Research Article

Parking Query in Vehicular Delay-Tolerant Networks with Privacy Protection Based on Secure Multiparty Computation

Haiping Huang,1,2,3,4 Juan Feng,1,2 Dan Sha,1,2 Jia Xu,1,2,3 and Hua Dai1,2,4

1College of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
2Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China
3Key Lab of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
4College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

Correspondence should be addressed to Haiping Huang; hhp@njupt.edu.cn

Received 18 October 2014; Revised 19 February 2015; Accepted 11 March 2015

Academic Editor: Fei Yu

Copyright © 2015 Haiping Huang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Within vehicular delay-tolerant network, conflict exists in the scenario of which two vehicles happen to choose the same parking space. To solve this problem, two protocols are proposed, respectively, which are called privacy protection protocol based on secure multiparty computation and routing protocol based on angle and density. The proposed methods prevent the leaking of privacy information of the vehicles involved during the parking space seeking process and improve the performance of the transmission ratio and reduce the transmission delay by unifying the directions of messages and choosing the vehicle of the highest distribution density as the next hop. The results of the simulation show the efficiency of our method.

1. Introduction

Many applications under the delay-tolerant network have been studied and extended to wireless network domains such as mobile ad hoc networks (MANET), vehicular ad hoc networks (VANET), and wireless sensor networks (WSN). In the VANET, communications between two vehicles are intermittent due to the changes of the driving speed and direction.

One key issue in VANET is the urban parking problem. It arises along with the rapid expansion of urban population. The intelligent parking space positioning system is developed to address this issue. In this paper, we assume a situation where two nearby vehicles happen to find the same parking space which causes a competition for the limited resource.

To solve the resource allocation problem, we propose a multiparty computation based protocol to detect the potential conflict. Once the vehicle detects that the parking space has been already allocated, it continues its searching process. Vehicular delay-tolerant network is full of potential maliciousness, such as attacks and unauthorized operations. The vehicle privacy is also a critical issue. In order to protect it, we design a privacy protection strategy during the secure multiparty computation, along with a routing protocol to increase the transmission ratio while decreasing the transmission delay. The distribution density and the directions of the vehicles are input parameters in estimation function. The direction of the vehicle is calculated by measuring the angle between the reference direction and the line linking itself to the base station. The vehicle near this line has the highest distribution density and will be chosen for the next hop.

In this paper, we briefly related work on security and routing protocol of delay-tolerant networks in Section 2. The privacy protection strategy based on multiparty computation is designed in Section 3, while the routing protocol based on angle and density is proposed in Section 4. In Section 5, we discuss the security of the proposed method, and the simulation results show the higher transmission ratio and lower transmission delay. Section 6 gives the conclusion of this paper.
2. Related Work

The communication interruption and the uncertain network topology are the main reasons that leave the security of delay-tolerant network a challenging issue. However, some existing application system fails to meet the basic requirements for security purpose. Ensuring the security in the delay-tolerant network is an active topic among researchers. Lu et al. [1] proposed a privacy protection strategy by using the filter. The filter is maintained by the corresponding node according to its own interest. Hur and Kang [2] proposed a secure data retrieval scheme that used the CP-ABE for decentralized delay-tolerant networks, and multiple key authorities manage their own attributes. Lv et al. [3] designed an efficient and noninteractive key exchange protocol based on a time-evolving topology model and a two-channel cryptography. A time-evolving model is used to formally analyze the periodic and predetermined behavior patterns, and therefore a node can schedule when and to whom it should send its public key. By analyzing the periodic and predetermined behavior patterns, the time-evolving model decided and prepared the receiver of the node for its public key. The third party methods have drawn the attention of many researchers in delay-tolerant network. Rane et al. [4] presented a scheme using biometric authentication and homomorphic encryption for secure calculation of Hamming distance while protecting the participants’ privacy. And they furthered their study by proposing a secure two-party computation protocol [5] of Euclidean distance using Paillier homomorphic encryption and this protocol is implemented for private querying of face images and maintains low communication overhead. Facial information is utilized for authentication, and communication overhead is kept as a minimum. Yang et al. [6] provided a quantum privacy comparison method. The presence of a semihonest third party allowed the matching of information without revealing the nodes’ privacy. Huang et al. [7] allow the participants to calculate the distance between each other based on an honest third party in order to realize comparison of local data. However, the private values of participants are fully grasped by the third party, which is followed by obvious information leakage and security issues that cannot be ignored. Gao et al. [8] encoded the original data for privacy purpose and select the top N nodes to perform the multicast in network by applying privacy protected data forwarding (PPDF) model.

The routing protocol for delay-tolerant network is an active topic in many different contexts. Samuel et al. [9] introduced the dominant set to the routing protocol. They took Markov model to predict the distribution of encountering interval and evaluate the utility value for the next hop. According to the historical statistic data of vehicle routes, Xu et al. [10] suggested the use of statistic method for encountering probability prediction. However, the statistic data might fail in the real scenario. Dunbar and Qu [11] applied the statistic method to preventing the location information of vehicles leaking by communication with RSUs. Hui et al. [12] binned the nodes into several areas according to their encountering probabilities simultaneously taking into account the community attribute and center degree. Fabbri and Verdone [13] considered the characteristic curve of social relations against the time series to plan the routing. Lee et al. [14] extended the current geographical routing protocol by forming a two-level hierarchy for heterogeneous network. However, existing methods either are computationally expensive or are having considerable network delay, not to mention the security issue.

In this paper, we design a secure multiparty computation protocol for privacy protection. By using the direction and distribution density to decide the next hop, higher transmission ratio and lower transmission delay have been achieved.

3. Privacy Protection Protocol Based on Multiparty Computation

In order to find conflict of the same parking spaces, vehicles must take part in multiparty computation and meanwhile have to exchange the already owned parking space information with others. As a result, a vehicle may excavate some privacy information of other vehicles, and obviously it is dangerous. In the proposed protocol, as the third party, the base station instead of the vehicles will finally calculate the common parking spaces. Space information of each vehicle will be packed with polynomial function before being sent, and then the base station and other vehicles taking part in calculation cannot acquire the real space information. So privacy is protected. In this paper, we consider a scenario where there are three vehicles searching for parking spaces within a certain area.

Firstly, each vehicle participating in calculation will search for the parking spaces within a certain communicated area and then generate a set according to the parking spaces discovered by it. Secondly, it will generate the special polynomial function. Thirdly, it will send the function to the base station. Finally, the base station will figure out the common parking spaces and return the result.

3.1. Problem Description. Assuming that there are three vehicles within a certain communication area, for example, A, B, and C, the sets they generate according to the parking spaces they have found are 
\[ S_A = \{a_1, a_2, a_3, \ldots, a_l\}, \]
\[ S_B = \{b_1, b_2, b_3, \ldots, b_m\}, \]
\[ S_C = \{c_1, c_2, c_3, \ldots, c_n\}, \]
in the case of 
\[ n \leq m \leq l. \]

The three vehicles expect to deduce common parking spaces without leaking out their private information during the computing process.

3.2. Description of the Protocol. Vehicle A and vehicle B generate polynomial functions according to 
\[ S_A = \{a_1, a_2, a_3, \ldots, a_l\} \]
and 
\[ S_B = \{b_1, b_2, b_3, \ldots, b_m\}, \]
denoted by 
\[ f(x) \]
and 
\[ g(x) \]
separately:
\[
f(x) = (x - a_1) \times (x - a_2) \times (x - a_3) \times \cdots \times (x - a_l),
\]
\[
g(x) = (x - b_1) \times (x - b_2) \times (x - b_3) \times \cdots \times (x - b_m).
\]

And then vehicle C will calculate 
\[ f(c_i) \]
and 
\[ g(c_i) \]
if 
\[ f(c_i) = 0 \]
and 
\[ g(c_i) = 0, \]
then element 
\[ c_i \]
must be in sets 
\[ S_A \]
and 
\[ S_B; \]
in other words,
\[
f(c_i) + g(c_i) = 0 \land f(c_i) \times g(c_i) = 0.
\]
It is equivalent to the fact that
\[ f(c_i) = 0 \land g(c_i) = 0. \]  
(3)

So, \( c_i \in S_a \land c_i \in S_b \), which means that element \( c_i \) is one of the
common parking spaces of vehicles A, B, and C.

3.3. Implementation of the Protocol. (1) Vehicles A, B, and C
send request message to the base station, respectively, telling
the base station that they want to inquire common parking spaces.
(2) After the base station receives the request messages, it sends response message to vehicles A, B, and C, and then
connection is established.
(3) Vehicle A generates polynomial function as follows:
\[ f(x) = (x - a_1) \times (x - a_2) \times (x - a_3) \times \cdots \times (x - a_l) \]
\[ = \sum_{i=1}^{l} p_i x^i = \sum_{i=0}^{l} q_i x^i + \sum_{i=0}^{r} r_i x^i, \]  
(4)
where \( q_i, r_i \ (i = 1, 2, \ldots, l) \) are all nonzero real numbers.
In addition, we assume that \( f_i(x) = \sum_{i=0}^{q} q_i x^i \), \( f_c(x) = \sum_{i=0}^{l} r_i x^i \), \( f_a(x) : A \to B \), and \( f_b(x) : A \to C \).
(4) Vehicle A then sends \( f_b(x) \) and \( f_c(x) \) to the base station
using the routing protocol we proposed in the following sections.
(5) Vehicle B generates polynomial function as follows:
\[ g(x) = (x - b_1) \times (x - b_2) \times (x - b_3) \times \cdots \times (x - b_m) \]
\[ = \sum_{i=0}^{m} e_i x^i = \sum_{i=0}^{m} s_i x^i + \sum_{i=0}^{t} t_i x^i, \]  
(5)
where \( s_i, t_i \ (i = 1, 2, \ldots, l) \) are all nonzero real numbers.
In addition, we assume that \( g_i(x) = \sum_{i=0}^{s} s_i x^i \), \( g_c(x) = \sum_{i=0}^{l} t_i x^i \), \( g_a(x) : B \to A \), and \( g_b(x) : B \to C \).
(6) Vehicle B then sends \( g_a(x) \) and \( g_b(x) \) to the base station
using the routing protocol we proposed in the following sections.
(7) The base station finally receives value of \( f_b(x), f_c(x), g_a(x), \) \( g_b(x) ; \) then it calculates \( h_i(x) \) and the parameter
0.5 is considered according to previous simulation results or
experience:
\[ h_i(x) = f_b(x) \times g_c(x) + 0.5 \times g_a(x) \times f_b(x) \].  
(6)
(8) The base station then sends \( g_a(x) \) to vehicle A.
(9) After receiving \( g_a(x) \), vehicle A calculates \( u(x) \) and
\( v(x) \):
\[ u(x) = f(x) + g_a(x) = \sum_{i=0}^{l} a_i x^i \quad (j = \max(l, m)), \]
\[ v(x) = g_a(x) \times f_c(x) + 0.5 \times g_a(x) \times f_b(x) \]
\[ = \sum_{i=0}^{k} \beta_i x^i \quad (k = l + m). \]  
(7)
Vehicle A then generates private vectors on the basis
of (7) as follows:
\[ \mathbf{X}_1 = (a_0, a_1, \ldots, a_I), \]
\[ \mathbf{X}_2 = (\beta_0, \beta_1, \ldots, \beta_k). \]  
(8)
Afterwards, vehicle A sends vectors \( \mathbf{X}_1 \) and \( \mathbf{X}_2 \) to the base station.
(11) The base station packs \( \mathbf{X}_1, \mathbf{X}_2, f_c(x), g_c(x), \) and \( h_i(x) \)
and then sends the package to vehicle C.
(12) After receiving package of \( \mathbf{X}_1, \mathbf{X}_2, f_c(x), g_c(x), \) and \( h_i(x) \), vehicle C then calculates \( h(x) \):
\[ h(x) = f_c(x) \times g_c(x) + h_i(x). \]  
(9)
(13) Following that, vehicle C implements the following
substeps using elements \( c_i \ (i = 1, 2, \ldots, n) \) of set \( S_c \):
(a) Generating private vectors:
\[ \mathbf{Y}_1 = (1, c_i, \beta_i^2, \ldots, \beta_i^k), \]
\[ \mathbf{Y}_2 = (1, c_i, \beta_i^2, \ldots, \beta_i^k). \]  
(10)
(b) Computing vectors \( \mathbf{U}_1 \) and \( \mathbf{U}_2 \):
\[ \mathbf{U}_1 = \mathbf{X}_1 \times \mathbf{Y}_1, \]
\[ \mathbf{U}_2 = \mathbf{X}_2 \times \mathbf{Y}_2. \]  
(11)
(c) Calculating \( g_a(c_i) \) and \( h(c_i) \), judging whether \( \mathbf{U}_1 + g_a(c_i) = 0 \) and \( \mathbf{U}_2 + h(c_i) = 0 \) in the meantime. If it
is true, then \( c_i \in (S_a \cap S_b) \); otherwise, \( c_i \notin (S_a \cap S_b) \).
(14) Vehicle C will finally obtain all elements \( c_i \) which satisfy
\( c_i \in (S_a \cap S_b) \), and then it sends \( S_a = \{c_i, c_j \in (S_a \cap S_b), i = 1, 2, \ldots, n\} \) to the base station.
(15) The base station sends the common parking spaces
set \( S_a \) to vehicle A and vehicle B. Eventually, the three vehicles
acquire their common parking spaces without obtaining
private information of others.

4. Routing Protocol Based on
Angle and Density

During the calculation of common parking spaces, parking
information is transmitted in the network, so we propose a
routing protocol for vehicles to decide how to choose routes
along to the base station when sending messages.
In vehicular delay-tolerant networks, wireless communica-
tion devices are equipped with vehicles. When the distance
of two vehicles is shorter than the communication radius,
they can connect and exchange messages. While in some
blind areas or in some periods of time, there may be no
continuous connections between the source vehicle and the
destination vehicle due to the sparse distribution, signal
shielding, and high speed mobility of vehicles, which are the
fundamental characteristics of delay-tolerant networks, also
called intermittent connectivity. If a vehicle wants to send a message, it will firstly carry this message, until it encounters the other vehicle, and then it forwards the message. Due to the “storage-carry-forward” scheme, transmission delay is always an important issue. Consequently, research of routing algorithms and message distribution algorithms is significant to reduce transmission delay.

As described above, considerable literatures have studied the characteristics of transmission delay. Liu et al. [15] analyze transmission delay in vehicular delay-tolerant networks with a bidirectional traffic model and it is demonstrated that transmission delay is linearly associated with transmission distance and subsequently indicates that a certain relation exists between transmission delay and vehicle density in the road. The research conclusion will be used in this paper.

4.1. Network Model. Figure 1 manifests the network model of vehicular delay-tolerant networks, and message is forwarded by assistant node from the source nodes to the base station. In other words, message is transmitted from one vehicle to another vehicle in the range of communication.

Different vehicles, as a general rule, may have different speeds; for example, the vehicle in the fast traffic lane usually runs faster than those in the slow traffic lane. We can set \( n \) levels of the vehicle speed, from slow to fast, which are denoted by \( v_1, v_2, \ldots, v_n \), respectively. For convenience sake, we firstly consider vehicles traveling in the same direction. We can assume the set \( S_i = \{x_{ij}(t), j \in N\} \), \( i = 1, 2, \ldots, n \), is the set of vehicles traveling at the speed \( v_i \), where \( x_{ij}(t) \) indicates the \( j \)th vehicle of the set \( S_i \) at time \( t \) and \( t \) is discrete, \( t \in N \), and \( N \) is the natural number.

Assume the relationship of vehicle speed \( v \) and vehicle density \( \lambda \) is as follows:

\[
v = a - b\lambda; \tag{12}\]

when \( \lambda = 0 \), the vehicle density is 0, and then the vehicle speed \( v \) can achieve the largest value \( v_f \); that is, when \( \lambda = 0 \), then \( a = v_f \). When \( \lambda = \lambda_f \), it means the vehicle density achieves the largest value \( \lambda_f \), and then the vehicle speed will be 0 and the road is congested; that is, when \( \lambda = \lambda_f \), then \( b = v_f/\lambda_f \). Thus it can be seen that the relationship of vehicle speed \( v \) and vehicle density \( \lambda \) is

\[
v = a - b\lambda = v_f - \frac{v_f}{\lambda_f}\lambda = v_f\left(1 - \frac{\lambda}{\lambda_f}\right). \tag{13}\]

4.2. Definition of Transmission Delay. In vehicular delay-tolerant networks, transmission delay is mainly caused by message retransmission due to communication breakdown or signal interference. While compared with the time of a message transmitted from one vehicle to the other vehicle, message retransmission delay is short enough. So we can ignore it.

Assuming that a vehicle \( N_i \) broadcasts a message at the time \( t = 0 \), we can take \( I(t) \) as the set of vehicles having received the message from \( N_i \) at time \( t \) and take \( T(k) = \inf\{t \geq 0 : x_{ik} \in I(t)\} \) as the time when vehicle \( N_k \) receives the message, and then the transmission delay from vehicle \( N_p \) to vehicle \( N_q \) can be defined as follows:

\[
D(p, q) = T(q) - T(p) = \sum_{k=p}^{q-1}[T(k+1) - T(k)]. \tag{14}\]

4.3. Details of Routing Protocol. In the routing protocol based on angle and density (abbreviated to RPAD) proposed in this paper, the density and direction of vehicle are used for estimate. When a vehicle wants to send message to the base station, it will compute the angle between itself and the base station in order to choose relay vehicles in the suitable direction along to the base station, and meanwhile it will confirm the next hop after predicting vehicle density.

Assuming vehicle \( O \) is the source node, we create a coordinate and take \( O \) as the center, shown in Figure 2. Vehicles A and B are in the communication range of vehicle \( O \), and vehicle C is in the communication range of vehicle B. To reduce the transmission distance of a message and then to reduce the transmission delay, we need to unify the direction of the next hops and the message could be transmitted in the unified direction along to the base station as a guarantee of delivery ratio. Vehicle O obtains the angle between itself and the base station by the GPS device it equips, and if the angle value is larger than \( 45^\circ \), then it will choose those vehicles whose angle between themselves and the base station is smaller than \( 45^\circ \) as the next hops. In Figure 2, the angle between vehicle B and the base station is \( \angle 1 < 45^\circ \), while that between vehicle A and the base station is \( \angle 2 > 45^\circ \), and then vehicle O will choose vehicle B as the next hop and sends message to vehicle B. Similarly, through the comparison of angles, vehicle B will choose vehicle C as the next hop. Consequently, the message of vehicle O will be forwarded along the direction like a stepped appearance shown in Figure 2 finally to the base station.

However, there may be many vehicles satisfying the condition of angle direction. When a vehicle decides the next hop, it cannot send a copy of the message to all the condition-satisfied vehicles for the purpose of energy-efficiency. It is found by studies that, in the area of high vehicle density,
a source vehicle can transmit messages rapidly step by step through other vehicles as a relay until the destination vehicle, instead of carrying the messages until the source vehicle encounters the destination vehicle. Thus, message can be delivered faster to the destination, and then transmission delay is reduced.

Yazhi demonstrates the following theorem [13] through theoretical analysis and simulation experiment.

**Theorem 1.** There exists a relationship between the transmission delay \( T_{0,m} \) and corresponding transmission distance \( m \):

\[
\lim_{m \to \infty} \frac{T_{0,m}}{m} = \alpha. \tag{15}
\]

Based on (15), when the vehicle density and speed are fixed, \( \alpha \) is a constant:

\[
\alpha = \lim_{m \to \infty} \frac{E(T_{0,m})}{m}. \tag{16}
\]

Theorem 1 demonstrates that the limited ratio of transmission delay and transmission distance is \( \alpha \), and \( \alpha \) is a constant when vehicle density is fixed, so transmission delay is linearly associated with transmission distance. The upper bound of the coefficient of the linear relation changes with vehicle density and speed, and so transmission delay decreases with the increase of vehicle density.

In RPAD, after selecting a direction, the vehicle will decide to transmit messages to those vehicles with higher density in their own areas.

Taking vehicle O for an example, \( S_i = \{x_{i,j}(t), j \in N\} \), \( i = 1, 2, \ldots, n \), is the set of vehicles traveling at the relative speed \( v_i \). In the next time \( s \), \( S = \{x_{i,j}(t) + v_i(s - t), i = 1, 2, \ldots, n, j \in N\} \) represents the relative distance between vehicles that satisfied the requirement of angle direction and vehicle O. Vehicle O will further choose those vehicles with higher area density as next hops according to the relative distance and then sends messages to them. Other vehicles repeat the above process until the base station receives the messages.

5. **Experiment Simulation Results and Analysis**

5.1. **Correctness Proof of Privacy Protection Protocol**

5.1.1. **Certification.** It is obvious from Section 3 that

\[
U_1 = X_1 \times Y_1 = a_0 + a_1 \times c_i + \cdots + a_j \times c_i^j + g(c_i) = u(c_i) + g(c_i) = f(c_i) + g(c_i),
\]

\[
U_2 = X_2 \times Y_2 = b_0 + b_1 \times c_i + \cdots + b_k \times c_i^k + h(c_i) = v(c_i) + h(c_i) = f(c_i) \times g(c_i).
\]

If \( U_1 = 0 \) and \( U_2 = 0 \), then

\[
f(c_i) + g(c_i) = 0,
\]

\[
f(c_i) \times g(c_i) = 0.
\]

Therefore, \( f(c_i) = 0 \) and \( g(c_i) = 0 \).

Based on (1), \( c_i \in S_a \) and \( c_i \in S_b \).

5.1.2. **Disproof.** If \( c_i \in S_a \) and \( c_i \in S_b \), then, with (1), \( f(c_i) = 0 \) and \( g(c_i) = 0 \).

While \( U_1 = f(c_i) + g(c_i) \) and \( U_2 = f(c_i) \times g(c_i) \), \( U_1 = 0 \) and \( U_2 = 0 \).

So \( U_1 = 0 \cap U_2 = 0 \iff c_i \in S_a \cap S_b \cap S_c \).

In conclusion, the privacy protocol is proved to be correct.

5.2. **Security Proof of Privacy Protection Protocol.** Next, it will be proved that vehicles A, B, and C will finally obtain the information of common parking spaces without leaking out their respective private information of parking spaces.

(a) **Vehicles A and B.** Vehicle A has \( g_a(x) \) and vehicle B has \( f_b(x) \), while \( g_a(x) \) is justly the part of \( g(x) \) and \( f_b(x) \) is the part of \( f(x) \), and as a result vehicle A cannot get \( g(x) \) from \( g_a(x) \) and vehicle B cannot get \( f(x) \) from \( f_b(x) \). In other words, vehicle A will not obtain private parking space information of vehicle B, and so does vehicle B.

(b) **Vehicle C.** Vehicle C has \( f_c(x) \) and \( g_c(x) \), while \( f_c(x) \) is justly the part of \( f(x) \) and \( g_c(x) \) is the part of \( g(x) \). In addition, \( h_c(x) = f_c(x) \times g_c(x) + 0.5 \times g_a(x) \times f_b(x) \) So vehicle C cannot get \( f(x) \) and \( g(x) \); that is, vehicle C will not obtain private parking space information of vehicles A and B.

Above all, private parking space information of the three vehicles has not been leaked out, so the protocol is secure.

5.3. **Performance Analysis of Privacy Protection Protocol.**

Here, the complexity of communication round and computation is evaluated. Performance comparison results of some privacy protection schemes are shown in Table 1.
Table 1: Performance comparison of some privacy protection schemes.

<table>
<thead>
<tr>
<th>Scheme in this paper</th>
<th>Communication round complexity</th>
<th>Computation complexity</th>
<th>Degree of privacy protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme in this paper</td>
<td>3</td>
<td>O(n)</td>
<td>Zero leakage</td>
</tr>
<tr>
<td>Shantanu’s scheme [4]</td>
<td>n</td>
<td>O(n)</td>
<td>Zero leakage</td>
</tr>
<tr>
<td>Shantanu’s promoted scheme [5]</td>
<td>n</td>
<td>O(n^3)</td>
<td>Zero leakage</td>
</tr>
<tr>
<td>Yang’s scheme [6]</td>
<td>4</td>
<td>O(n^3)</td>
<td>Zero leakage</td>
</tr>
<tr>
<td>Huang’s scheme [6]</td>
<td>3</td>
<td>O(n^2)</td>
<td>The TP obtains all messages from two participants</td>
</tr>
</tbody>
</table>

Table 2: The main simulation parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation time (hour)</td>
<td>10</td>
</tr>
<tr>
<td>Simulation range (width, height: meter)</td>
<td>80000, 58400</td>
</tr>
<tr>
<td>Number of vehicles</td>
<td>100–200</td>
</tr>
<tr>
<td>Vehicle speed (high, low: meter/s)</td>
<td>24, 6</td>
</tr>
<tr>
<td>Communication distance (meter)</td>
<td>150</td>
</tr>
<tr>
<td>Number of copies of SW/SF</td>
<td>10</td>
</tr>
</tbody>
</table>

Obviously from Table 1, the scheme proposed in this paper has the same communication rounds with Huang’s scheme that is superior to other schemes whose communication cost is proportional to original vector dimensions n. Meanwhile, on the premise of privacy zero leakage, our scheme obtains the best computation complexity O(n), owing to the lightweight mathematical method rather than traditional homomorphism encryption applied in other schemes.

5.4. Simulation Results and Analysis of Routing Protocol. We use ONE (opportunistic network environment) to realize the simulations on RPAD proposed in this paper. ONE is specially designed for simulations in delay-tolerant networks, having implemented some classical routing algorithms, like epidemic, SW, SF, and so on. Some main simulation parameters are described in Table 2.

In the experiment, the transmission ratio is defined as the ratio of a number of messages that have been transmitted successfully and that have been generated. Transmission delay is defined in Section 3.2. To evaluate the performance of these algorithms RPAD, SW, SF, and PER, we vary the vehicle speed and the number of vehicle nodes.

5.4.1. Influence of Vehicle Speed. Figures 3 and 4 indicate the influence of vehicle speed on transmission ratio and transmission delay, respectively. When the vehicle speed increases, the transmission ratio increases and transmission delay decreases, because when the vehicle runs at a higher speed, messages carried by vehicles are forwarded faster; that is, the time from the source node to the destination node will be shorter. It can be concluded from Figures 3 and 4 that RPAD performs better than SW, SF, and PER.

5.4.2. Influence of Total Number of Vehicle Nodes. Figures 5 and 6 indicate the influence of total number of vehicles on...
transmission ratio and transmission delay. When the total number of vehicles increases, the transmission ratio increases and transmission delay decreases. In fact, when there are many vehicles in network, messages are transmitted from one vehicle to another quickly, and vehicles do not need to carry the messages for a long time. It can be seen from Figures 5 and 6 that RPAD is superior to SW, SF, and PER.

5.4.3. Influence of Time to Live (TTL). Figures 7 and 8 demonstrate the influence of the total number of time to live values on transmission ratio and transmission delay. If the value of TTL is low, all algorithms perform terribly. When the value of TTL increases, transmission ratio increases, while transmission delay decreases, and when more and more nodes are dead, it will take longer for nodes to transmit.
messages to others. It is clearly observed from Figures 7 and 8 that RPAD holds the higher transmission ratio and shorter transmission delay.

6. Conclusions

In this paper, we address the conflict of two vehicles happening to choose the same parking space in vehicular delay-tolerant network. We design the routing protocol RPAD from the direction and distribution density of the vehicle and the base station is considered as a reference. The vehicles having the same direction of that along the reference direction and higher distribution density are chosen for the next hop. A multiparty computation based privacy protection scheme is also proposed for security consideration.

The remaining work is the validations of our scheme on real data and applications in various delay-tolerant environments where generalizing the assumptions will be taken. Due to the limited time and conditions, now we do not have so many vehicles to solidify the proposed approach, and the demonstration of the validity through some real cases will be done in the further work.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported in part by grants from the National Natural Science Foundation of China (nos. 61202355, 61201163, 61100199, and 61373138), the Natural Science Foundation of Jiangsu Province (no. BK20141429), Scientific and Technological Support Project (Industry) of Jiangsu Province (no. BE2013666), and Natural Science Key Fund for Colleges and Universities in Jiangsu Province (no. 12KJA520002).

References

Submit your manuscripts at
http://www.hindawi.com