A UAV-assisted Ubiquitous Trust Communication System in 5G and Beyond Networks

Mingfeng Huang, Anfeng Liu, Neal N. Xiong*, *Senior Member*, *IEEE*, Jie Wu, *Fellow*, *IEEE*

***Abstract*—UAV-assisted wireless communications facilitate the applications of Internet of Things (IoT), which employ billions of devices to sense and collect data with an on-demand style. However, there are numerous malicious Mobile Data Collectors (MDCs) mixing into the network, stealing or tampering with data, which greatly damages IoT applications. So, it is urgent to build a ubiquitous trust communication system. In this paper, a UAV-assisted Ubiquitous Trust Evaluation (UUTE) framework is proposed, which combines the UAV-assisted global trust evaluation and the historical interaction based local trust evaluation. We first propose a global trust evaluation model for data collection platforms. It can accurately eliminate malicious MDCs and create a clean data collection environment, by dispatching UAVs to collect baseline data to validate the data submitted by MDCs. After that, a local trust evaluation model is proposed to help select credible MDCs for collaborative data collection. By letting UAVs distribute the data verification hash codes to MDCs, the MDCs can verify whether the exchanged data from the interacted MDCs is reliable. Extensive experiments conduct on a real-life dataset demonstrate that our UUTE system outperforms the existing trust evaluation systems in terms of accuracy and cost.**

***Index Terms*—5G and beyond networks, unmanned aerial vehicles, trust evaluation, incentive mechanism, data quality.**

I. Introduction

In the 5G and upcoming beyond 5G era, billions of sensing devices are connected to the Internet of Things (IoT) to sense and collect data collaboratively, thus greatly promoting the development of IoT based applications [1], [2]. According to IoT Analytics, the number of IoT devices worldwide is expected to reach 22 billion by 2025 [3], and they will generate more than 90 zettabytes of data [4]. On the one hand, these widely deployed IoT devices enable the network to monitor targets and collect data in a timely, accurate and comprehensive way, thus constructing a ubiquitous data collection platform. On the other hand, there are more and more malicious participants mixing into the network, stealing or tampering with data, causing data-based applications to pose huge threats to security and data quality [5], [6], [7].

Manuscript received September 29, 2020; revised January 21, 2021; accepted April 12, 2021. Date of publication ***, 2021; date of current version ***, 2021. (Corresponding author: Neal N. Xiong)

Mingfeng Huang and Anfeng Liu are with the School of Computer Science and Engineering, Central South University, Changsha, 410083 China. (e-mail: {mingfenghuang, afengliu}@csu.edu.cn)

Neal N. Xiong is with the Department of Mathematics and Computer Science, Northeastern State University, OK, 74464, USA. (e-mail: xiongnaixue@gmail.com)

Jie Wu is with the Center for Networked Computing, Temple University, Philadelphia, PA, 19122, USA. (e-mail: jiewu@temple.edu).

Currently, almost all applications are based on data collection and analysis. Typical examples include VTrack [8], Waze [9] and WeatherLah [10], where VTrack and Waze provide comprehensive traffic information by collecting vehicle operating status information [8], [9], WeatherLah provides fine-grained climate status based on meteorological data collection [10]. Real and credible data is the basis and prerequisite for constructing high-quality services, malicious data not only deteriorates the service quality, but also causes serious human and material losses [6], [7]. Therefore, it is urgent to construct a ubiquitous trust communication system.

To this end, the trust mechanism is proposed by researchers, which can protect the system from internal attacks by establishing a quantitative evaluation system [11] [12]. However, as far as we know, there are many problems in the existing researches to build a ubiquitous trust communication system.

First, from the perspective of the data collection platform, constructing a credible computing environment faces many challenges. Creating a credible computing environment has always been the goal pursued by researchers. However, even in the traditional network, it is difficult to achieve. With the development of 5G and beyond networks, the number of IoT devices connected to the network has increased exponentially. In the context of such a heterogeneous, wide-ranging, and large-scale network, building a ubiquitous trust communication platform is particularly difficult. Also, the trust evaluation methods in the past are often constructed for specific applications. On the one hand, the cost is very high and not practical in real life; on the other hand, it is not universal and is not applicable to common scenarios. Furthermore, the past methods often obtain trust by observing the interactive behavior and relationship of the evaluated objects. Therefore, the reliability is not high, it is easy to be deceived and attacked, and the accuracy of the evaluation result is difficult to verity.

Second, from the perspective of mobile data collectors, there are many difficulties in constructing a trusted interaction environment. As we all know, interactive behavior is the privacy attribute of the evaluated object, so it is difficult to obtain from the outside due to privacy and security reasons. And observing the evaluated object requires certain infrastructure and resources, however, these resources are unavailable or not allowed in many scenarios. What's more, all trust evaluations come from feedback from others, so it is difficult to determine their accuracy. For example, when collusion or good/bad mouth attacks are initiated, the feedback is invalid [12] [13]. It is more difficult to ensure the accuracy of trust evaluation based on these uncertain feedbacks. Finally, the trust evaluation in the past method is a passive evaluation, which is very limited in critical applications, such as in the initialization of the network or in a sparse network, there is little or no interaction between

data collectors. More importantly, some evaluated subjects do not interact during normal times, but only work under certain circumstances. Therefore, the previous methods have problems such as difficulty in obtaining interactive behavior, inaccurate evaluation results, and limited application scenarios.

The emergence of Unmanned Aerial Vehicles (UAVs) provides an opportunity to solve the above problems. UAVs could be deployed as aerial Base Stations (BSs), Access Points (APs), or relays to assist 5G and beyond wireless communications from the sky [14], leading to another paradigm known as UAV-assisted communications [15], [16], [17]. UAV-assisted communications have several promising advantages, such as the ability to facilitate on-demand deployment, high flexibility in network reconfiguration, and high chance of having Line of Sight (LoS) communication links [18], [19]. Applications of UAVs have been fast growing during the past few years. One of the pivotal applications is data collection in various data-based applications.

Here, we argue that UAV-assisted wireless communications can facilitate creating a ubiquitous trust communication system in 5G and beyond networks, which is significantly different from conventional communication systems. Therefore, we propose a UAV-assisted Ubiquitous Trust Evaluation (UUTE) system in this paper, and its contributions are as follows:

- A ubiquitous trust communication system is constructed, which contains two trust evaluation models to provide reliable data collection and communication in 5G and beyond networks. One is the global trust evaluation model, which can help data collection platforms exclude malicious MDCs, thereby constructing a clean data collection environment. The other is the local trust evaluation model, which can help MDCs create a trusted personal interaction environment, thus choosing reliable MDCs to exchange data.
- A novel UAV-assisted global trust evaluation model is proposed in UUTE, which can realize proactive and verifiable trust evaluation. Different from previous studies, we make full use of the convenience of UAV-assisted communications, and dispatch UAVs to specific sites to obtain baseline data to evaluate the data provided by MDCs. When the data reported by MDCs is consistent with the baseline data, we increase its trust to enhance the possibility of data being adopted. Otherwise, its trust is reduced to punish it for its negative behavior. The sites selected by UAVs are dynamically planned according to frequency and cost. Therefore, it is an evaluation method that can be initiated on demand, and does not rely on the interaction between evaluated objects.
- A historical interaction based local trust evaluation model is proposed in UUTE, which can expand the trust relationship, and enable MDCs to obtain a credible personal interaction environment. In local trust evaluation, UAVs distribute the data verification hash code to the MDCs on the flight way. Based on the verification code, the data collector can verify the data obtained from other MDCs that have interacted with it, and make a local trust evaluation on other MDCs. Due to the one-way and irreversible characteristics of the verification code, local trust evaluation can be safely implemented while preventing malicious data collectors from deriving the data backwards. Compared with the previous interactive verification, this is a safe trust evaluation method.
- An algorithm for selecting winning MDCs based on incentive mechanism is proposed. In the incentive mechanism, the data center selects winning MDCs by weighing the trust and cost, so as to improve the data quality while considering the cost. Experiments conduct on a real-life dataset demonstrate that the UUTE proposed in this paper can more accurately identify malicious MDCs, greatly improve the speed of trust evaluation and evolution, expand the scope of evaluation, and reduce the data collection cost by up to 34.96%.

The rest of this paper is organized as follows. Section II introduces related works. The system model and definitions are presented in Section III. In Section IV, we propose the UUTE framework. Then, Section V and VI provide theoretical and experimental analysis. Finally, conclusion and future work are given in Section VII.

II. Related Work

In the past, it has been assumed that the data collectors in data-based applications are trustworthy. Recently, with the expansion of the network scale, more and more malicious attackers enter the network. They behave illegally for various reasons. For example, in data collection based on incentive mechanisms, many data collectors submit false data to get payment, and some malicious data collectors tamper and destroy the data of others in order to achieve the purpose of attack, which greatly damages the quality of the collected data [13], [20]. Therefore, how to identify malicious participants from numerous data collectors to ensure the data security and credibility is an important issue.

Trust mechanism is an effective means to suppress malicious data collectors. By establishing a quantitative system, the trust is used to measure the credibility of data collectors, which also reflects the subjective attitude to participate in tasks [11], [21].

Researchers first adopted the rating mechanism for trust evaluation. In such a mechanism, the evaluator submits a rating of the interaction to the system, and then the trust of the evaluated object is computed based on the submitted rating. Generally, the rating closer to the current time is more important, and decays with the passage of time [22]. Therefore, the time decay mechanism is introduced, that is, different ratings submitted at different times are given different degrees of importance, then all ratings within the valid time are weighted to obtain a comprehensive trust [6]. Kim et al. [21] proposes a computational social trust framework, which is based on user feedback rating data to predict trust connectivity between a pair of users. The single rating mechanism assumes that all the evaluators provide objective and credible feedback. However, some evaluators may submit false ratings, making this trust rating unreliable. So, the dual-rating mechanism is proposed. In the dual-rating mechanism, both parties of the interaction must submit a rating, and only when the ratings submitted by both parties are consistent can it be regarded as a valid rating. In the case of the first interaction without historical information, Dangelo et al. [23] proposes an algorithm to evaluate the truthfulness of a tuple (recommender-data/recommendation). The algorithm uses association rules to express a confidence-based measure (reputation rank), which is used as a reliability ranking of the recommender-data. Although the dual-rating mechanism can prevent false evaluations from one party, it cannot identify the colluding data collectors because they both submit higher feedbacks.

TABLE I
Comparison of trust methods

Methodology	Basic idea	Advantages	Disadvantages	References
Single-rating mechanism	Each evaluator submits a feedback rating, and compute the trust of the evaluated object by weighting the feedback ratings	Simple to implement	Affected by false ratings	[21]
Dual-rating mechanism	Both parties of the interaction submit a rating, and only when their ratings are consistent can it be regarded as a valid rating	Prevent false evaluations from one party	Can't resist collusion attacks	[13] [20]
Direct trust	Trust is inferred based on direct interactive behavior or relationship of the evaluated object	Trust updates fast	Not suitable for interactive sparse scenes	[7] [24]
Recommend/Indirect trust	For situations where there is no direct interaction, introduce a third party who has directly interacted with the evaluated object to infer trust indirectly	Wide range of evaluation	Affected by the reliability of third-party recommenders	[23] [25]
Active trust	Dispatch trusted equipment to obtain baseline data, and infer trust through comparison with baseline data	Accurate, verifiable, initiated on demand	Limited evaluation scope and high cost	[6] [22]

Recent studies have recognized the shortcomings of rating-based evaluation. Trust reasoning and calculations must be judged based on interactive behaviors of data collectors. Therefore, interactive behavior is an important basis for measuring the trust of data collectors. Laniepce et al. [24] surveys reputation mechanisms that use a monitoring system to overhear the next hop node, as a way to watch behavior inside the neighborhood. Shabut et al. [25] proposes a recommendation-based trust model that uses clustering technology to dynamically filter out attacks. Recommended nodes are selected based on the number of interactions, the compatibility of information and the closeness between nodes. Trust evaluation based on interactive behavior is divided into direct trust and indirect trust [6], [22]. Among them, direct trust is the trust evaluation made by the two parties based on the interaction process and results after they have directly interacted. Indirect trust is when the evaluation object and the evaluated object have no direct interaction, but both of them have interacted with a third party, thus relying on the trust evaluation made by the third party indirectly. For example, $\mathcal{M}_A$ has no direct interaction with $\mathcal{M}_C$, but $\mathcal{M}_A$ has a direct interaction with $\mathcal{M}_B$, their direct trust is $T_{A,B}$, $\mathcal{M}_B$ and $\mathcal{M}_C$ also have direct trust $T_{B,C}$. In this way, the indirect trust of $\mathcal{M}_A$ and $\mathcal{M}_C$ can be derived, $T'_{A,C} = T_{A,B} \times T_{B,C}$. Obviously, indirect trust strongly depends on the reliability of the third party, if $\mathcal{M}_B$ is untrustworthy, then the indirect trust is meaningless. Many studies usually give a certain weight to direct evaluation and indirect evaluation to obtain comprehensive trust evaluation. Jiang et al. [7] proposes an Efficient Distributed Trust Model (EDTM) for WSNs. This model calculates direct trust, recommendation trust and indirect trust based on the received data packets and other information. This interaction-based trust evaluation is more advanced than the traditional method, but there are some shortcomings, such as difficulty in obtaining interaction, lack of interaction in the initial trust period and limited application.

Therefore, researchers began to study active trust evaluation. Aiming at the black hole attack, Liu et al. [6] proposes an active trust routing in wireless sensor network. Different from the previous research on how to judge the trust through the interaction between nodes, the system initiates an active detection route to quickly detect and obtain trust.

In recent years, with the development of communication technology, especially Unmanned Aerial Vehicles, researchers hope to find an active and verifiable trust evaluation method, that is, to make an accurate trust evaluation by comparing the data submitted by data collectors with the real data. Different from previous studies, in the paper of Jiang et al. [22], the UAVs are dispatched to collect baseline data for evaluating the data reported by sensor nodes. However, in their paper, the UAVs obtains data directly from the cluster head, and these cluster heads are the easiest to be attacked, which makes the scheme less secure.

In summary, trust methods can be roughly divided as single-rating mechanism, dual-rating mechanism, direct trust, recommend/indirect trust and active trust. The basic idea of these methods and their respective advantages and disadvantages are given in Table I.

III. System Model and Definitions

A. System Model

The ubiquitous trust communication system proposed in this paper considers a wide range of application scenarios. It can not only be used as a trust evaluation system for urban data collection, but is also suitable for trust evaluation of maritime data collection. The simplified model is shown in Fig. 1, which includes sensing devices, mobile data collectors, unmanned aerial vehicles and data center.

- Sensing devices. Sensing devices are heterogeneous IoT devices deployed in various areas, such as cameras, mobile phones, computers, smart trash cans in cities, monitors and detectors in the ocean [26], [27]. These statically or dynamically deployed sensing devices constitute the data collection infrastructure. Since they are deployed by the system, we assume sensing devices are credible, the data they sense is also credible.
- Mobile Data Collectors (MDCs). MDCs move according to preplanned or temporarily planned routes to collect data from sensing devices, and finally upload it to data center. As shown

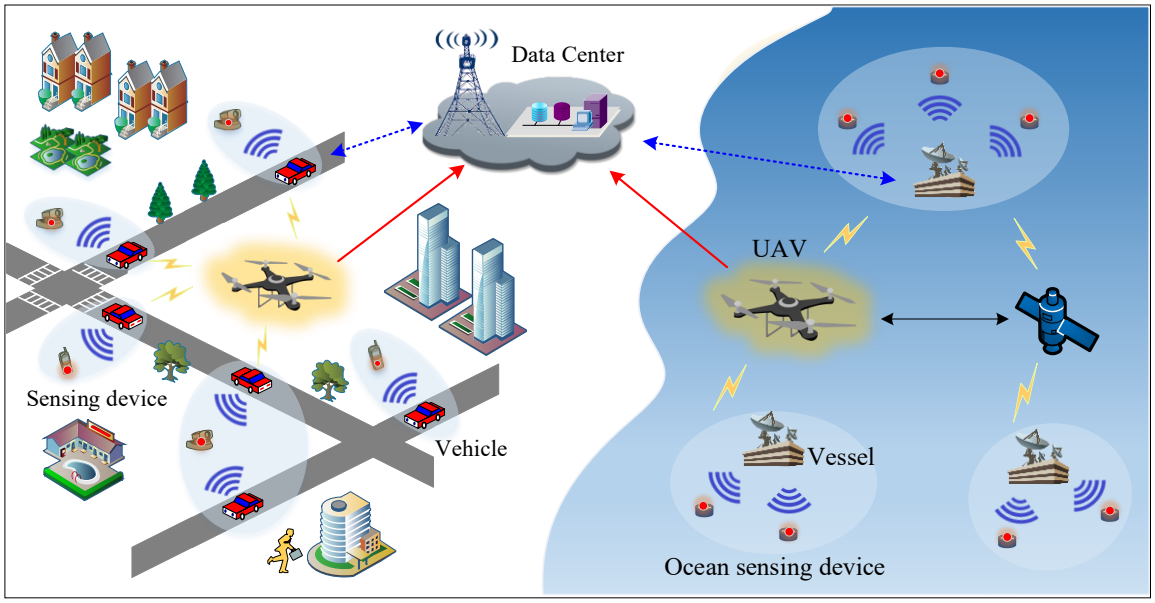

Fig. 1. Integrated application scenario of ocean and city

in Fig. 1, vehicles in the city act as mobile data collectors. They collect data from nearby sensing devices during driving, and then transmit data to the data center through 5G network communication facilities. Here, an incentive mechanism is adapted to stimulate more MDCs to actively collect data. After the system publishes tasks, the MDCs who provide effective data are rewarded [26], [28]. On the way of consistently moving for data collection, each MDC continuously exchanges data with other MDCs it encounters, thus obtaining more data and compensation. As a result, some MDCs fabricate false and malicious data in order to cheat on payments.

- Data center. The data center is the data analysis and storage center of the entire network, and the data is eventually uploaded to the data center through MDCs. In the trust evaluation model of this article, another important role of the data center is to make the global trust evaluation for mobile data collectors. After the UAVs obtain the baseline data from the designated sites, the data center compares the data provided by MDCs with the baseline data, and makes a global trust evaluation based on the verification results.
- Unmanned Aerial Vehicles (UAVs). In previous studies, on the one hand, UAVs act as communication relays to support the network connection in weak coverage areas and remote areas [15], [27]. On the other hand, they can be temporary edge nodes for simple data processing [16], [17]. With the development of 5G and beyond networks, the role of UAVs in this regard is waning. In the trust evaluation of this article, UAVs have two functions. One is to collect data from part sites as baseline data to help the data center to conduct global evaluation; the other is to send data verification hash codes to MDCs within visual range during flight, so as to help MDCs make local trust evaluation on objects who have interacted with them. Because UAVs are dispatched by the system, it is credible. Using UAVs to collect baseline data can perform a confirmatory evaluation for the data reported by MDCs, which has not been achieved in previous studies. It is worth noting that, the trust communication system proposed in this paper can be applied to many general scenarios. The task is an abstraction, which can specifically be data collection [27], event perception, and computational offloading [28], etc.

The normalized network is defined as follows: assuming that the set of data packets is $\mathbb{D}$, $\mathbb{D} = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_i, \dots\}$; the set of MDCs is $\mathbb{M}$, $\mathbb{M} = \{\mathcal{M}_1, \mathcal{M}_2, \dots, \mathcal{M}_i, \dots\}$, $\mathcal{M}_i$ represents the *i-th* mobile data collector in the set; the set of UAVs is $\mathbb{U}$, $\mathbb{U} = \{\mathcal{U}_1, \mathcal{U}_2, \dots, \mathcal{U}_i, \dots\}$, $\mathcal{U}_i$ represents the *i-th* UAV in the set.

B. Definitions

Metrics used to evaluate the effectiveness of the proposed method are as follows:

(1) Cost

Cost includes the remuneration paid to incentivize MDCs to report data and the cost of dispatching UAVs for baseline data collection. It is calculated as follows:

$$C = \sum\nolimits_{\mathcal{M}_i \in \mathbb{W}} \mathcal{P}_{\mathcal{M}_i} + \sum_{j=1}^{M} \alpha \mathcal{L}_{\mathcal{U}_j}. \tag{1}$$

Where $\mathbb{W}$ is the set of the winning MDCs in the incentive mechanism, $\mathcal{P}_{\mathcal{M}_i}$ is the task remuneration obtained by the winning mobile data collector $\mathcal{M}_i$, $\mathcal{L}_{\mathcal{U}_j}$ is the flight distance of the UAV $\mathcal{U}_j$, and α is the conversion factor from distance to cost.

(2) Data coverage

Data coverage is the coverage of sites that can be achieved by data provided by MDCs. Assuming that there are N sites in the network, for the *i-th* site, if its data is covered by $\mathcal{M}_j$, then $\mathcal{F}_i^j = 1$, otherwise $\mathcal{F}_i^j = 0$. The data coverage of the entire network can be expressed as:

$$F = \sum_{i=1}^{Z} \sum_{j=1}^{N} \mathcal{F}_i^j. \tag{2}$$

(3) Trust

The data quality of applications is determined by the data reported by winning MDCs. The higher the trust of the data providers, the higher the quality of the data they provide. Assuming that the number of winning MDCs is K, the trust of the *m-th*

data collector is $\mathcal{T}_m$, then the trust of winning MDCs is calculated as follows:

$$Q = \sum_{m=1}^{K} \mathcal{T}_m \Big/ K. \tag{3}$$

We hope to maximize data coverage so that the system can collect high-quality data at a low cost. Therefore, the research objectives can be summarized as follows:

$$\begin{cases} Min\ C, C = \sum_{\mathcal{M}_i \in \mathbb{W}} \mathcal{P}_{\mathcal{M}_i} + \sum_{j=1}^{M} \alpha \mathcal{L}_{\mathcal{U}_j}, \\ Max\ F, F = \sum_{i=1}^{Z} \sum_{j=1}^{N} \mathcal{F}_i^j, \\ Max\ Q, Q = \sum_{m=1}^{K} \mathcal{T}_m \Big/ K. \end{cases} \tag{4}$$

IV. Our Proposed UUTE System

A. Overall Design of the UUTE System

In this paper, we propose a UAV-assisted ubiquitous trust evaluation system that integrates global and local trust evaluation models, referred to as UUTE. In order to explain the UUTE more clearly, we use urban data collection as a typical application scenario to illustrate. First, the running mechanism is given:

- Before a round of data collection, the data center issues data collection tasks and rewards, and informs MDCs of the location of the sensing devices;
- According to task and payment information, MDCs determine whether to participate in data collection. If participating, MDCs move freely or regularly to visit sensing devices, and establish communication with sensing devices to obtain data through opportunistic routing; at the same time, they exchange data with other MDCs on the way;
- When data collection is completed, MDCs report their data, quality and price information to the data center. Based on the information provided by all MDCs and combined with the data collection requirements, the data center selects some MDCs as winners, receives the data they report, and gives them payments;
- Based on the data reported by MDCs, the data center determines the sites where UAVs to visit for collecting baseline data, and dispatches UAVs for collection;
- The data center verifies the data received in this round, compares it with the baseline data collected by UAVs, and makes the global trust evaluation for MDCs who submitted the data; at the same time, it generates a data verification hash code for each baseline data;
- During the new round of baseline data collection, UAVs distribute the data verification hash code to MDCs within the line of sight, so as to help MDCs make local trust evaluation for objects they have interacted with.

The above process is executed cyclically to continuously update the global and local trust of MDCs. Here, we use an incentive mechanism to encourage MDCs to actively participate in data collection. At the end of each round of data collection, select some MDCs as winners, purchase the data they reported and pay them rewards. Obviously, the data provided by winning MDCs determines the data quality of the application. To ensure the performance of data collection, the incentive mechanism should consider both data quality and data collection cost. Therefore, we set the objective function:

Algorithm 1: *Algorithm for selecting the winning MDCs*

Input: $\mathbb{M}_+$ set of all MDCs participating in data collection
Initial: $\mathcal{F}_{tot}$=null, $\mathbb{W}^*$=$\mathbb{M}_+$
1: Compute the maximum data coverage $\mathcal{F}_{MAX}$
2: **While** $\mathcal{F}_{tot} \neq \mathcal{F}_{MAX}$ **Do**
3: β_{MAX}=-1
4: **For** each $\mathcal{M}_+^i \in \mathbb{W}^*$ **Do**
5: **If** $\beta_{MAX} < \frac{\mathcal{T}_{his}^i}{\mathcal{P}_{\mathcal{M}_i}}$ **Do**
6: $\beta_{MAX} = \frac{\mathcal{T}_{his}^i}{\mathcal{P}_{\mathcal{M}_i}}$
7: index=i
8: **End if**
9: **End for**
10: Let $\mathcal{M}_+^{index} \in \mathbb{W}$, $\mathcal{M}_+^{index} \notin \mathbb{W}^*$
11: $\mathcal{F}_{tot} = \mathcal{F}_{tot} \cup \mathcal{F}_{index}$
12: **End while**
13: **For** each $\mathcal{M}_+^i \in \mathbb{W}$ **Do**
14: **If** $\mathcal{F}_{tot} - \mathcal{F}_i = \mathcal{F}_{MAX}$ **Do**
15: Let $\mathcal{M}_+^i \notin \mathbb{W}$
16: **End if**
17: **Else**
18: β_{MAX}=-1
19: **For** each $\mathcal{M}_+^j \in \mathbb{W}^*$ **Do**
20: **If** $\beta_{MAX} < \frac{\mathcal{T}_{his}^j}{\mathcal{P}_{\mathcal{M}_j}}$ **Do**
21: $\beta_{MAX} = \frac{\mathcal{T}_{his}^j}{\mathcal{P}_{\mathcal{M}_j}}$
22: index=j
23: **End if**
24: **If** $(\mathcal{F}_{tot} - \mathcal{F}_i) \cup \mathcal{F}_{index} = \mathcal{F}_{MAX}$ and $\mathcal{P}_{\mathcal{M}_{index}} < \mathcal{P}_{\mathcal{M}_i}$ **Do**
25: Let $\mathcal{M}_+^{index} \in \mathbb{W}$, $\mathcal{M}_+^i \notin \mathbb{W}$
26: **End if**
27: **End for**
28: **End for**
Output: the set $\mathbb{W}$ of winning MDCs

$$\boldsymbol{Max} \sum_{\boldsymbol{\mathcal{M}_i \in \mathbb{W}}} \frac{\boldsymbol{\mathcal{T}_{his}^i}}{\boldsymbol{\mathcal{P}_{\mathcal{M}_i}}}. \tag{5}$$

Where $\mathbb{W}$ is the set of winning MDCs, $\mathcal{T}_{his}^i$ is the historical comprehensive trust of the mobile data collector $\mathcal{M}_i$, and $\mathcal{P}_{\mathcal{M}_i}$ is the payment of $\mathcal{M}_i$. The above optimization function is considered in terms of trust and payment, which is consistent with the desire of the data center to obtain high-quality data at a lower cost. For any two MDCs, the function value of the data collector with a lower price is higher when they have the same trust, and the function value of the data collector with higher trust is higher when they have the same payment.

The algorithm for selecting winning MDCs under the incentive mechanism is as follows. After the data center obtains the data and price information from MDCs, compute the maximum coverage $\mathcal{F}_{MAX}$ achieved by all MDCs. Then, based on the objective function shown in Formula 5, each time find a mobile data collector $\mathcal{M}_i$ with the maximum function value, and let $\mathcal{M}_i$ join the set of winning data collectors $\mathbb{W}$ until $\bigcup_{\mathcal{M}_i \in \mathbb{W}} \mathcal{F}_i = \mathcal{F}_{MAX}$, that is, the set of winning data collectors that can achieve the maximum data coverage are found. Let the remaining MDCs be in the set $\mathbb{W}^*$. Finally, make optimal verification for each mobile data collector $\mathcal{M}_i$ in $\mathbb{W}$. If $\mathcal{M}_i$ is deleted,

$\bigcup_{\mathcal{M}_i \in \mathbb{W}} \mathcal{F}_i = \mathcal{F}_{MAX}$ still holds, then $\mathcal{M}_i$ is deleted. If there is a vacancy in the data coverage after deletion, try to find a mobile data collector $\mathcal{M}_k$ from $\mathbb{W}^*$, if $\mathcal{M}_k$ satisfies $\bigcup_{\mathcal{M}_i \in \mathbb{W}} \mathcal{F}_i = \mathcal{F}_{MAX}$ and $\mathcal{P}_{\mathcal{M}_k} < \mathcal{P}_{\mathcal{M}_i}$, replace $\mathcal{M}_i$ with $\mathcal{M}_k$, and let $\mathcal{M}_k$ be the winning mobile data collector and update $\mathbb{W}$. Repeat this until the elements in $\mathbb{W}$ are no longer updated.

Assuming that the set of MDCs participating in data collection is $\mathbb{M}_+$, $\mathbb{M}_+ = \{\mathcal{M}_+^1, \mathcal{M}_+^2, \mathcal{M}_+^3 \dots\}$, the historical comprehensive trust of the $\mathcal{M}_+^i$ is $\mathcal{T}_{his}^i$, its data payment is $\mathcal{P}_{\mathcal{M}_i}$ and its data coverage is $\mathcal{F}_i$, the process of selecting winning MDCs can be represented by Algorithm 1.

B. Global Trust Evaluation Model in UUTE

The global trust evaluation of MDCs is made by the data center, and is computed based on the comparison with baseline data collected by UAVs. Global trust evaluation is an important basis for the data collection platform to select winning data providers. It can help the platform exclude malicious data collectors and create a clean data collection environment, thereby ensuring the quality of data-based applications. As shown in Fig. 2, the steps of global trust evaluation are as follows:

- Sensing devices sense surrounding environment and generates data packets. These sensing devices are deployed by the system, so they are trusted. Whenever the sensing device generates a packet, the data packet is marked in a specific format:

$$\mathcal{D} = [\tau_c, Dec_c, Tlink, Abs_D, Data]. \quad (6)$$

τ_c is the time stamp, Dec_c is the identification of the sensing device, $Tlink$ is the data transmission chain, which records the transmission process of data from generation to submission to the data center. Assuming that the data packet $\mathcal{D}_x$ is generated by a device and submitted to the data center via the mobile data collector $\mathcal{M}_k$, then the $Tlink$ of this data is recorded as: $\mathcal{M}_k$. If $\mathcal{M}_k$ shares $\mathcal{D}_x$ with the data collector $\mathcal{M}_A$ during the movement, and $\mathcal{M}_A$ shares $\mathcal{D}_x$ with another data collector $\mathcal{M}_N$, the $Tlink$ when $\mathcal{D}_x$ is submitted to the data center via $\mathcal{M}_N$ is recorded as: $\mathcal{M}_k \to \mathcal{M}_A \to \mathcal{M}_N$. Abs_D is abstract information of data.

- MDCs collect data from sensing devices. Mobile data collectors can be divided into two types, one is full-time MDCs who specialize in collecting data and do not engage in other tasks, and the other is part-time MDCs who have their main tasks to do, but in order to get some extra rewards, collect data in their spare time or on the way to work. For full-time MDCs, their goal is to obtain more data at the least cost in exchange for more rewards. Therefore, such MDCs often plan reasonable moving routes based on the tasks and rewards issued by the data center, which involves the trajectory optimization of UAVs [17], [18]. For part-time MDCs, they do not plan their moving routes in advance, but dynamically collect data according to their work conditions. MDCs communicate with surrounding objects through opportunistic routing during the movement. If they find there is a sensing device in communication range, they establish a connection and collect data from the device. When the data is transferred to the MDC, its $Tlink$ updates.

- Data exchange between MDCs. MDCs exchange data with other MDCs during the movement, so as to obtain more data in exchange for more rewards. The reference for data exchange is local trust, which we will introduce in the next section.

- MDCs submit data to the data center. After MDCs complete data collection, they establish a connection with the data center through 5G or beyond communication facilities, and submit the data collection information to the data center.

Let $\mathbb{M} = \{\mathcal{M}_1, \mathcal{M}_2, \dots, \mathcal{M}_N\}$ represent N MDCs in the system, each MDC declares to the data center its attributes such as data size and data quality. The attribute information claimed by the $\mathcal{M}_i$ is expressed as:

$$\mathcal{Q}_{self}^i = \left[\mathcal{Q}_{self}^{i,1}, \mathcal{Q}_{self}^{i,2}, \dots, \mathcal{Q}_{self}^{i,k}, \dots, \mathcal{Q}_{self}^{i,U}\right]. \quad (7)$$

$\mathcal{Q}_{self}^{i,k}$ is the quality of the *k-th* attribute declared by $\mathcal{M}_i$, and U is the dimension of attributes. The attributes declared by N MDCs is stored in the system through a matrix, expressed as:

$$\mathcal{Q}_{self}^{ALL} = \begin{bmatrix} \mathcal{Q}_{self}^{1,1} & \mathcal{Q}_{self}^{1,2} & \dots & \mathcal{Q}_{self}^{1,U} \\ \mathcal{Q}_{self}^{2,1} & \mathcal{Q}_{self}^{2,2} & \dots & \mathcal{Q}_{self}^{2,U} \\ \dots & \dots & \dots & \dots \\ \mathcal{Q}_{self}^{N,1} & \mathcal{Q}_{self}^{N,2} & \dots & \mathcal{Q}_{self}^{N,U} \end{bmatrix}. \quad (8)$$

To normalize the U-dimensional attributes into a comprehensive data quality, use ω_k to represent the weight of the *k-th* attribute. For $\mathcal{M}_i$, its declared normalized data quality is:

$$\mathcal{Q}_{self}^i = \sum_{k=1}^{U} \omega_k \mathcal{Q}_{self}^{i,k},$$
$$\text{where} \sum_{k=1}^{U} \omega_k = 1, 0 \le \omega_k \le 1. \quad (9)$$

The normalized data quality declared by all MDCs is:

$$\mathcal{Q}_{self}^{NORM} = \left[\mathcal{Q}_{self}^1, \mathcal{Q}_{self}^2, \dots, \mathcal{Q}_{self}^i, \dots, \mathcal{Q}_{self}^N\right]. \quad (10)$$

Call the operation that MDC reports data information to the data center once as a data interaction. For $\mathcal{M}_i$, its interaction with the data center can be expressed as:

$$\mathcal{R}_{\mathcal{M}_i} = \left[\mathcal{M}_i, \mathcal{D}_i, \mathcal{Q}_{self}^i, \tau_{rep}\right]. \quad (11)$$

$\mathcal{M}_i$ is the identification of MDC participating in data interaction, $\mathcal{D}_i$ is the set of submitted data, $\mathcal{D}_i = \{\mathcal{D}_i^1, \mathcal{D}_i^2, \dots, \mathcal{D}_i^m \dots\}$, $\mathcal{Q}_{self}^i$ is the data attribute quality declared by $\mathcal{M}_i$. τ_{rep} is the data report timestamp. To improve the accuracy of the trust evaluation, a cycle is divided into several timestamps. For a data packet, the information reported is $(\tau_c, Dev_c, Abs_D, Tlink, \mathcal{Q}_{self}, \mathcal{P}_D)$. And τ_c, Dev_c, Abs_D is the time, sensing device and abstract information of the data, $Tlink$ is the data transmission chain, $\mathcal{Q}_{self}$ is the data quality declared by itself and $\mathcal{P}_D$ is payment.

In the system, the data interaction between the data center and all MDCs is stored in a set of records. Considering the storage cost, for each MDC, we only save its latest Z interactions. The available interaction matrix is:

$$\mathcal{R}_{\mathcal{M}}^{HIS} = \begin{bmatrix} \mathcal{R}_{\mathcal{M}_1}^1 & \mathcal{R}_{\mathcal{M}_1}^2 & \dots & \mathcal{R}_{\mathcal{M}_1}^Z \\ \mathcal{R}_{\mathcal{M}_2}^1 & \mathcal{R}_{\mathcal{M}_2}^2 & \dots & \mathcal{R}_{\mathcal{M}_2}^Z \\ \dots & \dots & \dots & \dots \\ \mathcal{R}_{\mathcal{M}_N}^1 & \mathcal{R}_{\mathcal{M}_N}^2 & \dots & \mathcal{R}_{\mathcal{M}_N}^Z \end{bmatrix}. \quad (12)$$

After each round of data collection, the data center selects winning MDCs through Algorithm 1 based on the price and trust declared by them.

- When MDCs collect data, the system dispatches UAVs to designated sites to collect baseline data. Since the flight cost of UAVs is directly proportional to flight distance and the number of visiting sites, when the number of sites to be collected is larger, the system obtains more baseline data and can verify data of more MDCs. However, at the same time, the greater the

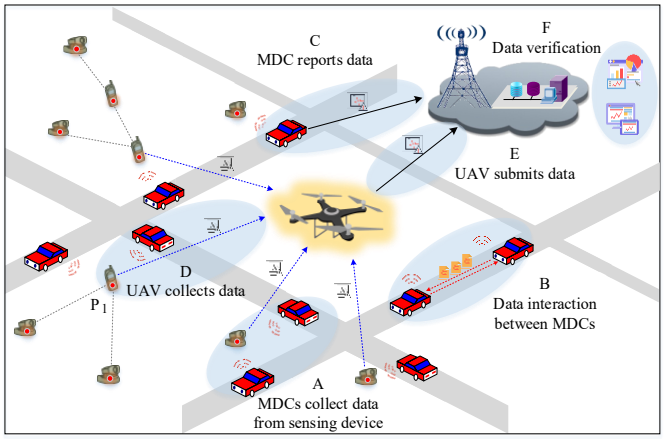

Fig. 2. Global trust evaluation in UUTE

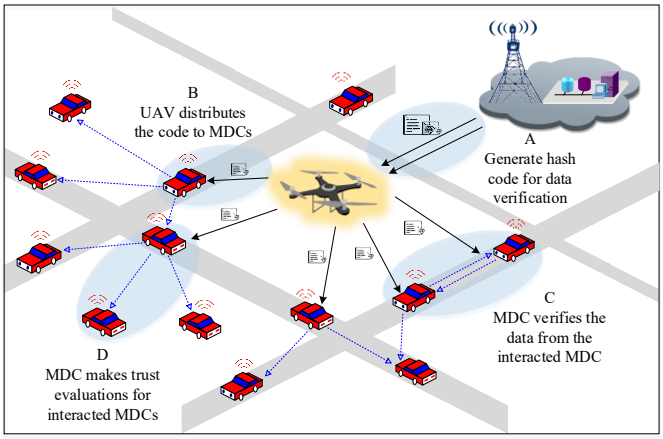

Fig. 3. Local trust evaluation in UUTE

flight consumption of UAVs, the greater the cost of data collection. Therefore, let UAVs visit $\mathcal{H}$ sites each time, these $\mathcal{H}$ sites are the most frequently collected by MDCs during the data collection process. The collection frequency refers to the number of times that the site is acquired by MDCs. By selecting data from sites with high collection frequency as baseline data, more MDCs can be evaluated under the fixed cost of $\mathcal{H}$ sites.

- The data center makes global trust evaluation based on the baseline data submitted by UAVs. Assume that the data collected by UAVs is $\mathbb{D}_{UAV} = \{\mathcal{D}_{UAV}^1, \mathcal{D}_{UAV}^2, \dots, \mathcal{D}_{UAV}^i, \dots\}$, then by comparing these data with the data submitted by MDCs, the verification result can be obtained. There are two situations:

First, if part of the data submitted by $\mathcal{M}_i$ overlaps with the data collected by UAVs, then use this overlapped data for trust evaluation. Assuming that there are Φ data collected by $\mathcal{M}_i$ that coincides with the baseline data, and the attribute dimension of each data is U, then the global trust of $\mathcal{M}_i$ is

$$\mathcal{T}_{DC}^i = \left(\sum_{j=1}^{\Phi} \sum_{k=1}^{U} \omega_k \left| \mathcal{Q}_{UAV}^{i,j,k} - \mathcal{Q}_{self}^{i,j,k} \right| \right) \Big/ \Phi,$$

$$\text{where} \sum_{k=1}^{U} \omega_k = 1, 0 \le \omega_k \le 1. \tag{13}$$

$\mathcal{Q}_{self}^{i,j,k}$ is the quality of the *k-th* attribute of the *j-th* data declared by $\mathcal{M}_i$, $\mathcal{Q}_{UAV}^{i,j,k}$ is the actual quality of it collected by the UAV, and ω_k is the weight of the *k-th* attribute. The trust evaluation of $\mathcal{M}_i$ in the latest Z interactions is $\{\mathcal{T}_{DC}^{i,(1)}, \mathcal{T}_{DC}^{i,(2)}, \dots, \mathcal{T}_{DC}^{i,(k)}, \dots, \mathcal{T}_{DC}^{i,(Z)}\}$, $0 \le \mathcal{T}_{DC}^{i,(k)} \le 1$, $k \in [1, Z]$, Z is maximum valid records. $\{\mathcal{T}_{DC}^{i,(1)}, \mathcal{T}_{DC}^{i,(2)}, \dots, \mathcal{T}_{DC}^{i,(k)}, \dots, \mathcal{T}_{DC}^{i,(Z)}\}$ are arranged in the order of interaction time, $\mathcal{T}_{DC}^{i,(1)}$ is the oldest interaction, $\mathcal{T}_{DC}^{i,(Z)}$ is the most recent interaction. Based on the most recent Z interactions, the comprehensive global trust of $\mathcal{M}_i$ is:

$$\mathcal{T}_{his}^i = \sum_{k=1}^{Z} \mathcal{T}_{DC}^{i,(k)} h(k) \Big/ Z. \tag{14}$$

$h(k)$ is the decay function, which is used to reasonably weigh the trust evaluations that occur at different timestamps. The interaction closer to present has a higher weight, while interaction far away from the present has a lower weight. The decay function is defined as:

$$h(k) = \begin{cases} 1, k = Z, \\ h(k+1) - \dfrac{1}{z}, 1 \le k < Z. \end{cases} \tag{15}$$

Num_{suc} and Num_{fail} indicate the number of successful and failed interactions of MDCs. It is updated based on the verification results. In the data list submitted by MDCs to the data center, there is a $Tlink$ field for each packet, which records all MDCs who have transmitted the data from the sensing device to the data center. Compare the data with the baseline data, if it is consistent, then all MDCs recorded in $Tlink$ are added a successful interaction record $Num_{suc} = 1$. Otherwise, all MDCs recorded in $Tlink$ are added a failed interaction $Num_{fail} = 1$. This is not only helpful for identifying malicious MDCs, but also allow MDCs to be more cautious when exchanging data with other MDCs.

Algorithm 2: *Algorithm for global trust evaluation*

Input: $\mathbb{M}_+$ set of all MDCs participating in data collection
Initial: $\mathcal{T}_{DC}^i = null$
1: **For** each $\mathcal{M}_+^i \in \mathbb{M}_+$ **Do**
2: $\mathcal{M}_+^i$ submits a data list $\mathbb{L}_i$ to the data center
3: Let $\mathbb{L}_i \in \mathbb{L}$
4: **End for**
5: Compute the set $\mathbb{W}$ of winning MDCs using Algorithm 1
6: Data center purchases the data $\mathbb{D}_{win}$ from the winning MDCs
7: UAVs submit baseline data $\mathbb{D}_{UAV}$ to the data center
8: **For** each $\mathcal{M}_i \in \mathbb{W}$ **Do**
9: $\mathbb{D}_{SAME} = null$
10: **For** each $D_k \in \mathbb{D}_i$ of $\mathcal{M}_i$ **Do**
11: **For** each $D_{UAV}^k \in \mathbb{D}_{UAV}$ **Do**
12: **If** D_k and D_{UAV}^k are data about the same site **Do**
13: Compute the trust $\mathcal{T}_{DIFF}^k = \sum_{k=1}^{U} \omega_k \left| \mathcal{Q}_{UAV}^{i,k} - \mathcal{Q}_{self}^{i,k} \right|$
14: Let $D_k \in \mathbb{D}_{SAME}$
15: $\mathcal{T}_{DC}^i = \mathcal{T}_{DC}^i + \mathcal{T}_{DIFF}^k$
16: **End if**
17: **End for**
18: **End for**
19: Compute the one-time trust of $\mathcal{M}_i$, $\mathcal{T}_{DC}^i = \mathcal{T}_{DC}^i / |\mathbb{D}_{SAME}|$
20: Compute the comprehensive trust of $\mathcal{M}_i$ using Formula 14
21: **End for**
Output: the global trust of MDCs in $\mathbb{W}$

Second, if there is no data submitted by $\mathcal{M}_i$ that overlaps with the data collected by UAVs, we cannot conduct trust evaluation on $\mathcal{M}_i$, then let the global trust of $\mathcal{M}_i$ be $\mathcal{T}_{DC}^i = null$.

Assuming the set of MDCs participating in data collection is $\mathbb{M}_+$, the set of winning MDCs is $\mathbb{W}$, the set of data provided by winning MDCs is $\mathbb{D}_{win}$, $\mathbb{D}_{win} = \{\mathbb{D}_1, \mathbb{D}_2, \dots \mathbb{D}_i \dots\}$, where $\mathbb{D}_i$ is set of data reported by $\mathcal{M}_i$. The set of data list submitted by all MDCs is $\mathbb{L}$, and the data list of $\mathcal{M}_i$ is $\mathbb{L}_i$, $\mathbb{L}_i = \{L_{D_1}, L_{D_2}, \dots\}$, where L_{D_1} is the record of data packet D_1, L_{D_1}=$[\tau_c, Dev_c, Abs_D, Tlink, Q_{self}, \mathcal{P}_D]$. The set of baseline data provided by UAVs is $\mathbb{D}_{UAV} = \{\mathcal{D}_{UAV}^1, \mathcal{D}_{UAV}^2, \dots, \mathcal{D}_{UAV}^i, \dots\}$. Then the global trust evaluation can be represented by Algorithm 2.

C. Local Trust Evaluation Model in UUTE

Local trust helps MDCs decide whether to exchange data, so that data can be collected collaboratively between trusted MDCs. Based on the data verification hash code issued by UAVs, MDCs make local trust evaluation for other MDCs that have exchanged data with them.

Each MDC has a table storing the interaction history locally, which records all MDCs who have exchanged data with it, as shown in Table 1.

TABLE II
Data interaction records of MDCs

$\mathcal{M}_{index}$	Num_{suc}	Num_{fail}	Tru_{his}
MDC_010	6	1	[0.85, 0.73, 0.88…]
MDC_010	2	3	[0.80, 0.75, 0.20…]
…	…	…	…

$\mathcal{M}_{index}$ is the identification of the interactive MDC, Num_{suc} is the record of successful interaction, Num_{fail} is the record of failed interaction, Tru_{his} is the local trust evaluation made by the current MDC to the interactive opponent in the past data interactions.

According to the success and failure interactions and past local trust of MDCs, the trust reference value for data interaction is calculated as follows:

$$T_{itac} = \omega_1 \frac{Num_{suc}}{Num_{suc} + Num_{fail}} + \omega_2 \sum_{k=1}^{Z} Tru_{his}^k \frac{h(k)}{Z}, \quad \text{where } \omega_1 + \omega_2 = 1, \omega_1 < \omega_2. \tag{16}$$

ω_1 and ω_2 are weight factors, because Num_{suc} and Num_{fail} not only record the interactions between MDCs, but also the interactions between MDC and the data center. And Tru_{his} is the trust evaluation made by the current MDC on the evaluated object, so we assign a higher weight to ω_2. Before deciding whether to interact, the MDC has an expected trust T_{exp}. If $T_{itac} > T_{exp}$, then agree to the data exchange, otherwise no data exchange occurs.

We mark data exchange between MDCs in a specific format. For $\mathcal{M}_i$, a data exchange is expressed as:

$$\mathcal{R}_{MDC}^i = [N_{itac}, Itac_{his}, \mathcal{M}_{index}, Abs_D, Tru_{itac}, \tau_{itac}]. \tag{17}$$

N_{itac} is the interaction number; $Itac_{his}$ is used to identify whether there has been data interaction with the MDC before; $\mathcal{M}_{index}$ is the identification of the interactive MDC; Abs_D is the abstract information of the interaction data; Tru_{itac} is the trust evaluation of $\mathcal{M}_{index}$ made by $\mathcal{M}_i$ in this interaction. Tru_{itac} can be evaluated after data exchange, or after local evaluation based on hash verification code, τ_{itac} is interaction timestamp.

Algorithm 3: *Algorithm for local trust evaluation*

For each $\mathcal{M}_i$ wants to exchange data **Do**
  Compute trust T_{itac} of $\mathcal{M}_{itac}$ using Formula 16
  If $T_{itac} > T_{exp}$ **Do**
    Add an interaction record, and exchange data
    Let $D_{itac} \in \mathbb{D}_{itac}^i$
  End if
End for
UAVs distribute data verification hash code to MDCs
For each $\mathcal{M}_i$ receives data verification hash code **Do**
  For each $D_i \in \mathbb{D}_{itac}^i$ of $\mathcal{M}_i$ **Do**
    If D_i corresponds to a data verification hash code $\hbar_v$ **Do**
      $\mathcal{M}_i$ generates the data verification hash code $\hbar_i$ of D_i
      If $\hbar_i$ matches $\hbar_v$ **Do**
        Let $Num_{suc} = 1$ of $\mathcal{M}_i$ and $\mathcal{M}_{itac}$
      End if
      Else
        Let $Num_{fail} = 1$ of $\mathcal{M}_i$ and $\mathcal{M}_{itac}$
  End for
  Compute local trust of MDCs interacted with $\mathcal{M}_i$ using Formula 18
End for
Output: the local trust of MDCs participating in data exchange

The steps of local trust evaluation are shown in Fig. 3:

- Generate hash code for data verification. After the data center obtains the data from the winning MDCs, it generates hash verification codes for the data. The data verification hash code is obtained based on the hash function. According to the characteristics of the hash function, it is a one-way derivation mode. That is, the data verification hash code can be derived from the data, but the data cannot be deduced through the hash verification code. This prevents malicious MDCs from stealing data after obtaining the hash verification code. Then the data center sends the hash verification codes to UAVs;
- UAVs distribute the code to MDCs. On the way to collecting data from sites, the UAVs send the data verification hash code to MDCs in the line of sight;
- MDCs verify the data obtained from the interacted objects. After MDCs obtain the hash verification code, they first analyze whether the data has been collected by themselves. If it has been collected, they also use the hash function to generate the data verification hash code for their own data;
- MDCs make trust evaluations for interacted MDCs. MDCs compare the hash code generated by themselves with the hash code issued by UAVs, and if they are consistent, let $Num_{suc} = 1$ of the MDC that interacts with, otherwise Num_{fail}=1. Based on the verification result of data hash code, a trust evaluation is obtained:

$$\mathcal{T}_{local} = \frac{Num_{suc}}{Num_{suc} + Num_{fail} + 1} + \frac{\vartheta}{Num_{suc} + Num_{fail} + 1}, \quad \text{where } \vartheta = 0.5. \tag{18}$$

Suppose the MDC that wants to exchange data is $\mathcal{M}_i$, and the MDC interacted with it is $\mathcal{M}_{itac}$, $\mathbb{D}_{itac}^i$ is the data set obtained by $\mathcal{M}_i$ through exchange, D_{itac} is the data exchanged. The data verification hash code distributed by UAVs is $\hbar_v$. Then local trust evaluation can be expressed by Algorithm 3.

TABLE III
Malicious attacks in the trust model

Attacks	Performance	Communication	Data	Reputation
Man-in-the-middle attack	Intercept communication; tamper with or sniff data	√	√	
Selective forwarding	Discard part or all critical data		√	
Sybil attack	Tamper with or falsify data; steal data		√	
Packet tampering	Abnormality of data packets		√	
On-off attack	Perform bad or good behaviors alternately	√	√	
Bad/good mouth attack	Provide bad evidence for legitimate participants and good evidence for malicious attackers			√

V. Theoretical Analysis

In this section, we conduct a theoretical analysis on UUTE in terms of security, reliability and correctness.

First, we analyze common malicious attacks. Malicious data collectors launch various attacks after entering the network. Typical attacks include man-in-the-middle attack, selective forwarding, sybil attacks, packet tampering, etc. [5], [7]. In the man-in-the-middle attack, assume that the communication between MDC_a and MDC_b is forwarded by MDC_c, then MDC_c can intercept normal communication and perform data tampering and sniffing. However, both parties in the communication have no knowledge of this. In the selective forwarding attack, the relay node discards part or all critical information when forwarding data packets. In sybil attacks, active attackers tamper and forge messages, and passive attackers intercept or eavesdrop on related data. In addition, there are some attacks that specifically target the trust model, such as on-off attacks and bad/good mouth [12]. In on-off attacks, malicious nodes alternately perform positive and negative behaviors. After launching a malicious attack for a period of time, the attacker resumes normal behavior to avoid detection. In bad/good mouth, malicious attackers provide bad evidence for legitimate participants and good evidence for malicious attackers [12]. The performance and impact of these attacks are given in Table III.

As summarized in Table III, the damage to network performance caused by malicious attacks is mainly reflected in the following aspects: (1) Communication. Malicious attacks intercept or block the communication between normal participants through various means, so that normal nodes cannot communicate successfully, and increase the extra cost of the network due to message retransmission. (2) Data quality. Malicious attacks intercept and steal communication messages, thereby causing data leakage, and even worse attackers tamper or forge illegal data, thereby reducing data quality. (3) Reputation. Malicious attackers provide false trust evaluations, making the network unable to accurately distinguish between ordinary participants and malicious attackers.

Based on the above manifestations of malicious attacks, we analyze the security, reliability and correctness of UUTE below.

Security. Malicious attacks mainly affect communication security and data security. Therefore, security can be ensured by detecting abnormal communication and data behaviors [7], [12]. First, for communication security, the local trust evaluation model proposed in UUTE can be realized by analyzing the data interaction behavior of the evaluated object within a valid time. In the local trust evaluation model, any two directly interacting nodes conduct mutual trust evaluation, and the number of successful and failed interactions of nodes accumulate with the frequency of interactions. Therefore, by analyzing the success and failure of the evaluated object in the continuous massive data interaction, it can be accurately judged whether the evaluated object has made a malicious attack in communication. In addition, the global trust evaluation model proposed in UUTE can ensure data security. In the global trust evaluation model, by comparing the data submitted by the evaluated object with the baseline data obtained by UAVs, the difference between the submitted data and the real value can be accurately analyzed, thus determining whether the evaluated object has tampered with or forged the data. Moreover, in UUTE's local trust evaluation model, the authenticity of the data is verified through the data verification hash code distributed by UAVs, and this verification code is based on the original data through hash function processing, so it has one-way and irreversible characteristics. This means that even if a malicious node gets a data validation hash code, it cannot roll back the data against the verification code, thus preventing the data from being stolen.

Reliability. In UUTE, the global trust evaluation model is used to evaluate the credibility of the evaluated object in terms of data, and the local trust evaluation model evaluate the performance of the evaluated object both in data and communication. Therefore, assuming that unexpected situations such as drone hijacking occur during the implementation of global trust evaluation, trust evaluation can also be conducted through the local trust evaluation model. Although this has a certain impact on the accuracy of the evaluation, it can still ensure the implement of the trust evaluation. And the local trust evaluation is implemented by observing the interactive relationship between the evaluated objects. This evaluation method is feasible in general scenarios, even in scenarios with sparse interactions, through the combination of global and local models, trust evaluation is also feasible.

Correctness. The correctness of trust evaluation is considered from data and reputation. Judging from the data accuracy, the accuracy of UUTE is relatively high. In UUTE's global trust evaluation, the data submitted by evaluated objects are compared with the baseline data obtained by UAVs. This is an objective and confirmatory evaluation method, which is not affected by the subjective attitude of the evaluator as the previous passive evaluation, so it has a high accuracy. From the reputation perspective, UUTE can also resist the false reputation provided by attacks such as bad/good mouth. In this article, each evaluated object exchanges data with a large number of other entities during data collection, so even if a small number of malicious nodes provide false reputation information, the large

percentage of ordinary nodes provide real reputation. Suppose that MDC_a interacts with m nodes, and n nodes are malicious and provide false reputation. When m is large and n is small enough, the reputation trust provided by n malicious attackers has little impact on the entire trust evaluation. Especially in the context of 5G and beyond networks, the number of IoT devices in the network is very large, that is, m is a large number.

VI. Experimental Analysis

A. Experiment Setup

We use urban data collection as a typical scenario for the experiment in this article. In the experimental scenario, the data center is deployed in the city center, and many taxis act as mobile data collectors to move around the city for data collection. To make the experiment more realistic, the urban taxis use a real vehicle trajectory dataset [29], [30]. The dataset contains the GPS trajectories of 10,357 taxis during the period of Feb. 2 to Feb. 8, 2008 within Beijing. The total number of points in this dataset is about 15 million and the total distance of the trajectories reaches 9 million kilometers. Each track record in the dataset contains the following fields: taxi id, date time, longitude, latitude. The longitude and latitude information of the vehicle trajectory in the original dataset is converted into plane coordinates. Fig. 4 is a map of the trajectory of these taxis in a day. In the trajectory shown in Fig. 4, some records are invalid, and some records have nothing to do with the experiment. Therefore, we preprocess the dataset to filter out the illegal records, while retaining the trajectory information of 1600 vehicles. These taxis are richer in activity trajectories.

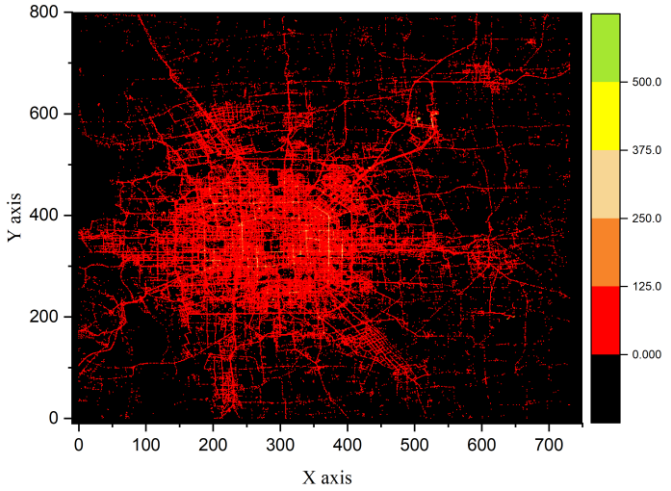

Fig. 4. Trajectory of vehicles in dataset in one day

Other experimental settings are as follows: (a) Based on the vehicle trajectories and city maps in the dataset, we selected 500 data collection sites. Among them, the urban center area with huge traffic is densely deployed, and the edge area is sparsely deployed. Each data collection site is deployed with a sensing device, and each sensing device generates five packets in one round. (b) When the vehicle is within 30 meters from the sensing device, data can be obtained from the sensing device. And when the vehicle is moving, it can exchange data with other vehicles within communication range. The expected trust of data exchange is T_{exp}=0.5. Only when the trust of opponent is higher than T_{exp}, the current vehicle agrees to exchange data with it. (c) The payment for each packet of vehicles is 0.3-0.9. Before the first interaction, the global and local initial trust of vehicles is 1, and the initial number of successful and failed interactions is 0. (d) In each round, the collection frequency of data collection sites is counted, and 10% of the sites with the highest frequency are selected as the sites for UAVs to obtain baseline data.

We evaluate the effectiveness of UUTE based on the following metrics: a) Data coverage. Data coverage refers to the maximum sites' coverage achieved by the data provided by vehicles. b) Cost. Cost refers to the total expenditure of the system for collecting data. c) Trust. Trust is the reliability of vehicles based on their data quality and interaction performance.

For comparison, we chose two reference schemes. The first is the Cost Minimization scheme based on Passive Trust evaluation (CMPT), which is based on the Trust-based Minimum Cost and Quality Aware Data Collection Scheme proposed in [26], by introducing a passive trust evaluation mechanism. In CMPT, the data center selects vehicles with low data collection prices as winning data providers each time. To save costs, UAVs are not introduced in trust evaluation, and the trust is computed by observing the interactive behaviors of MDCs. At the same time, in order to obtain more interactive behaviors to judge trust accurately, we set T_{exp}=0.3. The second is the Quality Optimization scheme based on Active Trust evaluation (QOAT), which is an improvement on the scheme proposed by Jiang et al. in [22]. In QOAT, the data center selects the data submitted by the most trusted MDC each time. In order to better verify the authenticity of data, in addition to making local evaluations based on interactive behaviors, UAVs are dispatched to collect baseline data from 30% of sites with the highest frequency for global trust evaluation.

B. Data Coverage

The data center selects part vehicles from all the vehicles that provide the data list, purchases the data submitted by them, and gives them data collection payment. Those vehicles that are selected to submit data and get payments are called winning vehicles. Fig. 5–Fig. 7 show the data coverage of winning vehicles. Usually, the greater the data coverage, the more data about the sites provided by winning vehicles. Hence, the larger the data space, the better the data quality.

We select winning vehicles on the condition that the maximum coverage is reached, i.e., for each data collection site that generates data packets, it is guaranteed that it has at least one vehicle providing data. Therefore, in Fig. 5-Fig. 7, the number of sites is the same, and 500 data collection sites are all covered, but the data coverage of each site is different. In the UUTE, the maximum data coverage is about 335, the data coverage of sites in the central area is mostly at 134.6-335, and the data coverage of sites in the peripheral area is mostly at 1-67.8. In the CMPT, the data coverage is up to about 289, the data coverage of sites in the center area is mostly at 116.2-289, and the data coverage of sites in the edge area is mostly at 1-58.6. In the QOAT, the maximum data coverage is about 353, most of the data coverage of sites in the central area is at 141.8.2-353, and that of the sites in the edge area is at 1-71.4. It can be seen that the largest data coverage is QOAT, while the data coverage of CMPT is significantly smaller than the other two solutions. This is because CMPT adopts a low-price priority vehicle selection mechanism, so there may be some vehicles with very low data payments that

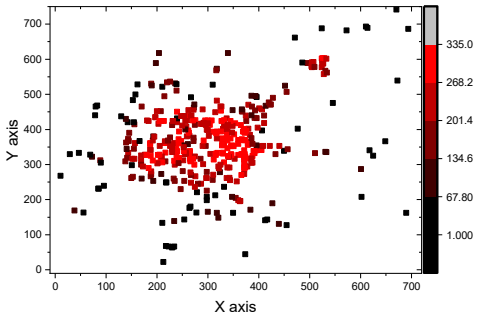

Fig. 5. Data coverage reached by winning vehicles in UUTE

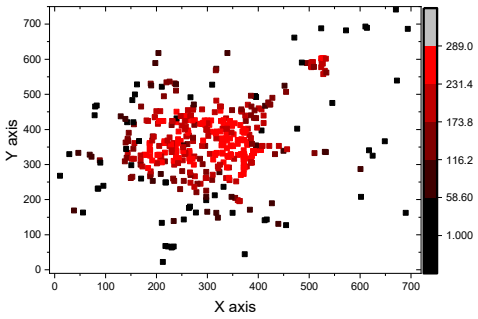

Fig. 6. Data coverage reached by winning vehicles in CMPT

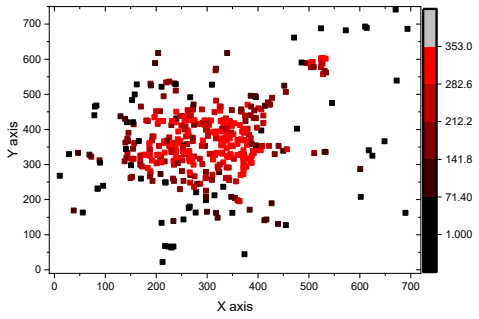

Fig. 7. Data coverage reached by winning vehicles in QOAT

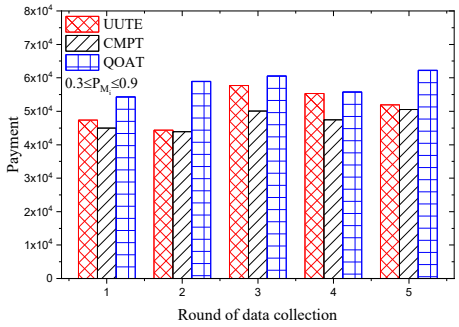

Fig. 8. Payment for purchasing data from winning vehicles in each round

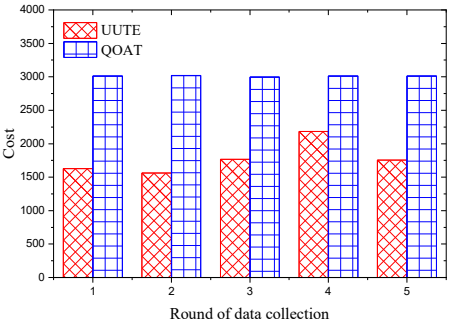

Fig. 9. Cost of UAVs for collecting baseline data in each round

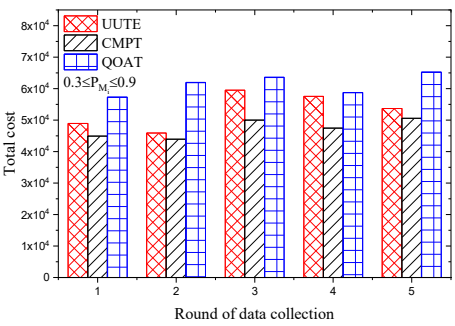

Fig. 10. Total data collection cost in each round

are actually malicious mobile data collectors with low trust, so the data they provide is invalid, which reduces actual data coverage. QOAT uses a high-trust-first vehicles selection mechanism, which most of the data provided are trustworthy, so the actual data coverage is high. The UUTE proposed in this article considers both payment and trust. The results show that its data coverage is slightly smaller than QOAT, and it can also achieve a good data coverage.

C. *Cost*

Cost includes the payment for purchasing data from winning vehicles and the overhead of dispatching UAVs to collect baseline data. In this paper, the process of all vehicles traversing once according to the trajectory in the dataset and submitting the data packets to the data center is called a round of data collection. Assuming that the payment for each data packet submitted by the vehicle is between 0.3 and 0.9, and Algorithm 1 is used to select the winning vehicles that provide the data, then the payment for purchasing data from winning vehicles in each round is shown in Fig. 8. As shown in Fig. 8, CMPT purchases the cheapest packets each time so its payment is the lowest. UUTE considers price as a key factor when selecting winning vehicles, so its payment is slightly higher than CMPT, while QOAT only focuses on trust of vehicles, so its data collection cost is much higher. The data collection payment of UUTE is 0.94%-16.58% higher than CMPT, and 0.76%-32.9% lower than QOAT.

Assuming that the conversion factor α in UUTE and QOAT is a fixed constant, UUTE selects 10% of baseline sites, and QOAT selects 30% of baseline sites, then the cost of dispatching UAVs to collect baseline data is illustrated in Fig. 9. The cost is directly proportional to the flight distance, and the flight distance is directly proportional to the number of sites. As shown in Fig. 9, the cost of UAVs of UUTE is significantly lower than QOAT, which is about 51.69%-72.49% of QOAT.

Fig. 10 is the total cost of the three schemes. Compared with CMPT, the total cost of UUTE is increased by 4.49%-21.18%; compared with QOAT, the cost is reduced by 2.17%-34.96%.

D. *Trust*

The trust of vehicles includes global and local trust. Global trust refers to the trust evaluated by the data center based on baseline data. Local trust refers to the trust evaluation given by other vehicles based on data exchange. Assuming that the initial trust of all vehicles is 1, the data exchange trust threshold is 0.5 (the threshold of CMPT is 0.3), one-time trust is the value obtained from a trust evaluation, comprehensive trust is the weighted result of multiple trust evaluations considering time decay. And the maximum historical trust record Z=10, then the local and global trust of vehicles can be obtained, as shown in Fig. 11-Fig. 14.

Fig. 11 shows the local trust of credible vehicles. The local trust is given by other vehicles. The more vehicles that provide evaluation, the more accurate the local trust of the vehicle, because even a small number of vehicles conspire to give high evaluations to increase mutual trust. Most vehicles provide true evaluations. In Fig. 11 and Fig. 12, the one-time trust of credible vehicles fluctuates greatly, and most vehicles are above 0.5. However, due to data interaction, credible vehicles obtain false data from malicious vehicles, which affects their data quality, resulting in a very low one-time trust of some credible vehicles. The comprehensive trust is based on multiple data submissions or interactions. Even though credible vehicles may be affected by one-time malicious interaction, due to its credible nature, it

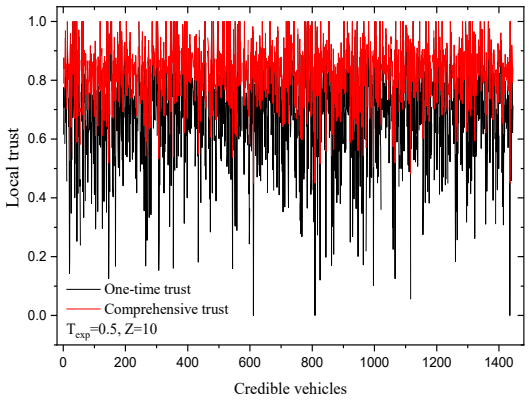

Fig. 11. Local trust of credible vehicles in UUTE

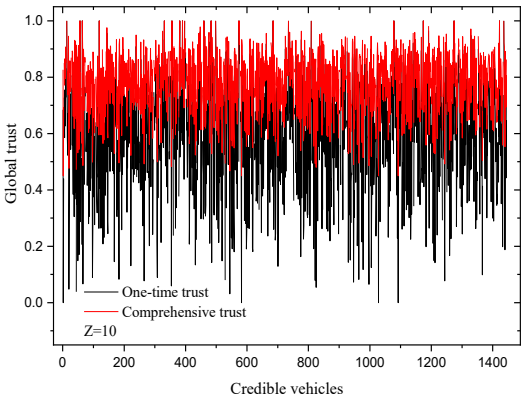

Fig. 12. Global trust of credible vehicles in UUTE

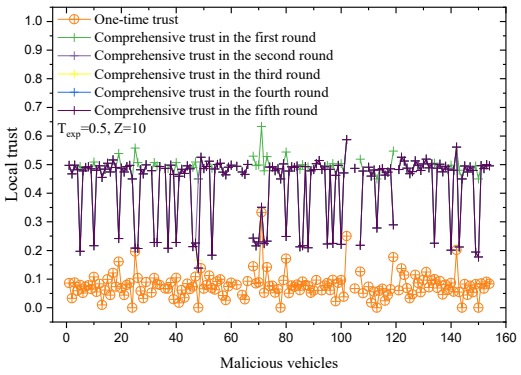

Fig. 13. Local trust of malicious vehicles in UUTE

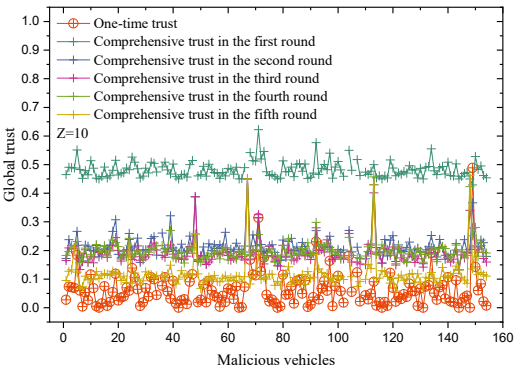

Fig. 14. Global trust of malicious vehicles in UUTE

provides credible data in most cases. Therefore, the comprehensive trust of almost all vehicles is above 0.6, which shows that the trust evaluation of UUTE for credible vehicles is accurate.

Fig. 13 and Fig. 14 are the local trust and global trust of malicious vehicles. Since the data provided by malicious vehicles is false, it can be found to be unreliable through one data verification, so the one-time trust is very low. It can be seen from Fig. 13 that the five rounds of comprehensive local trust have little difference. This is because in the data interaction under the UUTE, when the trust of objects to exchange data is lower than 0.5, it refuses to interact with it. As a result, after the trust of malicious vehicles is below 0.5, data interaction does not occur again, so its local trust has not changed in the following rounds. Unlike the local trust, in the global trust shown in Fig. 14, the comprehensive global trust of malicious vehicles is gradually reduced in each round, and the trust of most vehicles has been reduced to about 0.1 in the fifth round. Because when using UAVs to obtain baseline data to evaluate the data of malicious vehicles globally, as long as the data sites collected by the vehicle are consistent with the UAVs, they can be compared and verified, and the sites collected by UAVs are sites with highest frequency. Therefore, with each comparison with baseline data, the bad attributes of malicious vehicles become more and more obvious. Comparing Fig. 13 and Fig. 14, it can be found that compared to the local trust based on interactive behavior, the global trust assisted by UAVs can be more dynamic and accurate in evaluating the trust of malicious vehicles.

Similar to the trend in Fig. 11-Fig. 14, Fig. 15-Fig. 16 shows the average trust of credible and malicious vehicles under the UUTE, CMPT and QOAT schemes. Overall, whether it is average local trust or average global trust, the trust of credible vehicles gradually increases with the number of rounds, and the trust of malicious vehicles gradually decreases with the number of rounds, which are gradually getting closer to their true trust. Comparing the trust evaluation of the three schemes, the evaluation results of QOAT are more accurate for credible vehicles, and the results of UUTE are closer to QOAT. For malicious vehicles, the evaluation results of CMPT are more accurate.

The trust of winning vehicles directly determines the data quality. The higher the trust of the vehicles, the higher the credibility of the data it provides, and the better the data quality. Fig. 17 depicts the trust of winning vehicles. Whether it is global trust or local trust, the trust of winning vehicles under QOAT is the highest, followed by UUTE. Compared with CMPT, trust of winning vehicles under UUTE is about 0.11 higher. Some of the selected winning vehicles may be malicious vehicles in disguise, so the data they provide is not only useless to the system, but also affects network coverage and data quality. Fig. 18 shows the proportion of malicious vehicles under the three schemes. Although the proportion of malicious vehicles in each round changes somewhat, overall, the ratio of malicious vehicles in QOAT is very small. Only about 0.03-0.08 vehicles are malicious vehicles. While the ratio of malicious vehicles in CMPT is much higher, the maximum is about 0.F. The proportion of malicious vehicles in UUTE proposed in this article is relatively stable, basically between 0.06-0.09 in each round.

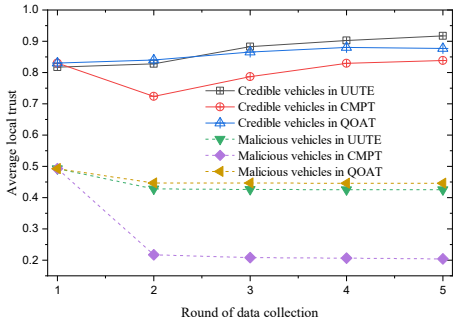

Fig. 15. Average local trust of vehicles in each round

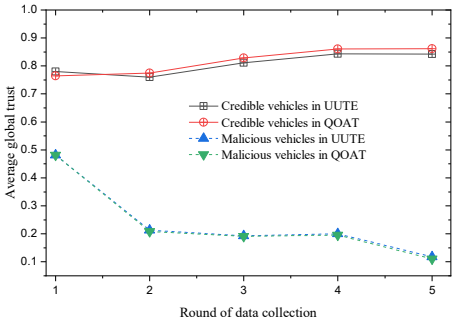

Fig. 16. Average global trust of vehicles in each round

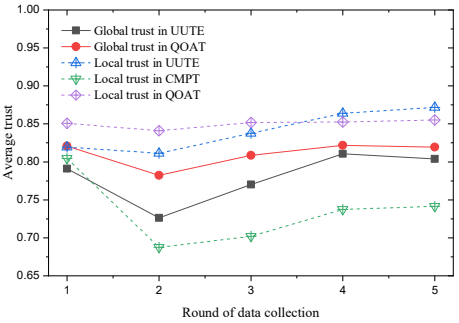

Fig. 17. Average trust of winning vehicles in each round

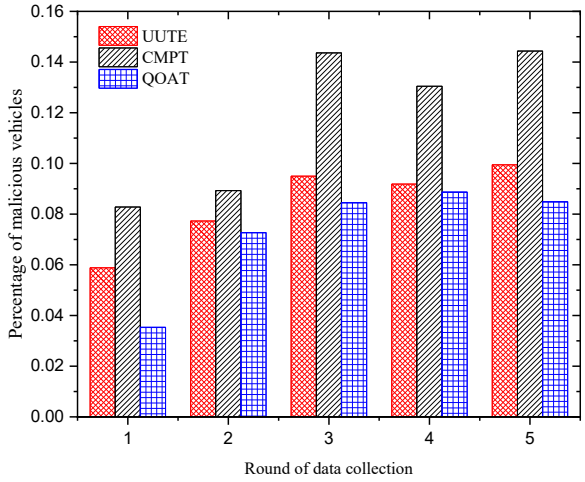

Fig. 18. Percentage of malicious winning vehicles in each round

VII. Conclusion And Future Work

In this paper, we propose a UAV-assisted ubiquitous trust communication system, which can achieve low-cost and high-quality data collection in 5G and beyond networks. We select urban data collection as a typical scenario and use incentive mechanisms to stimulate more MDCs to participate in tasks. Specifically, for the data collection platform, when selecting data providers, we propose a UAV-assisted global trust evaluation model to help the data center identify malicious participants from a large number of MDCs. Regarding the data interaction between MDCs, to avoid malicious MDCs from harming trusted participants, we propose a local trust evaluation model that allows MDCs to conduct trust evaluations of data collectors who have interacted with them. Experimental results demonstrate that, compared with the previous evaluation methods, the UUTE can make more accurate trust evaluations for credible and malicious data collectors, at the same time reduce the data collection cost. For the further works, we consider using trusted MDCs as sub-benchmarks to accelerate the evolution and scope of trust, while conducting in-depth analysis of possible security threats to drones to improve system robustness.

Acknowledgement

This work was supported by the National Natural Science Foundation of China under Grant No. 61772554, 62072475, and supported by the Hunan Provincial Innovation Foundation for Postgraduate, Grant No. CX20200212, 2020zzts139.

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," IEEE Internet of Things journal, vol. 1, no. 1, pp. 22-32, 2014.

[2] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From iot to 5g i-iot: the next generation iot-based intelligent algorithms and 5g technologies," IEEE Communications Magazine, vol. 56, no. 10, pp. 114-120, 2018.

[3] K. L. Lueth, "State of the IoT 2018: Number of IoT devices now at 7B-Market accelerating," IoT Analytics. [Online]. Available: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/, 2018.

[4] D. Reinsel, J. Gantz, and J. Rydning, "Data age 2025: the digitization of the world – from edge to core," IDC White Paper Doc#US44413318, pp. 1-29, 2018.

[5] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, and M. Guizani, "Smart cities: A survey on data management, security, and enabling technologies," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2456-2501, 2017.

[6] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2013-2027, 2017.

[7] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5, pp. 1228-1237, 2015.

[8] A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, and J. Eriksson, "VTrack: accurate, energy-aware road traffic delay estimation using mobile phones," In the Proceedings of the 7th ACM conference on embedded networked sensor systems, pp. 85-98, 2009.

[9] W. Mobile, "WAZE Outsmarting Traffic, Together," [Online]. Available: http://www.waze.com/, 2015.

[10] Buuuk, "WeatherLah iPhone application," [Online]. Available:http://itunes.apple.com/us/app/weatherlah/id411646329?mt=8, 2012.

[11] G. Theodorakopoulos, and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 318-328, 2006.

[12] G. Han, Y. He, J. Jiang, N. Wang, M. Guizani, and J. A. Ansere. "A synergetic trust model based on svm in underwater acoustic sensor networks," IEEE Transactions on Vehicular Technology, vol. 68, no. 11, pp. 11239-11247, 2019.

[13] S. Abdelhamid, H. S. Hassanein, and G. Takahara, "Reputation-aware, trajectory-based recruitment of smart vehicles for public sensing," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 5, pp. 1387-1400, 2017.

[14] M. Gapeyenko, V. Petrov, D. Moltchanov, S. Andreev, N. Himayat, and Y. Koucheryavy, "Flexible and reliable UAV-assisted backhaul operation in 5G mmWave cellular networks," IEEE Journal on Selected Areas in Communications, vol. 36, no. 11, pp. 2486-2496, 2018.

[15] X. Xu, Y. Zeng, Y. L. Guan, and R. Zhang, "Overcoming Endurance Issue: UAV-Enabled Communications With Proactive Caching," IEEE Journal on Selected Areas in Communications, vol. 36, no. 6, pp. 1231-1244, 2018.

[16] Z. Hadzi-Velkov, S. Pejoski, N. Zlatanov, and R. Schober, "UAV-assisted Wireless Powered Relay Networks with Cyclical NOMA-TDMA," IEEE Wireless Communications Letters, DOI: https://doi.org/10.1109/LWC.2020.3013296, 2020.
[17] X. Hu, K. K. Wong, K. Yang, and Z. Zheng, "UAV-Assisted Relaying and Edge Computing: Scheduling and Trajectory Optimization," IEEE Transactions on Wireless Communications, vol. 18, no. 10, pp. 4738-4752, 2019.
[18] Q. Wu, Y. Zeng, and R. Zhang, "Joint Trajectory and Communication Design for Multi-UAV Enabled Wireless Networks," IEEE Transactions on Wireless Communications, vol. 17, no. 3, pp. 2109-2121, 2018.
[19] Q. Wu, J. Xu, and R. Zhang, "Capacity Characterization of UAV-Enabled Two-User Broadcast Channel," IEEE Journal on Selected Areas in Communications, vol. 36, no. 9, pp. 1955-1971, 2018.
[20] I. Pinyol, and J. Sabatermir, "Computational trust and reputation models for open multi-agent systems: a review," Artificial Intelligence Review, vol. 40, no. 1, pp. 1-25, 2013.
[21] Y. A. Kim, and R. Phalak. "A trust prediction framework in rating-based experience sharing social networks without a Web of Trust," Information Sciences, vol. 191, pp. 128-145, 2012.
[22] B. Jiang, G. Huang, T. Wang, J. Gui, and X. Zhu, "Trust based energy efficient data collection with unmanned aerial vehicle in edge network," Transactions on Emerging Telecommunications Technologies, DOI: https://doi.org/10.1002/ett.3942, 2020.
[23] G. Dangelo, F. Palmieri, and S. Rampone, "Detecting unfair recommendations in trust-based pervasive environments," Information Sciences, vol. 486, pp. 31-51, 2019.
[24] S. Laniepce, J. Demerjian, and A. Mokhtari, "Cooperation monitoring issues in ad hoc networks", In the Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, pp. 695-700, 2006.
[25] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs," IEEE Transactions on Mobile Computing, vol. 14, no. 10, pp. 2101-2115, 2015.
[26] Y. Ren, Z. Zeng, T. Wang, S. Zhang, and G. Zhi, "A Trust-based Minimum Cost and Quality Aware Data Collection Scheme in P2P Network," Peer-to-Peer Networking and Applications, vol. 7, pp. 2300–2323, 2020.
[27] M. Huang, K. Zhang, Z. Zeng, T. Wang, and Y. Liu, "An AUV-assisted Data Gathering Scheme based on Clustering and Matrix Completion for Smart Ocean," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9904-9918, 2020.
[28] H. A. Alameddine, S. Sharafeddine, S. Sebbah, S. Ayoubi, and C. Assi, "Dynamic task offloading and scheduling for low-latency IoT services in multi-access edge computing," IEEE Journal on Selected Areas in Communications, vol. 37, no. 3, pp. 668-682, 2019.
[29] J. Yuan, Y. Zheng, X. Xie, and G. Sun, "Driving with knowledge from the physical world," In the 17th ACM SIGKDD international conference on Knowledge Discovery and Data mining, pp. 316-324, 2011.
[30] J. Yuan, Y. Zheng, C. Zhang, W. Xie, X. Xie, G. Sun, and Y. Huang, "Tdrive: driving directions based on taxi trajectories," In the Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems, pp. 99-108, 2010.

Mingfeng Huang received her B.E. degree in the school of Engineering and Design, Hunan Normal University, China, in 2017. She is currently pursuing her Ph.D. degree in the school of Computer Science and Engineering, Central South University, China. Her research interests include trusted computing and wireless sensor networks. She has published 10 papers, and has so far been SCI-cited more than 100 times, published journals include IEEE internet of things journal, IEEE transactions on systems, man, and cybernetics, etc.

Anfeng Liu is a Professor at the School of Computer Science and Engineering, Central South University, China. He is also a Member (E200012141 M) of the China Computer Federation (CCF). He received his M.Sc. and Ph.D. degrees from Central South University, China, 2002 and 2005, both in computer science. His research interest is wireless sensor network.

Neal N. Xiong (S'05–M'08–SM'12) is an Associate Professor at Department of Mathematics and Computer Science, Northeastern State University, OK, USA. He received his both PhD degrees in Wuhan University (2007, about sensor system engineering), and Japan Advanced Institute of Science and Technology (2008, about dependable communication networks), respectively. Before he attended Northeastern State University, he worked in Georgia State University, Wentworth Technology Institution, and Colorado Technical University (**full professor about 5 years**) about 10 years. His research interests include Cloud Computing, Security and Dependability, Parallel and Distributed Computing, Networks, and Optimization Theory.

Jie Wu (F'09) is the Director of the Center for Networked Computing and Laura H. Carnell professor at Temple University. He served as Chair of Department of Computer and Information Sciences from the summer of 2009 to the summer of 2016 and Associate Vice Provost for International Affairs from the fall of 2015 to the summer of 2017. His research interests include mobile computing and wireless networks, routing protocols, cloud and green computing, network trust and security, and social network applications. Dr. Wu regularly publishes in scholarly journals, conference proceedings, and books. He serves on several editorial boards, including IEEE Transactions on Mobile Computing, IEEE Transactions on Service Computing, Journal of Parallel and Distributed Computing, and Journal of Computer Science and Technology. Dr. Wu is a Fellow of the AAAS and a Fellow of the IEEE. He is the recipient of the 2011 China Computer Federation (CCF) Overseas Outstanding Achievement Award.