Chinese Journal of Electronics
vol. 33, no. 1, pp. 30–42, January 2024
https://doi.org/10.23919/cje.2022.00.007

RESEARCH ARTICLE

Privacy Preserving Algorithm for Spectrum Sensing in Cognitive Vehicle Networks

Hongning LI[1], Tonghui HU[1], Jiexiong CHEN[1], Xiuqiang WU[2], and Qingqi PEI[3]

1. *Guangzhou Institute of Technology, Xidian University, Guangzhou 510555, China*
2. *Guangzhou CEPREI, Guangzhou 511370, China*
3. *Shaanxi Key Laboratory of Blockchain and Secure Computing, Xi'an 710071, China*

Corresponding author: Xiuqiang WU, Email: wuxiuqiang@ceprei.com
Manuscript Received January 14, 2022; Accepted August 16, 2022

Abstract — The scarcity of spectrum resources fails to meet the increasing throughput demands of vehicular networks. There is an urgent need to maximize the utilization of spectrum bands in mobile networks. To ascertain the availability of spectrum bands, users should engage in wireless channel sensing and collaboration. However, spectrum sensing data always involves users' privacy, such as their location. This paper first introduces sensing trajectory inference attack in cognitive vehicular networks and then proposes a data confusion-based privacy-preserving algorithm and a cryptonym array-based privacy-preserving aggregation scheme for spectrum sensing in cognitive vehicular networks. Unlike existing methods, the proposed schemes transmit confused data during the aggregation process. This deliberate obfuscation makes it almost impossible to infer users' location from the transmitted data. The analysis demonstrates the resilience of the proposed schemes against sensing trajectory inference attack.

Keywords — Location privacy preservation, Cognitive radio network, Cooperative spectrum sensing.
Citation — Hongning LI, Tonghui HU, Jiexiong CHEN, *et al.*, "Privacy Preserving Algorithm for Spectrum Sensing in Cognitive Vehicle Networks," *Chinese Journal of Electronics*, vol. 33, no. 1, pp. 30–42, 2024. doi: 10.23919/cje.2022.00.007.

I. Introduction

With the continuous progress of smart city and intelligent transportation system (ITS) technology [1]–[3], there has been extensive attention to research on dependability and security in cognitive vehicular networks (CVN) [4]. The increasing ITS applications have exacerbated spectrum scarcity. Today's wireless communication systems follow fixed spectrum assignment policies, which leads to the contradiction between the scarcity of spectrum and the underutilization of existing spectrum due to the increasing number of users. Maximum utilization of the idle spectrum has become an effective way to alleviate this contradiction [5]. Cognitive radio (CR) is an enabling technology with the potential to increase spectrum utilization and provide desired interference protection to licensed users [6]. Cognitive radio networks (CRN) can improve channel utilization to meet the growing demand for wireless communication bandwidth [7], [8]. The application of CR technology enables a subset of vehicles to work as secondary users and opportunistically use the spectrum. As a result, the concept of CVN appeared. The same as CRN, vehicles within CVN can utilize idle channels but must obtain the channels' state before request. Cooperative spectrum sensing used in CR systems [9]–[13] is also applicable to CVN to improve spectrum sensing efficiency. One of the main technical challenges in dynamic spectrum access (DSA) system is to detect the existence of primary users' transmission, so as to determine the availability of a certain channel [14]–[16]. Cooperation among multiple secondary users, using their spatial diversity, is employed to enhance spectrum sensing performance [17]–[19]. Therefore, cooperative spectrum sensing has been widely used in CR system standard recommendations, such as IEEE802.22WRAN, CogNeA, IEEE802.11af, and WhiteFi [20].

Cooperative spectrum sensing also is vulnerable to a range of security threats [21]–[23]. In this paper, we consider privacy-preserving as the location privacy or trajectory privacy of vehicle users. Privacy protection in the network has received significant attention. For instance,

Associate Editor: Prof. Debiao HE, Wuhan University.

to achieve user anonymity in the network [24], Wang *et al.* designed a two-factor authentication scheme [25], [26] that can resolve various issues related to user corruption and server compromise. This scheme eliminates the long-standing security-usability conflicts, and offers security guarantees beyond the conventional optimal security bound. However, due to the unknown topology information and lack of privacy protection [27], the privacy issues cannot be adequately addressed in CVN.

Different technologies can be deployed to obtain vehicles' location in intelligent transportation system. In this paper, we focus on the spectrum sensing data that is related to users' location. We consider a new type of attack named sensing trajectory inference attack in CVN. Vehicles on the road continuously exchange sensing data with the surrounding vehicles and the roadside base stations [28], [29]. Therefore, malicious attackers can locate users with CR sensing report according to correlation between sensing report and physical location. The privacy breach allows attackers to obtain users' privacy and gain improper benefits [30]. Studies have shown that location privacy issues arise when multiple service providers (SPs) learn collaborative spectrum availability. Specifically, malicious authorized users (SP) or secondary users (SU) can use existing technology to locate corresponding users according to shared sensing data. These malicious entities may be untrusted SP/SU or external attackers. In such situations, the location privacy of mobile users may be leaked to untrusted entities, such as wireless service providers [31], [32].

In cooperative spectrum sensing, a potential solution to prevent the disclosure of location privacy is privacy-preserving aggregation technology. The fusion center (FC) can acquire spectrum availability data from various CR devices with privacy-preserving aggregation while ensuring the concealment of spectrum sensing data without any leakage [33], [34]. In this paper, we assume that the authentication center is absolutely credible while vehicles, roadside base stations and fusion centers are considered semi-honest. The FC can honestly perform the sensing aggregation report but has a curiosity regarding users' location information. Research also indicates that in illegal or even legal cases, untrusted wireless service providers may compromise the location privacy of mobile users [35], [36]. Therefore, if an FC is run by an untrusted service provider, it may illegally use reports to track individuals. The dynamic character of CR networks renders the privacy protection aggregation technology of static networks unsuitable [37], [38]. In addition, a new type of attack named differential location privacy (DLP) attack appears due to the dynamic network. In these attacks, attackers can estimate the report submitted by a specific user and infer its location information by comparing the change in aggregation results when the node joins or leaves the network [39], [40].

To solve the above problems in collaborative sensing, we propose a privacy-preserving algorithm for data aggregation based on two-party data confusion, called the data confusion-based privacy-preserving algorithm (DCPPA) for CVN spectrum sensing. The entities consist of vehicle users, roadside base stations, certification centers and integration centers. Among these entities, the authentication center is considered fully trusted, responsible for the distribution and authentication of user identity. Except for the authentication center, all other users are considered semi-honest models. The DCPPA comprises local sensing, user identity distribution and pairing, data segmentation and confusion, data package exchange and data aggregation. It divides and confuses generated privacy data, transmits the confused data through an intermediate layer, and aggregates data finally [41]. We also consider the scenario where no trusted certificate authority server is present. In such cases, we propose a cryptonym array-based privacy-preserving aggregation (CAPPA) scheme which can confuse sensing data with a cryptonym array.

The contributions of this paper can be summarized from two perspectives. First, for the location leakage issue caused by sensing data in CVN, we propose a DCPPA, which can achieve confusion by eliminating data features and allow each user to confuse its data with its corresponding paired user. Second, considering the scenario without trusted certificate authority servers, we propose a CAPPA method to preserve users' location. CAPPA enables each user to confuse its data with its antecedent and subsequent user in the array.

The remainder of this paper is constructed as follows. Section II describes the sensing trajectory inference attack. Section III presents the model and protocol of the proposed privacy-preserving algorithm in detail. Section IV involves a stimulation of the algorithms and compares them with other similar methods. Finally, Section V concludes this paper.

II. Sensing Trajectory Inference Attack

Cognitive vehicle network users face threats not only from traditional vehicle networks attacks such as CAN Bus protocol attack and communication hijacking attack, but also from trajectory tracking attacks caused by the leakage of sensing data. To accurately judge the spectrum states, cognitive vehicles continuously sense channels and interact with the surrounding vehicles to obtain spectrum-sensing data. The uploaded sensing data is related to users' privacy information. If these data are exposed, attackers can infer the vehicle's trajectory based on the channel's information, which results in the leakage of vehicle location privacy.

1. Attack description

A vehicle on the road continuously exchanges data with the surrounding vehicles and the roadside base stations. These data include signaling messages and media data for maintaining the collaboration and service of the Internet of vehicles (IoV). In the context of CVN, vehi-

cles gain access to the idle spectrum through cooperative sensing, and in this process, all participating users are required to submit sensing data to fusion centers. In the static cognitive wireless network, users usually sense the spectrum within the coverage area and upload the corresponding sensing data. However, in a mobile cognitive vehicle network environment, a vehicle traverses different spectrum coverage areas due to its mobility, requiring the detection of different channels. The trajectory of cognitive vehicles poses a risk of privacy leakage during this process.

On the one hand, a primary user in CVN is generally a roadside base station established for VANET communication. The signal coverage of a primary user is generally predetermined. After a vehicle uploads the sensing data of a primary user, it may expose its current location area and reveal its driving trajectory in the process of continuously sensing different channels.

On the other hand, the spectrum sensing information uploaded by a vehicle carries the characteristic of signal strength. According to the RSSI theorem, the signal strength can be used to predict the distance between the signal transmitter and the receiver. Consequently, the specific location of the vehicle becomes vulnerable to disclosure. When a vehicle uploads spectrum sensing information for different channels, its accurate location can be deduced through the existing positioning algorithm.

2. Attack models and assumptions

In a vehicular network, vehicles can only move on the road, and their locations are confined to overlapping areas of signal coverage and roads. The trajectory of the vehicle can be inferred using the city's road setting, the target PU location, and transmit power. This trajectory inference remains effective even in areas covered by multiple PUs. Once the fusion center obtains sensing data from the vehicle at different times, it attempts to infer the vehicle's trajectory. Attackers only need to obtain the sensing data of the vehicle at different times, and they can try to infer the approximate trajectory of the vehicle.

Figure 1 shows the attack model of CVN, where Vehicle A is in the coverage of Ch1 in the beginning. In the network, Vehicles B, C and D participate in spectrum sensing as cooperative users, sensing different channels in in their respective areas. To illustrate, we consider three spectrum channels, Ch1, Ch2 and Ch3, with their corresponding coverages shown in Figure 1. The roadside base stations R1 and R2 participate in data transmission as assistant nodes, and the sensing data fusion is completed by a third-party fusion center. Each fusion center aggregates data from one channel over a period of time. Vehicle users and fusion centers in CVN are considered semi-honest models, cooperating and distributing data according to predefined rules set before but susceptible to leaking data for additional benefits.

In addition, potential attackers may eavesdrop on data transmission and obtain other vehicles' private information through collaboration with vehicles and fusion centers. The attack steps are as follows.

Step 1 Vehicle A senses Band1, obtains sensing data D1 and uploads encrypted data S1 to the fusion center for Band1, with A's digital signature, which is defined as

$$S_1 = E(M_1) \cdot Sig(A) \tag{1}$$

In the equation (1), data is generally transferred through common channels.

Step 2 Attacker T intercepts the sensing data towards Ch1. Since the vehicle signature is contained in S_1, the attacker obtains the information that vehicle A is sensing Ch1. According to the spectrum location database of Ch1, the attacker infers that vehicle A is in the coverage of Ch1.

Step 3 The attacker colludes with the fusion center to obtain the real sensing data M_1 about Vehicle A and infer more accurate location of vehicle A according to the RSSI theorem. According to the semi-honest model in our paper, the fusion center, while decrypting the data packets and fusing the spectrum sensing data following the protocol, may leak the data for additional benefits. Therefore, through collusion, the attacker easily obtains the real sensing data M_1 of vehicle A, generally reflected by the received signal strength. The signal propagation loss model of the environment is defined as follows.

$$P_R(d) = \frac{P_T G_T G_R \lambda^2}{(4\pi)^2 d^2 L} \tag{2}$$

In the equation (2), P_T is the radiation power of the antenna, G_T is the gain of the transmitting antenna, G_R is the gain of the receiving antenna, L is a system loss factor independent of propagation, λ is the wavelength, in meters. When the antenna gain is 1, the formula simplifies to

$$L_p = 33dB + Nlog_{10}(d) + 20log_{10}(f) \tag{3}$$

After obtaining M_1, the attacker calculates the distance between vehicle A and the authorized primary user (PU_1). Vehicle A is located on the circumference with PU_1's position (x_{PU_1}, y_{PU_1}) as the center and the distance d as the radius. The current position of Vehicle A (x_1, y_1) is defined as follows.

$$(x_1 - x_{PU_1})^2 + (y_1 - y_{PU_1})^2 = {d_1}^2 \tag{4}$$

Coordinates can be set up with the origin at the position of any roadside base stations, without affecting subsequent data calculation.

Step 4 Ch1, Ch2 and Ch3 are sensed successively by vehicle A during moving. The attacker repeated Steps 2 and 3, colluding with the corresponding fusion centers

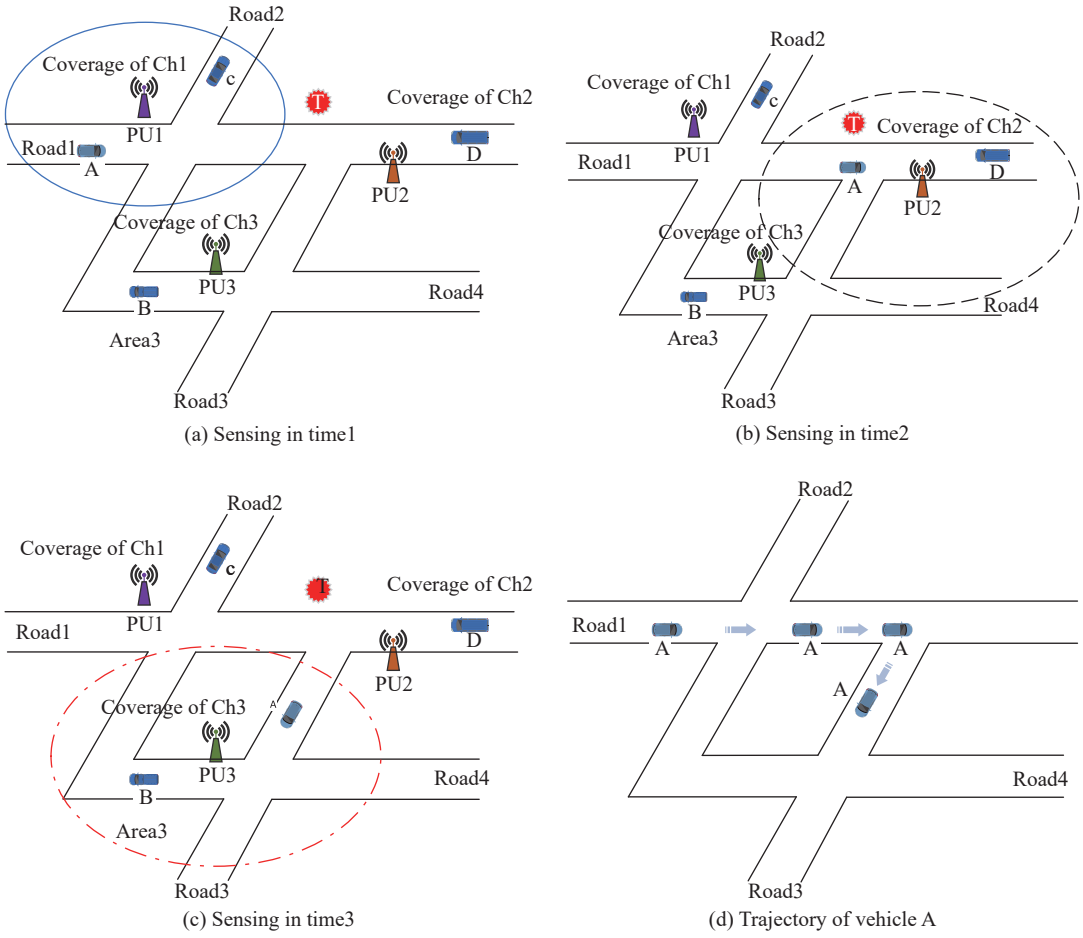

Figure 1 Process of inferring trajectory of vehicle A.

of these channels, to obtain the approximate trajectory of Vehicle A. The equations of the approximate trajectory are shown as follows.

$$(x_2 - x_{\mathrm{PU}_2})^2 + (y_1 - y_{\mathrm{PU}_2})^2 = {d_2}^2 \tag{5}$$

$$(x_3 - x_{\mathrm{PU}_3})^2 + (y_3 - y_{\mathrm{PU}_3})^2 = {d_3}^2 \tag{6}$$

In equations (5) and (6), the approximate trajectory of Vehicle A is from (x_1, y_1) to (x_2, y_2) to (x_3, y_3). The speculated path of Vehicle A is from Road1 to Road3, or from Road2 to Road4.

Step 5 When Vehicle A moves to the common coverage area of Ch1, Ch2, and Ch3, it uploads sensing information for multiple channels. An attacker can obtain the accurate location of Vehicle A through a positioning algorithm. Taking the three-point positioning algorithm as an example, the positioning point (x_4, y_4) is the intersection position of three circles expressed in equation (7).

$$\begin{cases} (x_4 - x_{\mathrm{PU}_1})^2 + (y_4 - y_{\mathrm{PU}_1})^2 = d_1'^2 \\ (x_4 - x_{\mathrm{PU}_2})^2 + (y_4 - y_{\mathrm{PU}_2})^2 = d_2'^2 \\ (x_4 - x_{\mathrm{PU}_3})^2 + (y_4 - y_{\mathrm{PU}_3})^2 = d_3'^2 \end{cases} \tag{7}$$

Equation (7) only has a unique solution, which is the exact position of the vehicle A at that time. According to the existing trajectory information, the attacker can draw more accurate tracking trajectory of Vehicle A. In this case, the driving path of Vehicle A is from Road1 to Road3, as shown in Figure 1. Therefore, the real path of the vehicle is leaked.

III. Data Confusion-Based Privacy Preserving Algorithm for Spectrum Sensing in CVN

In this section, we propose two privacy-preserving algorithms for spectrum sensing that protect private data based on user group and encryption array, respectively. Before delving into the proposed algorithms, we give a list of notations used in this paper, detailed in Table 1.

1. Data confusion-based privacy-preserving algorithm

In this section, we propose DCPPA. The details are as follows:

In the DCPPA, we adopt two-party data confusion. The network is composed of vehicle users, primary users, roadside base stations, certificate authority (CA) servers, public cloud and fusion centers. The CA server is assumed absolutely credible, responsible for the distribution and authentication of users' identity. Except for the authentication center, all users are considered semi-honest models. These semi-honest users will complete their

Table 1 Notation

Notation	Description
SP	Service providers
PU	Primary user, whose channel states can be sensed by spectrum sensing
SU	Secondary user, in this context, refer to vehicle users
CR	Cognitive radio
CRN	Cognitive radio network
CVN	Cognitive vehicular networks
DSA	Dynamic spectrum access
FC	Fusion centre
DLP	Differential location privacy
Honest	The behavior of the honest party is absolutely credible and will not betray or falsify
Semi-honest	Semi-honest will aggregate data according to the protocol, but it is more curious about the user's location information and may leak data illegally
STIA	Sensing trajectory inference attack
ITS	Intelligent transportation system
IoV	Internet of vehicles

own calculation and interaction tasks in accordance with the protocol. However, they are curious about the real data of other users. There is a possibility of collusion among them to obtain the real data of target users for additional benefits. The structure of the network is shown in Figure 2.

IoV is committed to improving travel safety and experience using collected information to monitor and manage vehicles. IoV entities include vehicles, roadside units, data centers, and people [42]. The proposed DCPPA is composed of five components: local sensing, user identity distribution and user pairing, data slicing and confusion, data packet exchange, and data aggregation. In the data fusion process, vehicle users act as secondary users (SU), CA and FC correspond to data centers, and edge nodes represent roadside units in the IoV. The details are shown in Figure 3.

1) Local sensing

First, vehicle users perform local sensing based on their respective locations and the existing spectrum in corresponding areas. M_i represents local spectrum sensing results of U_i. Next, the vehicle cooperates with the nearby vehicle users to aggregate data.

2) User identity distribution and user pairing

Before participating in data aggregation, the CA server verifies each user and ensures the credibility of their identity information. When the number of users n is even, the CA server randomly divides n users $(U_1, U_2, \ldots, U_n)$ into $n/2$ pairs, denoted as $G_1, G_2, \ldots, G_{\frac{n}{2}}$, and generate sequences $\{k_1, k_2, \ldots, k_n\}$ of a fixed length. The sequences satisfy the following conditions: $\forall i,\ i \in \{1, 2, \ldots, n\},\ \exists j,\ j \in \{1, 2, \ldots, \mathrm{n}\},\ j \neq i,\ k_i \oplus k_j = (1\ 1\ \cdots\ 1)$. $\nexists j',\ j' \in \{1, 2, \ldots, n\},\ j' \neq j,\ k_i \oplus k_{j'} = (1\ 1\ \cdots\ 1)$. The CA server then divides these sequences into $n/2$ groups with the rule of $k_i \oplus k_j = (1\ 1\ \cdots\ 1)$ and distributes the $n/2$ groups sequences to $n/2$ pairs of users randomly. The sequences distributed to each pair of users are referred to as pairing sequences. Each sequence in different pairs is unique and irrelevant. For each pair of users U_i and U_j, the corresponding sequences satisfy conditions as follows:

$$k_i \oplus k_j = (1\ 1\ \cdots\ 1) \tag{8}$$

The pairing sequence is used in subsequent pairing and verification as an identity symbol. Users in a pair form paired users of each other.

Each user has its own sequence and the sequences of the paired users conform to the above conditions in equation (8). There is no correlation between different paired sequences. The pairing sequence only works in the cur-

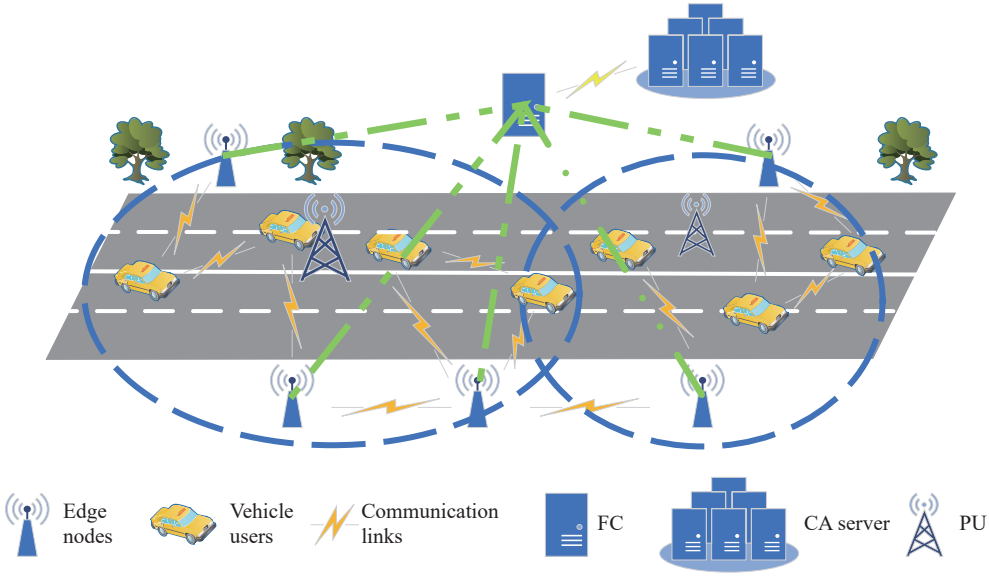

Figure 2 Structure of the network.

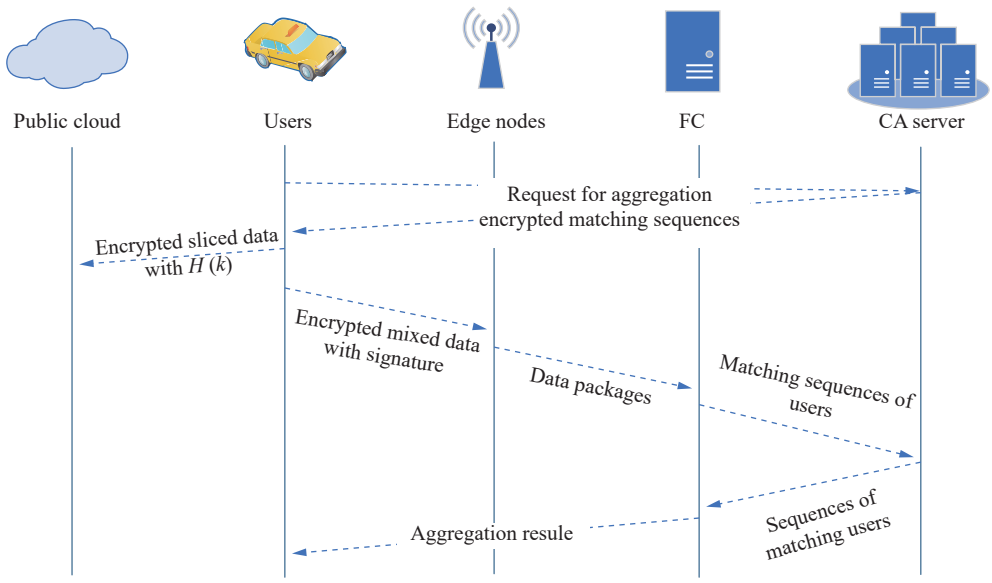

Figure 3 Process of DCPPA.

rent data aggregation round. To participate next round data aggregation, each user must request to the CA server for a new pairing sequence. Besides, the CA server transmits pairing sequences with timestamps of the current round to thwart replay attacks. When the CA server distributes the corresponding pairing sequences to users, shared keys are applied to ensure the security and verifiability of the distribution process.

Once a user U_i receives sequence k_i from the CA server, it calculates the hash value $H(k_i)$ corresponding to the pairing sequence.

When the CA server identifies that the number of users participating in this aggregation round is odd, it randomly selects one user as a single user and communicates its identity. The user designated as a single user will receive a single sequence as its pairing sequence.

Briefly, the user pairing algorithm is shown as Algorithm 1.

Algorithm 1 User pairing

while $n = even$ do
  CA divides n users into $n/2$ groups;
  CA generates and transmits k_i for user U_i;
  for each k_i do
    There is $k_j \oplus k_i = 1 \ldots 1$;
  end
  for each U_i do
    U_i slices data M_i to M_{i1} and M_{i2};
    U_i uploads $(H(k_i) \cdot E_{k_i}(M_{i2}))$;
    U_i searches for $H(k_j)$;
    if $H(k_j) = H(\sim k_i)$ then
      U_j is the paired user of U_i;
    end
  end
  User uploads data $\{E_{k_i}(M_i') \cdot E_{CA}[D_{U_i}(k_i) \cdot k_i]\}$;
end
while $n = odd$ do
  Repeat above;
  CA chooses one user as the alone user and transmit k_i to it;
  Alone user uploads data $\{E_{k_i}(M_i) \cdot E_{CA}[D_{U_i}(k_i) \cdot k_i]\}$;
end

3) Data slicing and confusion

Users first randomly split their own spectrum sensing data into two components, defined as

$$M_i = M_{i1} + M_{i2} \tag{9}$$

In equation (9), we illustrate with the example of a user U_i. User U_i splits sensing data M_i into M_{i1} and M_{i2}.

Subsequently, User U_i encrypts a part of its own data M_{i2}, using its paired sequence k_i through symmetric encryption, and packages it with the hash value of the pairing sequence to form the intermediate data, defined as

$$N_i = (H(k_i), E_{k_i}(M_{i2})) \tag{10}$$

User U_i attaches a timestamp to N_i and uploads it to the public cloud, which serves exclusively for data storage and sharing. All users have access to the data shared on the public cloud.

After the upload of all users, User U_i searches for N_j, uploaded by its paired user U_j on the public cloud, defined as

$$H(k_j) = H(\sim k_i) \tag{11}$$

In cases of multiple consistent data, the user places trust in the data with the earliest timestamp. User U_i uses the key $\sim k_i$ to decrypt $E_{k_j}(M_{j2})$ and obtain M_{j2} to calculate the confusion sensing data, defined as

$$M_i' = M_{i1} + M_{j2} \tag{12}$$

Then, U_i encrypts the confused data M_i' with the key of the fusion center, defined as

$$E_i = \left(E_{FC}\left(M_i'\right), E_{CA}\left[D_{U_i}\left(k_i\right), k_i\right]\right) \tag{13}$$

In equation (13), U_i signs the sequence k_i, and encrypts the signed k_i and k_i with the public key of CA. U_i combines the encrypted signature and encrypted data.

In the case that the number of users is odd, the single user packs its sensing data and sequence, and sends the encrypted data to directly FC, without the need for data confusion.

4) Data package exchange

In our scheme, an intermediate layer exists between vehicle users and the fusion center, generally composed of assistant roadside base stations. These intermediate layer nodes serve as edge nodes for data packaging and distribution to reduce data link losses caused by multi-hop transmission. Similar to vehicle users, these intermediate layer nodes adhere to a semi-honest model.

After vehicle users complete data slicing and confusion, a randomly selected group of authorized nodes is required to complete a ring signature for data E_i. The specific steps are as follows:

First, we define a function as follows:

$$\begin{aligned} C_{k,v}(y_1, y_2, \ldots, y_r) = {} & E_k(y_r \oplus E_k(y_{r-1} \oplus E_k(y_{r-2} \\ & \oplus E_k(\cdots \oplus E_k(y_r \oplus v) \cdots)))) \end{aligned} \tag{14}$$

In equation (14), E_k is the symmetric encryption algorithm, and k is the symmetric key of E_k. Each member in the ring has an RSA public key $P_i = (n_i, e_i)$. We define $f_i\left(x\right) = x^{e_i} \left(\mathrm{mod}\, n_i\right)$. The message m is represented by bits, satisfying $m = q_i n_i + r_i$, which is defined as

$$g_i(m) = \begin{cases} q_i n_i + f_i(r_i), & \text{if } (q_i+1)n_i \leq 2^b \\ m, & \text{otherwise} \end{cases} \tag{15}$$

Assuming the message to be signed is m, the symmetric key is $k = h\left(m\right)$. If the signer is the S-th member of the ring r, the signer randomly selects its initial value v from $\{0,1\}^b$. The signer selects x_i from $\{0,1\}^b$ for other ring members and calculates y_i by $y_i = g_i\left(x_i\right)$. Then calculate y_s by solving the equation $C_{k,v}(y_1, y_2, \ldots, y_r) = v$. The signer calculates x_s by solving $x_s = {g_s}^{-1}\left(y_s\right)$. The signature of message m is defined as

$$CS = (P_1, P_2, \ldots, P_r; v; x_1, x_2, \ldots, x_r) \tag{16}$$

After the signature is completed, the user packages the signature CS and E_i as (CS, E_i) and sends it to the adjacent edge nodes.

All edge nodes verify the signature upon receiving packets. One edge node may receive several encrypted confused data. After each edge node packs these data, it exchanges data with adjacent nodes and ensure that each edge node exchange packet at least once before transferring the packet to the fusion center.

5) Data aggregation

Data aggregation is performed by the fusion center which can be a third-party service provider, or a large base station on the roadside. It is also assumed to be semi-honest in this paper.

After the fusion center receives the data from edge nodes, it decrypts the data packets with its own private key, separating the encrypted signature $E_{CA}[D_{U_i}\left(k_i\right), k_i]$ and the confusion data M_i'. The fusion center sends the encrypted signatures of all users it received to the CA server, which can check the authenticity of the pairing sequence. Then, the CA server checks and removes the lost sequences and the corresponding paired users, returning the completed paired sequences to the fusion center.

The fusion center receives the sequences from the CA server and then fuses these data, calculating the final fusion results.

For the condition of an odd number of users, even if the fusion center is aware that one user in the system is single, it has no knowledge of the single user's identity.

2. Cryptonym array-based privacy-preserving aggregation

In the DCPPA proposed above, the security of paired users relies on a trusted CA to a certain extent. In the scenario without trusted certificate authority server, we propose a cryptonym array-based privacy-preserving aggregation (CAPPA) scheme. The difference between CAPPA and DCPPA is the process of user selection.

We consider that the network consists of the vehicle users, a fusion center and a third-party sequencer (which can be a roadside unit). The users, FC and the sequencer are all semi-honest. The CAPPA scheme is comprised of three parts: array setup, data slicing and confusion, and data aggregation. When the data is already acquired by the users, an array of users will be set up by the third-party sequencer through interaction with users. The users slice and confuse data in accordance with the array sequence. The FC will aggregate the mixed data into the final result. The detailed steps are as follows.

1) Array setup

We propose an array setup algorithm with the characteristic of anonymity, through which all users can form an array according to a certain sequence. With the array setup algorithm, each user can only obtain the information of its antecedent and subsequent users in the array without knowledge of other users in the array.

Step 1 We denote the users that attend the aggregation as $U_1, U_2, \ldots, U_n$. The third-party sequencer generates n sequences with the same length, denoted as $\{S_1, S_2, \ldots, S_n\}$, and repacks the n sequences three by three as $\{(S_1S_2S_3), (S_2S_3S_4), \ldots, (S_nS_1S_2)\}$. There is no relation between the sequences and the users at this stage.

Step 2 Each user uses a ring signature and sends

its sharing key $k_i\,(i=1,2,\ldots,n)$ (encrypted with the public key of the third-party sequencer) anonymously to the sequencer. The sharing k_i meets $k_0+k_1+k_2+\cdots+k_n=0$, where k_0 is the sharing key of FC. The sequencer has no knowledge of all users' identities.

Step 3 After receiving all keys in step 2, the sequencer randomly chooses one sharing key $k_j\,(j=1,2,\ldots,n)$ and encrypts one repack sequence. The sequencer repeats this until all sequences are encrypted with different keys. After this, the sequencer will add the hash value of the corresponding keys and obtain the information, shown as

$$\{E_{k_i}\left(S_1S_2S_3\right)H\left(k_i\right),E_{k_j}\left(S_2S_3S_4\right)H\left(k_j\right),\ldots\} \tag{17}$$

Then, the sequencer shares the information in equation (17) in a public cloud.

Step 4 Each user $U_i\,(i=1\ n)$ searches the corresponding hash value of its key k_i, and extracts the corresponding sequences.

Step 5 After all users obtain the array sequences, each user compares its array sequence with all other users using the solution to Yao's Millionaires' Problem. Then, each user can obtain the identities of its antecedent and subsequent user in the array to continue the subsequent aggregation.

2) Data slicing and mixing

After the array setup, all users form a circle structure, where each user holds the identities of its antecedent and subsequent users in the circle. All users in the array remain unaware of the entire sequence of the circle.

To illustrate the data confusion process, let's consider user U_i. U_i holds actual data M_i, which is divided into two parts, M_{i1} and M_{i2}, defined as

$$M_i=M_{i,1}+M_{i,2} \tag{18}$$

In equation (18), U_i encrypts a part of its sliced data with the public key of its subsequent user U_{i+1}, attaching its signature to the encrypted data as the intermediate data N_i. U_i then transfers data N_i to its subsequent user U_{i+1}. N_i is represented as

$$N_i=\left(E_{i+1}\left(M_{i,2}\right),D_i\left[H\left(M_{i,2}\right)\right]\right) \tag{19}$$

Once U_{i+1} receives the data N_i from U_i, it decrypts N_i with its private key to obtain M_{i2}, and verifies the authenticity of data through the signature of U_i. Then, U_{i+1} calculates the data it needs to upload C_{i+1} as follows:

$$M_{i+1}=M_{i+1,1}+M_{i+1,2} \tag{20}$$

$$M'_{i+1}=M_{i+1,1}+M_{i,2} \tag{21}$$

$$C_{i+1}=E_{FC}(M'_{i+1}+k_{i+1}) \tag{22}$$

Each user in the array mixes part of its data with the antecedent users and sends the other part of its data to the subsequent user for further mixing.This process is shown in Figure 4.

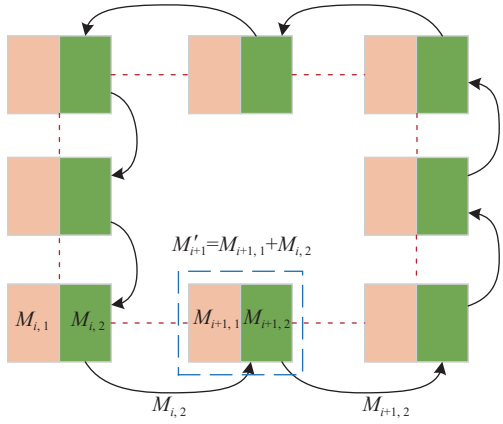

Figure 4 The data slicing and mixing in cryptonym array.

3) Data transmission and aggregation

After completing the data confusion, users need to generate a ring signature for the data ready for uploading in equation (22). Each user uploads the encrypted data $C_i\,(i=1\ n)$ with the generated ring signature to the FC.

After receiving all the data $(C_1,C_2,\ldots,C_n)$ from users, FC verifies the ring signature and then calculates the aggregation data as follows:

$$s=\sum_{i=1}^{n}\left(M_i{}'+k_i\right) \tag{23}$$

The DCPPA and CAPPA are designed to provide privacy protection for vehicle users. These schemes use a privacy protection method based on data confusion to process sensing data, eliminating the relationship between sensing data and users' location by data confusion. Therefore, they can effectively resist STIA.

IV. Simulation and Analysis

In this section, we analyze and simulate the security and efficiency aspects of the proposed schemes from data privacy, communication overhead and complexity, conspiracy attack and link failure [39]–[41].

1. Sensing data privacy

With the DCPPA algorithm proposed in this paper, the data submitted by users in the process of data aggregation cannot accurately reflect channel characteristics due to multiple rounds of data confusion and encryption. When an attacker intercepts these confused data, they are unable to infer the driving trajectory of any specific vehicle. This is because the confused data bears no direct relation to the actual data of any individual.

The proposed CAPPA algorithm is carried out in an environment without a trusted certification center. By implementing an anonymous sorting method in the CAP-

PA algorithm, vehicle users can form a queue with a certain order based on their needs. The complete sorting of the queue remains confidential, even to the vehicle users themselves, who are only aware of the user identities of their antecedent and subsequent vehicles, but lack knowledge of the complete queue order. For an attacker to obtain the data of a certain user, they must first obtain the encrypted confused data, decrypt it, identify the user's antecedent and subsequent vehicles and then launch a collusion attack. The security of CAPPA depends on public key encryption and data confusion.

Vehicle users are required to perform local sensing and interact with others to exchange split sensing data. The difference between DCPPA and CAPPA lies in the selection of data interaction objects. In DCPPA, each user must cooperate with its paired user to exchange split sensing data, and then transmit confused data during the aggregation process. On the other hand, CAPPA employs an array setup algorithm that generates an array. In CAPPA, each user mixes its data with its antecedent and subsequent user in the array to continue the subsequent aggregation. Both schemes can eliminate the individual sensing data characteristics. The underlying security logic of the two algorithms is basically the same, leading to similar privacy protection. For illustration, the DCPPA is used in this context.

In this section, we simulate scenarios where attackers attempt to collect transmitted sensing data from vehicle users and calculate these data to locate vehicle users. We use the MATLAB platform for simulation and set several roadside base stations and vehicle users to illustrate. Each primary user is characterized by corresponding signal parameters, including initial transmit power, approximate signal coverage, etc. The transmit power is set at 10 W (40 dBm), the frequency is around 5900 MHz, and the coverage generally extends to 500 m. Data beyond this range is considered white noise. Five vehicle users are randomly selected as the observation objects. The vehicle users calculate their receiving power according to the propagation loss model and upload the sensing results to the fusion center. If vehicle users submit their spectrum sensing data directly, attackers can easily locate vehicle users by intercepting spectrum sensing data. Subsequently, the attackers can draw the trajectory of vehicle users through road information and multiple positioning results. Due to Gaussian white noise in the environment, a positioning error of less than 20 m is deemed effective. In the evaluation, we set up a uniform axe of the network for convenience and ensure that the selection of the origin of coordinates does not influence the evaluation.

We use the above settings and the DCPPA privacy protection algorithm for sensing data aggregation and simulate attackers attempting to locate a vehicle user. Since the DCPPA scheme is set up identity anonymity, it is difficult for an attacker to obtain the real situation of the vehicle through some measures. The positioning error is shown in Figure 5.

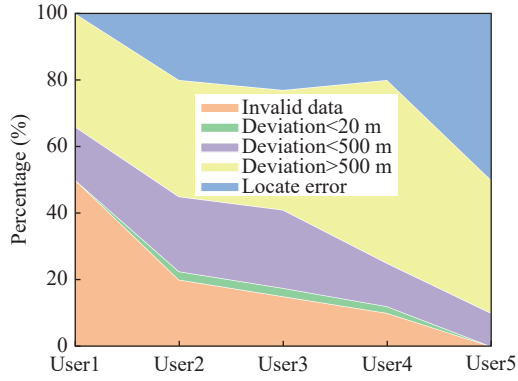

Figure 5 Location error.

From Figure 5 in our simulation, we can conclude that: 1) When the signal strength of the spectrum sensing data intercepted by the attacker is less than the environmental noise threshold, the data becomes meaningless, rendering users untraceable. 2) When the signal strength of the intercepted spectrum sensing data exceeds the base station emission intensity, the data loses its meaningfulness. 3) Except for the two cases above, the vehicle location obtained from the sensing data is quite different from the actual location. Therefore, attackers are unable to effectively track users using the data transmitted with DCPPA.

The experimental results demonstrate that most of the data processed by the DCPPA can confuse the real results, which has a significant resistance to the spectrum sensing trajectory reasoning attack of the cognitive vehicle network. The algorithm exhibits robust data protection performance.

2. Communication overhead and computational complexity

On the premise of data security, we discuss the performance of the DCPPA in terms of communication overhead and time complexity. A comparative analysis is conducted with four classical data aggregation privacy protection algorithms: PPA [30], CPDA [43], SMART [43] and PHES [44] for comparison. According to the respective protocols of the algorithms, CPDA and SMART share similarities. The calculation is mainly concentrated on the public key encryption, resulting in same time complexities, when utilizing the same public key encryption algorithm. Taking RSA as an example, it focuses on public key encryption and hash algorithms. The complexity of encryption and decryption is shown in Table 2.

It can be seen from Table 2 that the time complexity of DCPPA is of the same order of magnitude as CPDA and SMART schemes. PPA, although not disclosing its key generation algorithm, exhibits higher time complexity based on the encryption algorithm outlined in the protocol. On the other hand, PHES demonstrates slightly smaller time complexity than that of DCPPA, CPDA and SMART.

Table 2 Complexity of different algorithms

Privacy protection method	DCPPA	CPDA	SMART	PPA	PHES
Encryption	RSA, Hash	RSA	RSA	Self-defining	ECC
Decryption	RSA, Hash	RSA, Dematrix	RSA	Self-defining	ECC
Complexity	$O\left(n(\log n)^2\right)$	$O\left(n(\log n)^2\right)$	$O\left(n(\log n)^2\right)$	$O\left(n^2\right)$	$O(\sqrt{n})$

In terms of communication overhead, we consider the total overhead within the system, including the data flow of user nodes, roadside base stations and aggregation centers. We simulate in MATLAB and set several nodes in the network to calculate the communication overhead.

As shown in Figure 6, the introduction of roadside base stations results in a marginally higher cost for DCPPA than that of the SMART scheme, with both falling within the same order of magnitude. The overhead tendency for DCPPA is the same as CPDA and SMART schemes, exhibiting a linear increase with the growing number of nodes. The PPA scheme, because of the frequent key generation and exchange, sees quadratic growth in communication overhead with the increase in the number of nodes. With sufficient nods in the network, it incurs a much higher increase in communication overhead than other schemes.

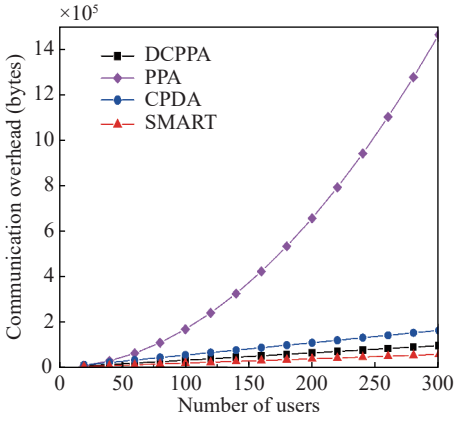

Figure 6 Comparison of scheme overheads.

In addition, we compare the communication overhead among different data aggregation schemes at the same level affected by cluster size (n) changes. As shown in Figure 7, CDPA and SMART are greatly influenced by cluster size.

3. Collusion attack

In this section, we consider collusion attacks in which attackers collaborate with other vehicle users to obtain sensitive information. As mentioned above, in DCPPA, all nodes except CA are semi-honest models. These users complete their own calculations and interactive tasks based on the calculation protocol while remaining curious about the data of other users, possibly leaking their own or other users' data for extra benefits. Considering this, attackers may collude with other vehicle users or fusion centers.

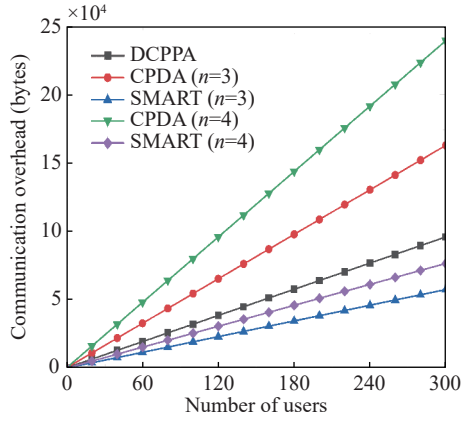

Figure 7 Comparison of cluster size effects.

Similarly, we compare our scheme with CPDA, SMART and PPA data aggregation privacy protection schemes. In the CPDA scheme, the probability of privacy leakage caused by collusion is related to the size of the cluster. Larger clusters require more colluding users for attackers to obtain the real data of a user. In the SMART scheme, the probability of privacy leakage caused by collusion is not only related to the size of the cluster, but also to the number of data fragments. For the PPA scheme, adopting the n-n threshold, attackers need to collude with all other users to obtain the data of the remaining users due to the existence of a secret sharing algorithm. It shows the same performance as the proposed DCPPA.

It can be seen from Figure 8 that in extreme cases where all users form a cluster in CPDA and SMART, the data leakage probability curves for the four schemes are coincident, with consistent resilience against collusion attacks. When the CPDA scheme and the SMART scheme reduce the cluster for convenience and time complexity, their collusion resistance performance decreases. The proposed DCPPA is consistent with the PPA scheme, requiring full collusion with all the other users to restore the real data of the remaining single user.

4. Link failure effects

Combining the additive homomorphic encryption schemes with additive homomorphic threshold secret sharing enables the private distribution and aggregation of multiple data streams, even in vulnerable networks [44]. We consider the impact of a single communication link failure on overall data aggregation. During vehicle-vehicle or vehicle-fusion center communication, disconnections in communication links and data loss can occur. In the pro-

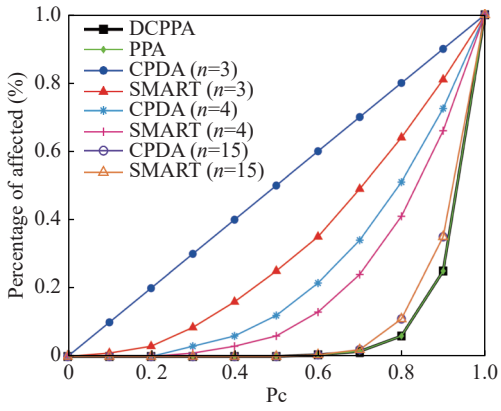

Figure 8 Data leakage probability comparison.

cess of sensing data aggregation, the utilization of a privacy protection algorithm for data evolution implies that the loss of a single link data may affect the overall data aggregation.

Through comparative experiments with 20 nodes in the three aggregation algorithms, we measure the affected data ratio. For CAPPA and DCPPA algorithms, a smaller number of clusters corresponds to a lesser impact of a single link failure on overall data. The PHES algorithm [44] solves data security and privacy by combining threshold secret sharing with homomorphic encryption. In the event of a disconnected link and data loss, it directly affects the data aggregation, rendering the data unable to be correctly aggregated. In DCPPA and CAPPA, the effect of communication link failure tends to increase with an increasing number of link failures. There is no significant influence with several link failures.

It can be concluded from Figure 9 that the homomorphic encryption used in PHES hardly considers the impact of link failure on the overall data aggregation. A failure in one data link within the network affects all other data. However, due to the data confusion between the two parties, the proposed DCPPA in this paper only affects the data of the paired user data when a single user link fails, with the aggregation of other paired users unaffected.

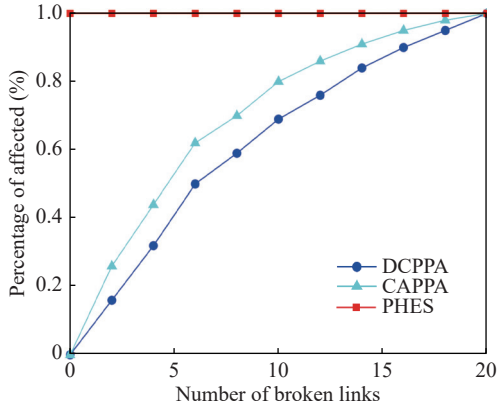

Figure 9 Link failure effects.

With data confusion, the proposed CAPPA exhibits similar performance in data protection and provides a defence against collusion attacks. Since the step of array setup involves solving Yao's Millionaires' Problem, the communication overhead is higher than DCPPA.

V. Conclusion

Location privacy is a growing concern nowadays. This paper delves into the issue of location privacy disclosure in cooperative spectrum sensing, with a focus on two types of attacks: sensing trajectory inference attack and collusion attack. To effectively preserve user location privacy, we propose a scheme named data confusion-based privacy-preserving algorithm (DCPPA) for cognitive vehicle networks, in which data aggregation is based on two-party data confusion. This scheme involves the division and confusion of the generated privacy data. The confused data is then transmitted through an intermediate layer, and aggregated at the final stage. Besides, we also introduce a cryptonym array-based privacy-preserving aggregation (CAPPA) method for scenarios without a trusted authentication center. We analyze and simulate the security and efficiency of DCPPA, accompanied by simulations to evaluate its performance. The experimental results show the effectiveness of our schemes. In our future work, we will optimize the data aggregation method without an authentication center.

Acknowledgement

This work was supported by the National Key Research and Development Program of China (Grant No. 2021YFB2700600), the National Natural Science Foundation of China (Grant No. 61902292), the Key Research and Development Programs of Shaanxi (Grant No. 2021ZDLGY06-03), and the High-level Innovation Research Institute Project (Grant No. 2021B0909050008).

References

[1] Y. W. Zhang, L. Li, G. F. Li, *et al.*, "Smart transportation systems for cities in the framework of future networks," in *Proceedings of the 4th International Conference on Artificial Intelligence and Security*, Haikou, China, pp. 70–79, 2018.

[2] Y. X. Li, J. Ni, J. B. Hu, *et al.*, "The design of driverless vehicle trajectory tracking control strategy," *IFAC-PapersOnLine*, vol. 51, no. 31, pp. 738–745, 2018.

[3] C. Chen, T. T. Xiao, T. Qiu, *et al.*, "Smart-contract-based economical platooning in blockchain-enabled urban internet of vehicles," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4122–4133, 2020.

[4] H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, 2008.

[5] C. Chen, J. C. Li, V. Balasubramaniam, *et al.*, "Contention resolution in Wi-Fi 6-enabled internet of things based on deep learning," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5309–5320, 2021.

[6] K. Arshad and K. Moessner, "Collaborative spectrum sens-

ing for cognitive radio," in *Proceedings of 2009 IEEE International Conference on Communications Workshops*, Dresden, Germany, pp. 1–5, 2009.

[7] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 79–89, 2007.

[8] A. O. Arafat, A. Al-Hourani, N. S. Nafi, *et al.*, "A survey on dynamic spectrum access for LTE-advanced," *Wireless Personal Communications*, vol. 97, no. 3, pp. 3921–3941, 2017.

[9] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[10] W. Zhang, R. K. Mallik, and K. B. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5761–5766, 2009.

[11] Y. L. Che, R. Zhang, and Y. Gong, "Opportunistic spectrum access for cognitive radio in the presence of reactive primary users," in *Proceedings of 2011 IEEE International Conference on Communications*, Kyoto, Japan, pp. 1–5, 2011.

[12] A. W. Min, K. H. Kim, J. Pal Singh, *et al.*, "Opportunistic spectrum access for mobile cognitive radios," in *Proceedings of 2011 Proceedings IEEE INFOCOM*, Shanghai, China, pp. 2993–3001, 2011.

[13] K. W. Choi, E. Hossain, and D. I. Kim, "Cooperative spectrum sensing under a random geometric primary user network model," *IEEE Transactions on Wireless Communications*, vol. 10, no. 6, pp. 1932–1944, 2011.

[14] M. di Felice, L. Bedogni, and L. Bononi, "DySCO: A dynamic spectrum and contention control framework for enhanced broadcast communication in vehicular networks," in *Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access*, Paphos, Cyprus, pp. 97–106, 2012.

[15] S. Pagadarai, B. A. Lessard, A. M. Wyglinski, *et al.*, "Vehicular communication: Enhanced networking through dynamic spectrum access," *IEEE Vehicular Technology Magazine*, vol. 8, no. 3, pp. 93–103, 2013.

[16] Y. Han, E. Ekici, H. Kremo, *et al.*, "Throughput-efficient channel allocation algorithms in multi-channel cognitive vehicular networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 757–770, 2017.

[17] S. Anjana and S. Nandan, "Energy-efficient cooperative spectrum sensing: a review," in *Proceedings of the 2018 Second International Conference on Inventive Communication and Computational Technologies*, Coimbatore, India, pp. 992–996, 2018.

[18] F. Li, Z. G. Sheng, J. Y. Hua, *et al.*, "Preference-based spectrum pricing in dynamic spectrum access networks," *IEEE Transactions on Services Computing*, vol. 11, no. 6, pp. 922–935, 2018.

[19] F. B. S. de Carvalho, W. T. A. Lopes, M. S. Alencar, *et al.*, "Cognitive vehicular networks: an overview," *Procedia Computer Science*, vol. 65 pp. 107–114, 2015.

[20] S. Pagadarai, A. M. Wyglinski, and R. Vuyyuru, "Characterization of vacant UHF TV channels for vehicular dynamic spectrum access," in *Proceedings of 2009 IEEE Vehicular Networking Conference*, Tokyo, Japan, pp. 1–8, 2009.

[21] K. D. Singh, P. Rawat, and J. M. Bonnin, "Cognitive radio for vehicular *ad hoc* networks (CR-VANETs): Approaches and challenges," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, no. 1, article no. 49, 2014.

[22] M. Di Felice, K. R. Chowdhury, and L. Bononi, "Cognitive radio vehicular ad hoc networks: Design, implementation, and future challenges," in *Mobile Ad Hoc Networking: Cutting Edge Directions*, S. Basagni, M. Conti, S. Giordano, *et al.*, Eds. John Wiley & Sons Inc., Hoboken, NJ, USA, pp. 619–644, 2013.

[23] C. Chembe, E. M. Noor, I. Ahmedy, *et al.*, "Spectrum sensing in cognitive vehicular network: State-of-art, challenges and open issues," *Computer Communications*, vol. 97, pp. 15–30, 2017.

[24] D. Wang and P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle and solutions," *Computer Networks*, vol. 73, pp. 41–57, 2014.

[25] D. Wang, D. B. He, P. Wang, *et al.*, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2015.

[26] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.

[27] I. H. Brahmi, S. Djahel, and Y. Ghamri-Doudane, "A hidden Markov model based scheme for efficient and fast dissemination of safety messages in VANETs," in *Proceedings of 2012 IEEE Global Communications Conference*, Anaheim, CA, USA, pp. 177–182, 2012.

[28] W. Wang and Q. Zhang, "Privacy-preserving collaborative spectrum sensing with multiple service providers," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1011–1019, 2015.

[29] J. W. Tong, M. Jin, Q. H. Guo, *et al.*, "Cooperative spectrum sensing: A blind and soft fusion detector," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2726–2737, 2018.

[30] S. Li, H. J. Zhu, Z. Y. Gao, *et al.*, "Location privacy preservation in collaborative spectrum sensing," in *Proceedings IEEE INFOCOM*, Orlando, FL, USA, pp. 729–737, 2012.

[31] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

[32] R. L. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[33] J. Ma, G. D. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 11, pp. 4502–4507, 2008.

[34] Z. Q. Li, F. R. Yu, and M. Y. Huang, "A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 383–393, 2010.

[35] C. I. Fan, S. Y. Huang, and Y. L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 666–675, 2014.

[36] Y. N. Liu, W. Guo, C. I. Fan, *et al.*, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1767–1774, 2019.

[37] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 32–39, 2018.

[38] L. Xing, Q. Ma, J. P. Gao, *et al.*, "An optimized algorithm for protecting privacy based on coordinates mean value for cognitive radio networks," *IEEE Access*, vol. 6 pp. 21971–21979, 2018.

[39] H. N. Li, Y. Gu, J. X. Chen, *et al.*, "Speed adjustment attack on cooperative sensing in cognitive vehicular networks," *IEEE Access*, vol. 7 pp. 75925–75934, 2019.

[40] J. X. Chen, S. S. Huang, H. N. Li, *et al.*, "PSO-based agent cooperative spectrum sensing in cognitive radio networks," *IEEE Access*, vol. 7 pp. 142963–142973, 2019.

[41] H. N. Li, J. X. Chen, L. Wang, *et al.*, "Privacy-preserving data aggregation for big data in financial institutions," in *Proceedings of IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops*, Toronto, ON, Canada, pp. 978–983, 2020.

[42] Q. Jiang, X. Zhang, N. Zhang, *et al.*, "Three-factor authentication protocol using physical unclonable function for IoV," *Computer Communications*, vol. 173 pp. 45–55, 2021.

[43] W. He, X. Liu, H. Nguyen, *et al.*, "PDA: privacy-preserving data aggregation in wireless sensor networks," in *Proceedings of the IEEE INFOCOM 2007–26th IEEE International Conference on Computer Communications*, Anchorage, AK, USA, pp. 2045–2053, 2007.

[44] J. Zouari, M. Hamdi, and T. H. Kim, "A privacy-preserving homomorphic encryption scheme for the Internet of Things," in *Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference*, Valencia, Spain, pp. 1939–1944, 2017.

Hongning LI received the B.S. degree in information and computing science, the M.S. degree in cryptography, and the Ph.D. degree in computer architecture from Xidian University, Xi'an, China, in 2007, 2010, and 2014, respectively. From 2014 to 2016, she held a postdoctoral position at Xidian University, where she is currently a Lecturer with the School of Telecommunications Engineering. Her research interests include wireless networks and security, security and privacy in cognitive radio networks, and cognitive vehicular networks. (Email: hnli@xidian.edu.cn)

Tonghui HU received the B.S. degree in network engineering from North China University of Water Resources and Electric Power, in 2021, where she is currently pursuing the M.S. degree in cyberspace security. Her research interests include privacy protection, wireless networks and security, and cognitive vehicular networks.
(Email: tonghuihu0314@gmail.com)

Jiexiong CHEN received the B.S. degree in information engineering, and the M.S. degree in telecommunication engineering from Xidian University, in 2018, and 2021, respectively. His research interests include privacy protection and cognitive vehicular networks.
(Email: jc872274253@live.com)

Xiuqiang WU received the B.S. degree in applied mathematics from Xianyang Normal University in 2007, and received the M.S. degree in applied mathematics from Xidian University in 2010. He is now working in CEPREI as a Network Security Engineer. His research interests include wireless networks security and privacy.
(Email: wuxiuqiang@ceprei.com)

Qingqi PEI received the B.S., M.S., and Ph.D. degrees in computer science and cryptography from Xidian University, in 1998, 2005, and 2008, respectively, where he is currently a Professor and a Member of the State Key Laboratory of Integrated Services Networks. His research interests include digital contents protection, wireless communication networks security, and information security. He is also a professional Member of the ACM and a Senior Member of the Chinese Institute of Electronics, and the China Computer Federation.