This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2009 proceedings.

# SPARK: A New VANET-based Smart Parking Scheme for Large Parking Lots

Rongxing Lu[†], Xiaodong Lin[‡], Haojin Zhu[†], and Xuemin (Sherman) Shen[†]
[†]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
[‡]Faculty of Business and Information Technology, University of Ontario Institute of Technology,
Oshawa, Ontario, Canada L1H 7K4
Email: {rxlu, h9zhu, xshen}@bbcr.uwaterloo.ca; Xiaodong.Lin@uoit.ca

***Abstract*— Searching for a vacant parking space in a congested area or a large parking lot and preventing auto theft are major concerns to our daily lives. In this paper, we propose a new smart parking scheme for large parking lots through vehicular communication. The proposed scheme can provide the drivers with real-time parking navigation service, intelligent anti-theft protection, and friendly parking information dissemination. Performance analysis via extensive simulations demonstrates its efficiency and practicality.**

***Keywords*— Vehicular communications; smart parking; navigation; anti-theft; information dissemination; security & privacy**

## I. Introduction

Finding a vacant parking space in a congested area or a large parking lot, especially, in peak hours, is always time-consuming and frustrating to drivers. It is common for drivers to keep circling a parking lot and look for a vacant parking space. To minimize hassle and inconvenience to the drivers, many parking guidance systems have been developed over the past decade [1]–[3], where the system provides accurate, real-time car park space availability to the drivers looking for parking spaces and then guides them to the available spaces by dynamically updated guide signs. The current parking guidance systems obtain the availability of parking spaces using the sensors installed across the whole parking lot. However, deploying sensors in a large parking lot can be very expensive. Furthermore, the sensors can become inaccurate and would stop functioning easily when time passes. Therefore, it is highly desired to have a reliable and cost effective way to track available parking spaces and guide drivers to the available parking spaces. Besides searching for available parking spaces, vehicle theft in large parking lots also has become a serious concern facing our lives. For example, statistics show that there have been over 170,000 vehicles stolen each year in Canada.

Recently, Vehicle Ad Hoc Networks (VANETs), as shown in Fig. 1, have been received particular attention both in industrial and academic levels [4]–[7]. With the advance and wide deployment of wireless communication technologies, many major car manufactories and telecommunication industries gear up to equip each car with the On Board Unit (OBU) communication device, which allows different cars to communicate with each other as well as roadside infrastructure, i.e., Roadside Units (RSUs), in order to improve not only road safety but also better driving experience [8], [10]. Therefore, it becomes possible to track the parking space occupancy, guide drivers to the empty parking spaces, and provide anti-theft protection in large parking lots through vehicular communications.

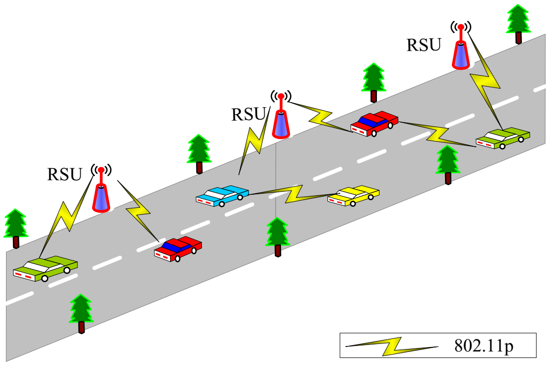


Fig. 1. Vehicular ad hoc network

In this paper, we are committed to developing a new VANET-based Smart PARKing (SPARK) scheme to provide drivers with convenient parking services in large parking lots. The SPARK scheme is characterized by employing parking lot RSUs to surveil and manage the whole parking lot using VANET communication technology. Specifically, the SPARK scheme makes the following contributions.

Firstly, the SPARK scheme can provide real-time parking navigation service to drivers in large parking lots. With the real-time parking navigation, the drivers can find the vacant parking space quickly. Therefore, the gasoline and time wasted in search of vacant parking space can be reduced. To the best of our knowledge, this is the first such effort in the context of VANET-based real-time parking navigation.

Secondly, the SPARK scheme provides VANET-based intelligent anti-theft protection service. With this service, all vehicles parked at the smart parking lot are guarded by the parking lot's RSUs. Once a vehicle is illegally leaving the parking lot, the RSUs can quickly detect the anomaly.

Thirdly, the SPARK scheme can provide friendly parking information dissemination service to the moving vehicles. With these friendly parking information, the drivers can conveniently and quickly choose their preferred parking lots close to their destinations.

978-1-4244-3513-5/09/$25.00 ©2009 IEEE

Finally, the SPARK scheme can also ensure the conditional privacy preservation of the OBUs, which is regarded as the basic security requirement in VANET communications [9]–[13].

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 SPARK scheme, followed by the security and performance analyses via simulations in Section IV and Section 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 smart parking lot by modeling the system and identifying the design goal.

### A. System Model

The system model consists of a trusted authority (TA), OBUs equipped on the vehicles, stationary parking lot RSUs and a large number of parking spaces.

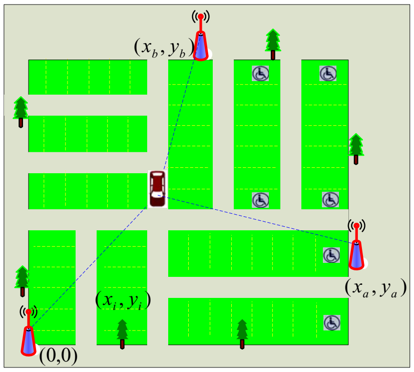


Fig. 2. Parking lot model under consideration

- TA is a trust and powerful entity, whose responsibility is in charge of the registration of both OBUs and the parking lot RSUs.
- OBUs are installed on the vehicles, which can communicate with each other and RSUs for achieving useful information, i.e., traffic information and parking lot information. Each OBU has an unique identifier $\mathrm{ID}_i$. In order to protect the privacy of the OBU, when an OBU with $\mathrm{ID}_i$ registers itself to TA, TA first converts the real identifier $\mathrm{ID}_i$ into a pseudo-ID $\mathrm{PID}_i$, and generates a private key $sk_i$ corresponding to the pseudo-ID of the OBU. When an OBU enters a smart parking lot, it will receive a pair of ticket ID and respective ticket key, which is only known to the driver.
- RSUs are important components for smart parking lots. As shown in Fig. 2[1], three RSUs, i.e., $\mathrm{RSU}_0$ at position $(0,0)$, $\mathrm{RSU}_a$ at position $(x_a, y_a)$ and $\mathrm{RSU}_b$ 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 surveillance of the three RSUs. After the smart parking lot with identifier $\mathrm{ID}_j$ is inspected by TA, TA will generate a private key $sk_j$ corresponding to the identifier $\mathrm{ID}_j$ and distribute the private key $sk_j$ to these parking lot RSUs.

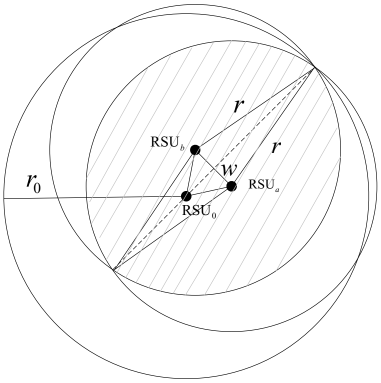


Fig. 3. Overlapped surveillance region $\mathbb{S}$ of three parking lot RSUs

Fig. 3 shows one placement of RSUs in a smart parking lot, where the distance between $\mathrm{RSU}_a$ and $\mathrm{RSU}_b$ is $w$, and the transmission ranges of $\mathrm{RSU}_a$, $\mathrm{RSU}_b$ and $\mathrm{RSU}_0$ are $r$, $r$ and $r_0 = \sqrt{r^2 - (\frac{w}{2})^2} + w$, 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, Fig. 4 shows the surveillance region $\mathbb{S}$ varies with the transmission range $r$, where $100 \le r \le 500$ m, which belongs to the transmission range recommended in the IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) standard [14]. From the figure we can see, when the transmission range $r$ expands, the surveillance region $\mathbb{S}$ will increase quickly. For example, when the transmission range $r = 300$ m, $\mathbb{S}$ can reach $252,800$ $\mathrm{m}^2$, which is large enough to surveil the practical parking lots.

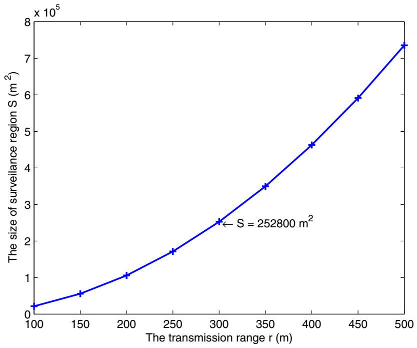


Fig. 4. The size of surveillance region v.s. different transmission range

- Parking space is a spatio-temporal resource recorded by the RSUs in a smart parking lot. Each parking space record, as shown in Table I, has the following attributes.

[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.

TABLE I
PARKING SPACE RECORD

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| POS | RES | OCC | PID | TID | TKEY | ST | LUT |

- 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, $\mathsf{RES} = 1$, otherwise, $\mathsf{RES} = 0$.
- Occupancy (OCC): The field denotes the occupancy status of the parking space. If the parking space is occupied, $\mathsf{OCC} = 1$. Else if the parking space is vacant, $\mathsf{OCC} = 0$.
- 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.

In a smart parking lot, since all parking space records are stored at the parking lot RSUs, the parking lot's RSUs can conveniently manage the whole parking lot by using these records.

### B. Design Goal

Before describing our design goal for smart parking scheme, we first make some necessary assumptions in our model.

- *Assumption 1.* TA is fully trusted by all OBUs and RSUs.
- *Assumption 2.* Each OBU is a tamper-proof device, fixed on the vehicle. Before a driver turns on the OBU, he/she must provide the password for authentication [15]. Therefore, it is reasonable to assume an adversary can't 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: *active* and *sleep*. In the *active* mode, the OBU consumes the vehicle power and unceasingly receives/sends the messages; while in the *sleep* mode, the OBU's energy consumption is low, the OBU can only use its inner battery to send beacon messages for a long period.
- *Assumption 3.* The three parking lot RSUs are expensive, 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 such as time of arrival (TOA) or time differences of arrival (TDOA) [16]. In addition, the three RSUs cooperatively and synchronically manage the whole parking lot.

Our design goal is to develop a smart parking scheme for large parking lots. Specifically, the smart parking scheme will achieve the following desirable requirements: real-time parking navigation, intelligent anti-theft protection, friendly parking information dissemination and conditional privacy preservation.

- *Real-time parking navigation.* In the smart 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 anti-theft protection.* In the smart 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, a mechanism to track the stolen vehicle should be provided.
- *Friendly parking information dissemination.* In the smart 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 in a smart parking lot, its real identifier $\mathrm{ID}_i$ should be kept secret. However, once an exceptional event occurs, the RSUs can learn the OBU's real identifier $\mathrm{ID}_i$ with the help of TA.

## III. PROPOSED SPARK SCHEME

In this section, we present the proposed VANET-based SPARK scheme. The SPARK scheme consists of four parts: system setting, real-time parking navigation, intelligent anti-theft protection, and friendly parking information dissemination. Before describing them, we first review the bilinear pairing technique [17], which serves as the basis of the proposed SPARK 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 $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, which satisfies the following three properties: 1) bilinear: $e(aP, bP) = e(P, P)^{ab}$, where $P, Q \in \mathbb{G}$ and $a, b \in \mathbb{Z}_q^*$; 2) non-degenerate: there exist $P, Q \in \mathbb{G}$ such that $e(P, Q) \neq 1_{\mathbb{G}_T}$; and 3) computability: there exists an efficient algorithm to compute $e(P, Q)$ 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 elliptic curve can give a good implementation of the admissible bilinear pairing [17]. A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter $k$ as input and outputs a 5-tuple $(q, \mathbb{G}, \mathbb{G}_T, e, P)$ 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 $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ and a generator $P$ of $\mathbb{G}$.

*Bilinear Diffie-Hellman Problem.* Let $(q, \mathbb{G}, \mathbb{G}_T, e, P)$ be a 5-tuple generated by $\mathcal{G}en(k)$. Given $aP, bP, cP \in \mathbb{G}$ with unknown $a$, $b$, $c \in \mathbb{Z}_q^*$, it is hard to compute $e(P,P)^{abc}$ [17].

### 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 5-tuple $(q, \mathbb{G}, \mathbb{G}_T, e, P)$ by running $\mathcal{G}en(k)$. Then, TA chooses a random number $s \in \mathbb{Z}_q^*$ as a *master key*, and computes the corresponding system public key $P_{pub} = sP$. Let $H, h$ be two secure cryptographic hash functions, where $H : \{0,1\}^* \rightarrow \mathbb{G}$ and $h : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, and $\mathbf{Enc}()$ is a secure symmetric encryption algorithm [18]. Then, the system parameters *params* are established, which include $\{q, \mathbb{G}, \mathbb{G}_T, e, P, P_{pub}, H, h, \mathbf{Enc}_k()\}$.

When an OBU with identifier ID$_i$ registers itself to the system, TA first checks its validity. If the identifier ID$_i$ passes the checking, TA executes the following two steps.

*Step 1.* Use the *master key* $s$ to encrypt the real identifer ID$_i$ into a pseudo-ID $\text{PID}_i = \mathbf{Enc}_s(\text{ID}_i)$. In procession of the pseudo-ID PID$_i$, the OBU can hide its real identity ID$_i$ to achieve identity privacy.

*Step 2.* Generate the private key of the OBU as $sk_i = sH(\text{PID}_i)$ and send $(\text{PID}_i, sk_i)$ back to the OBU via a secure channel.

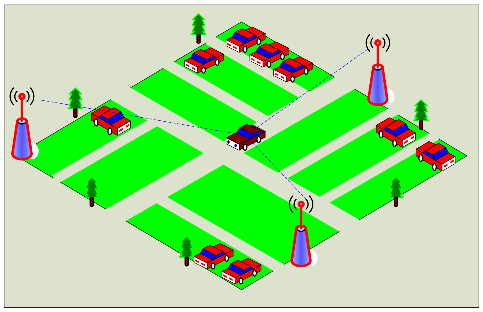


Fig. 5. A typical smart parking lot

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 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 surveillance of these three RSUs, as shown in Fig. 5. After TA inspects the parking lot, TA generates the private key $sk_j = sH(\text{ID}_j)$ and stores the same private keys $sk_j$ into the three RSUs. With these settings, a large smart parking lot is established.

### C. Real-time Parking Navigation

When a vehicle equipped with OBU ID$_i$ is ready to enter a smart 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. Fig. 6 shows the communication between the OBU and the parking lot RSUs, and the detailed protocol steps are described as follows.

OBU with PID$_i$ RSUs with ID$_j$

*1)* $T, \Delta = h(T||sk)$

*2)* $M_1 = \text{PID}_i||T||\Delta, C_1 = \mathcal{IBE}_{\text{ID}_j}(M_1)$

$$\xrightarrow{\quad C_1 \quad}$$

*3)* $T', C_1 \rightarrow M_1 = \text{PID}_i||T||\Delta$

$|T' - T| \overset{?}{\leq} \Delta T, \Delta \overset{?}{=} h(T||sk)$

*4)* $\langle \text{ticketID}, \text{ticketKey} \rangle, T, \Delta' = h(\text{ticketID}||\text{ticketKey}||T||sk)$

$M_2 = \text{ticketID}||\text{ticketKey}||\text{ID}_j||T||\Delta', C_2 = \mathcal{IBE}_{\text{PID}_i}(M_2)$

$$\xleftarrow{\quad C_2 \quad}$$

*5)* $T', C_2 \rightarrow M_2 = \text{ticketID}||\text{ticketKey}||\text{ID}_j||T||\Delta'$

$|T' - T| \overset{?}{\leq} \Delta T, \Delta' \overset{?}{=} h(\text{ticketID}||\text{ticketKey}||T||sk)$

accept $\langle \text{ticketID}, \text{ticketKey} \rangle$

Fig. 6. Communication between OBU and parking lot RSUs to get ticket ID and ticket Key.

*Step 1.* The OBU gains the current timestamp $T$, and computes the authentication information $\Delta = h(T||sk)$, where $sk = e(sk_i, H(\text{ID}_j)) = e(H(\text{PID}_i), H(\text{ID}_j))^s$ is the static key shared between OBU and the parking lot.

*Step 2.* The OBU formats the information $\text{PID}_i, T, \Delta$ as the message $M_1 = \text{PID}_i||T||\Delta$, uses the identity-based encryption algorithm $\mathcal{IBE}$ [17] to encrypt it into $C_1 = \mathcal{IBE}_{\text{ID}_j}(M_1)$, and then sends $C_1$ to the RSUs.

*Step 3.* On receiving $C_1$ at timestamp $T'$, one RSU decrypts $C_1$ with the private key $sk_j$ and parses the result $M_1$ into $\text{PID}_i, T, \Delta$. Then, the RSU checks $|T' - T| \leq \Delta T$, where $\Delta T$ is the expected valid time interval for transmission delay. If it holds, the RSU proceeds the next operation, and stops otherwise (since it could be a replaying attack). Based on the PID$_i$, the RSU also computes the static key $sk = e(H(\text{PID}_i), sk_j) = e(H(\text{PID}_i), H(\text{ID}_j))^s$ and checks whether $\Delta = h(T||sk)$. If it does hold, the RSU accepts the message $C_1$, and rejects otherwise.

*Step 4.* Once $C_1$ is accepted, the RSU chooses a pair of $\langle \text{ticketID}, \text{ticketKey} \rangle$ for the OBU, gains the current timestamp $T$, and computes the authentication information $\Delta' = h(\text{ticketID}||\text{ticketKey}||T||sk)$. Then, the RSU formats the information $\text{ticketID}, \text{ticketKey}, \text{ID}_j, T, \Delta'$ as the message $M_2 = \text{ticketID}||\text{ticketKey}||\text{ID}_j||T||\Delta'$, uses the identity-based encryption algorithm [17] to encrypt it into $C_2 = \mathcal{IBE}_{\text{PID}_i}(M_2)$, and sends $C_2$ 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 5.* Upon receiving $C_2$ at timestamp $T'$, the OBU decrypts $C_2$ with the private key $sk_i$ and parses the result $M_2$ into $\text{ticketID}, \text{ticketKey}, \text{ID}_j, T, \Delta'$. After checking $|T' - T| \leq \Delta T$ and the validity of $\Delta' = h(\text{ticketID}||\text{ticketKey}||T||sk)$, the OBU accepts the pair of $\langle \text{ticketID}, \text{ticketKey} \rangle$, which will be served for achieving navigation and guard 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 the 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 $(\mathrm{RSU}_0, \mathrm{RSU}_a, \mathrm{RSU}_b)$, the
      height $\mathtt{h}$ of RSUs and a threshold value $\varepsilon$ that is contingent upon
      the noise in the ranging measurement.
Result: Vehicle's current position $(x_v, y_v)$.
begin
    Convert $(d_0, d_a, d_b)$ to the plane distances $(D_0, D_a, D_b)$, where
        $D_0 = \sqrt{d_0^2 - \mathtt{h}^2}, D_a = \sqrt{d_a^2 - \mathtt{h}^2}, D_b = \sqrt{d_b^2 - \mathtt{h}^2}$   (2)
    Solve out two possible positions $(x_{v_1}, y_{v_1})$ and $(x_{v_2}, y_{v_2})$ from
        $\begin{cases} \sqrt{(x - x_a)^2 + (y - y_a)^2} = D_a \\ \sqrt{(x - x_b)^2 + (y - y_b)^2} = D_b \end{cases}$   (3)
    if $|\sqrt{x_{v_1}^2 + y_{v_1}^2} - D_0| \le \varepsilon$ then
        return $(x_{v_1}, y_{v_1})$
    else if $|\sqrt{x_{v_2}^2 + y_{v_2}^2} - D_0| \le \varepsilon$ then
        return $(x_{v_2}, y_{v_2})$
    end
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 $\mathrm{NavInfo}$ based on the position $(x_v, y_v)$.

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

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

$$\sqrt{(x_i - x_v)^2 + (y_i - y_v)^2} \le \varepsilon' \tag{4}$$

where $\varepsilon'$ is a threshold value that is contingent upon the noise in the ranging measurement, the RSUs believe the vehicle arrives at the appointed parking space $(x_i, y_i)$ and stop the navigation. Otherwise, the vehicle is still moving, and the parking lot RSUs go back to *Step 1*.

**Discussion.** The availability of Global Position System (GPS) has been widely used in land vehicle navigation applications. However, the positioning systems based on GPS may not be suitable for real-time parking navigation. The reason lies in the fact that the precision of many common-used GPSs may not reach positioning each parking space, and more importantly, the status of a parking space is dynamic. A parking space that is vacant at the current time could be occupied in the next time. Therefore, in the proposed SPARK scheme, the three parking lot RSUs can use TDOA or TDA [16] to cooperatively position the vehicle and achieve the real-time parking navigation.

### D. Intelligent Anti-Theft Protection in Large Parking Lots

One of the major concerns to the public is vehicle theft, especially, unattended parking lots. Next, we will illustrate how SPARK can be used to protect the vehicle theft.

When a vehicle parks at the parking space $(x_i, y_i)$, the parking lot RSUs gain 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 formatted as

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

to the RSUs, where $\mathrm{ID}_j$ is the parking lot's identifier, “*on*” is the status, $T_L$ is the current timestamp and $\Theta = h(\mathrm{ticketKey}||\text{“}on\text{”}||T_L)$. When the driver comes back to the parking lot, he enters his password to unlock the OBU, adjusts the OBU to the *active* mode. Then the OBU will send

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

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

TABLE II

UPDATE A PARKING SPACE RECORD

| POS | RES | OCC | PID | TID | TKEY | ST | LUT |
|---|---|---|---|---|---|---|---|
| $(x_i, y_i)$ | 0 | 1 | $\mathrm{PID}_i$ | ticketID | ticketKey | $T_S$ | $T_L$ |

**Intelligent Anti-Theft 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 the Algorithm 2 to detect whether there is an exception taking place on the vehicle that parks at position $(x_i, y_i)$.

If the returned value of the 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 is going to leave the parking lot. Since only the driver knows the password, and can unlock the OBU to change the *status* to “off”, the RSUs believe the vehicle is legally leaving. However, when the returned value is an exception, the RSUs can detect the vehicle-theft.

- Exception I means the current position $(x_v, y_v)$ of the vehicle is different from the position $(x_i, y_i)$. When the Exception I occurs, the RSUs can detect the vehicle is illegally moving, for example, 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 $\mathrm{ticketKey}$, he can't forge a valid $\Theta = h(\mathrm{ticketKey}||\text{“}off\text{”}||T_L)$ 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 the detection period of RSUs is too long. To avoid this exception to some extent, the optimal detection period should be determined as follows. Considering the speed limit in parking lot is 10 km/h ($\approx 2.7$ m/s) and the distance of the parking space that is closest to the entrance is 10 m. Then, the maximum detection period for a vehicle can be roughly 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.** Besides choosing the optimal detection period, an anticipant tracking stolen vehicle mechanism should be provided. Fortunately, since the OBU is a tamper-proof device and equipped with the inner backup battery, even though the vehicle power is cut off by the thief, the OBU still can periodically send $\text{beaconInfo} = \text{ID}_j||\text{ticketID}||\text{``}on\text{''}||T_L||\Theta$ 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 $\text{beaconInfo} = \text{ID}_j||\text{ticketID}||\text{``}on\text{''}||T_L||\Theta$ sent from a running vehicle, as shown in Fig. 1. Then, according to the parking lot's identifier $\text{ID}_j$, they can report the location of the stolen vehicle to the parking lot. In 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 enter the parking lot immediately. However, if the parking lot is full, the driver will leave the current parking lot and seek for another parking lot. Therefore, it is of special interest if the parking lot can provide the friendly parking information to the running vehicles.

Since the field OCC of one parking space record can identify the current space status, the parking lot RSUs can easily derive the total number of unoccupied parking space $\text{N}_{uoc}$. Therefore, before a vehicle enters the parking lot, the RSUs can provide $\text{N}_{uoc}$ to facilitate the parking decision of the driver.

Although the statistic $\text{N}_{uoc}$ is accurate, it changes with time. Therefore, it is not suitable to simply disseminate $\text{N}_{uoc}$ to those 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 running on the road by using the mechanism in [19]. In the following, we describe how the parking lot RSUs calculate the blocking probability $\mathbb{B}$. From the records in the history table, RSUs can get the vehicle arrival rate by the statistic of $T_s$ and obtain the mean parking time by the statistic of $T_L - T_S$.

**Algorithm 2**: DetectVehicleException()

```
Data: An occupied parking space record as shown in Table II
Result: An exception or $\perp$
begin
    if RSUs receive an updated beaconInfo with the same ticketID
    from the OBU within a predefined period then
        parse it as $[\text{ID}_j||\text{ticketID}||status||T_L||\Theta]$ and check the
        validity of $T_L$ to resist the replaying attack
        compute $\Theta' = h(\text{ticketKey}||status||T_L)$
        if $status ==$ "$on$" then
            relocate the position $(x_v, y_v)$ of the vehicle and compare
            it with the recorded $(x_i, y_i)$
            if $\sqrt{(x_v - x_i)^2 + (y_v - y_i)^2} \leq \varepsilon$ then
                update the field LUT with $T_L$
                return $\perp$
            else if $\sqrt{(x_v - x_i)^2 + (y_v - y_i)^2} > \varepsilon$ then
                detect an exception event
                update the field LUT with $T_L$
                return Exception-I
            end
        else if $status ==$ "$off$" then
            if $\Theta' == \Theta$ then
                update the field LUT with $T_L$, copy the record into
                a history table, and reset the record to its initial
                status.
                return $\perp$
            else if $\Theta' \neq \Theta$ then
                detect an exception event
                return Exception-II
            end
        end
    else if RSUs don't receive an update beaconInfo within a
    predefined period then
        detect an exception event
        return Exception-III
    end
end
```

Assume that a smart parking lot near a shopping mall can offer total $c$ parking spaces. By statistics, the arrival of vehicles follows a Possion process with a rate of $\lambda$ vehicles per minute, and the mean parking time is $E(t)$ hours. In the following, under the $M/G/c/c$ queue model, we estimate the blocking probability $\mathbb{B}$. Assume that the probability $p_n$ denotes there are $n$ vehicles in the parking lot, then the probability $p_c$ that all parking spaces are occupied is of special interest, since the blocking probability $\mathbb{B}$ is equal to $p_c$. According to the $M/G/c/c$ queue model [24], we can derive that

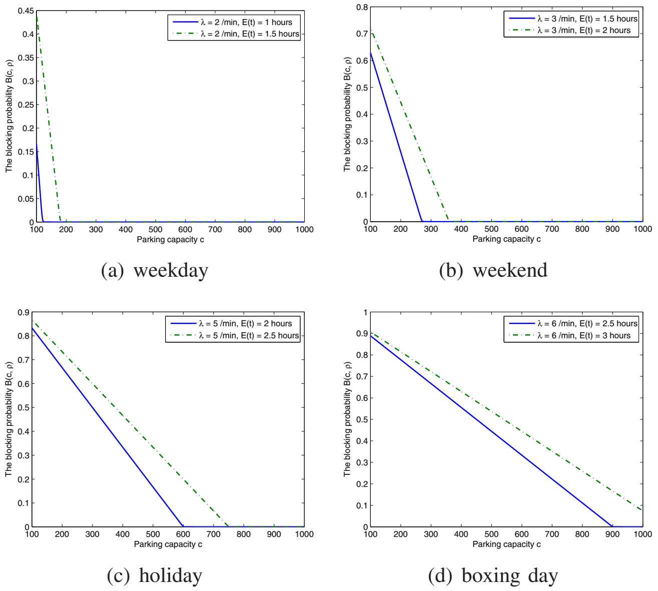
$$p_n = \frac{\rho^n}{n!} \cdot \left[\sum_{i=0}^{c} \frac{\rho^i}{i!}\right]^{-1}, \text{ for } n = 0, 1, 2, \cdots, c, \tag{5}$$

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

$$\mathbb{B}(c, \rho) = p_c = \frac{\rho^c}{c!} \cdot \left[\sum_{i=0}^{c} \frac{\rho^i}{i!}\right]^{-1} \tag{6}$$

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

Fig. 7 shows the blocking probability $\mathbb{B}(c, \rho)$ varies with the capability of the parking lot $c$ under the different parameters $(\lambda, E(t))$. From the figure we can see the higher $\lambda \cdot E(t)$, the higher blocking probability $\mathbb{B}(c, \rho)$; and with the increase of the parking lot's capacity $c$, the blocking



(a) weekday

(b) weekend

(c) holiday

(d) boxing day

Fig. 7. The blocking probability $\mathbb{B}(c, \rho)$ vs the capability of the parking lot $c$

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 these friendly parking information $(c, \mathbb{B})$, the drivers can conveniently choose their preferred parking lots close to their destinations.

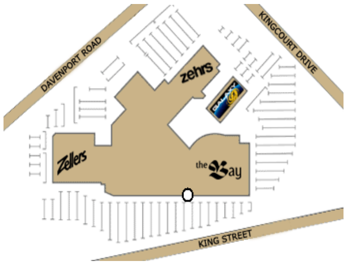
## IV. Security Analyses

In this section, we discuss security issues of the proposed SPARK scheme, i.e., the security of the ticketKey, conditional privacy preservation of the OBU and the selfishness issues atparking lots.

- *Security of the ticketKey.* The security of ticketKey is extremely important in the smart parking lot. If the ticketKey could be compromised, then the intelligent anti-theft protection doesn't work. In the proposed SPARK scheme, since the ticketKey is encrypted with $\mathcal{IBE}$ [17], i.e., $C_2 = \mathcal{IBE}_{\text{PID}_i}(\text{ticketID}||\text{ticketKey}||\text{ID}_j||T||\Delta)$, only the OBU, with the private key $sk_i = sH(\text{PID}_i)$, can recover it. As a result, the ticketKey is privacy protected.
- *Conditional privacy preservation of the OBU.* Since the OBU uses the pseduo-ID $\text{PID}_i$ during its communication with parking lot RSUs, the real identity $\text{ID}_i$ is protected. At the same time, with the help of TA, the parking lot RSUs can reveal the real identity $\text{ID}_i$ from $\text{PID}_i$, since TA has the ability to decrypt $\text{PID}_i = \mathbf{Enc}_s(\text{ID}_i)$ by using the *master key* $s$. Therefore, the conditional privacy preserving of the OBU is achieved.
- *Selfishness issues.* In ordinary free parking lots, when some drivers are looking 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 [20]. However, in the proposed SPARK scheme, since the whole parking lot is under surveillance of the three parking lot RSUs. Once the selfish behaviors take place, the RSUs can detect them immediately. Therefore, the selfishness issues don't exist in the proposed SPARK scheme.

## V. Performance Evaluation

In this section, simulations are conducted to verify the efficiency of the proposed SPARK scheme, where the comparison is made with a parking lot without any parking guidance system in the aspect of the searching time delay (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 it finds a desired parking space.



*Courtesy of Conestoga Mall, Waterloo, Ontario, Canada

Fig. 8. Conestoga mall parking lot

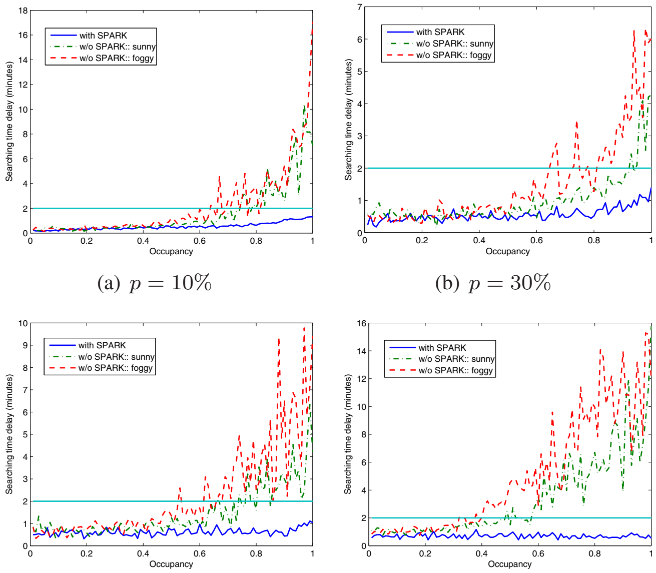
### A. Simulation Environment

The large parking lot adopted throughout our simulation is the one at Conestoga Mall, shown in Fig. 8, which is a major shopping mall in Waterloo, Ontario, Canada [21]. 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 over 1,000 parking stalls, and there are three different entrances to the parking lot. For simplicity, we don't consider special services for parking lot, such as handicapped parking, reserved parking, and reserved bus lanes.

In the parking lot, there are two types of drivers: 1) those 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) those looking for any available parking and parking in the first empty space they saw in the lot. The mobility model throughout our simulation is as follows: when a driver enters the parking lot, with the probability of $p$, the driver is a type 1 driver. Otherwise, the driver is a type 2 driver with the probability of $1-p$. Each vehicle is driving with a randomly fluctuated speed in a range of 10 percent centered at the parking lot speed limit. As a type 1 driver, the driver will be looking for a parking spot close to the main entrance of the mail and keep circling around until the driver finds the nearest legal parking space to park. For a type 2 driver, instead, the driver just parks anywhere they can. When the driver is driving in the parking lot and entering an intersection, the driver will proceed with a random direction equally 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 |



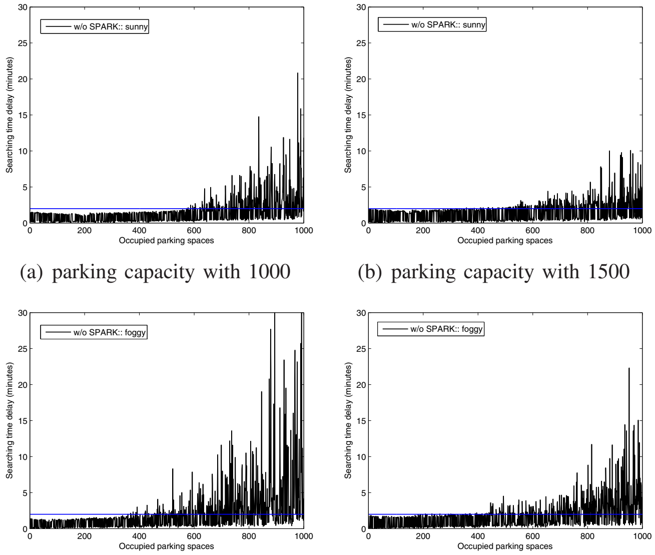
(a) $p = 10\%$

(b) $p = 30\%$

(c) $p = 50\%$

(d) $p = 80\%$

Fig. 9. The occupancy factor of parking lot vs. the searching time delay



(a) parking capacity with 1000

(b) parking capacity with 1500

(c) parking capacity with 1000

(d) parking capacity with 1500

Fig. 10. Comparisons of the searching time delay with different parking capacity when $p = 80\%$

### B. Simulation Results

First, we investigate the impact of the occupancy factor of the parking lot on the searching time delay. We test in a parking lot with SPARK navigation, without SPARK navigation in sunny or foggy day, where the sunny day represents good visibility and reflects earlier discovery of an available parking space and the foggy day represents bad visibility. For each case, we test 10 times, and the average searching time delay over all these experiments is reported. As shown in Fig. 9, for a parking lot without SPARK navigation system in sunny or foggy day, with the increase of the occupancy factor, the searching time delay (STD) for an available parking space increases significantly after the occupancy factor reaches 50 percent. Especially, in foggy day when the occupancy factor is above 80 percent, the time that a driver uses to find an available parking space is too long, and it becomes intolerable to most of drivers. However, with the help of the proposed smart parking system, the searching time delay (STD) for an available parking space becomes low. Furthermore, the weather condition doesn't have any impact on the SPARK.

Another interesting observation, as shown in Fig. 10, is that when the parameter $p = 80\%$, the increase of parking space doesn't improve the STD very much especially after the occupancy factor of parking lot becomes large. The possible reason is that $80\%$ 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. 9 (a), (b), (c) and (d), this interesting observation can be also confirmed.

Furthermore, due to the friendly parking information dissemination, there is another benefit from the proposed SPARK 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.

## VI. RELATED WORK

Recently, several previous research works related to the parking lots have been appeared in [19], [20], [22], [23].

In [20], Panayappan *et al.* provide a VANET-based approach for parking space availability. In the appraoch, the parking lots are managed by RSUs, and these RSUs can provide open parking space information to the drivers, which is very similar as the proposed SPARK scheme. In addition, the approach also provides a security architecture to solve some possible security vulnerabilities. However, the approach doesn't provide the real-time parking navigation in large parking lots, nor any anti-theft protection function [20]. In [22], Song *et al.* present a sensor-network-based vehicle anti-theft system. In the system, the 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 [22]. In [19], based on the VANET techniques, Caliskan *et al.* propose a topology independent scalable information dissemination algorithm for free parking places discovery. With those friendly parking lot information disseminated by the parking automats and inter-vehicle broadcast, the drivers can conveniently find their preferred free parking lot.

Table IV compares the achieved goals of the above three schemes and the proposed SPARK scheme. From the table, we can see the proposed SPARK scheme is more practical.

TABLE IV

COMPARISONS OF FOUR SMART PARKING SCHEMES

| Goals | Scheme [19] | Scheme [20] | Scheme [22] | SPARK |
|---|---|---|---|---|
| real-time parking navigation | × | × | × | ✓ |
| intelligent anti-theft protection | × | × | ✓ | ✓ |
| parking information dissemination | ✓ | ✓ | × | ✓ |

## VII. CONCLUSIONS

In this paper, we have proposed a new VANET-based smart parking scheme (SPARK) for large parking lots. With SPARK scheme, RSUs installed across a parking lot can surveil the whole parking lot, and provide three convenient services for drivers: 1) real-time parking navigation; 2) intelligent anti-theft protection; and 3) friendly parking information dissemination. In addition, the SPARK scheme also provides conditional privacy preservation for OBUs. Extensive simulations have also been conducted to demonstrate that the SPARK scheme can efficiently reduce the searching time delay for an available parking space, and subsequently save the fuels and driver's parking time.

## ACKNOWLEDGMENT

The research is financially supported by Natural Sciences and Engineering Research Council of Canada (NSERC).

## APPENDIX

We will show how to compute $\mathbb{B}(c,\rho)$ for large $c!$. From Eq. (6), we have

$$\mathbb{B}(c,\rho)=\frac{\rho^c/c!}{\rho^c/c!+\sum_{i=0}^{c-1}\rho^i/i!} \tag{7}$$

and

$$\mathbb{B}(c-1,\rho)=\frac{\rho^{c-1}/(c-1)!}{\sum_{i=0}^{c-1}\rho^i/i!} \tag{8}$$

Then, from Eqs. (7)-(8), we have

$$\mathbb{B}(c,\rho)=\frac{\rho/c}{\rho/c+1/\mathbb{B}(c-1,\rho)}=\frac{\rho\mathbb{B}(c-1,\rho)}{c+\rho\mathbb{B}(c-1,\rho)} \tag{9}$$

Since $\mathbb{B}(0,\rho)=1$, we can apply the relation in Eq. (9) to subsequently compute $\mathbb{B}(i,\rho)$, for $i=1,2,\cdots,c$. In the end, we can gain the value of $\mathbb{B}(c,\rho)$. ■

## REFERENCES

[1] V. Tang, Y. Zheng, and J. Cao, "An intelligent car park management system based on wireless sensor networks," in *Proc. of the First International Symposium on Pervasive Computing and Applications*, Urumchi, Xinjiang, P.R. China, pp. 65-70, August 2006.

[2] J. Chinrungrueng, U. Sunantachaikul, and S. Triamlumlerd, "Smart parking: an application of opticalwireless sensor network," in *Proc. of the the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*, Hiroshima, Japan, pp. 66-69, January 2007.

[3] Y. Bi, L. Sun, H. Zhu, T. Yan, and Z. Luo, "A parking management system based on wireless sensor network," *ACTA AUTOMATICA SINICA*, Vol. 32, No. 6, pp. 38-45, Nobember 2006.

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

[5] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles", *IEEE Security and Privacy Magazine*, Vol. 2, No. 3, pp. 49-55, 2004.

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

[7] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Medium access control protocol design for vehicle-vehicle safety messages", *IEEE Transaction on Vehicular Technology*, Vol. 56, No. 2, pp. 499-518, 2007.

[8] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks", *Journal of Computer Security*, Vol. 15, No. 1, pp. 39-68, 2007.

[9] C. Zhang, X. Lin, R. Lu, P.-H. Ho and X. Shen, "An Efficient Message Authentication Scheme for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, Vol. 57, No. 6, pp. 3357-3368, 2008.

[10] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, Vol. 46, No. 4, pp. 88-95, 2008.

[11] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM'08*, Phoenix, AZ, USA, April 14-18, 2008.

[12] 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. IEEE INFOCOM'08*, Phoenix, AZ, USA, April 14-18, 2008.

[13] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 6, pp. 3442-3456, 2007.

[14] Task Group, *IEEE P802.11p: Wireless Access in Vehicular Environments (WAVE)*, draft standard ed., IEEE Computer Society, 2006.

[15] R. Lu and Z. Cao, "Efficient remote user authentication scheme using smart card," *Computer Networks*, Vol. 49, No. 4, pp. 535-540, 2005.

[16] L. Cong and W. Zhuang, "Hybrid TDOA/AOA mobile user location for wideband CDMA cellular systems," *IEEE Transactions on Wireless Communications*, Vol. 1, No. 3, pp. 439-447, July 2002.

[17] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", in *Advances in Cryptology - CRYPTO 2001*, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[18] W. Mao, *Modern Cryptography: Theory and Practice*, Prentice Hall PTR, 2003.

[19] M. Caliskan, D. Graupner, and M. Mauve, "Decentralized discovery of free parking places," in *Proc. of the Third ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2006)*, Los Angeles, CA, USA, pp. 30-39, Sept. 2006.

[20] R. Panayappan, J. Trivedi, A. Studer, and A. Perrig, "VANET-based approach for parking space availability," in *Proc. of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2007)*, Montréal, Québec, Canada, pp. 75-76, Sept. 2007.

[21] Conestoga Mall. [online] Available at: http://conestoga.shopping.ca/

[22] H. Song, S. Zhu, and G. Cao, "SVATS: A sensor-network-based Vehicle Anti-Theft System," in *Proc. IEEE INFOCOM'08*, Phoenix, AZ, USA, April 14-18, 2008.

[23] M. Caliskan, A. Barthels, B. Scheuermann, and M. Mauve, "Predicting parking lot occupancy in vehicular ad-hoc networks," in *Proc. of the 65th IEEE Vehicular Technology Conference (VTC 2007 Spring)*, Dublin, Ireland, pp. 277-281, April 2007.

[24] J. W. Cohen, *On regenerative processes in queueing theory*, Springer, Berlin, 1976.