IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURITY AND TRUSTED COMPUTING FOR INDUSTRIAL INTERNET OF THINGS

Received February 28, 2018, accepted April 18, 2018, date of publication April 30, 2018, date of current version May 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2831898

A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion

JIE YUAN[1], (Member, IEEE), AND XIAOYONG LI[1,2], (Member, IEEE)

[1]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Xiaoyong Li (lixiaoyong@bupt.edu.cn)

This work was supported in part by the National Nature Science Foundation of China under Grant 61672111, in part by the National Key Research and Development Program of China under Grant 2016QY03D0605, and in part by the Beijing Natural Science Foundation under Grant 4162043.

ABSTRACT The integration of Internet of Things (IoT) and edge computing is currently a new research hotspot. However, the lack of trust between IoT edge devices has hindered the universal acceptance of IoT edge computing as outsourced computing services. In order to increase the adoption of IoT edge computing applications, first, IoT edge computing architecture should establish efficient trust calculation mechanism to alleviate the concerns of numerous users. In this paper, a reliable and lightweight trust mechanism is originally proposed for IoT edge devices based on multi-source feedback information fusion. First, due to the multi-source feedback mechanism is used for global trust calculation, our trust calculation mechanism is more reliable against bad-mouthing attacks caused by malicious feedback providers. Then, we adopt lightweight trust evaluating mechanism for cooperations of IoT edge devices, which is suitable for large-scale IoT edge computing because it facilitates low-overhead trust computing algorithms. At the same time, we adopt a feedback information fusion algorithm based on objective information entropy theory, which can overcome the limitations of traditional trust schemes, whereby the trust factors are weighted manually or subjectively. And the experimental results show that the proposed trust calculation scheme significantly outperforms existing approaches in both computational efficiency and reliability.

INDEX TERMS Internet of Things, edge computing, trust computing mechanism, feedback trust, multi-source feedback information fusion, objective information entropy theory.

I. INTRODUCTION

The Internet of Things (IoT) is a new computing pattern that is rapid growth and application with the development of wireless communication technologies [1]. IoT can incorporate seamlessly and transparently a large number of heterogeneous smart devices or end systems, while providing open access to selected subsets of data for the development of a plethora of digital services [2], [3]. Edge computing could optimize cloud computing systems by performing data processing at the edge of the distributed networks, and edge computing services significantly decrease the volumes of data that have to be traveled, cut down the consequent network traffic and the distance of data travelling [4]–[6]. Meanwhile, edge computing also covers a wide range of technologies, including IoT edge computing [7]–[12], mobile edge computing [5], [13]–[16], cloud computing [17]–[20], fog computing [21], [22], distributed data storage [23], [24], autonomic self-healing networks [25], remote cloud services [26], augmented reality [27], and so on [28], [29].

A. MOTIVATION OF THIS WORK

The integration of IoT and edge computing is currently a new research hotspot [7]–[12]. However, the lack of trust between IoT edge devices has hindered the universal acceptance of edge computing as outsourced computing services. Trust calculation is currently considered as a survival foundation of distributed applications, such as IoT edge computing [10], ad hoc network [30], P2P computing [31], wireless sensor network [32], cloud computing [33]–[35] and many more [36]–[38]. Unlike traditional authentication

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

mechanism in network security, trust computing mechanism provides dynamic behavior perceiving capability in service providing and it could take precautionary measures against malicious service behaviors from authenticated service providers [33], [34]. While as a complementary technology with traditional network security, trust mechanism solves the problem of providing the corresponding access control by judging quality of the service, and it makes traditional security services more reliable by ensuring that all communicating devices are trustworthy during service cooperation [35].

Various security risks and attacks have been introduced in IoT, including physical attacks on network devices and communication attacks, such as message forging, message tampering and reply attacks [39]. This situation leads to the lack of trust between IoT devices, which has hindered the universal acceptance of IoT edge computing as outsourced computing services. Therefore, IoT edge computing providers should establish trust to alleviate the concerns of numerous users [40]. To ensure the quality of collaborative service behaviors and help to establish trust between IoT edge devices, the trust mechanism is used, which is particularly relevant since devices in edge computing possess very different skill levels and diverse abilities, and there may even be malicious devices who maximize their own benefits. In fact, IoT edge computing is suffering from a variety of malicious behaviors such as fake feedbacks, bad-mouthing attacks and collusive cheating [41]. And how to construct an effective trust computing mechanism to ensure the successful implementation of the task, has become a hot topic in IoT edge computing applications and systems [10]. However, IoT edge computing services are also in the face of numerous serious challenges as well, of which one crucial issue is how to calculate trustworthiness of IoT devices in an edge computing environment.

Several scholars have been attracted by the trust problem of edge computing and some novel studies have been carried out [10], [39]–[44]. Such as, Soleymani *et al.* [39] proposed a secure trust model based on fuzzy logic in vehicular ad hoc networks in fog computing. Their solution can detect malicious attackers and faulty nodes, and overcomes the uncertainty and imprecision of data in vehicular networks in both line of sight and non-line of sight environments. Huang *et al.* [40] proposed a distributed reputation management for secure and efficient vehicular edge computing and networks. Numerical results indicate that their model has great advantage in optimizing misbehavior detections and improving cognitive level of misbehaving vehicles. Goh *et al.* [43] proposed three architectures for trusted data dissemination in edge computing. Their study shows that each scheme offers different security features, and imposes different demands on the edge servers, user machines and interconnecting network. Unfortunately, previous studies have some key limitations. Firstly, almost no study is designed for IoT edge computing to focus on the reliability issue of the trust computing mechanism itself. Secondly, most recent studies, such as [39] and [10], [41]–[44], completely ignore the problem of collusion or retaliation caused by the feedback mechanism itself, although feedback mechanism is undoubtedly a fundamental requirement for a trust calculation system, and this will reduce the reliability of these trust systems drastically. Thirdly, current studies are lack of adaptability in global trust aggregation calculation. Besides, many of previous studies, which using the subjective method for assigning weights to trust decision factors, cannot reflect the adaptability of trust decision process, and may lead to misjudgment of trust calculation. As we see, an universal and expanded trust scheme designed specifically for an IoT edge computing environment is still absent.

B. OUR CONTRIBUTIONS

Comprehensively considering rapidity, real-time, effectiveness, accuracy, and focusing on those issues of trust calculation in IoT edge computing, in this study, we originally propose a multi-source feedback based trust computing mechanism for IoT edge devices. First, due to the multi-source feedback mechanism is used for global trust calculation, our trust computing mechanism is more reliable to against bad-mouthing attacks caused by malicious feedback providers. Then, we adopt lightweight trust evaluating mechanism for cooperations of network devices in IoT edge computing, which is suitable for large-scale IoT edge computing because it facilitates low-overhead trust computing algorithms. At the same time, we adopt a feedback information fusion algorithm based on objective information entropy theory, which can overcome the limitations of traditional trust schemes, whereby the trust factors are weighted manually or subjectively.

To our best knowledge, based on the most fundamental requirements of IoT edge computing, this work is the first to construct an integration solving scheme for trust computing mechanism which can simultaneously meet effectiveness and reliability from the user's point of view. The key features of the proposed trust computing mechanism go beyond existing approaches in terms of the following three aspects:

- **A trustworthy IoT edge computing architecture based on trust computing mechanism with cloud platform.** We adopt the idea that GTD (global trust degree) of devices comprises three parts: direct trust (based on direct interaction records between devices), feedback trust from other edge devices and feedback trust from service brokers. The direct trust is a subjective evaluation for the quality of the service provided by edge devices. In IoT edge computing environments, feedback could provide an efficient and effective approach to build a reputation-based trust relationship between IoT edge devices. And our trust mechanism is more reliable because it integrates another important two feedback factors into edge devices evaluation.
- **A lightweight trust mechanism for cooperations of IoT edge devices.** In the proposed multi-source feedback based trust computing mechanism, trust calculation is fully completed by broker layer and device layer,

and it does not require the participation of the central network. Feedback is completely produced at the edge of the network, therefore, it would be more efficient to process the trust calculation at the edge of the network. Thus, it is suitable for IoT edge computing because it is low-overhead in trust computing.

- **A reliable and adaptive algorithm to aggregate overall trust of IoT devices based on objective information entropy theory.** Trust in general is the level of confidence in a person or a thing. From the perspective of security and QOS guaranteeing, trust is used as a measure of provider's competence in providing required service. Thus, as a dynamic and complex concept, trust should involve multidimensional decision-making factors. In this work, we adopt a feedback information fusion algorithm based on objective information entropy theory, which can overcome the limitations of traditional trust schemes, whereby the trust factors are weighted manually or subjectively. Thus, the proposed mechanism obtains better adaptability and higher reliability.

Therefore, the trust mechanism presented in this paper should be a hybrid approach, the key idea of which is by combining three different methodologies, the resulting integrated framework improves the constituent methodologies and the overall assessment of IoT edge devices. These innovative designs collectively make the proposed trust computing mechanism a lightweight, highly reliable, adaptive one that can be used in IoT edge computing environment. Experimental results show that the proposed trust mechanism outperforms existing approaches in both computing overhead and reliability.

The remainder of the paper is organized as follows. Section II gives an overview of related work. Section III describes the IoT edge computing architecture with trust mechanism. Section IV outlines the details of feedback-based and hierarchical trust computing mechanism. The experimental results are presented in Section V. Section VI concludes the paper and presents directions for improvement.

II. RELATED WORK

Several research groups both in academia and the industry are working in the area of trust mechanism in edge computing environment. This section will take an in depth look at the recent developments in this area.

Roman *et al.* [5] gave a survey and analysis of security threats and challenges in mobile edge computing. They analyze the issues of trusted edge computing from what a user would expect with respect to their data in terms of security and privacy. The authors pointed out that trust management is another security mechanism of which trust is great importance for edge paradigms. In this context, the concept of trust goes beyond the idea of ''not knowing who I am interacting with,'' which is mostly solved by implementing authentication mechanisms and establishing trust relationships between trust domains. The reason is simple: we also have to deal with the concept of uncertainty, or ''not knowing how my partner is going to behave.'' All entities have a variety of collaborating peers at their disposal: users can have various service providers available in their vicinity, service providers can choose from many infrastructure providers, and so on. However, such peers might not meet our expectations: the service latency might be high, the anomaly detection rate might be low, or the data might be inaccurate. There are even worse situations: peers might behave egoistically or maliciously. It is then necessary to seriously consider the deployment of trust management infrastructures in this context.

Soleymani *et al.* [39] proposed a secure trust model based on fuzzy logic in vehicular ad hoc networks in fog computing. The authors adopted a fuzzy trust model based on experience and plausibility is proposed to secure the vehicular network. The proposed trust model executes a series of security checks to ensure the correctness of the information received from authorized vehicles. Moreover, fog nodes are adopted as a facility to evaluate the level of accuracy of event's location. The analyses show that the proposed solution not only detects malicious attackers and faulty nodes, but also overcomes the uncertainty and imprecision of data in vehicular networks in both line of sight and non-line of sight environments.

Huang *et al.* [40] proposed a distributed reputation management for secure and efficient vehicular edge computing and networks. The authors focus on reputation management to ensure security protection and improve network efficiency in the implementation of vehicular edge computing. A distributed reputation management system (DREAMS) is proposed wherein vehicular edge computing servers are adopted to execute local reputation management tasks for vehicles. The authoe utilize multi-weighted subjective logic for accurate reputation update in DREAMS. To enrich reputation usage in DREAMS, service providers optimize resource allocation in computation offloading by considering reputation of vehicles. Numerical results indicate that DREAMS has great advantages in optimizing misbehavior detection and improving recognition rate of misbehaving vehicles. Meanwhile, the authors demonstrate the effectiveness of their reputation based resource allocation algorithm.

Goh *et al.* [43] proposed three architectures for trusted data dissemination in edge computing. The authors aim to address the challenges of ensuring data integrity in edge computing. They study three schemes that enable users to check the correctness of query results produced by the edge servers. Two of the schemes are our original contributions, while the third is an adaptation of existing work. Their study shows that each scheme offers different security features, and imposes different demands on the edge servers, user machines, and interconnecting network. In other words, all three schemes are useful for different application requirements and resource configurations. To profile the security properties and resource requirements of the proposed schemes, they compare the schemes against a third scheme that is adapted from existing work. Their study shows that the three schemes present different security and resource

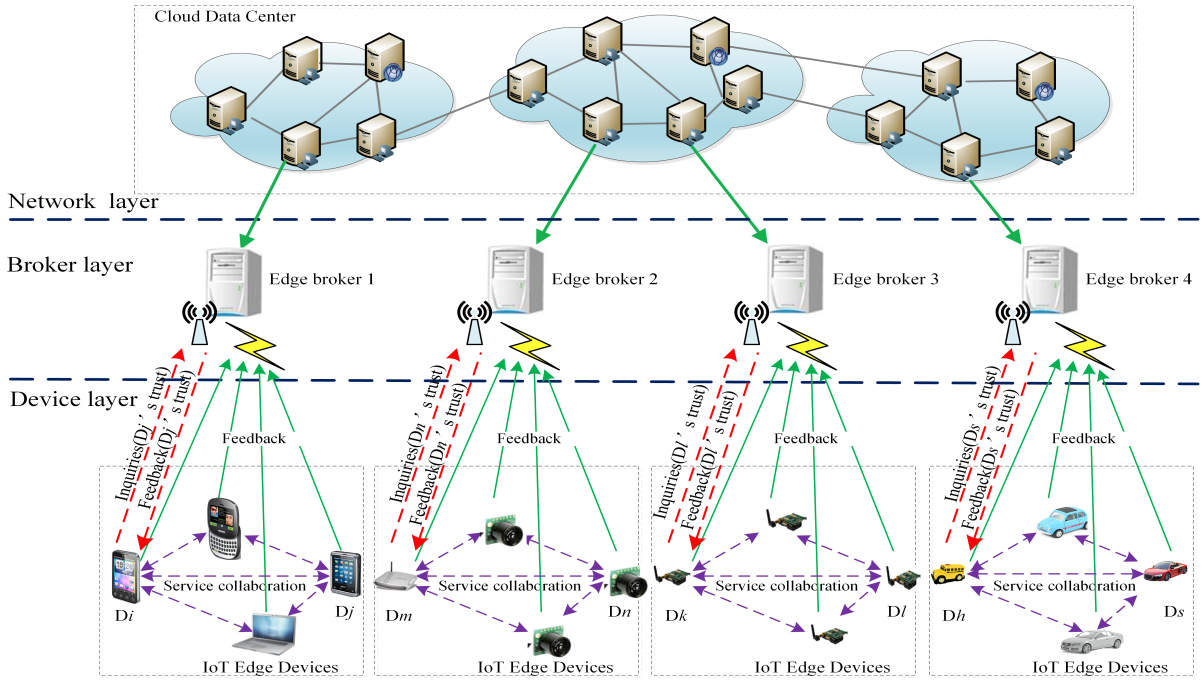

FIGURE 1. IoT edge computing architecture based on multi-source feedback trust computing mechanism with cloud platform.

tradeoffs, and are useful for different application scenarios and resource configurations.

Pinto *et al.* [10] proposed IIoTEED: an enhanced, trusted execution environment for industrial IoT edge devices. The authors demonstrate how IIoTEED can meet the real-time and security requirements of IIoT edge devices, dictated by the three elements of CIA. They propose a TrustZone-based architecture that implements the basic building blocks of a TEE as a lower priority thread of a real-time operating system (RTOS). The RTOS was slightly modified to support trusted applications (TAs) and to schedule the REE only during the idle periods. Experiments demonstrate security is assured while the system's real-time properties remain nearly intact.

Kim *et al.* [44] proposed a software update method in trusted connection of IoT networking. The proposed method employs low power wide area network (LPWAN) as long-range IoT networking technology and uses a mobile edge cloud to improve computing efficiency in an access network that consists of IoT devices with insufficient resources. In the proposed method, the mobile edge cloud is integrated into a gateway, and processes sensing data and remote software updates of LPWAN. IoT devices can receive software functions from the mobile edge cloud. The proposed method analyzes statistical information about connections in an access network and determines the LPWAN trusted connections. Then, software updates can be performed over the trusted connection. Using trusted connections leads to an increased packet delivery rate and reduced transmission energy consumption. The proposed method is compared to currently available systems through computer simulation and the proposed method's efficiency is validated.

As mentioned above, recent studies ignored the problem of collusion or retaliation caused by the feedback mechanism itself, although feedback mechanism is undoubtedly a fundamental requirement for a trust system, and this will reduce the reliability of these trust systems drastically. At the same time, current studies are lack of adaptability in global trust aggregation calculation. Besides, many of previous studies, which using the subjective method for assigning weights to trust decision factors, cannot reflect the adaptability of trust decision process, and may lead to misjudgment of trust calculation. A reliable and lightweight trust mechanism designed specifically for IoT edge devices is still needed.

III. IoT EDGE COMPUTING ARCHITECTURE WITH TRUST MECHANISM

In this section, we first present the IoT edge computing architecture, which is based on multi-source feedback trust computing mechanism. We also discuss the main attack patterns that threaten the establishment of a trust relationship in IoT edge computing applications.

A. EDGE COMPUTING ARCHITECTURE WITH TRUST

Fig. 1 shows the trustworthy edge computing architecture based on multi-source feedback fusion computing mechanism with cloud platform. Edge computing pushes part of the calculation task from cloud data centers to proxy servers at the

edge of the network when data processing, and this will bring several potential advantages. Such as, dealing with applications at the edge reduces network latency and produces faster responses to service requests from users; adding edge servers close to device clusters is likely to be a cheaper way to achieve scalability than fortifying the servers in the cloud data center and also could provide more network bandwidth for users; by lowering the dependency on cloud data center, edge computing removes the single point of failure in the infrastructure, and this will reduce its susceptibility to denial of service attacks and improve service availability [43].

As shown in Fig. 1, the IoT edge computing architecture based on feedback trust computing mechanism comprises three layers: network layer, broker layer and device layer.

- First, about network layer. Network layer is supported by the traditional cloud computing platform. The central server that hosts the master database is located within a professionally managed cloud data center. Cloud computing promises more power, safer data, and easier access to the information and tools needed for success in any industry or organization. In this condition, we can assume that the cloud data center is reliable and always available, while attacks and other risks to the central server are beyond the scope of this work.
- Second, about broker layer. Broker layer is used to monitor service behavior of IoT devices and to aggregate feedback from IoT devices. As we know, in an open edge computing environment, there may be a large number of undependable (or malicious) devices and feedback from these undependable devices will yield incorrect evaluation results. However, currently, limited work is focus on a reliable feedback mechanism for an edge computing environment. Hence, we extend traditional feedback mechanisms so that feedback can come from not only devices but also brokers, and then effectively reduce networking risk and improve system reliability. More importantly, different from the traditional feedback aggregation mechanisms, in the proposed trust mechanism, trust aggregating calculation based on feedback information is entirely undertaken by brokers. This can reduce the energy costs of devices, and make the proposed trust mechanism a lightweight scheme from perspective of device energy cost.
- And the third, about device layer. Device layer consists of various IoT edge devices. In the process of service coordination, multiple participating devices communicate with the brokers through the Internet via WiFi or cellular access points. Devices are divided into different domains based on their location and features, and each domain is managed by a broker. In the area of wireless computer networking, the broker's mission can be borne by the base station, and it is a radio receiver/transmitter that serves as the hub of the local wireless network, and may also be the gateway between a wired network and the wireless network. It typically consists of a low-power transmitter and wireless router. After completing a service collaboration, both IoT devices will submit mutual evaluation information to the broker. Before collaborative service of two devices, a device will send a request message to its broker for the trustworthiness of the collaborator.

B. TRUST RELATIONSHIP ANALYSIS IN IoT EDGE COMPUTING

In the proposed multi-source feedback based trust mechanism, trust calculation is fully completed by broker layer and device layer, and it does not require the participation of the central network. Feedback is increasingly produced at the edge of the IoT network, therefore, it would be more efficient to process the trust calculation at the edge of the network. If all feedback needs to be sent to the cloud for processing, the response time would be too long, not to mention that current network bandwidth and reliability would be challenged for its capability of supporting a large number of IoT devices in one area. In this case, the process of trust calculation needs to be executed at the edge for shorter response time, more efficient executing and less network pressure.

Based on the inherent relationship between IoT devices and brokers, we first study and construct a trust mechanism systematically based on feedback from both devices and brokers first (Fig. 1). In Fig. 1, according to the function of the network devices in edge computing, there are total two kinds of sources involved in feedback providing - devices and brokers, therefore two kinds of entity sets can be formed - a device set ($D = \{d_1, d_2, \cdots, d_i, \cdots, d_n\}$, where i is the ID of a device, n is the total number of devices in a cluster of IoT edge computing) and a broker set ($B = \{b_1, b_2, \cdots, b_k, \cdots, b_m\}$, where k is the ID of a broker, m is the total number of brokers). And there are two kinds of basic feedback relationship among these network entities - one feedback is between a device and other devices which is the most fundamental trust relationships for encouraging cooperation between devices, while another feedback is a broker to its devices which is the special trust relationship adopted by this work and it is a key factor for reducing risk caused by malicious devices and more important for deploying an edge computing service successfully. Then next, referring to the methods in [32], we give the trust relationship definitions that involved in the trust calculation of this work.

Definition 1 [Direct Trust About a Device d_j to Another Device d_i (Called D-to-D Direct Trust)]: So-called D-to-D direct trust is a quantified value in the competence of a device to complete the requesting task, which is based on history of interactive records between the two devices.

Definition 2 [Feedback Trust From a Broker b_k About a Device d_j (Called B-to-D Feedback Trust)]: B-to-D feedback trust is a rating based on the broker's objective calculation. A broker b_k will compute the device d_j real-time trust after a data computing (or forwarding) task completed. When another device d_i request it, the broker will send the value to the requester (d_i).

Definition 3 (Overall Trust From a Device d_j to Another Device d_i (Called D-to-D Overall Trust)]: So-called D-to-D overall trust is a quantified value in the competence of a device (the device is the object of trust evaluation) to complete the requesting task. Trust calculation is based on direct trust, and feedback from its broker.

Definition 3 shows that D-to-D overall trust is a result of fusion calculations by multiple trust factors, including D-to-D direct trust and multiple devices' feedback information. In traditional trust computing mechanisms, such as in [40], trust mainly comes from D-to-D direct evaluation, which could bring many issues, such as malicious attacks and feedback sparseness. While, in the proposed scheme, trust comes from multiple devices' feedback information. At the same time, we adopt an efficient, fast and adaptive algorithm to aggregate overall trust of an IoT device based on objective information entropy theory, which can overcome the limitations of traditional trust schemes, whereby the trust factors are weighted manually or subjectively. Hence, this feedback mechanism possesses higher reliability and could effectively reduce networking risk and improve system reliability.

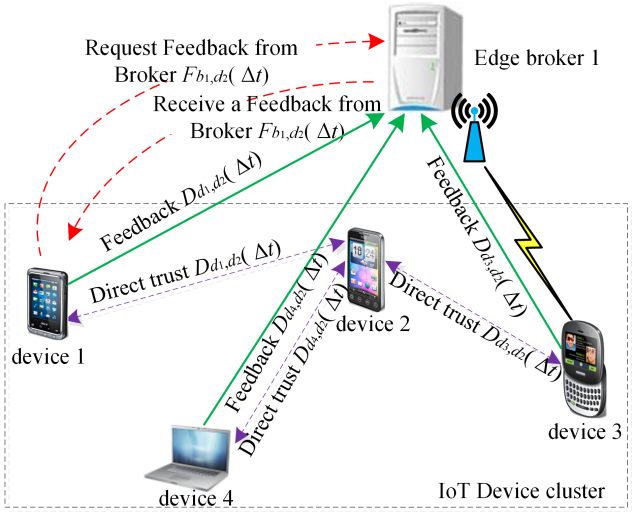

FIGURE 2. An example of trust calculation in IoT edge computing.

Through analysis of Definitions 1-3, the proposed trust mechanism needs to maintain overall trust for devices. In this work, B-to-D feedback trust is represented by $F_{b_k,d_j}(\Delta t)$ and D-to-D direct trust is represented by $D_{d_i,d_j}(\Delta t)$, where $d_i \in D, d_j \in D$. Because trust is a dynamic value with time changing, we added a time-stamp Δt in the expression. An example of D-to-D overall trust computing is depicted in Fig. 2. In this example, if device d_1 wants to obtain the overall trust of device d_2, d_1 first computes d_2's D-to-D direct trust according to d_2's service behavior, and simultaneously asks for B-to-D feedback trust from its broker B_1. The other devices (such as d_3 and d_4) will send their feedback to B_1. B_1 will aggregate these feedback information to obtain a B-to-D feedback trust, then send its feedback $B_{b_1,d_2}(\Delta t)$ to d_1. Then d_1 can get a overall trust $G_{d_1,d_2}(\Delta t)$ about d_2 based on a fusion calculation method. The formal description for the proposed lightweight trust calculation based on multi-source feedback information fusion is detailed in Algorithm 1.

Algorithm 1 Overall Trust of a Device d_i to Another Device d_j

Input: a device set ($D = \{d_1, d_2, \cdots, d_i, \cdots, d_n\}$, a broker set ($B = \{b_1, b_2, \cdots, b_k, \cdots, b_m\}$; and the time window Δt for trust calculation;
Output: $G_{d_i,d_j}(\Delta t)$;
Begin
device d_i send a request message to its Broker b_k for d_j's feedback trust $F_{b_k,d_j}(\Delta t)$;
if ($\Delta t > 0$) **then**
  for (z=1 to n, and $d_z \in D$) **do**
    d_z send the D-to-D direct trust $D_{d_z,d_j}(\Delta t)$ to their broker b_k;
  end for
  b_k aggregates these feedback to obtain $F_{b_k,d_j}(\Delta t)$ and sent it to d_i;
  d_i computes d_j's D-to-D direct trust $D_{d_i,d_j}(\Delta t)$ according to d_j's service behavior;
  d_i aggregates $D_{d_i,d_j}(\Delta t)$ and $F_{b_k,d_j}(\Delta t)$ to obtain $G_{d_i,d_j}(\Delta t)$;
end if
End

Different from the traditional feedback aggregation mechanism, from Algorithm 1, within the feedback trust aggregation, the B-to-D feedback trust of a device is evaluated by its broker. Thus each device does not need to maintain the feedback from other devices, which will reduce the communication overhead and eliminate the possibility of a bad-mouthing attack by compromised devices.

IV. TRUST AND FEEDBACK CALCULATION

As shown in Definitions 1-3, there are one direct trust relationship and one indirect feedback relationship in the proposed trust computing mechanism. Calculation approaches for these trust factors are different because their properties are fully heterogeneous. In this section, we will present the related computing mechanisms for these trust factors.

A. TRUST FACTORS CALCULATION

1) D-TO-D DIRECT TRUST CALCULATION

D-to-D direct trust is given by the knowledge of the devices's nature or past interactions in the service cooperation, without requesting information from a trusted third party (TTP). D-to-D direct trust is generated every time after an interaction takes place. Supposing that d_i has rated the quality of service on the latest Δt interactions with d_j as a time-based series probabilistic ratings:

$$h_{d_i,d_j}(\Delta t) = \{\tau^{(1)}_{d_i,d_j}, \tau^{(2)}_{d_i,d_j}, \cdots, \tau^{(z)}_{d_i,d_j}, \cdots, \tau^{(\Delta t)}_{d_i,d_j}\} \quad (1)$$

where $\tau^{(z)}_{d_i,d_j} \in [0,1]$, and (Δt) is a time window of history interactions, which refers to the largest number of history records considered by the trust model. After an interaction (called an experience), d_i will give a score for d_j according to its performance. And the value of $\tau^{(z)}_{d_i,d_j}$ can be defined according to the success rate of the service. Such as, the value of $\tau^{(z)}_{d_i,d_j}$ can be set 1 to a successful service, and be set 0 to a failed interaction.

For the sake of risk reduction, D-to-D direct trust is defined as the following risk probabilistic model:

$$D_{d_i,d_j}(\Delta t) = \frac{(\sum h_{d_i,d_j}(\Delta t)^+) + 1}{(\sum h_{d_i,d_j}(\Delta t)^+) + (\sum h_{d_i,d_j}(\Delta t)^-) + 2} \quad (2)$$

where $\sum h_{d_i,d_j}(\Delta t)^+$ is the total number of positive ratings ($\tau^{(z)}_{d_i,d_j} \geq 0.5$) during the past Δt interactions, while $\sum h_{d_i,d_j}(\Delta t)^-$ is the total number of negative ratings ($\tau^{(z)}_{d_i,d_j} < 0.5$). In special cases, if $\sum h_{d_i,d_j}(\Delta t)^+ \neq 0$ and $\sum h_{d_i,d_j}(\Delta t)^- = 0$, we set $D_{d_i,d_j}(\Delta t) = 1$. If $\sum h_{d_i,d_j}(\Delta t)^+ + \sum h_{d_i,d_j}(\Delta t)^- = 0$, which denotes that there is no interaction between devices d_i and d_j during time Δt, we set $D_{d_i,d_j}(\Delta t) = 0$. For example, if $\alpha = 2$, the trust value is 0.90 with 1 unsuccessful and 10 successful interactions while the trust value is 0.5952 with 2 unsuccessful and 10 successful interactions.

2) B-TO-D FEEDBACK TRUST CALCULATION

Supposing that there are n devices $D = \{d_1, d_2, \cdots, d_i, \cdots, d_n\}$ exist in an IoT edge computing cluster, the broker b_k will periodically broadcast the request packet within the cluster. In response, all devices in the cluster will forward their trust values toward other devices to d_i. Then, b_k will maintain these trust values in a matrix $f_{b_k \to d_j}(\Delta t)$, as shown below:

$$f_{b_k \to d_j}(\Delta t) = \begin{pmatrix} D_{d_1,d_1}(\Delta t) & \cdots & D_{d_i,d_1}(\Delta t) & \cdots & D_{d_n,d_1}(\Delta t) \\ D_{d_1,d_2}(\Delta t) & \cdots & D_{d_i,d_2}(\Delta t) & \cdots & D_{d_n,d_2}(\Delta t) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ D_{d_1,d_j}(\Delta t) & \cdots & D_{d_i,d_j}(\Delta t) & \cdots & D_{d_n,d_j}(\Delta t) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ D_{d_1,d_n}(\Delta t) & \cdots & D_{d_i,d_n}(\Delta t) & \cdots & D_{d_n,d_n}(\Delta t) \end{pmatrix} \quad (3)$$

where $D_{d_i,d_j}(\Delta t)$ is the D-to-D trust about devices d_j to devices d_i. And when $i = j$, this value will be the device's rating towards itself. To reduce boasting, this value will be discarded by b_k during feedback trust aggregating. We use objective information entropy theory to compute $F_{b_k,d_j}(\Delta t)$ [45]–[47], which can overcome the limitations of traditional trust schemes, whereby the trust factors are weighted manually or subjectively. According to objective information entropy theory, the inputting data needs to be normalized to eliminate the impact of physical dimensions. In Eq. 2, the value of $D_{d_i,d_j}(\Delta t)$ belongs to [0,1], so the matrix $f_{b_k \to d_j}(\Delta t)$ should be a normalized matrix. The formal description for the proposed B-to-D feedback trust calculation based on multi-source information fusion is detailed in Algorithm 2.

Algorithm 2 B-to-D Feedback Trust Calculation Based on Objective Information Entropy Theory

Input: the normalized matrix $f_{b_k \to d_j}(\Delta t)$;
Output: $F_{b_k,d_j}(\Delta t)$;
Begin
for (i=1 to n) **do**
  for (j=1 to n) **do**
    According to the definition of information entropy, calculate information entropy of each data in $f_{b_k \to d_j}(\Delta t)$: $E_i = -ln(n)^{-1} \sum_{i=1}^{n} p_{ij} ln p_{ij}$, where $p_{ij} = D_{d_i,d_j}(\Delta t) / \sum_{i=1}^{n} D_{d_i,d_j}(\Delta t)$;
    if ($p_{ij} = 0$) **then**
      we can set $\lim_{p_{ij}=0} p_{ij} ln p_{ij} = 0$
    end if
  end for
end for
According to information entropy theory, we can obtain a series $\{E_1, E_2, \cdots, E_n\}$;
Calculate the weight of each index through information entropy: $W_i = (1 - E_i)/(n - \sum E_i)(i = 1, 2, \cdots, n)$;
Calculate F-to-D feedback trust: $F_{b_k,d_j}(\Delta t) = \sum_{i=1}^{n} D_{d_i,d_j}(\Delta t) * W_i$;
End

In Algorithm 2, we adopt a feedback information fusion algorithm based on objective information entropy theory, which can overcome the limitations of traditional trust schemes, whereby the trust factors are weighted manually or subjectively. Thus, the proposed trust computing mechanism is more reliable to against bad-mouthing attacks caused by malicious feedback providers.

B. AGGREGATION OF GLOBAL TRUST

Through Eqs. (1), (2) and Algorithm 2, we get two trust factors, D-to-D direct trust $D_{d_i,d_j}(\Delta t)$ and B-to-D feedback trust $F_{b_k,d_j}(\Delta t)$. According to Definition 3, D-to-D overall trust is a result of fusion calculations by the two trust factors, including D-to-D direct evaluation and B-to-D feedback. In order to improve the reliability of the trust calculation, we use an adaptive approach to calculate global trust relationship of a device d_i to another device d_j.

$$G_{d_i,d_j}(\Delta t) = \varpi * D_{d_i,d_j}(\Delta t) + (1 - \varpi) * F_{b_k,d_j}(\Delta t) \quad (4)$$

where ϖ and $(1 - \varpi)$ are the weights for these two trust factors. In the traditional methods of trust calculation, the authors use a manually approach to assign values to ϖ and $(1 - \varpi)$, e.g., they were set as (0.5, 0.5). So it is lack of adaptability in weight assignments for trust factors. Focusing on this issue, we adopt an adaptive aggregating approach for D-to-D overall trust, which can overcome insignificance in

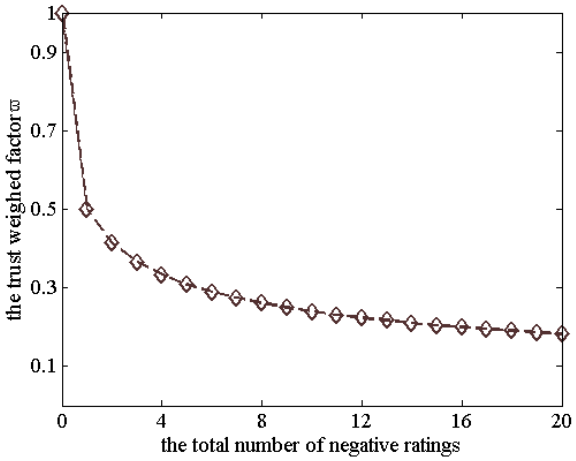

FIGURE 3. An example of the trust weighed factor ϖ.

traditional method.

$$\varpi = \frac{1}{1 + \sqrt{\sum h_{d_i,d_j}(\Delta t)^-}} \tag{5}$$

where $\sum h_{d_i,d_j}(\Delta t)^-$ is the total number of negative ratings ($\tau^{(m)}_{d_i,d_j} < 0.5$) in Eq. 1. And Fig. 3 shows an example of the trust weighed factor ϖ with the the total number of negative ratings ($\sum h_{d_i,d_j}(\Delta t)^-$). From Eq. (5) and Fig. 3, we can see that expression $\varpi = 1/(1 + \sqrt{\sum h_{d_i,d_j}(\Delta t)^-})$ will approach 0 gradually with an increase of the number of unsuccessful interactions, which indicates the strict punishment feature of the D-to-D direct trust for unsuccessful interactions. The strict punishment feature of D-to-D direct trust can effectively prevent sudden attacks from malicious nodes with higher accumulated trustworthiness.

C. ANALYSIS OF TIME COMPLEXITY AND SPACE COMPLEXITY

The proposed trust computing mechanism is a lightweight scheme. Unlike most existing feedback or trust models which rely on broadcast-based strategy to collect feedback from the whole cluster and consequently increasing the system communication overhead significantly, our trust mechanism does not utilize a broadcast-based strategy but instead sets the value of feedback based on the feedback reported by the broker about a specific device. Thus, each device does not need to share trust information with its collaboration devices.

Theorem 1: Space complexity. Using the proposed trust computing mechanism, the maximum communication overhead which involves in trust information delivering is no more than $total_{message}(\Delta t)$,

$$total_{message}(\Delta t) = m * (n + 2n) * \delta = 3mn\delta$$

Proof: Supposed that the IoT edge computing consists of m clusters and that the average size of clusters is n. In a given time window (Δt), the maximum number of trust computing is δ.

According to Fig.2, in B-to-D trust computing based on feedback information, device d_i will send a maximum of one feedback request to its broker and receive a maximum of one feedback response from the broker. Thus, the total number of request information is $2 * n$. Each device d_i will use its self-feedback information to its broker. Thus, the total number of feedback reporting information is n. Consider the case of m clusters, the maximum communication overhead to complete a trust computing is: $m * (n + 2n)$. In a given time window (Δt), the maximum communication overhead is $total_{message}(\Delta t) = m * (n + 2n) * \delta = 3mn\delta$.

Theorem 1. shows that the communication overhead of our trust computing mechanism is linear growth with the number of devices and the number of clusters. This feedback aggregating algorithm is lightweight and need less space overhead, compared with traditional feedback aggregation mechanisms, such as broadcasting mechanism. Given that the feedback between devices need not be considered, this mechanism can significantly reduce network communication overhead, thus improving system resource efficiency. This feedback aggregating mechanism has other advantages such as the effective mitigation of the effect of malicious feedback, thereby reducing the networking risk in an open or hostile edge computing environment.

Theorem 2: *Time complexity. Using the proposed trust computing mechanism, the total time complexity of D-to-D overall trust computing is no more than* $total_{time}(\Delta t)$,

$$total_{time}(\Delta t) = O(n^2)$$

Proof: Supposed that the IoT edge computing consists of m clusters and that the average size of clusters is n.

According to Algorithm 2, in a given time window Δt, the total time complexity of D-to-D overall trust computing is decided by the number of executions of the algorithm. Due to the maximum number of cycles reaches n^2, the total time complexity should be $total_{time}(\Delta t) = O(n^2)$.

Theorem 2 shows that the time complexity of the proposed trust computing mechanism is far superior to some existing schemes, such as the fuzzy-based trust mechanism, whose the time complexity is $O(n^3 log_2 n)$. In Algorithm 2, we adopt an efficient, fast and adaptive mechanism to aggregate overall trust of a collaborative device based on objective information entropy theory. Compared with traditional trust aggregation mechanisms, such as fuzzy theory, support vector machine, neural network and etc, this trust computing mechanism is more lightweight and requires less time overhead.

V. EXPERIMENT-BASED ANALYSIS AND EVALUATION

In this section, we first describe how to set up the experimental methodology in a simulated IoT edge computing environment, including how to deploy the proposed trust scheme on the simulated environment and how to set the experiment configurations. Then, the experimental results are reported.

A. EXPERIMENTAL METHODS AND PARAMETERS

To validate and analyze the effectiveness of the proposed trust computing mechanism, extensive experiments have been conducted by using the NetLogo event simulator [32], which provides a multi-agent programmable modeling environment, and is implemented in JAVA in the AI community. It can easily model the parallel and independent agents to simulate interacting entities among IoT edge computing environment. For the purpose of comparison, we also add PSM (Personalized Similarity Measure) [40] and DRM (Distributed Reputation Management) [40] into the simulator, because the proposed mechanism, PSM and DRM are independent of any specific routing mechanisms in IoT edge computing environment.

In the proposed trust computing mechanism based on multi-source feedback aggregation, the main threat is caused by malicious feedback from IoT edge devices. We have designed several performance mechanisms for a comprehensive comparison with other trust mechanisms. Due to the restrictions of paper length, we mainly evaluate the performance based on the following two aspects: computational efficiency and reliability under different percent of malicious devices.

In order to make the experiments more close to a real IoT computing environment, two kinds of devices are deployed in the simulator based on their identities totally-edge devices and brokers. The feedback provider (FP) can be one of two types: honest devices (HDs) or malicious devices (MDs). And a HD always provides the correct feedback for any devices, whereas a MD always gives an opposite feedback of the actual data for other devices. In the simulator, the behavior of a broker as a feedback provider can always be trustworthy, because the brokers are managed by some TTP (such as well-known cloud service providers).

TABLE 1. Parameters and their possible values.

Symbol	Description	Possible Values
n	the total number of devices	1000
m	the number of brokers in the network	20
t	time-steps of simulation running	200
Δt	time-window for trust computing	20
PCD	the percentage of collaborative devices	10%,20%,40%
MD	the percentage of MDs	10%,20%,40%

The simulation parameters used in the experiments are listed in Table 1. The configuration of simulated computer is CPU 3.4G, memory size 16G and hard disk 1T. There are total 1000 devices deployed in the simulator, and total 20 brokers deployed in the network. The total time-steps of simulation running is 200, and the time-window for trust computing is 20. The percentage of MDs is set to 10%, 20% and 40%. The percentage of collaborative devices (PCD) is set 10%, 20% and 40%, which means the IoT edge computing system correspondingly are idle, busy and highly busy.

B. EVALUATION OF COMPUTATIONAL EFFICIENCY

We use global convergence time (GCT) to evaluate the computational efficiency of the proposed trust mechanism. GCT is the total time of trust aggregation. GCT is useful to evaluate the computational efficiency of the whole network system [31]. Most previous works focused on the system behavior when the system is stable. Here we argue that the convergence time is an important metric to measure how fast the system can reach a stable state, especially in a dynamic and large-scale IoT computing environment.

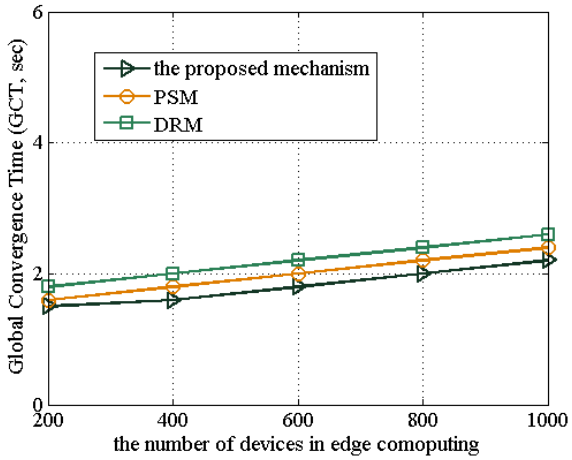

FIGURE 4. Proportion of MDs is 10%, and PCD is 10%.

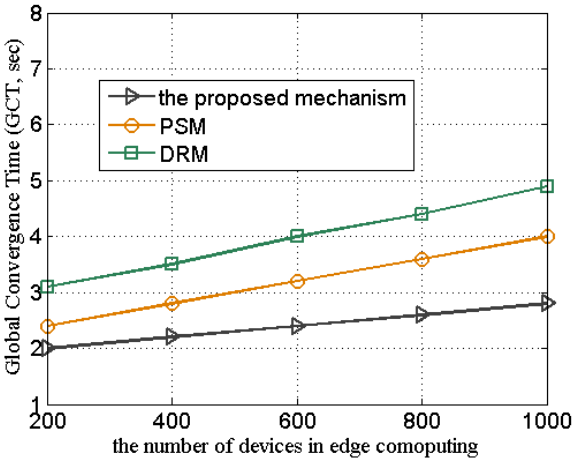

FIGURE 5. Proportion of MDs is 20%, and PCD is 20%.

Figs. 4 to 6 show the compared outcomes of GCT under an IoT edge computing network with 1000 devices. In this group of experiment, we set the percentage of MDs to 10%, 20% and 40%, which respectively indicates that the IoT network environment is relatively honest, dishonest and highly dishonest. In Fig. 4, proportion of MDs is 10%, and PCD is 10%, which means the system is idle and honest. The proposed trust mechanism outperforms PSM and DRM from the viewpoint of GCT. In this relatively honest IoT computing environment, the GCT of the proposed trust mechanism is close to that of PSM and DRM.

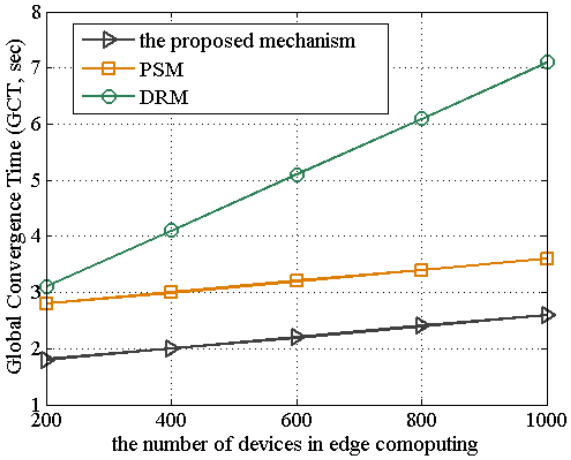

FIGURE 6. Proportion of MDs is 40%, PCD is 40%.

In Fig. 5, proportion of MDs is 20%, and PCD is 20%, which means the system is busy and dishonest, in which 20% devices are dishonest and 20% devices requests cooperation with other devices. The same as in Figs. 4, the proposed trust mechanism outperforms PSM and DRM from the viewpoint of GCT. In this dishonest and busy IoT edge computing environment, the GCT of the proposed trust mechanism is obviously less than that of PSM and DRM. With the rapid increase in the network scale, GCT increases regularity in the proposed trust mechanism. This shows that the proposed trust mechanism has better computational efficiency than PSM and DRM in a dishonest and busy IoT computing environment.

In Fig. 6, proportion of MDs is 40%, and PCD is 40%, which means the system is a highly busy and highly dishonest, in which 40% devices are dishonest and 40% devices request cooperation with other devices. From Fig. 6, the proposed trust mechanism outperforms PSM and DRM from the viewpoint of GCT. In this highly dishonest and highly busy IoT computing environment, the GCT of the proposed trust mechanism is only the half that of PSM and DRM. This shows that the proposed trust mechanism has better computational efficiency than PSM and DRM in a highly dishonest and highly busy IoT computing environment.

As mentioned above, the proposed trust computing mechanism is a lightweight scheme. In our trust mechanism, a device does not utilize a broadcast-based strategy to collect feedback information. Feedback trust aggregating task is mainly undertaken by the brokers. One of the advantages of this mechanism is that it can improve system efficiency and decrease global convergence time of trust aggregation. Another reason for performance improvement is that we adopt an efficient, fast and adaptive algorithm to aggregate overall trust of a collaborative device based on objective information entropy theory. This method can also improve system efficiency and decrease global convergence time of trust aggregation.

C. RELIABILITY WITH DIFFERENT PERCENT OF MDs

We compute *the task failure ratio* (TFR) [32] to reflect the reliability of the trust computing systems. A lower value of TFR indicates a higher reliability of the trust mechanism. In this group of experiments, we suppose that most brokers in the IoT edge computing are trustworthy collaborators. And this IoT edge computing environment closely resembles an actual situation, where most brokers are honest and trustworthy. There kinds of edge computing environment are considered in this group experiments:(1) an honest and idle IoT computing environment; (2) a busy and dishonest IoT computing environment; (3) a highly dishonest and highly busy IoT computing environment.

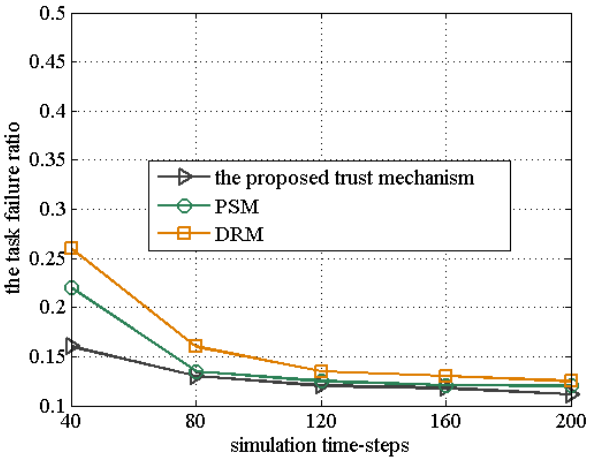

FIGURE 7. Proportion of MDs is 10%, and PCD is 10%.

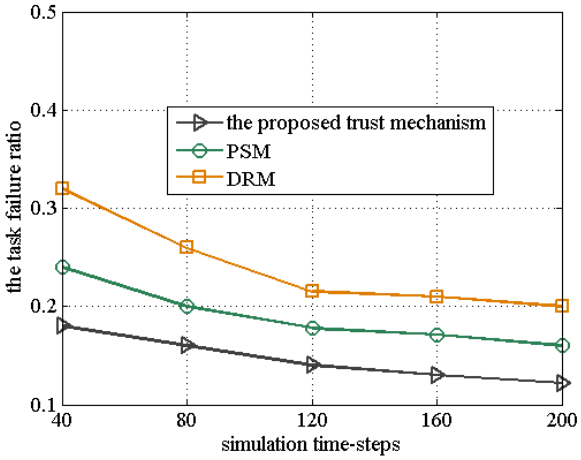

FIGURE 8. Proportion of MDs is 20%, and PCD is 20%.

Figs. 7 to 9 show the comparison results of the task failure ratio in different percentages of MDs. In this group of experiments, we suppose that this IoT computing environment is a trustworthy network community, where all of the brokers are honest. We set the percentage of MDs to 10%, 20% and 40%, which respectively indicates that the network environment

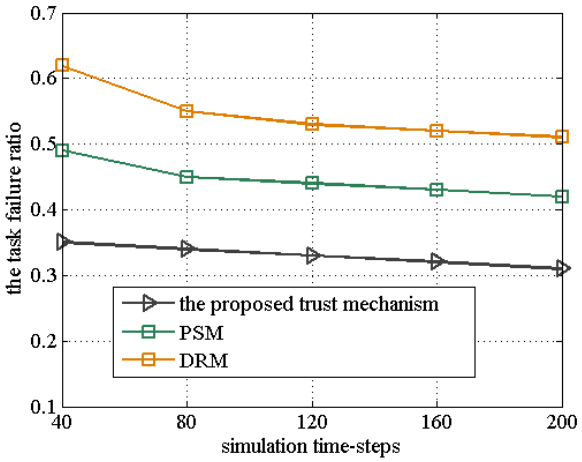

FIGURE 9. Proportion of MDs is 40%, and PCD is 40%.

is honest, dishonest and highly dishonest. Fig. 7 shows an honest and idle network environment, where the percentage of MDs is only 10%. All the three kinds of network environments have a low value of task failure ratio, which are averagely less than 13.21%. These results reflect that the three kinds of network environments exhibit high reliability with few malicious nodes.

In order to evaluate the performance of the trust mechanism in a more dynamic network environment, we gradually increase the proportion of MDs. In Fig. 8, proportion of MDs is 20%, and PCD is 20%, which means the system is dishonest. The results indicate larger differences compared with that when MDs is set to 10%. With the increase of the percentage of MDs, the performance of PSM and DRM mechanism exhibits a marked decline. In Fig. 8, when the proportion of MDs is set to 20%, the task failure ratio of PSM averagely increases to 20.45%, and the task failure ratio of DRM mechanism is up to 24.28%. This shows that the proposed trust mechanism has lower task failure ratio than PSM and DRM in a dishonest and busy IoT computing environment.

In Fig. 9, proportion of MDs is 40%, and PCD is 40%, which means the system is highly busy and highly dishonest, in which 40% devices are dishonest and 40% devices requests cooperation with other devices. From Fig. 9, the proposed trust mechanism outperforms PSM and DRM from the viewpoint of TFR. When the proportion of MDs is set to 40%, the task failure ratio of the proposed trust mechanism is 33.71, and the task failure ratio of PSM increases to 44.21%, and the task failure ratio of DRM is up to 53.37% or higher. These results are consistent with the actual situation, i.e., in a highly dishonest network environment, MDs may conduct bad-mouthing attacks, which can significantly affect the performance of IoT edge computing.

A robust trust mechanism should have a strong ability against malicious feedback behavior from MDs. As mentioned above, in this work, we adopt a feedback information fusion algorithm based on objective information entropy theory, which can overcome the limitations of traditional trust schemes, whereby the trust factors are weighted manually or subjectively. This mechanism can significantly improve the successful implementation of the task and decrease the task failure ratio. At the same time, in D-to-D overall trust aggregating calculation, we adopt an adaptive aggregating approach, which can overcome insignificance in traditional method. This mechanism can also improve the successful implementation of the task and decrease the task failure ratio.

VI. CONCLUSION

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. Edge computing services significantly decrease the volumes of data that have to be traveled, cut down the consequent network traffic and the distance of data travelling, and thereby reducing transmission costs, shrinking latency and improving quality of services. Currently, the integration of IoT and edge computing is a new research hotspot [7]–[12]. However, the lack of trust between IoT edge devices has hindered the universal acceptance of IoT edge computing as outsourced computing services. In order to increase the adoption of IoT edge computing applications, firstly, IoT edge computing architecture should establish trust to alleviate the concerns of numerous users.

In this work, we proposed a reliable and lightweight trust mechanism for IoT edge devices based on multi-source feedback information fusion. First, due to the multi-source feedback mechanism is used for global trust calculation, our trust computing mechanism is more reliable against bad-mouthing attacks caused by malicious feedback providers. Then, We adopt lightweight trust evaluating mechanism for cooperations of network devices in IoT edge computing, which is suitable for large-scale IoT edge computing because it facilitates low-overhead trust computing algorithms. At the same time, we adopt a feedback information fusion algorithm based on objective information entropy theory, which can overcome the limitations of traditional trust schemes, whereby the trust factors are weighted manually or subjectively. And the experimental results show that the proposed trust computing mechanism significantly outperforms existing approaches in both computing speed and reliability.

However, there are still many open issues and much improvement we can apply to the current trust computing mechanism. First, we are interested in combining trust management with incentive mechanism to encourage collaboration between IoT devices. And implementing and evaluating our proposed trust computing mechanism on various IoT computing systems, such as Internet of Vehicles, is another direction for future research.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] M. M. Gaber, J. B. Gomes, and F. Stahl, "Pocket data mining," in *Big Data on Small Devices* (Studies in Big Data). Cham, Switzerland: Springer, 2014.

[5] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Generat. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.

[6] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.

[7] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the Internet of Things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, Aug. 2016.

[8] H. Jayakumar, A. Raha, and V. Raghunathan, "Energy-aware memory mapping for hybrid FRAM-SRAM MCUs in IoT edge devices," in *Proc. IEEE 15th Int. Conf. Embedded Syst. (VLSID)*, Jan. 2016, pp. 264–269.

[9] F. Samie, V. Tsoutsouras, L. Bauer, S. Xydis, D. Soudris, and J. Henkel, "Computation offloading and resource allocation for low-power IoT edge devices," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 7–12.

[10] S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, "IIoTEED: An enhanced, trusted execution environment for industrial iot edge devices," *IEEE Internet Comput.*, vol. 21, no. 1, pp. 40–47, Jan./Feb. 2017.

[11] M. W. Condry and C. B. Nelson, "Using smart edge IoT devices for safer, rapid response with industry IoT control operations," *Proc. IEEE*, vol. 104, no. 5, pp. 938–946, May 2016.

[12] X. Sun and N. Ansari, "EdgeIoT: Mobile edge computing for the Internet of Things," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 22–29, Dec. 2016.

[13] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[14] A. Ahmed and E. Ahmed, "A survey on mobile edge computing," in *Proc. 10th Int. Conf. Intell. Syst. Control (ISCO)*, Jan. 2016, pp. 1–8.

[15] Y. C. Hu *et al.*, "Mobile edge computing a key technology towards 5G," *ETSI White Paper*, vol. 11, no. 11, pp. 1–16, 2015.

[16] Y. Mao, J. Zhang, Z. Chen, and K. B. Letaief, "Dynamic computation offloading for mobile-edge computing with energy harvesting devices," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3590–3605, Dec. 2016.

[17] M. Singhal *et al.*, "Collaboration in multicloud computing environments: Framework and security issues," *Computer*, vol. 46, no. 2, pp. 76–84, 2013.

[18] H. F. Mohammadi, R. Prodan, and T. Fahringer, "A truthful dynamic workflow scheduling mechanism for commercial multi-cloud environments," *IEEE Trans. Parallel Distrib. Syst.*, vol 24, no. 6, pp. 1203–1212, Jan. 2013, doi: 10.1109/TPDS.2012.257.

[19] F. Paraiso, N. Haderer, P. Merle, R. Rouvoy, and L. Seinturier, "A federated multi-cloud paas infrastructure," in *Proc. 5th IEEE Int. Conf. Cloud Comput. (CLOUD)*, Jun. 2012, pp. 392–399.

[20] P. Jain, D. Rane, and S. Patidar, "A novel cloud bursting brokerage and aggregation (CBBA) algorithm for multi cloud environment," in *Proc. 2nd Int. Conf. Adv. Comput. Commun. Technol. (ACCT)*, Jan. 2012, pp. 383–387.

[21] K. Skala, D. Davidović, E. Afgan, I. Sović, and Z. Šojat, "Scalable distributed computing hierarchy: Cloud, fog and dew computing," *Open J. Cloud Comput.*, vol. 2, no. 1, pp. 16–24, Mar. 2015.

[22] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in *Proc. 3rd IEEE Workshop Topics Web Syst. Technol. (HotWeb)*, Nov. 2015, pp. 73–78.

[23] Y. Li, K. Gai, L. Qiu, M. Qiu, and Z. Hui, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," *Inf. Sci.*, vol. 387, pp. 103–115, May 2017.

[24] N. Shimbre and P. Deshpande, "Enhancing distributed data storage security for cloud computing using TPA and AES algorithm," in *Proc. Int. Conf. Comput. Commun. Control Autom. (ICCUBEA)*, Feb. 2015, pp. 35–39.

[25] K. Guo *et al.*, "Conductive elastomers with autonomic self-healing properties," *Angew. Chem.*, vol. 127, no. 41, pp. 12295–12301, 2015.

[26] S. Abdelwahab, B. Hamdaoui, M. Guizani, and A. Rayes, "Enabling smart cloud services through remote sensing: An Internet of everything enabler," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 276–288, Jun. 2014.

[27] M. Billinghurst, A. Clark, and G. Lee, "A survey of augmented reality," *Found. Trends Human-Comput. Interact.*, vol. 8, nos. 2–3, pp. 73–272, 2015.

[28] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. ACM Workshop Mobile Big Data*, Jun. 2015, pp. 37–42.

[29] P. G. Lopez *et al.*, "Edge-centric computing: Vision and challenges," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 37–42, 2015.

[30] A. Boukerche, X. Li, and K. El-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Comput. Commun.*, vol. 30, pp. 2413–2427, Sep. 2007.

[31] X. Li, F. Zhou, and X. Yang, "Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10, pp. 1944–1957, Oct. 2012.

[32] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924–935, Jun. 2013.

[33] F. Azzedin and A. Ridha, "Feedback behavior and its role in trust assessment for peer-to-peer systems," *Telecommun. Syst.*, vol. 44, nos. 3–4, pp. 253–266, 2010.

[34] X. Li, H. Ma, F. Zhou, and X. Gui, "Service operator-aware trust scheme for resource matchmaking across multiple clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 429–1419, May 2015.

[35] X. Li, H. Ma, F. Zhou, and W. Yao, "T-broker: A trust-aware service brokering scheme for multiple cloud collaborative services," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1402–1415, Jul. 2015.

[36] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 318–328, Feb. 2006.

[37] H. Yu, Z. Shen, C. Miao, and B. An, "Challenges and opportunities for trust management in crowdsourcing," in *Proc. IEEE/WIC/ACM Int. Joint Conf. Web Intell. Intell. Agent Technol.*, vol. 2. Dec. 2012, pp. 486–493.

[38] Y. Sun, Z. Han, and K. J. Ray Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Comm. Mag.*, vol. 46, no. 2, pp. 112–119, Feb. 2009.

[39] S. A. Soleymani *et al.*, "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, pp. 15619–15629, Jul. 2017.

[40] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, Nov. 2017.

[41] Y. Wang, T. Uehara, and R. Sasaki, "Fog computing: Issues and challenges in security and forensics," in *Proc. IEEE 39th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2015, pp. 53–59.

[42] R. Pettersen, H. D. Johansen, and D. Johansen, "Secure edge computing with ARM trustzone," in *Proc. 2nd Int. Conf,. Internet Things, Big Data Secur. (IoTBDS)*, 2017, pp. 102–109.

[43] S. T. Goh, H. H. Pang, R. H. Deng, and F. Bao, "Three architectures for trusted data dissemination in edge computing," *Data Knowl. Eng.*, vol. 58, no. 3, pp. 381–409, 2006.

[44] D. Y. Kim, S. Kim, and J. H. Park, "Remote software update in trusted connection of long range IoT networking integrated with mobile edge cloud," *IEEE Access*, to be published, doi: 10.1109/ACCESS.2017.2774239.

[45] R. Xu and D. Wunsch, "Survey of clustering algorithms," *IEEE Trans. Neural Netw.*, vol. 16, no. 3, pp. 645–678, May 2005.

[46] H. Wang and S. Tang, "Analysis and modification on existing objective weighting methods in MADM," in *Proc. 3rd Int. Conf. Genet. Evol. Comput.*, Oct. 2009, pp. 162–165.

[47] Z. Xu, "Two methods of maximizing deviations of multi-attribute decision making," *J. Ind. Eng. Eng. Manage.*, vol. 15, no. 2, pp. 21–29, 2001.

JIE YUAN received the master's degree in software engineering from the Beijing University of Posts and Telecommunications in 2010, where she is currently the Ph.D. degree of cyberspace security with the Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education. She has published several papers in journals and conference proceedings. Her current research focuses on cloud computing, network security, and trusted systems.

XIAOYONG LI received the Ph.D. degree in computer science from Xi'an Jiaotong University in 2009. He is currently a Full Professor of computer science with the Beijing University of Posts and Telecommunications. As the first author or corresponding author, he has published over 100 papers in journals and conference proceedings. His current research interests mainly include cloud computing, network security, and trusted systems. In 2009, he was honored as one of the outstanding doctoral graduates in Shaanxi Province, China. In 2012, he was a recipient of the New Century Excellent Talents in University, China. In 2015, he received the IET Premium Award in Information Security.