Participant Selection Strategy With Privacy Protection for Internet of Things Search

PENG YANG\textsuperscript{1,2,3,4}, XUYUAN KANG\textsuperscript{1,3,4}, QIMING WU\textsuperscript{1,3,4}, BORAN YANG\textsuperscript{1,3,4}, AND PUNING ZHANG\textsuperscript{1,3,4}

\textsuperscript{1}West Institute of CAICT of MIIT, Chongqing 401336, China
\textsuperscript{2}School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
\textsuperscript{3}Optical Communication and Networks Key Laboratory of Chongqing, Chongqing 400065, China
\textsuperscript{4}Ubiquitous Sensing and Networking Key Laboratory of Chongqing, Chongqing 400065, China

Corresponding author: Peng Yang (yangpeng@caict.ac.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant (61901071, 61771082, 61871062), in part by the Program for Innovation Team Building at Institutions of Higher Education in Chongqing CXTDX201601020, in part by the General Project of Natural Science Foundation of Chongqing under Grant cstc2019jcyj-msxmX0303, and in part by the Science and Technology Research Program of Chongqing Municipal Education Commission under Grant KJQN201800615.

\textbf{ABSTRACT} Nowadays, with the rapid developments of the Internet of Things, the information on physical entities has shown explosive growth. The emergence of Internet of Things search technology has facilitated the storage, organization, and management of massive entity information. Aiming at the issues of security and privacy and the target to obtain the optimal perceiving results by selecting participants to ensure the quality of service of the IoT platform, this paper proposes a participant selection strategy with privacy protection for IoT search (PSSPP). Firstly, the search task requester and the task contents are anonymized and blinded respectively, and then individual attributes of participants are mapped to hide the identity information of participants. Secondly, in order to choose the participants who meet the task requirements, the participants are preliminarily selected based on the bloom filter. Finally, the perceiving trust value and relative credibility of participants in participating tasks are dynamically evaluated. Simulation results demonstrate that the proposed scheme can reduce the attack probability of malicious users toward task requesters and participants, and rationally select the appropriate task participants.

\textbf{INDEX TERMS} IoT search, mobile crowd sensing, participant selection, privacy-preserving, bloom filter.

\textbf{I. INTRODUCTION}

In recent years, the developments of the Internet of things have promoted the deployment of a large number of intelligent sensing devices into the physical world, and also facilitated the applications of intelligent objects in the industrial field [1], especially the developments of smart cities, artificial intelligence and other intelligent industries [2]. In the future world where everything is connected, every person and every object will become the carrier of data information and also the user of data information, which leads to the explosive growth of Internet of things information and the increase of the difficulties of effective storage [3], [4] and rational use of information.

With the gradual deepening of the research on the Internet of Things, the integration of physical space and cyberspace has gradually deepened [5], and users’ demands for real-time, effective and reliable access to physical entity information are increasingly improved, which promotes the birth of Internet of things search technology [6]. Physical information (such as objects, people, etc.) can be obtained by adopting the Internet of things search technology, and then these information will be managed and stored in an organized and ordered way to facilitate users to search [7]–[9]. The entity state information is perceived and observed by its associated sensor, and the user can search the entity by specifying the demand state [10] via its sensor. For example, the user may query the suitable and free meeting rooms in the current office building, or search for a restaurant that is quiet and has fewer people. The search contents include not only the static properties of meeting rooms, restaurants and other entities, but also the dynamic spatio-temporal properties such as current and nearby, as well as time-varying state such as temperature suitability. Traditional Internet search methods are designed...
only for static virtual resources [11], which are unsuitable for searching for physical entities search whose state changes dynamically.

However, in the actual IoT applications, the entity information monitored by the deployed sensing devices may be insufficient. Meanwhile, as the deployers of sensing devices are individuals with social attributes [12] and own the characteristic of selfishness, the deployed sensing devices only observe the entity information they need, which leads to incomplete or even missing of entity information. Therefore, when a user executes a search request, due to insufficient entity information, the user may make wrong decisions which cause unnecessary losses, thereby further affecting the user’s search experience. Aiming at this problem, this paper adopts the idea of mobile crowd sensing to solve the incomplete problem of entity information due to the differences in the deployment location and purpose of the sensing devices.

Currently, with the popularity of mobile intelligent devices, such as smart phones, tablets and wearable devices, sensors with diverse functions have been integrated in the smart devices, which gives these devices sensing, storage, communication, and computing capabilities. This makes it possible to obtain environmental state by means of mobile crowd sensing to improve the physical information collected by the Internet of things platform. However, in mobile crowd sensing [13], the person who initiates the search task and the participant who performs the perception task are ones with social attributes. Thus, the information security and privacy of the personnel interacting with the Internet of things platform is one of the key issues [14] that must be solved. At the same time, the inherent personal preferences may lead to the deviation of participants’ perception task results [15]. Therefore, selecting trusted task participants [16] that are compatible with the search task request is the key process for improving the search service experience of the search task requester.

In order to solve the incompleteness of the information collected by the IoT platform due to the difference in the deployment location and purpose of the sensing device, this paper introduce the idea of mobile crowd sensing method to solve this problem. A participant selection strategy with privacy protection for Internet of things search is proposed to improve the service quality of the IoT platform. Anonymous and secure attribute mapping schemes are adopted to avoid malicious user attacks, and then the optimal participants are selected to perform the perceiving tasks by calculating the match ability of the participants, thereby enhancing the service quality of the IoT-search. The main contributions are listed below:

- A security method based on pseudonyms and partially blind signatures is proposed. By blinding the identity of the search task requester during the participation in the task and the content of the task, the source identity information of the requester is hidden to ensure the privacy of the requester during the task process.
- An attribute representation method based on the attributes of participants and requesters is presented. By utilizing the Bloom filter, a binary data structure with higher space efficiency is used to store and protect the privacy of participants and requesters, and select candidate participants.
- A participant selection method based on dynamic assessment of trust state is devised. According to the participants’ perceiving trust value and relative credibility, the optimal participants are selected to obtain efficient and reliable perception results.

The rest of this paper is organized as follows: Section II introduces the related work. Section III describes the system model. Section IV proposes an anonymous and secure attribute mapping scheme. Section V designs the comprehensive selection method for participants. Section VI verifies the proposed scheme. Section VII concludes this paper.

II. RELATED WORK

At present, in the field of IoT search, there are few research on mobile intelligent sensing device search. Existing achievements mainly focus on fixed deployed sensing device search. The user searches for the sensing device associated with the entity to physical entity state. Literature [17] constructed a fuzzy set on the observation sequences of the sensing devices, calculated the similarity between the observation sequence of the candidate sensing device and the user-specified observation sequence, thereby obtaining a set of sensing devices with similar output. Literature [18] proposed a similarity-based entity search method-PLSS in the Internet of Things. The similarity was estimated by calculating the Euclidean distance of the observation sequence between the specified entity and the candidate entity, and the matching entities were searched and ranked according to the similarity. However, when the fixed-deployment sensing device is deployed, its owner only concerns his own needs and purposes, which may lead to incomplete information obtained by the IoT platform. Because the requesters of different search tasks have individual requirements, in this case, it is difficult for the IoT platform to meet such requirements. However, the emergence of mobile crowd sensing can better solve this problem due to its enhanced sensing capabilities and the flexibility of sensing methods.

Some researches on privacy protection and participant selection in mobile crowd sensing networks has been carried out. Literature [19] proposed a participant selection strategy to protect the privacy of participants and task requesters. Task requesters can select participants according to their own needs, and only those who meet the requirements can submit data. In addition, this strategy protects geographic location information and personal privacy information of participants by introducing a cloud platform. Literature [20] presented a centralized security solution, and considered the privacy of task requesters. All task queries, including the identity of task requesters, were conducted through the third-party platform,
but the premise of this solution was that the third-party platform must be completely trusted. Literature [21] provided a way to choose participants with privacy protection. The task initiator published the perception task on the perception platform, and the participants downloaded the task and matched it to choose the task that best fits their own background. In this way, participants did not need to disclose any private information to the sensing platform in order to receive the sensing task, but the scheme neglected to consider the privacy of the task initiator. Literature [22] utilized the security assertion markup language (SAML)and the secure transport layer protocol (TLS)to establish trust between entities, while using inadvertent transport protocols to implement a privacy-secure entity communication protocol to achieve anonymous participant information. The establishment of various secret keys between participants effectively protected the privacy of the participants, but made the sensing platform unable to choose the participants, and chose to participate in the task autonomously in an active participant selection mode.

Other researchers have proposed privacy protection and participant selection strategies based on participant trust. Literature [23] proposed a distributed participant selection strategy based on maximizing social benefits. The trust value of participants was calculated locally instead of the sensing platform. Since participants did not need to expose their own privacy information in the process of participant selection, the privacy protection of participants was indirectly realized. Literature [24] presented a strategy for calculating participant levels based on the trust and ability, and considered both the reliability of the trust transfer path and the path’s privacy leakage probability in the participant selection process as the requirements for selecting participants, So as to achieve the purpose of selecting high-quality participants under the premise of privacy protection. Literature [25] implemented a privacy protection strategy based on trust management. The participants’ trust value was divided into several levels and was mapped with the privacy information sensitivity level, so that when evaluating the behaviors of the participants, it is impossible to infer the true ID of the participants, and finally completed the evaluation of the participants’ credibility in the case of anonymity, thereby achieving privacy protection and data trust management.

In this paper, a participant selection strategy with privacy protection for IoT search is proposed to solves security and privacy problems caused by attackers via anonymous task publishing and task participation and protect the privacy information of participants and requesters.

III. SYSTEM AND ATTACK MODEL
As shown in figure 1, the system model adopted in this paper includes three entities: IoT platform, search task requester and participant. First, as a search task requester, the user applies a pseudonym to the IoT platform, and then uses the pseudonym in the process of publishing the sensing task. The search task requester divides and partially blinds these attribute information according to the privacy of the task content, and then generates its own set of attribute requirements through the method of attribute mapping and sends it to the IoT platform. Then, after receiving the task, the participants choose whether to participate in the sensing task according to their own attributes. If participating in a sensing task, participants use attribute mapping to map participant attributes to Bloom filters and build participant Bloom filters, and upload requests to the IoT platform. The IoT platform uses privacy matching to select candidate participants to perform the sensing task. Finally, the IoT platform submits the candidate participants to the search task requester. The search task requester updates the historical interaction records with the candidate participants, and combines the participants’ historical task completion status and the quality of completed tasks to evaluate the participants’ comprehensive trust and select the optimal participant. The selection results will be sent to the optimal participants through the IoT platform to complete the sensing task. Consider that the system model may be subject to malicious attacks during the selection process of participants. However, the attack behaviors studied at present all assume that there is a potential attack behavior in one of the above three entities. Obviously, in the actual environment, such assumption is too idealistic and seriously overestimates the protection ability of the proposed method for privacy information. In order not to lose generality, the attack method mentioned in this paper does not target any functional entity in the network. The node that initiates the attack behavior can be the search task initiator, the node with the same sensing task, or even the IoT platform. This paper focuses on the types of attacks against search task requesters and participants performing tasks in the participant selection process.

In an attack against a search task requester, the attacker can use the task information to infer relevant information about the requester, since some sensitive information may be

FIGURE 1. System model.
displayed in the task published by the search task requester. Because the type and content of the task published by the requester of the search task requester are closely related to the privacy of the requester, the task type may expose the interest and hobbies of the requester as well as the geographical environment and so on. An attacker can infer valuable information related to the requester by collecting historical request tasks of the requester, thereby launching a malicious attack.

In an attack against a participant who performs a task, during the process of selecting and performing a sensing task by the participant, the participant needs to upload the sensing result to the IoT platform. In this process, private information such as the participant’s location, personal ability, and communication ability is easily leaked. At the same time, the situation and type of participants’ tasks are also easily exploited by malicious attackers.

### IV. ANONYMOUS AND SECURE ATTRIBUTE MAPPING SCHEME

When a search task requester publishes a sensing task, the sensitive information carried in the content of the published task may be the target of the attacker, thereby being stolen or attacked by the attacker. At the same time, in the process of participating in the task, participants will have a set of sensitive identity attributes, and this privacy is easily leaked. Therefore, this paper uses identity signatures and blinding to protect the requester’s information, and maps the participants’ attributes to a set of binary vectors and generates participant bloom filters. Similarly, the task requester’s task requirement attributes are mapped into a set of binary vectors to prevent the attacker’s attack.

#### A. ANONYMOUS TASK PUBLISHING

In the process of participants applying for tasks and performing sensing tasks, the task type, data submission time, and data content are all potentially useful information for the attacker, and the attacker can infer the requester’s privacy from these data. In order to protect the identity information of the requester, the requester first obtains a pseudonym on the IoT platform before task requests. The requester registers with his or her real ID, and the IoT platform authenticates and returns a seed $\tau = H(\text{sign}_{sk} \parallel N_{id})$ to the requester to indicate the legality of the pseudonym randomly generated by the requester. $\text{sign}_{sk}$ is the signature of the IoT platform and $N_{id}$ is the authenticity ID of the requester. The requester uses $\tau$ as a random seed to create a pseudonym $N_p$ to hide his or her true identity. The pseudonym $N_p$ is generated by a pseudo-random sequence function $f_k$, and $h$ represents a length-matched hash function as a generator of the random function, $M$ represents a system parameter, which is a constant.

$$N_p = h(f_k(\tau)) \mod M \quad (1)$$

The search task requester $Q$ uses $N_p$ to request the platform to publish a task, and the platform needs to sign the task to ensure the verifiability of the task during task distribution. However, the task requested by the requester may contain some sensitive information, and the task type may expose the interest and geographic location of the requester. Since the type and content of the task are closely related to the privacy of the requester $Q$, the IoT platform or malicious participants can use the task information to infer valuable information related to the requester $Q$, thereby launching a malicious attack. In this paper, the partial blind signature is used to protect the privacy of the requester during the task request before any sensitive information of the requester $Q$ is known to the IoT platform. The search task requester $Q$ is signed, while the privacy of $Q$ and the verifiability of the task are guaranteed.

In this paper, We divide the attribute information into common information $\text{ComInfo}$ and sensitive information $\text{SenInfo}$ according to the degree of privacy. Where $\text{ComInfo}$ refers to the basic requirements of the task, such as the start date, the deadline, and the amount of perceived data requested, which will not be related to the identity information of the requester $Q$. And $\text{SenInfo}$ refers to the requester’s specific requirements for the task, such as the perceived location, which may involve the requester’s specific interests, geographic location and environment. $\text{ComInfo}$ is visible to the platform, while $\text{SenInfo}$ is hidden. $h(\bullet)$ represents a secure cryptographic hash function, $r$ represents a random number, and $m = h(\text{SenInfo})$ represents a random number of the user’s sensitive information. $Q$, $S$ represent task requester, IoT platform respectively.

$$Q \rightarrow S : m_b = h(\text{SenInfo}) \cdot r^e \mod N, \text{ComInfo} \quad (2)$$

After receiving the request information of the requestor’s sensing task, the IoT platform $S$ first verifies whether its identity is legitimate. After successful verification, it signs the request information with the private key $sk$, and returns the signed information $m'$ to $Q$. In this process, the IoT platform $S$ only verifies the general information of the task and the identity of the requester, but does not know the specific situation of the task, which ensures that when the requester applies for the task, the IoT platform cannot infer the privacy of the requester through analyzing the data of the task.

$$S \rightarrow Q : m' = [m_b]_{sk} \quad (3)$$

$Q$ receives the information $m'$ returned from the IoT platform, removes the blind factor $r$, and obtains the task information sequence $m^*$ with the signature of the IoT platform, thereby submitting the sensing task to the IoT platform, and the IoT platform completes the release of the sensing task.

$$Q : m^* = r^{-1} \mod N = [h(\text{SenInfo})]_{sk} \quad (4)$$

#### B. ATTRIBUTE REPRESENTATION METHOD

In the system model proposed in this paper, in order to improve the efficiency of the services provided by the IoT platform, this paper uses Bloom Filter (BF) for attribute representation. BF is a probabilistic data structure with high space efficiency. It consists of a long binary vector and a
participate matches a task, including the participant’s profession, hobbies, behavioral characteristics, and so on. Where \(time(t)\) represents the user limitation, which is used to measure whether the participant can perform the sensing task in time, depending on the response time of participant and the deadline of the task. We use the growth curve function to quantify the limitation ability, as shown in equation (6), where \(t\) is participants idle time, \(d\) is the task deadline, \(x, b\) and \(c\) are model parameters. If the limitation ability score is higher, it indicates that the participant has completed the task earlier. As the score decreases and the time to complete task increases, the lowest value indicates that it can be completed near the task deadline.

\[
time(t) = 1 - \left[ (1 - x) e^{-b(e^{-ct})} \right] \text{ if } t < d \quad (6)
\]

On the participant side, after the participant completes his or her own profile, through the equation (5), the participant’s experience attribute can be expressed as \(\text{attributes}_P = \{Ap_1, Ap_2, \ldots, Ap_n\}\). For each element in the set, the participant uses his own private key to sign each attribute in the set \(\text{attributes}_P\). The signed attribute can be expressed as equation (7):

\[
\text{Ap}_i = H_0(\text{Ap}_i \parallel \text{ComInfo}) (H(\text{ComInfo}) + x)^{-1} \quad (7)
\]

where, \(H, H_0\) are hash functions, so the attribute set \(\text{Ap} = \{\text{Ap}_1, \text{Ap}_2, \ldots, \text{Ap}_n\}\) signed by the user can be obtained. Participant maps the signed attribute set to the Bloom filter, and selects the corresponding hash function set \(H = \{h_0, h_1, \ldots, h_{q-1}\}\) for each participant \(P = \{P_1, P_2, P_3, \ldots, P_n\}\) to be evaluated, where the hash function \(h_0, h_1, \ldots, h_{q-1}\) is independent of each other and the range is all \([0, w - 1]\), all the initial values of are set to \(1^0\)s, the length of \(BF\) is set to \(m\), and \(m \geq q\). As shown in Fig. 3(a), for all \(w_i \in W\) and \(0 \leq i \leq k - 1\), let \(BF[h_i(w_i)] = 1\), participant Bloom filter \(BFs\) is obtained, as shown in Fig. 3(b).

On the task requester side, the requestor’s task requirement attribute set can be expressed as \(\text{attributes}_Q = \{AQ_1, AQ_2, \ldots, AQ_m\}\). In order to hide the sensitive information of the task from the participants to avoid malicious attackers inferring the requester information based on the task

\[
\text{FIGURE 2.} \text{ The mapping principle of Bloom filter. (a) Initialization state. (b) Element mapping.}
\]

\[
\text{FIGURE 3.} \text{ Bloom filter for participant attribute mapping. (a) Participant initial state. (b) Participant attribute mapping.}
\]
Based on this, the task requester can get a blinded task attribute set $A_Q = \{A_{Q1}, A_{Q2}, \ldots, A_{Qn}\}$.

$$A_{Qi} = H_0(a_{Qi} \| ComInfo) \quad (8)$$

V. METHOD OF THE COMPREHENSIVE SELECTION OF PARTICIPANTS

In participant selection, the participant selection process is an important factor that affects the quality of sensing information. The goal of participant selection is to choose the optimal participant who can complete the sensing task and obtain high-quality sensory data. However, the sensitive data of some participants is easy for eavesdropping by malicious users to cause privacy leaks, and malicious users may publish false information and cause task quality to decrease. Therefore, in this paper, in the process of the comprehensive selection of participants, first of all, preliminary selection of candidate participants, and then selection of optimal participants.

A. CANDIDATE PARTICIPANTS SELECTION

Regarding the problem of trust matching in participant selection, most of the methods assume that each user has a set of attributes such as location, occupation, interest, professional, etc. When a task requester requests a sensing task, the requirements of the sensing task are also listed in a task attribute set, such as the task sensing location, the required time, and the sensing type. Before the task is released, the platform evaluates the matching degree between the participant’s attribute set and the task attribute set. The more the two sets share the element, the higher the user suitability for the task. The whole process does not reveal the user’s personal attribute information, but these schemes have certain limitations. The matching function only considers the number of common attributes, ignoring the difference in the user preference for each attribute. Simply relying on the existence of attributes, it is easy for attackers to steal user privacy through narrow task attacks. Therefore, this paper selects participants based on the degree of matching between participants and task requirements.

When a search task requester requests a task from the IoT platform, the requester may wish to define a set of requirements that require participants with specified expertise or similar experience to perform the task, or participants living in a specific geographic area. In this paper, the requester’s sensing task requirement is defined as an attribute vector, which contains the attributes of the sensing task requirement and preference degree. Among them, the attribute information is expressed as $attributes_Q = \{A_{Q1}, A_{Q2}, \ldots, A_{Qn}\}$. Because the requester may not meet the basic conditions of the task, first select candidate participants based on the attribute information, and then further measure the degree of participants’ preference for attributes, and optimize the process of trust evaluation.

First, participants generate their own profile information, sign it with a private key, and construct a Bloom filter based on their own profile information. On this basis, Bloom filter is used as the attribute storage structure, and the attribute characteristics meeting the task requirements are filtered by trust privacy matching. When participating in a task, the participant $P$ sends $BFs$ constructed by himself to the IoT platform, as shown in equation (9):

$$P \rightarrow S : BF_{s} \quad (9)$$

The requester sends task attribute attributes $A_Q = \{A_{Q1}, A_{Q2}, \ldots, A_{Qn}\}$ and $NP$ to the IoT platform, as shown in equation (10):

$$Q \rightarrow S : (NP, A_Q) \quad (10)$$

IoT platform receives $(NP, A_Q)$ and first verifies the legality of the requester identity. Then according to the received blind request task request attribute sequence and the trust file $BFs$ sent by the participant, utilizing the principle of the Bloom filter, each part of the task request is inserted into $BFs$ in order, and the calculation result is checked. If equation (11) is satisfied, it is proved that the participant’s experience includes the attribute $A_Q$.

$$[BF[h_0(A_Q)] = 1] \land [BF[h_1(A_Q)] = 1] \land \ldots \land [BF[h_k(A_Q)] = 1] \quad (11)$$

Because the Bloom filter is based on the verification of the hash function, and the hash function result is unique, the Bloom filter match results are not all one-to-one. In order to select the participants with the high matching degree, similarity calculation is needed for the results of privacy matching through the bloom filter. Assume that the number of bits occupied by the participant bloom filter and the task requester is $c$ and $d$, and the same number of matches is $g$, where $k \leq c \land k \leq d$. Similarity measures are used to comprehensively assess the degree of similarity between two things. The Dice coefficient is a set of similarity measure functions that calculates the similarity of two strings. This paper combines the Bloom filter to calculate the matching degree between the participant and the task requester, as shown in equation (12).

$$D_{Par.Req} = \frac{2g}{c + d} \quad (12)$$

Task requester inserts task requirements into the Bloom filter according to the trust file set $BF_{ps} = \{BF_{p1}, BF_{p2}, \ldots, BF_{pn}\}$ of participant $P = \{P_1, P_2, \ldots, P_n\}$ to be evaluated, and then, according to the privacy matching method, it determines whether participant has each attribute requirement of task and combines the Dice coefficient to select candidate participants, and this stage does not consider the degree of preference of participant’s attributes. Where the candidate participant set is represented by $P'$. After privacy matching, the requester can detect candidate participants who have the task attribute requirements. After this stage,
the IoT platform selects enough participants to complete the participants privacy matching phase and initially select candidate participants that meet task attribute requirements.

## B. OPTIMAL PARTICIPANT SELECTION

Throughout the perception process, the IoT platform is based on a large number of participants. Participants have a high degree of flexibility and mobility, and differences in the mobile devices they carry and their geographic locations result in different levels of trust among participants. Relative credibility is an important parameter for measuring data reliability. Higher relative credibility means stronger data reliability. Therefore, how to select participants with relatively high credibility to complete the sensing task accurately and in real-time has become a key technical challenge. The trust value is the quantification of the subjective trust degree of participants’ ability, security and credibility in a specific environment and in a specific period of time by the IoT platform. Compared with the security scheme based on the password system, the security scheme based on trust evaluation is more effective in preventing attacks from legitimate internal nodes. In this paper, the participant trust value is used to represent the reliability of the participants in the task execution process, so as to select the best participant that is more suitable for the task.

Participants may have the same task experience. The relative credibility of this paper aims to measure the trust relationship between participant \( P_i \) and requester \( Q_j \) through historical interaction records. Malicious participants often improve their credibility by continuously acquiring tasks, consequently intercepting task information in the network and launching an attack. Therefore, participant trust status can be estimated by task completion status and task completion quality. \( e_{ij}^{(k)} \) denotes the satisfaction degree of the requestor \( Q_j \) for the task being executed \( k_{th} \) times. \( E_{ij} = \{e_{ij}^{(1)}, e_{ij}^{(2)}, \ldots, e_{ij}^{(h)}\} \) denotes the satisfaction set of latest \( h \) times, where \(-1 \leq e_{ij}^{(k)} \leq 1, e_{ij}^{(k)} < 0 \) denotes \( Q_j \) is not satisfied with \( P_i \) generally, and the dissatisfaction increases with the decrease of the value; \( e_{ij}^{(k)} > 0 \) denotes \( Q_j \) is satisfied with the \( Q_i \) in general, and the higher the satisfaction with the increase of the value, \( h \) denotes the total number of interactions between \( P_i \) and \( Q_j \). The relative credibility \( R(P_i, Q_j) \) of \( P_i \) to \( Q_j \) can be calculated by equation (13), where \( \gamma(k) \) represents the attenuation factor. Among all the historical interaction, the weight value of satisfaction of the latest interaction is the largest. Therefore \( \gamma(k) \) is used to assign weight values to satisfaction at different times to ensure timeliness of relative credibility, which can be denoted as equation (14).

\[
R(P_i, Q_j) = \begin{cases} 
\sum_{k=1}^{h} e_{ij}^{(k)} & \gamma(k) \neq 0 \\
0 & \gamma(k) = 0 \end{cases} 
\]

\[\gamma(k) = \frac{k}{k + 1}\]  

After the privacy matching, the attribute preference that meets the task required in the candidate participant attributes can be denoted as \( \text{attributes}^{P_{CQ}} = \{A_{C1}, A_{C2}, \ldots, A_{Cn}\} \). By calculating the similarity between the degree of preference required by the task and the degree of preference of the participant, thereby obtaining the sensing trust value of participants in the task. \( \text{W}_{P_{CQ}} \) and \( \text{W}_{Q} \) respectively denotes the attribute preference of the candidate participants and task requirements, where \( \text{W}_{P_{CQ}} = (w_{c1}, w_{c2}, \ldots, w_{cn}) \), \( w_{ci} = \left( \frac{w_{qi}}{1}, 1, \ldots, 1, 0, 0, \ldots, 0 \right) \); \( \text{W}_{Q} = (w_{Q1}, w_{Q2}, \ldots, w_{Qn}) \).

\[
w_{qi} = \left( \frac{w_{qi}}{1}, 1, \ldots, 1, 0, 0, \ldots, 0 \right)
\]

The similarity function of task requirement vector and participant attribute vector can be calculated to obtain sensing trust \( \text{Strust} (P, Q) \) of the participant by equation (15).

\[
\text{Strust} (P, Q) = \frac{2 \sum_{i=1}^{w_{ci}=w_{qi}=w_{P_{CQ}}} \min (w_{ci}, w_{qi})}{\sum_{i=1}^{w_{ci}} w_{ci} + \sum_{i=1}^{w_{qi}} w_{qi}} 
\]

Selecting more reliable participants to complete tasks during the participant selection process can effectively improve the service quality of the IoT platform. The privacy matching first selects the participants, and then the IoT platform reports the candidate participants to the task requester, and the task requester selects the optimal participant. Whether a participant can participate in the task also depends on the relatively comprehensive trust status of the participant, that is, the perceived trust value and relative credibility, and then comprehensively consider the final trust value \( F\text{trust} (P, Q) \) of the participant to complete the participant selection process, as shown in equation (16). As can be seen from the above, \( h \) represents the number of interactions between the candidate participant and the task requester, and \( \text{time} \) is the time limit during which the participant can complete the task. The task requester will select the participant with a high final trust value among the candidate participants to perform the sensing task, thereby completing the trust state perception process of the participant.

\[
F\text{trust} (P, Q) = \frac{\text{time}(t)}{h^2 + \text{time}(t)} \cdot \text{Strust} (P, Q) + \frac{\text{time}(t)}{h^2 + \text{time}(t)} \cdot R (P, Q) 
\]

After candidate participants are obtained, task requester queries the historical interaction record with itself in \( \overline{P} \), and calculates the relative credibility of each participant in \( \overline{P} \), and finally obtains the final trust value through the comprehensive sensing trust evaluation of sensing trust value and relative credibility of participants. All candidate participants \( \overline{P} \) are iteratively screened in a manual search mode, as shown in Algorithm 1. After the sensing trust value and relative
credibility respectively satisfy the basic threshold $\phi$ and $\gamma$, the participant with the highest final trust value in the current iteration is selected as the optimal participant. Specifically, the participants set $\overrightarrow{P}$ is first determined. Then, for each $P_i \in \overrightarrow{P}$, which is selected by checking the following conditions: 1) the sensing trust value of any candidate participant $P_i$ is not less than a threshold $\phi$, that is $\forall Strust(P, Q)_{P_i} \geq \phi$; 2) the relative credibility of any candidate participant is not less than a threshold $\gamma$, that is $\forall R(P, Q)_{P_i} \geq \gamma$; 3) after 1) and 2), participant set $P_i$ is traversed and sorted, and task requester selects $\nu$ participants according to the task requirements and stores them into the selection list $SeleList$ to obtain the optimal participants set $\overrightarrow{P}$, as shown in equation (16). Finally, the task requester notifies the selected participant of the election result through the IoT platform. The pseudocode with the optimal participant selection mechanism is shown in Algorithm 1.

Algorithm 1 The Optimal Participant Selection Mechanism

1. **Input:** $\overrightarrow{P} = \{P_1', P_2', ..., P_j'\}$: Participant set, $\phi$: $Strust(P, Q)_{P_i}$ of the threshold, $\gamma$: $R(P, Q)_{P_i}$ of the threshold, $\nu$: Number of participants required for this mission, $SeleList$: Selected participants.
2. **Output:** $\overrightarrow{P}$: Optimal participant set.
3. **repeat**
4. Extract candidate participants $\overrightarrow{P} = \{P_1', P_2', ..., P_j'\}$;
5. for each candidate participant $P_i' \in \overrightarrow{P}$ do
6. if $\forall Strust(P, Q)_{P_i'} \geq \phi$ & $\forall R(P, Q)_{P_i'} \geq \gamma$ then
7. Participant set $P_i' \rightarrow P_i''$;
8. Calculate the final trust value of $Ftrust(P, Q)$;
9. end if
10. end for
11. Sorting final trust value $Ftrust(P, Q)$ of participant set $P_i''$;
12. Choose $\nu$ best participants and Store to list $SeleList$;
13. until All Candidate participants $\overrightarrow{P} = \{P_1', P_2', ..., P_j'\}$ are screened;

When the participant completes sensing task released by the IoT platform and the search task requester receives the data, the search task requester updates the trust value of the corresponding participant according to the optimal selection participant process, and then a pseudo-credit token $H_{\overrightarrow{P}}(Ftrust(P, Q))$ generated by a hash function is sent to the participant. After waiting for a random period, the participant sends it to task requester in a true identity $ID_P$, combined with a pseudo-credit token $H_{\overrightarrow{P}}(Ftrust(P, Q)), ID_P$. Task requester hashes the final trust value $Ftrust(P, Q)$ of the participant for verification. After successful verification, the trust value of the participant is updated to the latest value.

After the participant is updated, the participant enters the next task again.

VI. SIMULATION ANALYSIS

In this section, we validate the proposed scheme by employing the ONE [26] and make a comparison with the service discovery strategy proposed in [20] and [27]. Among them, the proposed participant selection strategy for privacy-preserving in [20] is a typical coordinated distribution method. The specific simulation parameters are shown in Table 1.

| Parameter                                      | Numerical value |
|-----------------------------------------------|-----------------|
| Simulation duration/s                        | 43200           |
| Network size/m²                              | 4500*3400       |
| Number of participants                       | 80              |
| Communication method                         | Bluetooth       |
| Transmission range/m                        | 10              |
| Transmission rate /KBps                      | 250             |
| Movement speed of participants m/s           | 0.5-1.5         |
| Message size /KB                            | 10-200          |
| Message generation interval /s               | 25-35           |
| Stay time of participants /s                 | 0-10            |
| Buffer size /M                              | 0.2             |

Table 1. Parameter settings.

Fig. 4-6 depict the changes in the task request success rate, the task completion rate, and the task load rate when the proportion of malicious users changes. Fig. 4 compares the impact of the proportion of malicious users on the task request success rate of three strategies. With the increase in the proportion of malicious users in the network, the task request success rate of the three strategies presents a downward trend. The PSSPP strategy proposed in this paper is 33.9% higher than SABA and 12.5% higher than PEPPeR. The reason is that malicious users in the network can intercept and maliciously discard sensitive information in the task request information in the transmission through illegal means, causing some task requests to fail. Compared with the other two strategies, the SABA strategy is greatly affected.
by malicious users. The PSSPP strategy takes full account of the user trust status and adopts an anonymous method to split the task request content to complete the task request process. Therefore, the PSSPP strategy can still guarantee the registration success rate of more than 66% in the case of more malicious users.

As shown in Fig. 5, the task completion rate of the PSSPP strategy is much higher than the other two strategies. The main reason is that the PSSPP strategy can select the appropriate participants and forward them based on the perceived participant trust value in a privacy-protected manner, which greatly restricts the damage of the malicious user to the data transmission process during the completion of the task. At the same time, the PSSPP strategy selects participants with high credibility and task completion ability through the evaluation of the trust status, which indirectly improves the task completion success rate of PSSPP. PEPPeR adopts the collaborative forwarding strategy, which increases the likelihood of attacks by malicious users. SABA adopts the distributed strategy among task participants, which makes it more exposed to malicious users, and as a result, the task completion rate of PSSPP is 48% higher than PEPPeR and much higher than SABA.

B. IMPACT OF TASK REQUEST INTERVAL ON PARTICIPANT SELECTION PERFORMANCE

In order to further validate the PSSPP strategy proposed in this paper, we consider the impact of different task request intervals on the three participant selection strategies in a network environment with 10% malicious users. Under different task request intervals, the performance of the three participant selection strategies is shown in Fig. 7-9. Fig. 7 shows the impact of the task request interval on the task request success rate. It can be seen from Fig. 7 that the task request success rate of PSSPP and PEPPeR strategy is relatively high, while the SABA is slightly lower. The task request success rate of PSSPP is 15.6% higher than SABA and 4.3% higher than PEPPeR. With the increase of task request interval, the task request success rate of the three participant selection
strategies increases. The reason is that the increase in the task request interval reduces the number of task requests sent to a certain extent. The participants inside the network have sufficient space to help forward, and sufficient interval time can better help the platform to judge the task information.

As shown in Fig. 8, the task completion rate of the PSSPP strategy is much higher than that of PEPPeR and SABA. The main reason is that the PSSPP strategy selects the user with higher credibility and task realization ability as the optimal participant through trust state perception in the participant selection process, thus the damage of malicious users in the task realization process is greatly reduced. Combined with the service query success rate of the three service discovery strategies, it can be seen that the task completion rate of the proposed PSSPP strategy is significantly improved compared with the other two strategies.

Fig. 9 depicts the task load rate with the task request interval. The task load rate of the two service discovery strategies of PSSPP and PEPPeR is larger. The main reason is that PSSPP uses Bloom filter to achieve privacy matching, in the process of selecting the participants, multiple rounds of iterations are needed. In order to achieve controllable privacy protection, we adopt a hybrid matching method and take into account the participant attributes and preference levels, which increases the number of message transmissions. PEPPeR adopts the participant selection strategy of cooperative forwarding and the number of forwarding in the network is high, resulting in a large task load rate. The SABA strategy has the lowest task load rate, mainly because it adopts the distributed strategy among the available task participants, which effectively reduces the task completion time, and reduces the number of messages forwarding in the participant selection process through the cloud.

VII. CONCLUSION

In this paper, the idea of mobile crowd sensing is used to solve the problem of incomplete information collection on IoT platform caused by the difference of deployment location and purpose of sensing devices. At the same time, in mobile crowd sensing, the information security and privacy of relevant personnel during the interaction with the IoT platform, as well as the social attributes and personal preferences of participants performing sensing tasks, will cause certain differences in sensing results. Therefore, this paper proposes a participant selection strategy with privacy protection for IoT search, thereby improving the service quality of the IoT platform. Anonymous and secure attribute mapping schemes are implemented to protect the privacy of participants and search task requesters, while avoiding attacks by malicious users, and then calculating the matching degree between participants and tasks to select the best participants to complete the perceived task. Finally, simulation results show that the proposed scheme has superior performance.

REFERENCES

[1] D. Wu, H. Shi, H. Wang, R. Wang, and H. Fang, “A feature-based learning system for Internet of Things applications,” IEEE Internet Things J., vol. 6, no. 2, pp. 1928–1937, Apr. 2019.

[2] D. Wu, Z. Zhang, S. Wu, J. Yang, and R. Wang, “Biologically inspired resource allocation for network slices in 5G-enabled Internet of Things,” IEEE Internet Things J., vol. 6, no. 6, pp. 9266–9279, Dec. 2019.

[3] P. Zhang, X. Kang, Y. Liu, and H. Yang, “Cooperative willingness aware collaborative caching mechanism towards cellular D2D communication,” IEEE Access, vol. 6, pp. 67046–67056, 2018.

[4] Z. Li, J. Chen, and Z. Zhang, “Socially aware caching in D2D enabled fog radio access networks,” IEEE Access, vol. 7, pp. 84293–84303, 2019.
[5] D. Wu, B. Liu, Q. Yang, and R. Wang, “Social-aware cooperative caching mechanism in mobile social networks,” J. Netw. Comput. Appl., vol. 149, Jan. 2020, Art. no. 102457.

[6] P. Zhang, X. Kang, D. Wu, and R. Wang, “High-accuracy entity state prediction method based on deep belief network toward IoT search,” IEEE Wireless Commun. Lett., vol. 8, no. 2, pp. 492–495, Apr. 2019.

[7] Z. Li, Y. Jiang, Y. Gao, L. Sang, and D. Yang, “On buffer-constrained throughput of a wireless-powered communication system,” IEEE J. Sel. Areas Commun., vol. 37, no. 2, pp. 283–297, Feb. 2019.

[8] D. Wu, Q. Liu, H. Wang, Q. Yang, and R. Wang, “Cache less for more: Exploiting cooperative video caching and delivery in D2D communications,” IEEE Trans. Multimedia, vol. 21, no. 7, pp. 1788–1798, Jul. 2019.

[9] Z. Zhang, C. Wang, C. Gan, S. Sun, and M. Wang, “Automatic modulation classification using convolutional neural network with features fusion of SPWVD and BFD,” IEEE Trans. Signal Inf. Process. Netw., vol. 5, no. 3, pp. 469–478, Sep. 2019.

[10] P. Zhang, X. Li, Y. Liu, X. Kang, and Y. Liu, “SDU: State-based dual-mode sensor search mechanism toward Internet of Things,” IEEE Access, vol. 7, pp. 147962–147974, 2019.

[11] R. Wang, J. Yan, D. Wu, H. Wang, and Q. Yang, “Knowledge-centric edge computing based on virtualized D2D communication systems,” IEEE Commun. Mag., vol. 56, no. 5, pp. 32–38, May 2018.

[12] Z. Zhang, T. Zeng, X. Yu, and S. Sun, “Social-aware D2D pairing for cooperative video transmission using matching theory,” Mobile Netw. Appl., vol. 23, no. 3, pp. 639–649, Nov. 2017.

[13] D. Wu, S. Si, S. Wu, and R. Wang, “Dynamic trust relationships aware data privacy protection in mobile crowd-sensing,” IEEE Internet Things J., vol. 5, no. 4, pp. 2958–2970, Aug. 2018.

[14] L. Wang, D. Zhang, Y. Wang, C. Chen, X. Han, and A. M’hammed, “Sparse mobile crowdsensing: Challenges and opportunities,” IEEE Commun. Mag., vol. 54, no. 7, pp. 161–167, Jul. 2016.

[15] Z. Zhang and L. Wang, “Social tie-driven content priority scheme for D2D communications,” Inf. Sci., vol. 480, pp. 160–173, Apr. 2019.

[16] P. Zhang, X. Kang, X. Li, Y. Liu, D. Wu, and R. Wang, “Overlapping community deep exploring-based relay selection method toward multi-hop D2D communication,” IEEE Wireless Commun. Lett., vol. 8, no. 5, pp. 1357–1360, Oct. 2019.

[17] C. Truong, K. Romer, and K. Chen, “Fuzzy-based sensor search in the Web of things,” in Proc. 3rd IEEE Int. Conf. Internet Things, Oct. 2012, pp. 127–134.

[18] S. Liu, Y. Liu, F. Wu, and W. Fan, “Sensor search based on sensor similarity computing in the Internet of Things,” J. Electron. Inf. Technol., vol. 40, no. 12, pp. 3020–3027, 2018.

[19] Y. Li, Y.-S. Jeong, B.-S. Shin, and J. H. Park, “Crowdsensing multimedia data: Security and privacy issues,” IEEE Multimedia Mag., vol. 24, no. 4, pp. 58–66, Oct. 2017.

[20] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, and N. Triandopoulos, “AnonySense: A system for anonymous opportunistic sensing,” Pervas. Mobile Comput., vol. 7, no. 1, pp. 16–30, Feb. 2011.

[21] S. Gisdakis, T. Giannetsos, and G. Han, “HySense: A hybrid mobile Crowdsensing framework for sensing opportunities compensation under dynamic coverage constraint,” IEEE Commun. Mag., vol. 55, no. 3, pp. 93–99, Mar. 2017.

[22] M. A. Alsheikh, Y. Jiao, D. Niyato, and Z. Han, “The accuracy-privacy trade-off of mobile crowdsensing,” IEEE Commun. Mag., vol. 55, no. 6, pp. 132–139, Jun. 2017.

[23] K. Wang, X. Qi, L. Shu, D.-J. Deng, and J. J. P. C. Rodrigues, “‘Towards trustworthy crowdsourcing in the social Internet of Things,” IEEE Wireless Commun., vol. 23, no. 5, pp. 30–36, Oct. 2016.

---

PENG YANG received the Ph.D. degree from Xidian University, China, in 2008. He currently works at the Western Academy of the China Academy of Information and Communications Technology. He has long been engaged in the researches of wireless communication, next-generation mobile communication technology, wireless ubiquitous networks, and the next-generation Internet theory and technology.

XUYUAN KANG is currently pursuing the M.S. degree in information and communication engineering with the Chongqing University of Posts and Telecommunications. His current researches focus on the IoT search and mobile crowd sensing.

QIMING WU is currently pursuing the M.S. degree in information and communication engineering with the Chongqing University of Posts and Telecommunications. His research interests include mobile crowd sensing, trust management, and privacy protection.

BORAN YANG received the B.S. and M.S. degrees from the Chongqing University of Posts and Telecommunications, in 2013 and 2016, respectively, where he is currently pursuing the Ph.D. degree. His research interests include edge computing, edge resource sharing, and network security.

PUNING ZHANG received the Ph.D. degree from the Beijing University of Posts and Telecommunications, China, in 2017. He currently works as a Lecturer with the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications. His research interests include D2D communication and the Internet of Things search.

---

* * *