Edge Computing based Trustworthy Data Collection Model in the Internet of Things

Tian Wang, Lei Qiu, Arun Kumar Sangaiah*, Anfeng Liu, Md Zakirul Alam Bhuiyan, Ying Ma

Abstract—It is generally accepted that Edge Computing paradigm is regarded as capable of satisfying the resource requirements for the emerging mobile applications such as the IoT (Internet of Things) ones. Undoubtedly, the data collected by underlying sensor networks is the foundation of both the IoT systems and IoT applications. However, due to the weakness and vulnerability to attacks of underlying sensor networks, the data collected is usually untrustworthy, which may cause disastrous consequences. In this paper, a new model is proposed to collect trustworthy data on the basis of edge computing in the Internet of Things. In this model, the sensor nodes are evaluated from multiple dimensions to obtain accurately quantified trust values. Besides, by mapping the trust value of a node onto a force for the mobile data collector, the best mobility path is generated with high trust. Moreover, a mobile edge data collector is used to both visit the sensors with quantified trust values and collect trustworthy data. The extensive experiment validates that the IoT systems based on trustworthy data collection model gain a significant improvement in their performance, in terms of both system security and energy conservation.

Index Terms—Trust value and virtual force, Data collection, Edge computing, IoT applications

1 Introduction

The rapid development of the Internet of Things (IoT) and mobile applications witnesses increasingly stringent requirements for cloud infrastructure and underlying wireless sensor networks(WSNs), including system security, ultra-low latency, low power consumption and data trustworthiness [1]. These demanding requirements cry for highly localized services on the edge of the network that is close to the user. Therefore, Mobile Edge Computing (MEC) emerges, which is a distributed open platform and integrates network, computing, storage, and applications with core capabilities on the edge of the network near the source or data source to provide edge intelligence services [2].

The data collected by the underlying sensor networks lays the foundation for IoT systems and applications, but the reality is that such data collected by the sensor network is untrustworthy [3] [4]. Sensor nodes are randomly deployed in unattended areas and harsh environments to perform a variety of complex tasks and play an important role in various fields such as battlefields surveillance, smart cities, medical monitoring, intrusion detection and emergency responses [5]. Due to the complex environment, the underlying sensor network is more vulnerable to attacks. As a result, sensors collect invalid or even misleading data. What is worse is that less than 49% of the data is valid and trustworthy [6] [7]. If the data collection in the sensor networks is problematic and untrustworthy, data protection and application in the upper layer is far beyond possible. Network security means protecting network systems or network resources from all types of attacks. In the underlying WSNs, attacks can be divided into two categories: internal attacks and external attacks. According to existing studies, internal attacks on the underlying IoT network are far more harmful than external ones [8]. Moreover, the security mechanisms for cryptographic authentication and routing protocols are effective against external attacks but have little effect on shattering internal ones. Trust evaluation is an effective and lightweight method to deal with malicious nodes inside a node [9] [10]. Meanwhile, it is an important part of computer security.

As to research on data acquisition in existing IoT systems, we also found that the common node at the bottom is used as an efficient mobile data collector, whose computing power, storage capacity and communication capacity are all very limited and the energy consumption is high [11]. In addition, when a traditional mobile data collector traverses most of the underlying nodes in the process of data collection, aside from long delay and fast energy consumption of nodes, the invalid data from malicious nodes accounts for a large proportion to all the collected data.

In order to solve the above problems, this paper proposes a technology of collecting trustworthy data based on virtual force mapped by trust value (VFDC). Compared with the traditional mobile data collection method, this technology comprehensively considers factors related to sensor nodes trustworthiness. After multidimensional trust evaluation of nodes, the virtual force mapped by the trust value of a node helps the formation of a path, through which the trustworthy data is collected. Besides, the edge node is introduced as the mobile data collector to collect trustworthy data.

The main contributions of this paper are summarized as follows:

1)We propose a new model for trustworthy data collection based

- *Tian Wang and Lei Qiu are with the College of Computer Science and Technology, Huaqiao University, Xiamen, Fujian, China, 361021.*
  $E-mail: cs\_tianwang@163.com, hqu\_qiulei@163.com.$
- *Arun Kumar Sangaiah is with the School of Computing Science and Engineering, VIT University, India.*
  $E-mail$: sarunkumar@vit.ac.in (corresponding author)
- *Anfeng Liu is with the School of Computer Science and Engineering, Central South University, China.*
  $E-mail: afengliu@mail.csu.edu.cn$
- *Md Zakirul Alam Bhuiyan is with the Department of Computer and Information Sciences, Fordham University, America.*
  $E-mail$: zakirulalam@gmail.com
- *Ying Ma is with the College of Computer and Information Engineering, Xiamen University of Technology, China.*
  $E-mail$: maying@xmut.edu.cn

Manuscript received August 1, 2019.

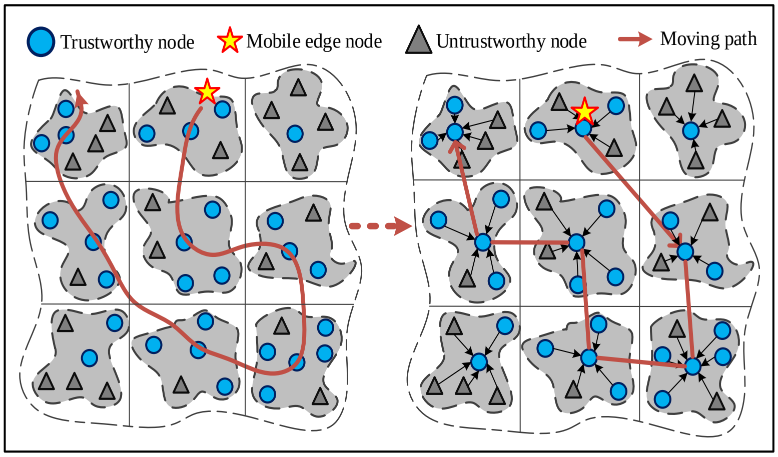


Fig. 1: Mobile path planned based on virtual force mapped by trust value

on edge computing in the Internet of Things. This model combines multi-dimensional node trust evaluation and a novel method for generating a mobile trustworthy path. The proposed method can effectively resist malicious attacks from inside the node and bypass untrustworthy nodes, thereby reducing energy consumption and extending the life cycle of the network.

2) We simulate the moving path into a magnetic cord and use the virtual force mapped by the trust value of the node to iterate continuously, thus pushing the path to a more trustworthy area away from the untrustworthy area. Furthermore, we use the integer interval to represent the trust value, which can save the memory space of the network node.

3) We introduce the edge node as the mobile data collector of the system, which can solve the problem of weak computing and storage capacities of the common low-level node. What is more, since the edge node is close to the edge network, its trustworthiness is higher and hence ensures the security of the data.

The remainder of this paper is structured as follows. Section II summarizes the related works, Section III illustrates the problem to be addressed. Section IV describes the trust evaluation method of the node as well as the specific quantization and division definition of the node trust value. Section V states the proposed method of generating trustworthy data collection path based on the virtual force mapped by trust value. The numerical analysis is presented in detail in Section VI. Finally, this paper is summarized in Section VII.

II Related works

Recently, many researchers have conducted research on the application of data collection and trust evaluation in the Internet of Things. It plays an important role in many aspects, such as fire monitoring, environmental protection and battlefield environmental monitoring [12]. In the existing trust evaluation research of IoT systems, the trust evaluation mechanisms for attack and defense scenarios are mainly divided into two categories. They are the trust mechanism based on network routing optimization and the node-based trust evaluation mechanism.

In trust evaluation, the route optimization scheme is an important one. Tang et al. [13]proposed a Trust-Based Secure Routing (TBSR) scheme using a traceback approach to improving the security of data routing. Compared with past solutions, their results indicate that the performance of the TBSR scheme has been improved. In addition, for new network attacks, different metrics can be used to ensure the security of routing. In paper [14], Hatzivasilis et al. proposed a SCOTRES-a trust-based system for secure routing in ad-hoc networks which advanced the intelligence of network entities by applying five novel metrics. However, their proposed method did not take into account the trust of key nodes in the network. Although routing optimization can enhance security to a certain extent, it can not fundamentally ensure the credibility of nodes and effectively reduce the energy consumption of nodes in mobile applications. Moreover, Although this type of method takes into account the credibility problem, the optimization of routing cannot fundamentally deal with the internal attacks faced by the node itself.

Another type of key research is concerned with the trust evaluation mechanism of nodes. As to trust measurement, parameters are offered based on the functional attributes of the nodes in the application context in paper [15]. In view of the fact that the existing models do not parameterize trust and inaccurately weigh trust proposals, CTRUST is proposed, where the trust is accurately parametrized while recommendations are evaluated through belief functions. In paper [16], Sharma et al. proposed a scheme to reduce the impact of false or dishonest suggestions in indirect trust calculation by carrying out objective and subjective evaluation. Similarly, in order to deal with worms and grey hole attacks caused by RPL protocol in Internet of things, Mehta et al. proposed a mechanism based on lightweight trust [17]. As to malicious node attacks in WSNs, in paper [18], an efficient belief based trust evaluation mechanism (BTEM) was proposed, which isolated the malicious nodes from trustworthy ones and fought against attacks. In order to cope with the resource constraints of WSNs, the exponential-based trust and reputation evaluation system (ETRES) was proposed for WSNs' node trust and reputation evaluation in paper [19]. The entropy theory is used to measure the uncertainty of direct trust values and indirect trust can strengthen interaction information when direct trust is not quite ensured. However, although the trust of the nodes is considered in this type of research, the direct and indirect trust evaluations of the nodes are mostly one-sided, and some papers do not give specific evaluation indicators to evaluate the direct trust, which thus makes the evaluation inaccurate and subjective. In addition, few studies have combined node trust values with specific applications.

In IoT systems, data collection applications are also carefully explored. In order to protect the privacy data of patients in the medical care of the Internet of things, Luo et al. [20]proposed a practical framework called privacy protector, patient privacy protected data collection, with the objective of preventing attacks. The experimental performance analysis shows that the proposed method can effectively deal with attacks, thus protecting patients' privacy data. Considering that the traditional scheme only provides security for the patient's health monitoring data during the communication process, a new data collection method called SecureData was proposed in paper [21]. The experimental results show that the proposed method has obvious advantages of reducing energy consumption and saving computing resources. In paper [22], in order to protect personal privacy, Liu et al. proposed a privacy preserving original data collection scheme for the Internet of things, in which the data of participants was collected and confused with the data of other participants in the group. The results show that the proposed scheme is feasible for the Internet of things system. In order to make better use of sensor systems in smart cities, Plageras et al. [23]proposed a new system to collect and manage sensor data in smart buildings. Using solar energy to integrate multiple technologies into the system provides a better solution for these cities. However, in these data collection applications, research focuses more on data privacy protection, data acquisition, and efficiency of data collection. Few applications consider combining energy-efficient mobile data collection methods with trust assessment issues at data collection points.

To sum up, in the trust evaluation mechanism, only a simple trust is taken into account, while the parameters of the direct trust evaluation are only simple data packets sent and received, which makes it difficult to accurately obtain the true trust value of the network nodes, and cannot better deal with the complex internal attacks of the network. As a result, the data collected goes to extremes being either completely untrustworthy or extremely invalid. Additionally, although in some research there is trust evaluation for the attacks in the network, there is no specific combination of trust evaluation and the underlying application. At the same time, in the application of data collection in most of the research of the Internet of Things system, the energy consumption is reduced by optimizing the routing. Faced with the limited energy of network nodes, this method is flawed. Therefore, a new method is needed to deal with the untrustworthy data due to the malicious attacks and weak computing power of existing IoT systems.

III Problem Formulation and Network Model

A. Problem Formulation

In the underlying network of the Internet of Things, there are m sensor nodes and several base station nodes in a two-dimensional plane of $L \times L$. When the network is established, all the nodes in the area are clustered by a clustering protocol, which includes s cluster head nodes, $m \gg s$. In addition, there are two types of nodes in the proposed edge network system: 1) trustworthy nodes and 2) malicious nodes. The trust of a trustworthy node is quantitatively evaluated by the cluster head nodes according to its behavior information. Define the data collected from a trustworthy node as trustworthy data and trust values are updated every other cycle.

As shown in Fig. 1, we give the network structure with several clusters. Within a cluster, the cluster head calculates the trust value of a node according to its behavior and characteristics. The nodes in each cluster are divided into trustworthy nodes and untrustworthy nodes. A pentagon represents the edge mobile node, which is responsible for collecting data [24]. In each cluster, a trustworthy node is verified based on its trust value and then selected as a cluster head node. Besides, the initial path is randomized but conditioned to pass through most head nodes of the clusters, along which the mobile edge nodes move and collect data from trustworthy cluster head nodes [25] [26]. As the moving path is simulated as a soft magnetic rope, the trustworthy nodes get attracted and untrustworthy ones repulsed. Then the resultant force of the interaction between attraction and repulsion pushes the moving path to a higher trustworthiness area. Moreover, since this area is away from the untrustworthy area, and the moving distance is shortend, so as to achieve the purpose of collecting trustworthy data efficiently. In a word, by shortening the moving distance, the mobile edge nodes get access to the trustworthy cluster head nodes, while minimizing the energy consumption of nodes.

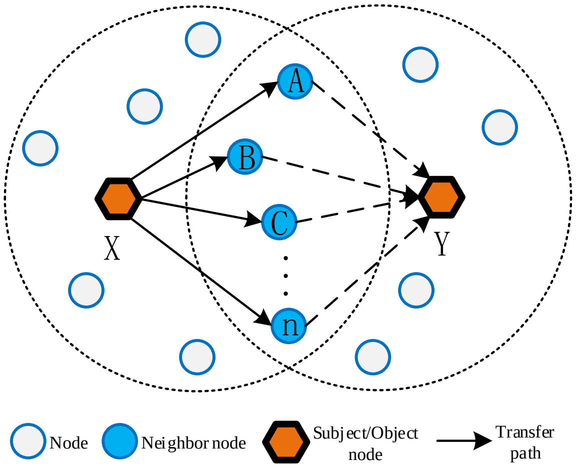


Fig. 2: Indirect trust delivery

B.Network Model

Supposing a network consists of m randomly deployed sensor nodes, the application scenario is the periodic data collection of nodes (such as for environmental monitoring) in the IoT service computing systems [27]. Then, several assumptions need to be stated regarding the network model:

1) The sensor nodes and the base stations in the network are fixed, that is, they do not move after the deployment. Besides, the energy consumption of these base station nodes is outside the scope of research. In other words, the energy is sufficient.

2) The mobile edge node used for data collection has an infinite buffer, which moves at a certain rate in the network deployment area of the network with sufficient energy and strong computing power.

3) Sensor nodes are isomorphic and have limited energy but with fusion capabilities, and each node has a unique identity (ID).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.2966870, IEEE Internet of Things Journal

4) In view of the distance between moving collection elements, the node can freely adjust its transmission power to save energy.

To reduce the energy consumption of nodes and meet time constraints, a tree architecture is devised to represent the network topology: figure $G(V, E)$ is a geometric tree with a root node B, and define the cluster head nodes as set V=$\{c_0, ..., c_i, ..., c_{n-1}\}$, where c_i denotes the cluster head node i. As mentioned above, the mobile edge node moves through a restricted path consisting of several cluster head (collection) nodes [28]. When the mobile edge node is close to the cluster head node, the node collecting data is selected as the cluster head node in the communication range and directly transmits the data to the mobile edge node. As to non-cluster head nodes, since they are not in the communication range, the existing routing method (for example, the Dijkstra algorithm) is adopted [29]. The data are transmitted to the cluster head collection node in the cluster by a multihop method to the mobile edge node.

IV Multidimensional Trust Value Evaluation of Nodes

Considering that the underlying data derives from sensor nodes, evaluating the underlying physical nodes effectively and comprehensively is critical in ensuring data trustworthiness. On the other hand, mobile trustworthy data collection requires the trustworthiness of nodes. By evaluating on nodes trust, the mobile edge nodes can access more trustworthy nodes and bypass malicious noes. As a consequence, end-to-end mobile delays can be reduced and the data acquisition can be obtained within a short distance.

In the network operation, let T_i be the initial trustworthiness of the node and $\triangle$ be the node's trustworthiness threshold. Trust values have different representations: some researchers express them as continuous values in real numbers, such as $(0, 1)$ (0 is totally untrustworthy, 1 is totally trustworthy), while other studies make them range from -1 (i.e. total untrustworthy) to 1 (i.e. total trustworthy) [30]. If the storage space of sensor nodes and unsigned integers each take up one byte, and the real numbers take up four bytes, 75% of the memory space can be saved by using $[0, 10]$, and less data needs to be transmitted between the nodes accordingly.

Definition 1: Trust Value and Trustworthiness *An interval is used to represent the trust range of the node. The interval is limited to* [0, 10], *and the initial trust value of the node is set to be 5. The trust value of this node at a certain time is expressed as* T_c. *When* T_c=0, *the node is totally untrustworthy, and* T_c=10 *indicates that the node is completely trustworthy.*

In previous studies, node trust is usually measured in a single one-dimensional attribute model, which may reflect biased performance of nodes [31]. In this paper, a multi-dimensional trust model is utilized to evaluate the trust of nodes. In such a model, there are parameters (such as energy, processing power, etc.) telling the state of the nodes and their interactive behaviors [32]. Direct trust is the basic evaluation index in trust evaluation. However, due to malicious attacks and other problems, direct trust may not be able to effectively represent the quality of all the nodes when few data packets between adjacent nodes is involved. Therefore, in the multidimensional trust model, there are two modules in terms of trust calculation: direct trust and indirect trust. Direct trust refers to the trust relationship between nodes that can communicate directly. When the nodes can not perform direct trust evaluation, then indirect trust evaluation is activated.

A. Evaluation of Direct Trust

1) Communication trust value Two adjacent nodes in the network communicate with each other. Label the number of successful communications S, the total number of communications C and the communication trust value T_c. Their interrelationship is formulated as follows:

$$\begin{gathered}\boldsymbol{T}_{\mathbf{com}} = \omega_{oldd} \times T_{oldd} + \omega_{newd} \times T_{newd} \\ T_{newd} = \frac{S}{C}\ ,\ \omega_{oldd} + \omega_{newd} = 1\end{gathered} \tag{1}$$

ω_{oldd} and ω_{newd} represent the weights of old and new trust values of nodes respectively, and T_{newd} and T_{oldd} denote their corresponding trust values. In the initial stage, T_{oldd}=0, ω_{oldd} and ω_{newd} are defined as variables.

2) Positional intimacy When a node is located closer to the cluster head node, it is more likely to successfully receive a packet and consumes less energy. The calculation of node locational intimacy follows the following equation:

$$\boldsymbol{T}_{\mathbf{l}} = 1 - \frac{D_s}{R} \tag{2}$$

T_l refers to the trust value of a locational node, D_s represents the distance between the node and the cluster head node, and R denotes the communication range of the node.

3) Packet loss In a wireless communication environment, packet loss rate implies link quality: the higher the packet loss rate, the worse the link quality [33] [34]. In addition, the trust value of a nodes packet loss rate can reveal the status of the communication behavior of the nodes in the data transmission link. Stipulate that the number of packets sent is P_s and the number of packets received is P_r, and then the trust value of packet loss rate T_p is:

$$\boldsymbol{T}_{\mathbf{p}} = \frac{P_s - P_r}{P_s} \tag{3}$$

4) Energy surplus As a key index of sensor nodes, energy consumption the lifetime of the nodes. If the initial energy of nodes is E_i and the residual energy is E_c, the energy trust value of the node T_e is expressed as the ratio of E_c to E_i.

Therefore, the trust values of the nodes in this section can be expressed as:

$$T^d_{i,\,j} = \omega_{com} \times T_c + \omega_l \times T_l + \omega_e \times T_e + \omega_p \times T_p \tag{4}$$

$T^d_{i,\,j}$ is the total direct trust value of nodes i and j. ω_{com}, ω_l, ω_e and ω_p represent the weight given by communication trust, distance trust, energy trust and packet loss rate respectively, and ω_{com} + ω_l + ω_e + ω_p =1.

B. Evaluation of Indirect Trust

Indirect trust is obtained via the interaction between a trustworthy subject and a third-party recommendation. If a neighboring node cannot have a direct trust value, it gains an indirect trust value from former interactions with the trustworthy object. In the calculation of indirect trust, the trust value of a node may be recommended by multiple nodes. Compared with the unrecommended counterparts, the recommended nodes may be malicious ones or manipulated manually, and hence need to be weighted where $\partial \in (0,\ 1)$. As shown in Fig. 2, node X gains an indirect trust value at node Y and the trust is transferred from node X to

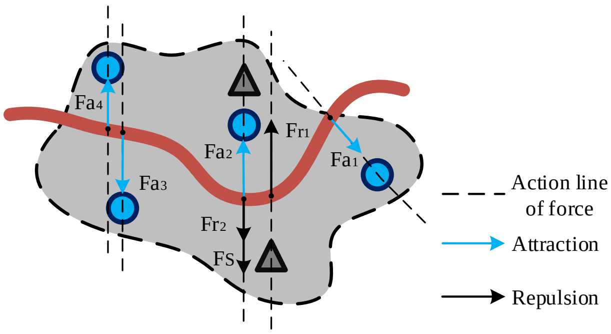


Fig. 3: Schematic diagram of the action forces on nodes along the moving path

node Y through their adjacent nodes (i.e. nodes A, B, C, etc.). The indirect trust value of node X at node Y can be calculated according to the following formula:

$$(T_{X,\,Y})_A = T_{X,\,A} \times T_{A,\,Y} \tag{5}$$

$(T_{X,\,Y})_A$ is the trust value of node X after it passes through node A to node Y. The weight of the recommended node is proportional to the direct trust value of its neighboring node, namely: $\partial_A = \frac{T_{A,\,Y}}{\sum_{n=1}^{m} T_{A,n}}$. Where m represents the number of adjacent nodes, $T_{A,\,Y}$ represents the direct trust value of nodes A and Y, and $\sum_{n=1}^{m} T_{A,n}$ refers to the sum of the direct trust value for the recommended nodes.
The indirect trust of X obtained at node Y is:

$$T_{i,\,j}^{ind} = T_{X,Y} = \sum_{A=1}^{m} \partial_A \times (T_{X,\,Y})_A \tag{6}$$

When a node can directly obtain its direct trust value, Equation 4 is executed. Otherwise, Equation 6 is activated.

V Trustworthy data collection based on virtual force mapped by trust value

To tackle malicious attacks from inside and outside the network and effectively prolong the life cycle of the network, a multi-dimensional node trust evaluation algorithm is proposed [35] [36]. As shown in Algorithm 1, first mark the node within the range of direct communication. For nodes that can communicate directly, execute the direct trust formula to calculate the trust value. As to nodes that are not in the communication range, calculate the indirect trust value based on the transfer link of neighboring nodes.

After the trust evaluation of nodes, the mobile edge nodes can avoid collecting mobile data from untrustworthy nodes. However, swaying factors include not only single nodes, but also the overall trust situation of a region and the requirements of data timeliness (within a limited mobile distance). Hence, the nodes need to move as far as possible to areas with low trustworthiness. According to our previous research, NP-hard hinders optimal data collection, in which context, another new model was designed [37] [38]. Nodes are differed in terms of their geographical distribution or clustering methods. The evaluation of trust values of nodes can distinguish trustworthy nodes from untrustworthy ones. As a rule, trustworthy nodes are given attraction, while untrustworthy nodes are given rejection. That is how a resultant force is produced.

Algorithm 1 Calculation of trust values in a cluster

```
Input: Node class; The number of cluster head nodes $s$; Node communication range $R$.
Output: Trust values of all member nodes in this cluster
for nodes in $s$ clusters do
    if distance from current node to cluster head node $< R$ then    // Not in the communication range of the node
        Marked as directly connected;    // Direct trust node
        Calculate the direct trust value of the node by Equations (1) ~ (4) and related descriptions;    // Get the trust value of the direct trust node
    else
        for the current node $N_i$ do
            if distance from $N_i$ to $N_j$ + distance from $N_j$ to cluster head $< R$ then
                Mark $N_j$ as a neighbor node of $N_i$;
                Calculate the indirect trust value of the node by Equations 6;    // Get the trust value of the indirect trust node
            end if
        end for
    end if
end for
```

Fig. 1 displays a magnetic soft rope in a region to simulate the moving path. The interaction of gravity and repulsion forces pushes the moving path to the trustworthy area and away from the untrustworthy one, so as to collect trustworthy data efficiently. The inferential rules concerning trust values, trustworthy and untrustworthy nodes, and the corresponding action forces, together with the moving path, are illustrated as follows:

Definition 2: Relationship between Trust Value and Force *If the trust value of the node $T_c > 5$, then this node is a trustworthy node, which receives attraction. If $T_c < 5$, then this node is an untrustworthy node, which receives a repulsive force. At the same time, the magnitude of the node force is proportional to the trust value T_c. The greater T_c is, the greater the attraction will be. Accordingly, the smaller the absolute value of T_c is, the smaller the repulsive force will be.*

Fig. 3 presents a force diagram of a cluster, where attraction and repulsion forces are involved and the little dots on the path curve are the projection points of the forces acting on the nodes around the moving path [39]. The direction of the attractive force points to the trustworthy node from the action point, and the direction of repulsive force points away from the trustworthy node. As a result, the mobile edge node can always move the route with the highest trustworthiness under the action of the trustworthy nodes virtual force.

Definition 3: Synthesis of the Force of the Node *The forces on the same side (or both sides) of the curve and the multiple nodes on the same line are algebraically synthesized in the direction of the attractive force or the direction of the repulsive force.* As shown in Fig. 3.

The virtual forces (including attractive and repulsive forces) that are projected by the moving path nodes can be expressed as:

$$F_S = \left(\sum_{i=1}^{p} F_a + \sum_{j=1}^{q} F_r\right) K \tag{7}$$

where p and q respectively represent the numbers of trustworthy nodes and untrustworthy nodes along the same straight line. F_a

and F_r denote the attractive and repulsive forces of a single node, which is numerically equal to the trust value T_c. K is the adjustment factor, whose value can be a fixed constant less than 10. Different values can be set according to the specific experimental requirements, mainly to accelerate the convergence speed of the path in the calculation of virtual force. F_S is the resultant force at the projection point on the path.

According to Equation 7, the resultant force F_S of the virtual force at the projection point of the node on the path can be calculated. The resultant force consists of one or more collinear attraction and repulsion forces, and its direction accords with that of the force with greater magnitude. Given the length constraints of the moving path, the process is implemented iteratively by changing the magnitude of gravity and repulsion (so the initial path is not very important) until the final output meets the data collection path (i.e., the moving distance limitation within a specified time) [40]. In view of the fact that the trust value of the node remains unchanged in a certain period of time, the resultant force is unchanged, which hence calls for the adjustment parameter k to change the resultant force and to meet the time limit of data collection. Under the virtual force of all sensor nodes, the moving path is formed, and the moving edge node can move along the planned path. Most nodes in the network can send data to the mobile edge node through single-hop transmission, while a few trustworthy nodes can send data to the nearest mobile edge node through multi-hop transmission to achieve trustworthy data collection.

The trust value of the node is obtained by the trust value evaluation algorithm of the node, and then the resultant force of the virtual force on the node with equal value mapped by the trust value of the node can be calculated according to the algorithm 2. Then synthesize the forces acted on the nodes and make the initial path move correspondingly according to the magnitude of the resultant force. In the meanwhile, for our simulated magnetic rope model, define the range of motion of adjacent nodes, iterate over and finally generate a trustworthy data collection path with higher trustworthiness. Security through trust evaluation is considered a viable solution to malicious attacks in the Internet of Things [41], to accomplish which, the trust status of the sensor nodes needs to be evaluated through the defined trust evaluation variables, and the trust values of the quantified nodes are calculated.

There are two main algorithms in our proposed trustworthy data collection model based on edge computing. Algorithm 1 is the calculation of the node trust value. In the best case, all node heads can communicate with each other, and the algorithm time complexity is $O\left(n^2\right)$. In the worst case, all nodes must obtain the trust value through trust transfer. The time complexity of the double-link trust value calculation is $O\left(n^3\right)$. Algorithm 2 is used to generate a trustworthy data collection path based on virtual forces. Based on the obtained node trust value, only the relationship between the node and the initial path node needs to be considered, and the displacement is calculated. The virtual force strategy is a simple force synthesis operation via coordinate addition and subtraction, and the algorithm time complexity is low, namely only $O(nlogn)$. So the global time complexity of the virtual force calculation is $O\left(n^2\right)$. Therefore, the time complexity of the proposed algorithm for trustworthy data collection based on edge computing is $O\left(n^3\right)$.

Algorithm 2 Path algorithm for trustworthy data collection in edge computing

```
Input: Coordinates of points on the initial path; Trust value of the
    node $T$; Position coordinates of the node; Single movement
    distance $D$; Virtual force of node trust value mapping $F_v$;
    Maximum distance between ropes $D_r$.
Output: Path point coordinates after movement
for Each node on the path and the nodes within the path of the
communication do    // Select nodes on and around the path
    $F_v \leftarrow T$;
    if $F_v < 5$ then    // The trust value for the initial state of
the node is 5
        $F_r \leftarrow F_v$;    // Repulsive force of node
    else
        $F_a \leftarrow F_v$;    // Atttractive force of node
    end if
    Calculate the superposition of the resultant force $F_s$;
    Moving ratio in corresponding direction $\frac{D}{T}$;    // Move-
ment rate of node coordinates
    Calculate the new coordinates of the point $(x, y)$ on the
path;
    Check coordinate movement range;    // Consider the
tension effect of soft rope itself
    if Moving distance > $D_r$ then
        Restore coordinates, recalculate position;
    else
        Return to the path coordinates after the move;
    end if
end for
```

VI EXPERIMENTS AND ANALYSIS

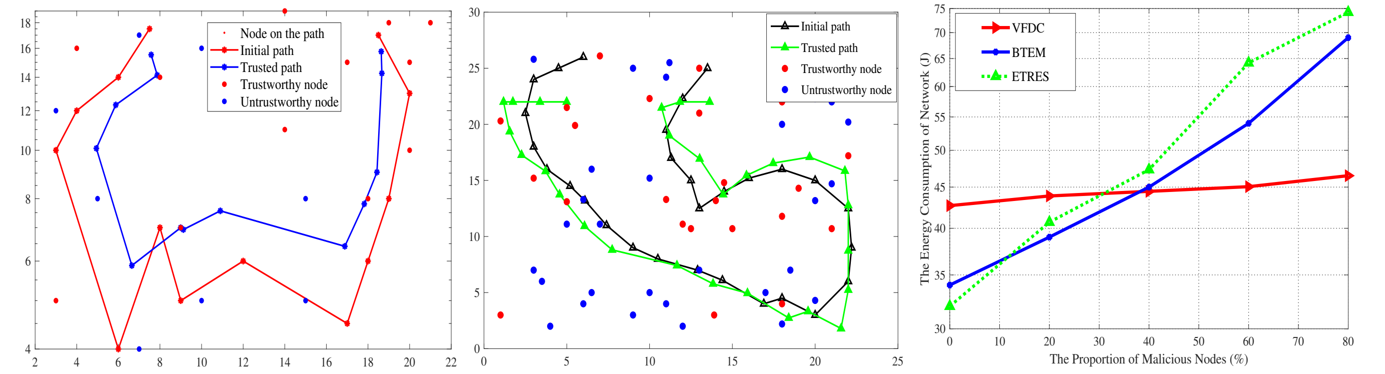
In this section, the performance of the trust evaluation of nodes and trustworthy data collection path model generated by virtual force are described and discussed.

A. Parameter Settings

MATLAB R2018a was used to build an experimental platform to analyze the proposed trustworthy data collection algorithm. The experimental environment is to randomly deploy 100 nodes in an area of 300 $m \times 300$ m, and select 30 nodes as cluster head nodes. The experimental setting consists of two IoTs,one cloud and one base station , where every IoT has an edge platform, and the cloud is at the top of the IoT. The underlying nodes are clustered independently and close to the base station nodes, and the users are located in the lower layer of the cloud. The transmission time from edge node to cloud is 16 ms, and the data transmission rate is 2×10^6 bit/s. It is assumed that the moving edge node starts moving at a uniform speed from the selected starting point, and the speed and communication radius can be adjusted. The minimum energy threshold of a node is set to be one thousandth of the initial energy of the node, and the minimum packet reception threshold is two thousandths of the threshold of the data from the node [42]. After the setup of the initial path without crossover, a path is generated with the largest trust value within the specified moving distance in accordance with the algorithm 2.

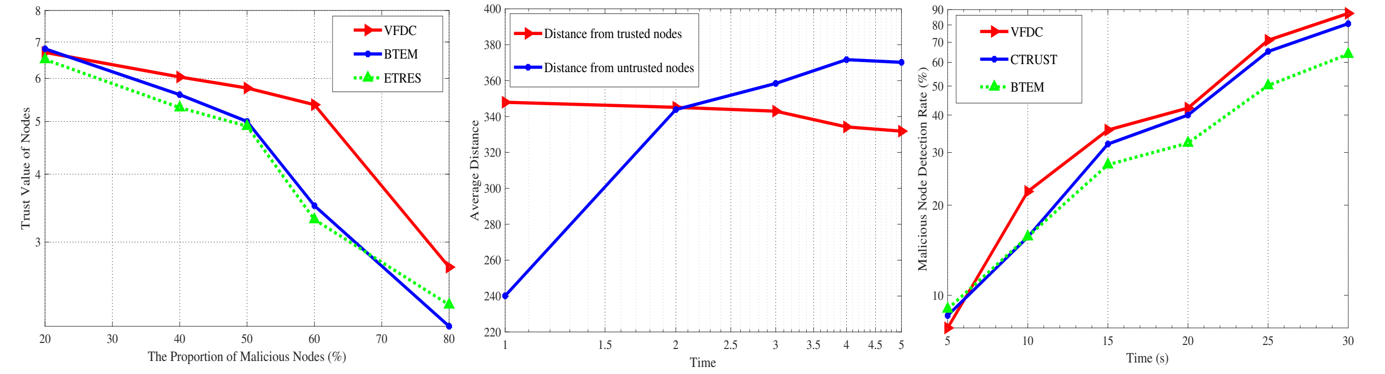
B. Impact of different numbers of nodes and initial trustworthy paths

As Fig. 4 shows, in order to show the experimental results more intuitively, different situations were simulated to generate trustworthy paths. In Fig. 4(a), 13 points were selected as the



(a) (b) (c)

Fig. 4: Trustworthy paths of nodes in different numbers and energy consumption in different trustworthy mechanisms. (a) 13-node trustworthy path in sparse distribution. (b) 30-node trustworthy path in high-density distribution. (c) Network energy consumption under different trust value evaluation methods.



(a) (b) (c)

Fig. 5: The impact of a proportion of malicious nodes on different trust evaluation mechanisms and the distance between nodes and trustworthy data collection paths. (a) Comparison of node trust value changes under different trust evaluation Methods. (b) Distance between nodes of different types and a trustworthy data collection path. (c) Detection rate of malicious nodes on different networks under different strategies.

initial path node, their trust values were set in correspondence with the distance of 1/2 unit on the coordinate, and then run 10 times to obtain a moving path of certain length. Judging from the results, it can be seen that the newly generated data collection path arising from the trustworthy virtual force is not only greatly shortened, but also away from untrustworthy nodes in position.

As the initial path becomes long and the number of nodes grows, the planned trustworthy data collection path will also become complex, as shown in Fig. 4(b). Accordingly, 30 experimental initial path nodes are distributed in higher density in the network. Similarly, compared to the original path, the newly generated path is shorter, and is nearer to the trustworthy node. In other words, the above experiments suggest that the proposed virtual force-based trustworthy data collection method can push the moving path to the trustworthy area and away from the trustworthy one, and then collect trustworthy data efficiently. In addition, a small number of compensating nodes are found on the path with an increasing trend. The reason is that some of the nodes are far apart when the path is calculated together, which will be discussed in our next study.

C. The impact of malicious nodes on trustworthy data collection

To verify the validity of the trust evaluation algorithm, the internal attacks of the nodes, mainly of selfish ones, were simulated by deploying a certain percentage of malicious nodes in the network. We have given the assumption that the energy consumed by a node receiving and sending a packet is the same. The current energy of a directly communicating node is E_p, the energy consumption of sending a unit packet is e. The energy consumption of the cluster head is E_{clu} , the computing energy consumption of the cluster head node is E_{co}. In the experiment, we only consider the standby energy consumption of the cluster head node. For directly trusted nodes, the current energy is $E_{nd} = E_{in} - e \times q$, q is the number of datagrams sent by the node, E_{in} is the initial energy of the node. For a node in a neighbouring location, the current energy is $E_{ne} = E_{in} - 2e \times q$. The energy consumption of the cluster head node is $E_{clu} = E_{in} - e \times q + E_{co} + E_d$, where E_d is the energy consumption of the node to maintain the standby state. In each round of data collection, the energy consumption of the nodes in the cluster and the energy consumption of the cluster head nodes are calculated separately.

From Fig. 4(c), we can see that as the number of malicious nodes increases from 20% to 80%, the network energy consumption grows rapidly in the ETRES method. What is more, when the proportion of malicious nodes in the network reaches 40%, the energy consumption rate under this method increases quite swiftly. On the other hand, the BTEM methods shares a very similar growth trend to that of ETRES in terms of the energy consumption, and both consumer much more than what the VFDC method proposed in this paper. Specifically, as the experimental results suggest, the energy consumption of the VFDC method increases slowly and slightly and depends on the proportion of different malicious nodes, but the overall consumption remains below 45. Therefore, the VFDC method is robust and stable, and can effectively resist malicious attacks from inside the node.

As Fig. 5(a) shows, when the proportion of malicious nodes in the network reaches about 50%, the trust value of the node will decrease rapidly, which also reflects the trustworthiness of the trust evaluation method. In contrast, the ETRES and BTEM methods gain similar results: When there is a large portion of malicious nodes in the network, the trust values of the nodes drop to a neutral level (the trust value is also the initial value of the node). Additionally, compared with the other two methods, the VFDC method has incomparable advantages when the proportion of malicious nodes is about 60%.

D. Impact of network uptime on trustworthy data collection

In order to visually illustrate the validity of the VFDC method of collecting trustworthy data, distances were calculated among the point on the trustworthy path and the trustworthy node and the untrustworthy node at different times (rounds), as shown in Fig. 5(b). As the initial path is repeated (i.e. as the experimental time passes by), the distance of the newly generated trustworthy path from the untrustworthy node increases rapidly. Although the curve of the trustworthy node is relatively flat, the distance decreases slowly. Furthermore, the experimental method of trustworthy data collection based on virtual force can push the moving path to the trustworthy area and away from the untrustworthy area due to the direction of the resultant force.

According to Fig. 5(c), we can see that as the number of iterations of the moving path increases, the recognition rate of the trust evaluation method increases correspondingly. In addition, the VFDC method usually has a slightly higher detection rate of malicious nodes than that of the CTRUST method and a much higher detection rate than that of the BTEM method except when it comes to the early stage of network operation.

In terms of the different network architectures and node deployments, energy consumption was tested in different methods. As the number of nodes (cluster heads) rises from 10 to 60, the energy consumption of the network nodes also increases. The average energy consumption of the nodes nuder the BTEM method is the fastest, followed by the CTRUST method with the largest growth rate. However, when the network structure adopts the model of the trustworthy cluster head node mentioned in this paper, not only the energy consumption of the network is minimal but also the average value is the most stable, which can balance the energy consumption of each node in the network and effectively prolong the life cycle of the network.

VII Conclusions

The rise of edge computing provides a whole new perspective on the limitations of the underlying Internet of Things. In order to avoid untrustworthy data caused by the weakness and vulnerability to attacks on underlying sensor network in the IoT systems and applications, a new model is proposed for trustworthy data collection and is based on edge computing in the Internet of Things. To be specific, a comprehensive trust evaluation method of the nodes from multiple perspectives is used to obtain the quantified trust values of the nodes. Then, the trustworthy node is attracted, while the untrustworthy one gets repulsed. The trustworthy data is collected efficiently via a trustworthy path. Moreover, extensive experiment validates that by use of virtual force to collect trustworthy data, the best mobility path can be generated with high trust and attacks from internal malicious nodes can be effectively defended against. In addition, the mobile edge node as a mobile data collector can help to improve the weak computing power and limited storage capacity of the underlying common nodes. At the same time, edge computing is framed more appropriately for the underlying nodes and trustworthy data.

However, there is still a lot of work to be done for the research of trustworthy data collection on the Internet of things system. The future research mainly aims at establishing a more systematic trustworthy data collection framework based on edge intelligence, from the node trust evaluation to the security of data application. This is because, with the development of edge computing and artificial intelligence, the traditional network architecture has changed greatly. These changes not only promote the development of technology but also introduce the threat of network attacks into the edge network. Attackers disguise malicious nodes as legitimate nodes or forge and destroy the data of nodes. Invalid and wrong data will bring disastrous results to system applications, so a data collection framework based on edge intelligence is imminent.

Acknowledgments

The above work was supported in part by grants from Open Fund of Key Laboratory of Data mining and Intelligent Recommendation, Fujian Province University under Gant No. DM201902 and the General Projects of Social Sciences in Fujian Province under Gant No. FJ2018B038 and National Natural Science Foundation of China (NSFC) under Grant No. 61872154, No. 61772148 and No. 61672441 and Natural Science Foundation of Fujian Province of China (No. 2018J01092) and the Fujian Provincial Outstanding Youth Scientific Research Personnel Training Program.

References

[1] J. Qi, P. Yang, M. Hanneghan, S. Tang, and B. Zhou, "A hybrid hierarchical framework for gym physical activity recognition and measurement using wearable sensors," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1384–1393, 2018.

[2] B. Cao, J. Zhao, P. Yang, P. Yang, X. Liu, and Y. Zhang, "3-d deployment optimization for heterogeneous wireless directional sensor networks on smart city," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1798–1808, 2018.

[3] T. Wang, Y. Liang, W. Jia, M. Arif, A. Liu, and M. Xie, "Coupling resource management based on fog computing in smart city systems," *Journal of Network and Computer Applications*, vol. 135, pp. 11–19, 2019.

[4] G. Zhang, T. Wang, G. Wang, A. Liu, and W. Jia, "Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system," *Concurrency and Computation: Practice and Experience*, 2018. [Online]. Available: https://doi.org/10.1002/cpe.5109

[5] T. Wang, J. Zeng, Y. Lai, Y. Cai, H. Tian, Y. Chen, and B. Wang, "Data collection from wsns to the cloud based on mobile fog elements," *Future Generation Computer Systems*, 2017. [Online]. Available: https://doi.org/10.1016/j.future.2017.07.031

[6] D. Cao, B. Zheng, B. Ji, Z. Lei, and C. Feng, "A robust distance-based relay selection for message dissemination in vehicular network," *Wireless Networks*, 2018. [Online]. Available: https://doi.org/10.1007/s11276-018-1863-4

[7] J. Qi, P. Yang, L. Newcombe, X. Peng, Y. Yang, and Z. Zhao, "An overview of data fusion techniques for internet of things enabled physical activity recognition and measure," *Information Fusion*, vol. 55, pp. 269–280, 2019.

[8] Y. Ren, W. Liu, T. Wang, X. Li, N. N. Xiong, and A. Liu, "A collaboration platform for effective task and data reporter selection in crowdsourcing network," *IEEE Access*, vol. 7, pp. 19 238–19 257, 2019.

[9] B. Huang, W. Liu, T. Wang, X. Li, H. Song, and A. Liu, "Deployment optimization of data centers in vehicular networks," *IEEE Access*, vol. 7, pp. 20 644–20 663, 2019.

[10] Y. Chen, W. Xu, J. Zuo, and K. Yang, "The fire recognition algorithm using dynamic feature fusion and iv-svm classifier," *Cluster Computing*, 2018. [Online]. Available: https://doi.org/10.1007/s10586-018-2368-8

[11] T. Wang, L. Qiu, G. Xu, A. K. Sangaiah, and A. Liu, "Energy-efficient and trustworthy data collection protocol based on mobile fog computing in internet of things," *IEEE Transactions on Industrial Informatics*, 2019. [Online]. Available: https://doi.org/10.1109/TII.2019.2920277

[12] X. Chu, X. Chen, K. Zhao, and J. Liu, "Reputation and trust management in heterogeneous peer-to-peer networks," *Telecommunication Systems*, vol. 44, no. 3-4, pp. 191–203, 2010.

[13] J. Tang, A. Liu, J. Zhang, N. Xiong, Z. Zeng, and T. Wang, "A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks," *Sensors*, vol. 18, no. 3, pp. 1–44, 2018.

[14] G. Hatzivasilis, I. Papaefstathiou, and C. Manifavas, "Scotres: secure routing for iot and cps," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2129–2141, 2017.

[15] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, Á. MacDermott, and X. Wang, "Ctrust: A dynamic trust model for collaborative applications in the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5432–5445, 2019.

[16] A. Sharma, E. S. Pilli, and A. P. Mazumdar, "Rrar: Robust recommendation aggregation using retraining in internet of things," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. IEEE, 2019, pp. 76–80.

[17] R. Mehta and M. Parmar, "Trust based mechanism for securing iot routing protocol rpl against wormhole &grayhole attacks," in *2018 3rd International Conference for Convergence in Technology (I2CT)*. IEEE, 2018, pp. 1–6.

[18] R. W. Anwar, A. Zainal, F. Outay, A. Yasar, and S. Iqbal, "Btem: Belief based trust evaluation mechanism for wireless sensor networks," *Future Generation Computer Systems*, vol. 96, pp. 605–616, 2019.

[19] J. Zhao, J. Huang, and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks," *IEEE Access*, vol. 7, pp. 33 859–33 869, 2019.

[20] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in iot-based healthcare systems," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 163–168, 2018.

[21] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured data collection with hardware-based ciphers for iot-based healthcare," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 410–420, 2018.

[22] Y.-N. Liu, Y.-P. Wang, X.-F. Wang, Z. Xia, and J.-F. Xu, "Privacy-preserving raw data collection without a trusted authority for iot," *Computer Networks*, vol. 148, pp. 340–348, 2019.

[23] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, and B. B. Gupta, "Efficient iot-based sensor big data collection–processing and analysis in smart buildings," *Future Generation Computer Systems*, vol. 82, pp. 349–357, 2018.

[24] K. Gu, W. Jia, G. Wang, and S. Wen, "Efficient and secure attribute-based signature for monotone predicates," *Acta Informatica*, vol. 54, no. 5, pp. 521–541, 2017.

[25] T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on fog computing in sensor–cloud system," *Future Generation Computer Systems*, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2018.05.049

[26] W. Zhang, W. Liu, T. Wang, A. Liu, Z. Zeng, H. Song, and S. Zhang, "Adaption resizing communication buffer to maximize lifetime and reduce delay for wvsns," *IEEE Access*, vol. 7, pp. 48 266–48 287, 2019.

[27] T. Wang, Y. Liang, Y. Tian, M. Z. A. Bhuiyan, A. Liu, and A. T. Asyhari, "Solving coupling security problem for sustainable sensor-cloud systems based on fog computing," *IEEE Transactions on Sustainable Computing*, 2019. [Online]. Available: https://doi.org/10.1109/TSUSC.2019.2904651

[28] S. He, W. Zeng, K. Xie, H. Yang, M. Lai, and X. Su, "Ppnc: Privacy preserving scheme for random linear network coding in smart grid," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 3, pp. 1510–1531, 2017.

[29] T. Wang, L. Hao, J. Zheng, and M. Xie, "Crowdsourcing mechanism for trust evaluation in cpcs based on intelligent mobile edge computing," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 6, pp. 62–80, 2019.

[30] T. Wang, Y. Li, W. Fang, W. Xu, J. Liang, Y. Chen, and X. Liu, "A comprehensive trustworthy data collection approach in sensor-cloud system," *IEEE Transactions on Big Data*, 2018. [Online]. Available: https://doi.org/10.1109/TBDATA.2018.2811501

[31] W. Li, Z. Chen, X. Gao, W. Liu, and J. Wang, "Multimodel framework for indoor localization under mobile edge computing environment," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4844–4853, 2018.

[32] W. Li, H. Xu, H. Li, Y. Yang, P. K. Sharma, J. Wang, and S. Singh, "Complexity and algorithms for superposed data uploading problem in networks with smart devices," *IEEE Internet of Things Journal*, 2019. [Online]. Available: https://doi.org/10.1109/JIOT.2019.2949352

[33] T. Wang, Z. Peng, S. Wen, G. Wang, B. Wang, and A. Liu, "A survey of fog computing in wireless sensor networks: Concepts, frameworks, applications and issues," *AD HOC & SENSOR WIRELESS NETWORKS*, vol. 44, no. 1-2, pp. 109–130, 2019.

[34] J. Wang, Y. Gao, X. Yin, F. Li, and H.-J. Kim, "An enhanced pegasis algorithm with mobile sink support for wireless sensor networks," *Wireless Communications and Mobile Computing*, 2018. [Online]. Available: https://doi.org/10.1155/2018/9472075

[35] J. Wang, X. Gu, W. Liu, A. K. Sangaiah, and H.-J. Kim, "An empower hamilton loop based data collection algorithm with mobile agent for wsns," *Human-centric Computing and Information Sciences*, vol. 9, no. 18, pp. 1–14, 2019.

[36] Z. Xia, Z. Fang, F. Zou, J. Wang, and A. K. Sangaiah, "Research on defensive strategy of real-time price attack based on multiperson zero-determinant," *Security and Communication Networks*, 2019. [Online]. Available: https://doi.org/10.1155/2019/6956072

[37] T. Wang, W. Wang, A. Liu, S. Cai, and J. Cao, "Improve the localization dependability for cyber-physical applications," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 1, pp. 6–21, 2018.

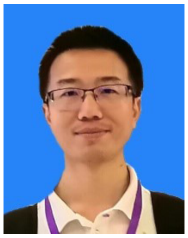
[38] M. Z. A. Bhuiyan, G. Wang, J. Wu, J. Cao, X. Liu, and T. Wang, "Dependable structural health monitoring using wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 4, pp. 363–376, 2015.

[39] B. Xiong, K. Yang, J. Zhao, and K. Li, "Robust dynamic network traffic partitioning against malicious attacks," *Journal of Network and Computer Applications*, vol. 87, pp. 20–31, 2017.

[40] Y. Wu, H. Huang, Q. Wu, A. Liu, and T. Wang, "A risk defense method based on microscopic state prediction with partial information observations in social networks," *Journal of Parallel and Distributed Computing*, vol. 131, pp. 189–199, 2019.

[41] B. Yin and X. Wei, "Communication-efficient data aggregation tree construction for complex queries in iot applications," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3352–3363, 2018.

[42] T. Wang, L. Hao, W. Jia, A. Liu, and M. Xie, "Mtes: An intelligent trust evaluation scheme in sensor-cloud enabled industrial internet of things," *IEEE Transactions on Industrial Informatics*, 2019. [Online]. Available: https://doi.org/10.1109/TII.2019.2930286



Tian Wang received his BSc and MSc degrees in Computer Science from the Central South University in 2004 and 2007, respectively. He received his PhD degree in City University of Hong Kong in in Computer Science in 2011. Currently, he is a professor in the College of Computer Science and Technology, Huaqiao University, China. His research interests include internet of things, edge computing and mobile computing. He has 18 patents and has published more than 250 papers in high-level journals and conferences. He has more than 3500 citations, according to Google Scholar. His H-index is 28 and the i10-index is 88. He has managed 5 national natural science projects (including 2 sub-projects) and 4 provincial-level projects.

Lei Qiu received his B.S. degree in Tongda College of Nanjing University of Posts and Telecommunications of China in 2017. Currently, he is a master candidate in the National Huaqiao University of China. His research interests include wireless sensor networks, mobile computing and Edge computing.

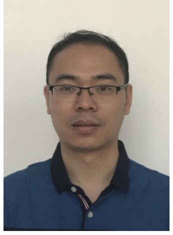
Arun Kumar Sangaiah (M' 09) received the Master of Engineering degree from Anna University, Chennai, India, in 2007, and the Ph.D. from the Vellore Institute of Technology,Vellore, India, in 2014.

He is currently an Associate Professor with the School of Computing Science and Engineering, Vellore Institute of Technology. He has authored or coauthored more than 250 scietific papers in high-standard Science Citation Index (SCI) journals. In addition, he has authored/edited more than eight books (Elsevier, Springer, Wiley, Taylor, and Francis) and 50 journal special issues in the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE COMMUNICATION MAGAZINE, the IEEE INTERNET OF THINGS, the IEEE CONSUMER ELECTRONIC MAGAZINE, etc. He holds one Indian patent in the area of computational intelligence.

He is an Editorial Board Member/Associate Editor for various international SCI journals. His research interests include software engineering, Internet of Things, computational intelligence, wireless networks.

Anfeng Liu is a Professor of School of Computer Science and Engineering, Central South University, China. He is also a Member (E200012141M) of China Computer Federation (CCF). He received the M.Sc. and Ph.D degrees from Central South University, China, 2002 and 2005 respectively, both majored in computer science. His major research interests are Cyber-Physical Systems, Service network, wireless sensor network.

Md Zakirul Alam Bhuiyan received the PhD degree and the M. Eng. degree from Central South University, China, in 2009 and 2013 respectively, and the BSc degree from International Islamic University Chittagong, Bangladesh, in 2005, all in Computer Science and Technology. He is currently an assistant professor (research) in the Department of Computer and Information Sciences at Fordham University. He is a member of the Center for Networked Computing (CNC). Earlier, he worked as a post-doctoral fellow at the Central South University, China, a research assistant at the Hong Kong PolyU, and a software engineer in industries. His research focuses on dependable cyber physical systems, wireless sensor network applications, network security, and sensor-cloud computing. He has served as a managing guest editor, program chair, workshop chair, publicity chair, TPC member, and reviewer of international journals/conferences. He is a member of IEEE and a member of ACM.



Ying Ma is the Deputy Director of Key Laboratory of Data Mining and Intelligent Recommendation, Fujian Province. He received the Distinguished Young Scholar Career Awards from Fujian Province. He is an Associate Professor with Xiamen University of Technology. He is awarded several grants including National Nature Science Foundation of China. He has published over 30 papers in top conferences and journals. His paper has been ranked as the 3rd most cited articles in information and software technology articles list (Elsevier). He has served on the editorial boards of Journal of Software EngineeringIJCSESCIREA Journal of Computer etc. He serves as the reviewer for IEEE Trans. and Information sciences.