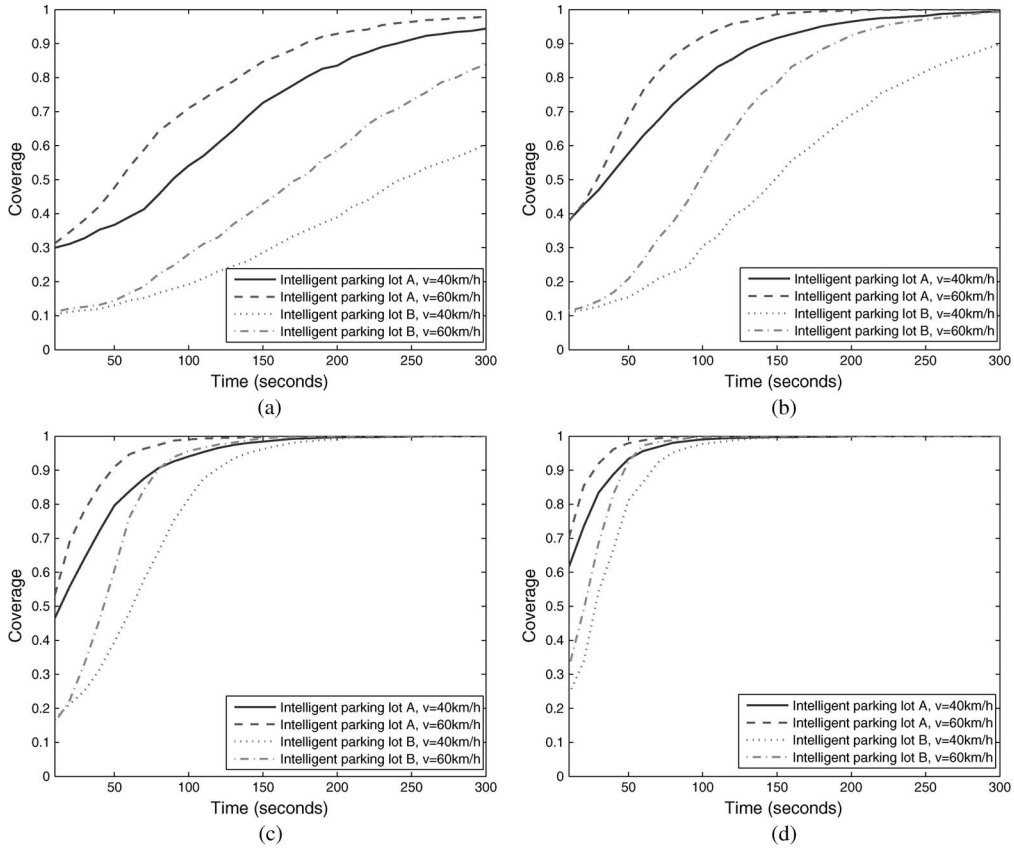


Fig. 12. Coverage ratio versus specified time period under different numbers of vehicles, with $\mathrm{R}_r = 1000$ m and $\mathrm{R}_v = 300$ m. (a) $n = 20$. (b) $n = 40$. (c) $n = 80$. (d) $n = 120$.

TABLE V
COMPARISON OF FOUR SMART PARKING SCHEMES

Goals	Scheme [25]	Scheme [28]	Scheme [31]	Proposed
real-time parking navigation	×	×	×	✓
intelligent anti-theft protection	×	×	✓	✓
parking information dissemination	✓	✓	×	✓

Then, based on (10) and (11), we have

$$\mathbb{B}(c,\rho) = \frac{\rho/c}{\rho/c + 1/\mathbb{B}(c-1,\rho)} = \frac{\rho\mathbb{B}(c-1,\rho)}{c+\rho\mathbb{B}(c-1,\rho)}. \quad (12)$$

Because $\mathbb{B}(0,\rho) = 1$, we can apply the relation in (12) to subsequently compute $\mathbb{B}(i,\rho)$, for $i = 1, 2, \ldots, c$. In the end, we can obtain the value of $\mathbb{B}(c,\rho)$. ■

REFERENCES

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A new VANET-based smart parking scheme for large parking lots," in *Proc. INFOCOM*, Rio de Janeiro, Brazil, Apr. 2009, pp. 1413–1421.

[2] V. Tang, Y. Zheng, and J. Cao, "An intelligent car park management system based on wireless sensor networks," in *Proc. 1st Int. Symp. Pervasive Comput. Appl.*, Urumchi, China, Aug. 2006, pp. 65–70.

[3] J. Chinrungrueng, U. Sunantachaikul, and S. Triamlumlerd, "Smart parking: An application of optical wireless sensor network," in *Proc. SAINTW*, Hiroshima, Japan, Jan. 2007, pp. 30–39.

[4] Y. Bi, L. Sun, H. Zhu, T. Yan, and Z. Luo, "A parking management system based on wireless sensor network," *Acta Autom. Sin.*, vol. 32, no. 6, pp. 38–45, Nov. 2006.

[5] Y. Peng, Z. Abichar, and J. M. Chang, "Roadside-aided routing (RAR) in vehicular networks," in *Proc. IEEE ICC*, Istanbul, Turkey, Jun. 2006, vol. 8, pp. 3602–3607.

[6] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy*, vol. 2, no. 3, pp. 49–55, May 2004.

[7] M. Lott, R. Halfmann, E. Schultz, and M. Radimirsch, "Medium access and radio resource management for ad hoc networks based on UTRA TD," in *Proc. ACM MobiHoc*, Oct. 2001, pp. 76–86.

[8] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Medium access control protocol design for vehicle–vehicle safety messages," *IEEE Trans. Veh. Technol.*, vol. 56, no. 2, pp. 499–518, Mar. 2007.

[9] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[10] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[11] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. INFOCOM*, San Diego, CA, Mar. 2010, pp. 1–9.

[12] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3357–3368, Nov. 2008.

[13] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. INFOCOM*, Phoenix, AZ, Apr. 2008, pp. 1229–1237.

[14] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. INFOCOM*, Phoenix, AZ, Apr. 2008, pp. 246–250.

[15] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

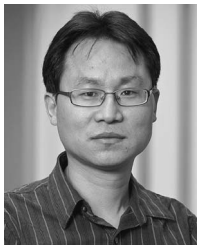
[16] X. Lin, X. Sun, X. Wang, C. Zhang, P. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4987–4998, Dec. 2008.

[17] H. Zhu, R. Lu, X. Lin, and X. Shen, "Security in service-oriented vehicular networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 16–22, Aug. 2009.

[18] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1454–1466, Mar. 2009.
[19] IEEE Std. P802.11p: Wireless Access in Vehicular Environments (WAVE), IEEE Comput. Soc., Washington, DC, T. Group, draft standard ed., 2006.
[20] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.
[21] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Implementation, performance, and research challenges," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 110–118, Nov. 2008.
[22] L. Cong and W. Zhuang, "Hybrid TDOA/AOA mobile user location for wideband CDMA cellular systems," *IEEE Trans. Wireless Commun.*, vol. 1, no. 3, pp. 439–447, Jul. 2002.
[23] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Adv. Cryptology—CRYPTO*, vol. 2139, *LNCS*, New York, 2001, pp. 213–229.
[24] W. Mao, *Modern Cryptography: Theory and Practice*. Englewood Cliffs, NJ: Prentice-Hall PTR, 2003.
[25] M. Caliskan, D. Graupner, and M. Mauve, "Decentralized discovery of free parking places," in *Proc. 3rd ACM VANET*, Los Angeles, CA, Sep. 2006, pp. 30–39.
[26] J. W. Cohen, *On Regenerative Processes in Queuing Theory*. Berlin, Germany: Springer-Verlag, 1976.
[27] T. Zhou, R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of Sybil attacks in vehicular ad hoc networks," in *Proc. 4th MobiQuitous*, Washington, DC, 2007, pp. 1–8.
[28] R. Panayappan, J. Trivedi, A. Studer, and A. Perrig, "VANET-based approach for parking space availability," in *Proc. 4th ACM VANET*, Montrèal, QC, Canada, Sep. 2007, vol. 8, pp. 75–76.
[29] *Conestoga Mall*. [Online]. Available: http://conestoga.shopping.ca/
[30] M. Caliskan, A. Barthels, B. Scheuermann, and M. Mauve, "Predicting parking lot occupancy in vehicular ad hoc networks," in *Proc. 65th IEEE VTC—Spring*, Dublin, Ireland, Apr. 2007, pp. 277–281.
[31] H. Song, S. Zhu, and G. Cao, "SVATS: A sensor-network-based vehicle antitheft system," in *Proc. INFOCOM*, Phoenix, AZ, Apr. 2008, pp. 2128–2136.

Rongxing Lu (S'09) is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

He is currently a Research Assistant with the Broadband Communications Research Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.



Xiaodong Lin (S'07–M'09) received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008.

He is currently an Assistant Professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON. His research interests include wireless network security, applied cryptography, computer forensics, and software security.

Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada Canada Graduate Scholarships–Doctoral and the Best Paper Award at the 2009 IEEE International Conference on Computer Communications and Networks, the Outstanding Achievement in Graduate Studies Award in 2008, and the Best Paper Award at the 2007 IEEE International Conference on Communications Computer and Communications Security Symposium.

Haojin Zhu (M'09) received the B.Sc. degree in computer science from Wuhan University, Wuhan, China, in 2002, the M.Sc. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2005, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2009.

He is currently an Assistant Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests include wireless network security, wireless communication, and mobile computing.

Dr. Zhu was a recipient of the Best Paper Award at the 2007 IEEE International Communications Conference Computer and Communications Security Symposium and the Third International Conference on Communications and Networking in China Wireless Communication Symposium.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree in electrical engineering from Dalian Maritime University, Dalian, China, in 1982 and the M.Sc. and Ph.D. degrees in electrical engineering from Rutgers University, Camden, NJ, in 1987 and 1990, respectively.

He is currently a Professor and the University Research Chair with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He serves as the Editor-in-Chief for *Peer-to-Peer Networking and Application* and as an Associate Editor for *Computer Networks* and *ACM/Wireless Networks*. He has also served as a Guest Editor for *ACM Mobile Networks and Applications*. His research is focused on resource management in interconnected wireless/wired networks, ultra-wideband wireless communications networks, wireless network security, wireless body area networks, and vehicular ad hoc and sensor networks. He is a coauthor of three books and has published more than 400 papers and book chapters about wireless communications and networks, control, and filtering.

Dr. Shen is a Registered Professional Engineer in Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society. He served as the Technical Program Committee Chair of the 2010 IEEE Vehicular Technology Conference, the Tutorial Chair for the 2008 IEEE International Communications Conference, the Technical Program Committee Chair of the 2007 IEEE Global Telecommunications Conference, a General Cochair for the 2007 Second International Conference on Communications and Networking in China and 2006 Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks, and the Founding Chair for the IEEE Communications Society Technical Committee on Peer-to-Peer Communications and Networking. He has also served as a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and as an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He has also served as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS, and *IEEE Communications Magazine*. He was the recipient of the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award from the University of Waterloo in 2004 and 2008, the Premier's Research Excellence Award from the Province of Ontario, in 2003, and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo in 2002 and 2007.