INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. 2016; **29**:694–706
Published online 2 February 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2930

A scheme of access service recommendation for the Social Internet of Things

Zhikui Chen[1,*,†], Ruochuan Ling[1], Chung-Ming Huang[2] and Xu Zhu[1]

[1]*School of Software, Dalian University of Technology, Liaoning, China*
[2]*Department of CSIE, National Cheng Kung University, Tainan, Taiwan*

SUMMARY

The rapid increase in the complexity and the extent of personalization of services in the Internet of Things (IoT) has led to a greater demand for frequent collaboration among heterogeneous devices. Moreover, with the inseparable relations between human and devices, the paradigm of Social IoT (SIoT) is gaining popularity in recent years. How to effectively facilitate the access to quality services and credible devices in large-scale networks via defining, establishing, and managing social architectures among things has become a critical issue. In this paper, a scheme of access service recommendation for the SIoT is presented with the understanding of inherent constraints and factors that influence the security and stability of IoT networks. In which, timeliness properties are considered in each transaction for dynamic performance enhancements. With the benefits of promoting service discovery and composition, social relationships among things are introduced in the proposed scheme. An energy-aware mechanism is also utilized as a restrictive factor in trustworthiness evaluation. Finally, the recommendation is based not only on the past performance but also on the social relationship and the energy status of nodes. Simulation experiments demonstrate the effectiveness and benefits of our scheme from three aspects including rating accuracy, dynamic behavior, and network stability. Copyright © 2015 John Wiley & Sons, Ltd.

Received 27 January 2014; Revised 22 December 2014; Accepted 31 December 2014

KEY WORDS: Internet of Things; access service recommendation; dynamic; social relation; energy awareness

1. INTRODUCTION

In the Internet of Things (IoT), a huge number of heterogeneous smart objects interconnect and constitute a variety of application scenarios, such as personal health care, intelligent living environment, private social applications, and so on [1–3]. With the further popularization and diversification of IoT applications, the complexity of services will continue to increase as well as the extent of personalization. Because one single device/object could not meet all the requirements, the future of the IoT will build increased intelligence to access and correlate services from heterogeneous human-related/owner-specific sources and require more mutual cooperation among objects [4–7]. Therefore, it is of great value to provide effective access service recommendations in IoT environments on the basis of the definition, establishment, and management of efficient social architectures among things [8].

Several research works have been recently proposed on social relationships and architectures in the IoT, for example, [9–12] and so forth. However, a majority of these papers addressed only the conceptual issues, such as the preliminary definition and introduction of social relationship in IoT. To the best of our knowledge, only a few works are focused on the practical application of the social

*Correspondence to: Zhikui Chen, School of Software, Dalian University of Technology, Liaoning, China.
†E-mail: zkchen@dlut.edu.cn

relationships and architectures among objects and presented relatively comprehensive schemes or models (e.g., a community of interest based system [13], a fuzzy reputation-based trust management model for IoT [14], an event-driven trust management protocol [15], and a subjective model for trustworthiness evaluation [16]) for access service evaluation and recommendation in the IoT environment. Although these works resolved the evaluation and recommendation issues to a certain extent, most of them considered only ideal scenarios in which (1) nodes have invariable status (e.g. good, normal, or malicious) and provide unchanging performance; (2) barely no fraud, attack, compromise, or other unpredictable behaviors exists; and (3) consumption and failures are not taken into account that the network topology will always be stable, thus, these proposals may not be sufficient for realistic IoT environments.

Until now, there is still a lack of comprehensive access service recommendation and evaluation schemes in IoT environments, especially the schemes that are able to effectively cope with the inherent constraints of IoT objects such as the vulnerability to attacks, the unstable status, the dynamic behaviors, and the energy and resources limitations [17]. With these problems in mind, we proposed a scheme of access service recommendation for the SIoT environment to address the issues mentioned earlier in this paper. The major contributions of the paper are as follows:

- Proposal of a dynamic access service recommendation scheme with novel considerations of the timeliness properties of transactions, which are proven to effectively improve the access service quality, evaluation accuracy, and response rate in dynamic environments. An energy-aware mechanism is also introduced for workload balance and system stability considerations.
- Definition of a new method for social relationship establishment. In the proposed method, social relationships are built based on not only external but also internal similarities among nodes. Moreover, the dynamic behavioral similarity is innovatively considered in social relationship exploration and evaluation among objects for optimized access service recommendations.
- Demonstration of the superiorities of the access service recommendation scheme in dynamic IoT environments, which shows that the proposed scheme can effectively provide the access to quality services and achieve better results in coping with changeable node behavior and unstable network status compared with related methods.

The rest of this paper is organized as follows. In Section 2, a survey of related research work is provided. Section 3 describes the structure of SIoT environment and gives a brief description of the proposed scheme. In Section 4, we present the detail of our access service recommendation scheme, whereas in Section 5, we provide the simulation results for performance demonstration. Finally, Section 6 concludes the paper and outlines future work.

2. RELATED WORK

Research work on access service recommendation for the social IoT environment is in its infancy. To our knowledge, there are very few articles that discussed evaluation and recommendation schemes from different aspects, however, not in much detail.

A number of meaningful research works on social relationships and architectures in the IoT are proposed in recent years. For instance, in [9], the authors conducted a research on the relationship and evolution of objects in IoT by building a social network among them. From the social perspective of the IoT, the authors in [10] presented an opportunistic IoT model that shares information/resource via social contact of the owners. In [11], the concept of SIoT was explicitly stated. Moreover, the architecture of the SIoT system as well as the categories and applications were described comprehensively in [12]. Objects in SIoT are allowed to establish social relationships with others autonomously so that the discovery, selection, and composition of information and services will be greatly facilitated. So far, most of these proposals have focused on the definition and concept introduction of social relationships in IoT. How to practically establish and apply the social relationships and architectures among objects remains a problem.

With the paradigm of SIoT, there are remarkable papers that proposed for access service evaluation and recommendation [11–16,18–24]. A community of interest-based system was described in [13],

DOI: 10.1002/dac

where objects are formed into communities of interest. The authors in [14] presented a fuzzy reputation-based trust management model for IoT. By establishing trust mechanisms among objects, the proposed model stimulates collaborations and facilitates the detection of untrustworthy objects, thus enhancing the network performance. In [15], the authors described an event-driven trust management protocol and demonstrated the proposed protocol with a trust-based service composition application. Analogously, a subjective model was proposed in [16], in which trustworthiness value is evaluated on the basis of own experience and common friends of objects. However, these papers only considered ideal environments with static node behavior and stable network status; thus, the models may not be suited to realistic environments. The authors in [22] described an experiment on power and resources consumption for cryptographic algorithms in IoT, but effective optimization mechanism was not mentioned. Very recently, in paper [23] and [24], the authors dealt with the changeable environment with a tolerance threshold and a temporal window, respectively. These methods are able to cope with the dynamic problems to a certain degree, however, the problem to find a general setting for the unpredictable IoT environments remains.

3. SYSTEM MODEL

A heterogeneous and decentralized SIoT environment with no trusted authority is considered, in which every smart node belongs to a specific owner and an owner could have several nodes, as depicted in Figure 1. Nodes can join and leave dynamically with the owners. Each node maintains individual profiles such as manufacturer, computing capacity, working environment, and interest. Interest here represents the functional features and emphasis of one specific node, as a single or multiple mapping from the connections or interests of owners in real world to the social relationships of devices in an IoT system. Different working environment, capacity, and interest lead to different trust assessments even for the same behavior, thereby forming different communities. The social relationship among nodes is established based on the common communities, the relationship forms [11, 12], and the social behaviors of the owners. It should be noted that in this paper, we focus on providing high-quality access service from the user's point of view, and the devices considered in our model are more personalized and owner specialized, such as mobile phones, tablets, wearable devices, and so on.

Every node might be a normal node or a misbehavior node, and the behaviors of these two categories are differentiated. A normal node provides quality services and is always active in providing proper recommendation for other nodes. while a misbehavior node affects the QoS and the stability of the network by (1) providing poor services and (2) launching malicious attacks, such as badmouthing attacks, on–off attacks, and intelligent behavior attacks [17, 25]. In addition, we assume that a normal node could be compromised and become malicious.

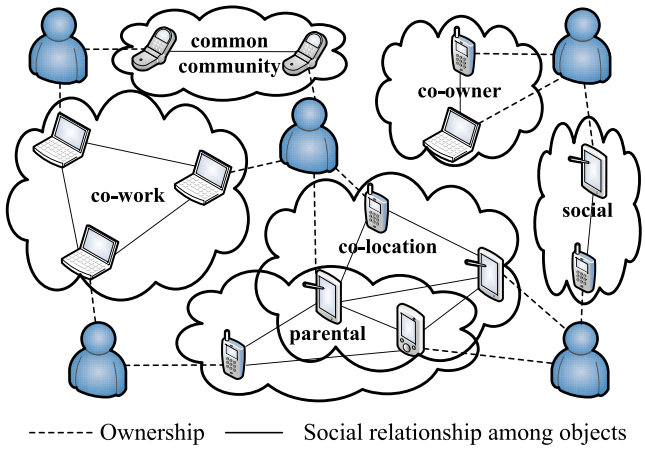


Figure 1. System architecture of the Social Internet of Things.

DOI: 10.1002/dac

In IoT environments, every node not only acts as an information/services provider but also a requester or a recommender. When a node requests a certain service, it broadcasts the requirements information in the network and selects the most appropriate node from the responders that could provide this service. Selections are made on the basis of the access service recommendation scheme. Each node maintains a transactional history and brief profiles for nodes interacted with. Both direct observations and indirect recommendations are considered in trustworthiness assessment along with social relationships and energy status. Nodes with higher trustworthiness are more likely to be recommended. At the end of each transaction, nodes rate for services and recommendations, respectively, and update the local transactional records and object profiles. A detailed description of the proposed scheme will be presented in Section 4.

4. ACCESS SERVICE RECOMMENDATION

The main objective of this paper is to design an access service recommendation scheme for efficient service composition, QoS improvement, and malicious attacks resistance, which is applicable to the dynamic and energy limited environments. To achieve this, three categories of trustworthiness evaluation factors are enumerated and a coherent recommendation metric is comprehensively described.

4.1. Evaluation parameters

In the proposed scheme, each node maintains transactional records and profiles toward other nodes. A node's trustworthiness is evaluated on the basis of direct and indirect reputation, social relationship, and current energy statue. Such trustworthiness is a combination of a given node's past performance and present status, which reflects the predictive credibility to the given node from other nodes in the network. Three categories of factors are identified for such evaluation:

- Factors in a feedback-based reputation system. A reputation system is utilized in our scheme to evaluate the past performance of a given node based on the feedback it received, in which the total number of transactions between two nodes and the feedback for each transaction are recorded. As transactions may differ from one another, a weight factor is introduced to reduce the risk of malicious attacks.
- Factors in social relationship. As a characteristic feature of SIoT, the relationship form [11, 12] is an important factor in trust evaluation. Table I shows the brief description and the weighted value of every relationship form. Basically, we assume that the nodes in a similar service environment or usage mode have a closer relationship, namely, a higher value and higher trustworthiness. In order to further enhance the role of social relationships, the difference between each relationship form is intensified in the proposed scheme, deviating from similar works [16, 23, 24]. Note that alternative values can be used under different conditions. The centrality is introduced for evaluating the importance of a node. In addition, the computation capability is also considered as a vital characteristic of SIoT members, because nodes with higher capability are able to provide better services and less likely to be compromised, nodes are categorized into precisely delineated levels, and each level is assigned with a weight value as shown in Table II.
- Factors in an energy awareness mechanism. In environments with limited node energy, the applying of trust management scheme will lead to a new problem that the nodes with high trustworthiness will have more work load and will run out in less time, thus affecting the network stability and overall performance. Therefore, the remaining energy factor and consumption rate

Table I. Social relationship form.

Relationship	Description	Value
Ownership	Among objects that belong to the same owner.	1.0
Co-work	Among objects that collaborate to provide common services.	0.8
Co-location	Among objects that are in the same or similar working environment.	0.6
Social	Among objects that occasionally or continuously interact with each other.	0.4
Parental	Among objects that belong to the same manufacturer or production batch.	0.2

DOI: 10.1002/dac

Table II. Computation capability level.

Capability	Samples	Value
Level 1	Sensor and recorder	0.2
Level 2	Setup box and smart camera	0.4
Level 3	Smart gateway and terminal	0.6
Level 4	Laptop, tablet, and smart phone	0.8

factor (reflected by running time) are denoted to determine the energy status of a node in the present. Nodes with less energy will have a restrictive trustworthiness value, and their opportunity for cooperation will decrease to make the network stable.

4.2. Recommendation metric

With the parameters discussed earlier, a recommendation metric that integrates these parameters in a coherent scheme are presented. We also describe the formulas that are used to compute the values for each parameter.

For considerations of dynamic environments, the trustworthiness between two nodes is computed with high timeliness and corresponds to a precise time point. Given a time point t, let $R_{u,v}(t)$, $S_{u,v}(t)$, and $E_{u,v}(t)$ denote the reputation, social relationship, and energy status of node v from node u's perspective, respectively. The trustworthiness of node v from the view of node u in time t denoted by $T_{u,v}(t)$, is defined in (1),

$$T_{u,v}(t) = \omega_1 R_{u,v}(t) + \omega_2 S_{u,v}(t) + \omega_3 E_{u,v}(t) \tag{1}$$

where ω_1, ω_2, and ω_3 denote the normalized weight parameters for reputation evaluation, social relationship, and current energy status, and $\omega_1 + \omega_2 + \omega_3 = 1$.

The metric consists of three parts. The first part is a reputation evaluation based on a weighted average value of amount of feedbacks and ratings for past transactions, which can be regarded as an assessment for past performance and a prediction for future transactions. Node u computes the trustworthiness of node v on the basis of own observation (denoted by$R^{\mathrm{dir}}_{u,v}(t)$) and of the recommendation of common friends with node v (denoted by $R^{\mathrm{ind}}_{u,v}(t)$). As shown in (2).

$$R_{u,v}(t) = a \cdot R^{\mathrm{dir}}_{u,v}(t) + (1-\alpha) \cdot R^{\mathrm{ind}}_{u,v}(t) \tag{2}$$

Both direct observation and indirect recommendation are in the range of [0, 1], and a weight parameter $\alpha \in [0, 1]$ is used to adjust the importance of these two parts. When node u needs the trustworthiness of node v, it checks the local transaction records and profiles for direct observation and asks for indirect opinions from friends in common with v. Formula (3) expresses the direct observation of node v from u:

$$R^{\mathrm{dir}}_{u,v}(t) = \sum_{i=1}^{I(u,v,t)} decay(t,i) \cdot DF(v,i) \cdot TF(v,i) \Big/ \sum_{i=1}^{I(u,v,t)} TF(v,i) \tag{3}$$

where $I(u,v,t)$ represents the total number of transactions between u and v until time point t, $DF(v,i)$ and $TF(v,i)$ indicates the direct feedback and transaction weight factor of the ith transaction, respectively. With full consideration of the dynamic IoT environment, a decay factor $decay(t,i)$ is designed for each transaction, which enables a node to take full advantage of the limited records and to obtain a more timely evaluation as well. The decay factor of the ith transaction is defined in (4) where t(i) indicates the occurrence time of this transaction:

DOI: 10.1002/dac

$$decay(t,i) = 1/\ln(|t - \mathrm{t(i)}|) \tag{4}$$

The indirect recommendation is computed on the basis of the opinions received from common friends. The number of common friends is denoted by *C(u,v,t)*. In our scheme, the trustworthiness of a node is considered as the credibility factor of its recommendation, as shown in (5). Opinions from trustworthy nodes are considered more credible and weighted more than those from untrustworthy nodes, thus reducing the risk of malicious attacks.

$$R^{\mathrm{ind}}_{u,v}(t) = \sum_{j=1}^{C(u,v,t)} R^{\mathrm{dir}}_{u,j}(t) \cdot R^{\mathrm{dir}}_{j,v}(t) \Big/ \sum_{j=1}^{C(u,v,t)} R^{\mathrm{dir}}_{u,j}(t) \tag{5}$$

The social relationship between two nodes is considered in the second part of the recommendation metric. By discovering the underlying social relationships, rapid distinguishing between credible and malicious nodes in large-scale network becomes feasible, which is conducive to the discovery and composition of quality services that is usually provided by trusted nodes. To find out more in-depth and comprehensive relationships between nodes, the dynamic behavioral similarities are introduced as the internal relationship in our scheme, and the similarity of two nodes is defined by the combination of both internal relationship and external social relationship factors as presented in (6).

$$S_{u,v}(t) = \beta \cdot S^{\mathrm{int}}_{u,v}(t) + (1-\beta) \cdot S^{\mathrm{ext}}_{u,v}(t) \tag{6}$$

For the evaluation of the internal relationship of two nodes, the Pearson correlation coefficient is utilized to compute the behavioral similarities by their trustworthiness toward common friends. As described earlier, we also introduce the social relationship forms, the centrality, and the computation capability as main factors in external relationship evaluation. The internal and external social relationship between nodes u and v are obtained as follows:

$$S^{\mathrm{int}}_{u,v}(t) = \frac{\sum_{k=1}^{C(u,v,t)} \left| R^{\mathrm{dir}}_{u,k}(t) - \overline{R^{\mathrm{dir}}_{u}(t)} \right| \cdot \left| R^{\mathrm{dir}}_{v,k}(t) - \overline{R^{\mathrm{dir}}_{v}(t)} \right|}{\sqrt{\sum_{k=1}^{C(u,v,t)} \left(R^{\mathrm{dir}}_{u,k}(t) - \overline{R^{\mathrm{dir}}_{u}(t)} \right)^2} \cdot \sqrt{\sum_{k=1}^{C(u,v,t)} \left(R^{\mathrm{dir}}_{v,k}(t) - \overline{R^{\mathrm{dir}}_{v}(t)} \right)^2}} \tag{7}$$

$$S^{\mathrm{ext}}_{u,v}(t) = \delta_1 \cdot Env(u,v,t) + \delta_2 \cdot Cen(u,v,t) + \delta_3 \cdot Cap(v,t) \tag{8}$$

where $S^{\mathrm{int}}_{u,v}(t)$ and $S^{\mathrm{ext}}_{u,v}(t)$ indicates the internal and external social relationship, respectively. *C(u,v,t)* denotes the common friends between nodes u, and v. $\overline{R}^{\mathrm{dir}}_{n}(t)$ is the mean rating value of node n. *Env (u,v,t)*, *Cen(u,v,t),* and *Cap(v,t)* represents the value of the social relationship forms, the centrality, and the computation capability, respectively. Weight parameters δ_i are used to adjust the importance of these three factors and $\delta_1 + \delta_2 + \delta_3 = 1$.

As the last part of the recommendation metric, the current energy status is also considered of great importance in trustworthiness evaluation for the reasons discussed earlier. From node u's perspective, the energy status of node v at time point t denoted by $E_{\mathrm{u,v}}(\mathrm{t})$, is computed by (9).

$$E_{u,v}(t) = \gamma \cdot RE(v,t) + (1-\gamma) \cdot \frac{1}{RT(v,t)} \tag{9}$$

where the weight parameter $\gamma \in [0, 1]$. According to (9), the judgment of a given node u's energy status is based on its remaining energy *RE(v,t)* and the energy consumption rate, which is reflected by

DOI: 10.1002/dac

running time $RT(v,t)$. A node with a less remaining energy and a higher consumption rate will be assigned with a lower energy level, thus decreasing its opportunity for cooperation and workload.

After the evaluation for each service responder node with formulas (1)–(9), the scheme generates a recommendation list based on the integrated trust values. Then the requester node selects one or multiple nodes with high trustworthiness according to service requirements, and interacts with them. At the end of each transaction, the requester node u assigns a feedback $feedback_{u,v}(t)$ to each provider node v according to the quality of the service received. Besides, as an incentive/penalty mechanism, node u also assigns the feedback to the friends for their recommendations. For each node j in $C(u,v,t)$, the $feedback_{u,j}(t)$ is computed as follows:

$$feedback_{u,j}(t) = 1 - ER_{u,j}(t) \tag{10}$$

where

$$ER_{u,j}(t) = \left| T_{u,v}(t) - R_{j,v}^{\mathrm{dir}}(t) \right| \tag{11}$$

According to formulas (10) and (11), if the recommendation from a friend node j is close to the actual QoS that node u received, namely node j provided a positive advice, then it will be assigned with a positive feedback. Otherwise, it will be assigned with a negative one. In the incentive/penalty mechanism, positive feedback is assigned not only to nodes that provide quality service but also to nodes that give positive recommendations. On the other hand, all nodes that provide poor service, carry out malicious attacks, or have a close relationship with the malicious nodes will be given a negative feedback. Because the trustworthiness of one node is based on both the QoSs and the accuracy of recommendations it provided, normal nodes accumulate credibility more rapidly and stably than malicious nodes, so that the scheme could distinguish between normal and malicious nodes more easily and makes optimum recommendation.

5. EXPERIMENTAL EVALUATION

In this section, we analyze the performance of the proposed scheme with simulation results obtained from a series of experiments. For more comprehensive demonstrations, experiments are conducted in three aspects including rating accuracy, dynamic behavior, and network stability.

5.1. Simulation setup

In our simulative IoT environment, $N = 100$ smart devices/nodes are randomly distributed in a $100\,\mathrm{m} \times 100\,\mathrm{m}$ square area and the effective communication distance between two nodes is 20 m. To establish social relationships among nodes, all these nodes are randomly distributed to $N_{\mathrm{owner}} = 10$ owners and $N_{\mathrm{community}} = 10$ communities. In addition, a set of profiles are set up randomly for each node including manufacturer, processing capacity level, and other information. By applying the relationship matrix in [26] and the characterization method provided in [11, 12], a social network among smart nodes is established.

In order to simulate a relatively realistic network, a social environment is considered, in which different types of nodes are assigned with different standard value (hereinafter called ground truth), which indicates the real service quality of them. A normal node provides quality services and has relatively higher social cooperativeness, while a misbehavior node acts maliciously by (1) simply providing poor services; (2) simply providing false recommendations; and (3) providing both poor services and false recommendations. Misbehavior nodes are randomly selected out from all nodes, as shown in Figure 2. The percentage of misbehavior nodes is denoted by *mnp* which varies in [10%, 90%] and is set by default to 20%. For each normal node and misbehavior node in type (2), a random number in [0.85, 0.95] is set as its ground truth, and for each misbehavior node in

DOI: 10.1002/dac

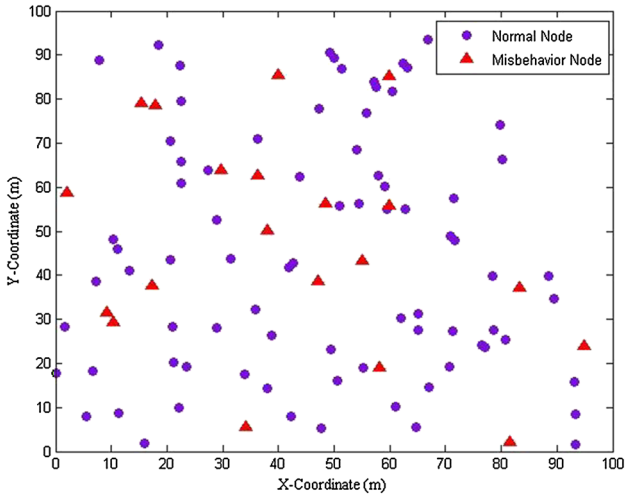


Figure 2. Distribution of nodes in simulation environment ($mnp = 20\%$).

type (1) or (3), its ground truth is set in [0.1, 0.2]. We denote with *map* the probability a misbehavior node acts maliciously.

To get an accurate result of each experiment, we carry out the simulation for 100 repetitions and get the final results from the average of them. Each repetition includes thousands of transaction rounds between nodes. At the start of each transaction, a node is randomly selected out as a requester, who requests a service and randomly selects $N_{\text{candidate}} = 10$ nodes that can provide the service as the candidates. Then the requester node chooses the most suitable candidate node as the provider of this transaction round based on the recommendation list and integrated trust value. For simplicity, all the transactions are considered to have the same importance and set transaction weight factor $TF = 1$ by default. To find the optimal setting, a series of comparative experiments using different parameters is conducted and the result is provided in Table III.

Considering the impact of energy consumption on network performance, each node is assigned with an initial energy value between 0.3 and 0.6 J corresponding to its capacity level. At the end of each transaction, every node consumes energy according to its role (requester/recommender/server) in the transaction. A node is dead once its energy value reaches 0 and would no longer participate in any interaction.

5.2. *Rating accuracy*

We first examine the rating accuracy of our scheme. To analyze the improvement we obtain with respect to the latest research, the performance of the proposed scheme is compared with the subjective approach described in [16, 23] and the dynamic protocol proposed in [24]. A situation without using any trust management or access service recommendation method is also considered in our experiment.

Table III. Optimal parameter setting.

Category	Parameter	Description	Value
Trustworthiness computation	ω_1	Weight of the reputation	0.5
	ω_2	Weight of the social relationship	0.3
	ω_3	Weight of the energy status	0.2
Reputation evaluation	α	Weight of the direct observation	0.7
Social relationship evaluation	β	Weight of the internal relationship	0.6
External relationship computation	δ_1	Weight of the relationship form	0.2
	δ_2	Weight of the centrality	0.5
	δ_3	Weight of the capability	0.3
Energy status evaluation	γ	Weight of the remaining energy	0.6

DOI: 10.1002/dac

Two main metrics, the success rate and mean absolute error (MAE), are used for this performance evaluation. The success rate is the ratio of the service quality value actually obtained by requester to the optimal value of all candidates, which reflects the ability to get the best quality service. Figure 3 shows the success rate of each method when *mnp* is set to 20% by default and the transaction round increases from 0 to 8000. We can observe that the former three methods achieve significant improvement compared with the method without trust management or access service recommendation. This is because these methods can effectively distinguish misbehavior nodes from normal ones by credibility evaluation, thus get better services. However, in the initial phase of transaction rounds, the advantage is not obvious because of the lack of adequate rating data. With the increasing number of transactions, the success rate of these methods improves rapidly. The subjective approach performs better in the beginning because of more emphasis on nodes' social and profile factors, this helps to select quality services in the absence of rating data. But the proposed scheme has a faster convergence and obtains a higher success rate. This happens because our scheme considers a more balanced and immediate computation method and gives more attention to explore the deeper social relations among nodes, which effectively facilitate the rapid discovery and composition of quality services.

Figure 4 shows the MAE of the rating value to the ground truth of one specific node with x-axis represents the number of transaction that the node is involved in. As the reasons described earlier, the proposed scheme obtains a minimal error in four methods and keeps the minimum MAE value after convergence.

5.3. Dynamic behavior

To demonstrate the dynamic behavior of the proposed scheme, three types of dynamic environments are considered: (1) increasing misbehavior node population; (2) rapid membership change; and (3) changeable behavior. In the dynamic environment of type (1), we vary *mnp* from 10% to 90% and study the changes of success rate in different environments. Figure 5 shows the variation curve of the proposed scheme in different *mnp* settings. With the increase of misbehavior node population, success rate decreases dramatically because the opinion and selection of a node is influenced by the increasing false recommendations and poor services.

For comparison, the performance of different methods is also investigated. As shown in Figure 6, the success rates of three methods are almost the same while *mnp* is less than 20%. Then success rates of all methods drop with the increase of *mnp* and the difference between methods emerges. The proposed scheme performs better than other two methods with higher success rates obtained when *mnp* is greater than 20%. This is due to the utilization of the timeliness properties in evaluation, which help to provide the latest states of nodes for recommendation.

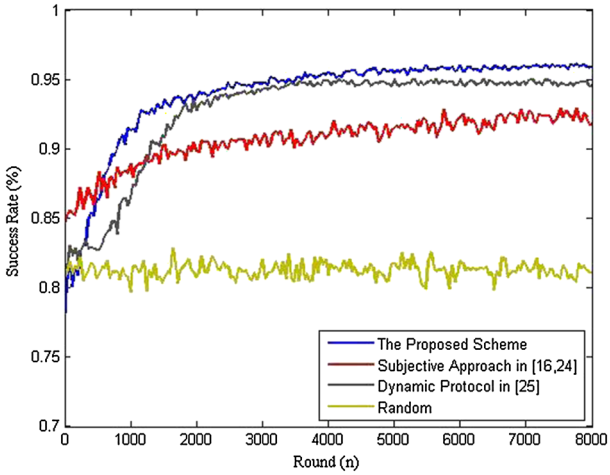


Figure 3. Comparison of the success rate (*mnp* = 20%).

DOI: 10.1002/dac

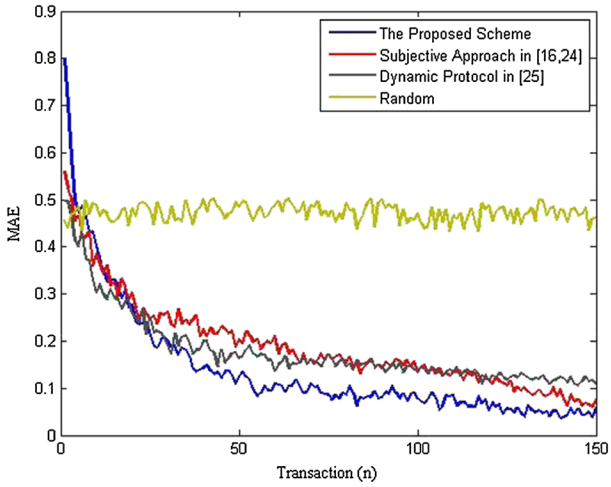


Figure 4. Comparison of the mean absolute error (MAE) value (*mnp* = 20%).

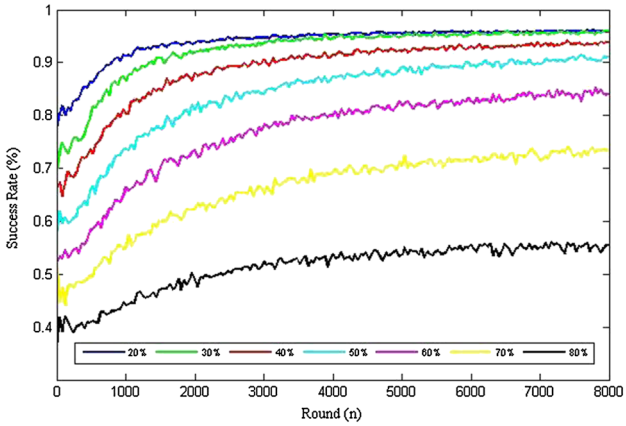


Figure 5. The success rate of the proposed scheme with variable *mnp* values.

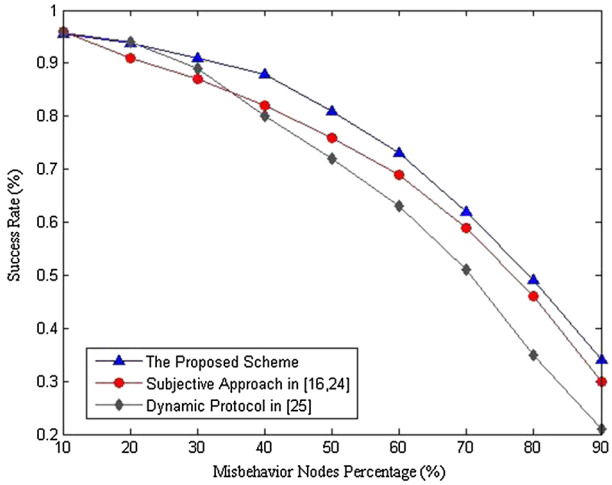


Figure 6. Comparison of the success rate with variable *mnp* values.

Moreover, the performance of three methods in dynamic environment of type (2) is investigated by studying how many transactions it will take to assess a new entrant node precisely in a stable system. According to the new entrant node, whether it is a normal node or not, experiment is

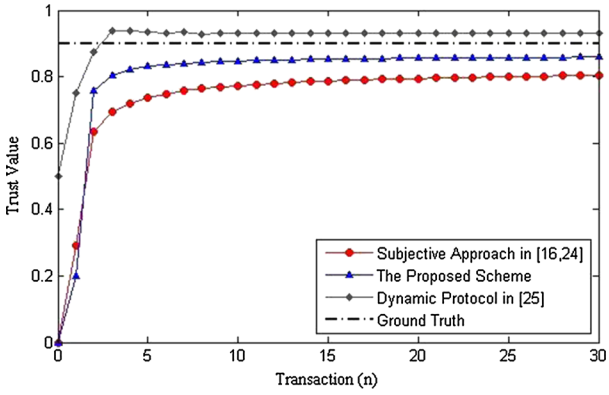
DOI: 10.1002/dac

conducted in two cases respectively. In the former case that the new entrant node is a normal node, as show in Figure 7(a), the dynamic protocol is the fastest to approach to the ground truth, followed by our scheme and the subjective approach. In the latter case as represented in Figure 7(b), both the proposed scheme and the subjective approach achieve ideal results, while the dynamic protocol fluctuates obviously. In general, the scheme presented in this paper is relatively more stable and effective than the other two methods. This is because the assessments in our scheme are based on not only the traditional feedback mechanisms but also on the appropriate incentive/penalty mechanisms and the intrinsic and extrinsic social similarities between nodes, which provide a more rapid and accurate approach for distinguishing between normal and malicious nodes.

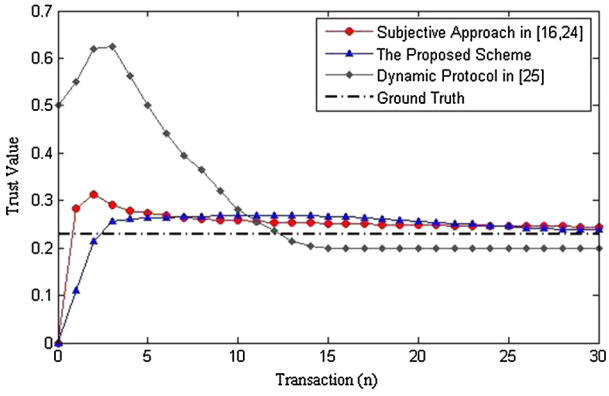
To study the performance of each method in changeable behavior scenarios, a dynamic environment is setup, in which the ground truth of a randomly generated node is oscillated for 50 normal transactions and 50 abnormal transactions. Figure 8 shows the computed trust value of a node that is changing its behavior repeatedly. As shown in the figure, the proposed scheme has a significant precision and response speed than the other methods. The reason is that our scheme considers a dynamic decay mechanism with timeliness properties attached to each transaction rather than a static time window, thus able to adapt to the change in the behavior of nodes. Besides, the utilization of incentive/penalty mechanism also helps to improve the reaction speed and evaluation precision.

5.4. Network stability

Finally, we focus on the ability of energy balancing among smart nodes. An initial energy is set to each node according to the regulations described in simulation setup part. For comparison, a greedy algorithm is also considered, in which a requester always selects the node with highest ground truth. As shown in Figure 9, the proposed scheme obviously outperforms the other methods in energy balancing. One reason is that both subjective approach and dynamic protocol consume a lot of



(a) Normal node



(b) Misbehavior node

Figure 7. Comparison of rapid membership change performance.

DOI: 10.1002/dac

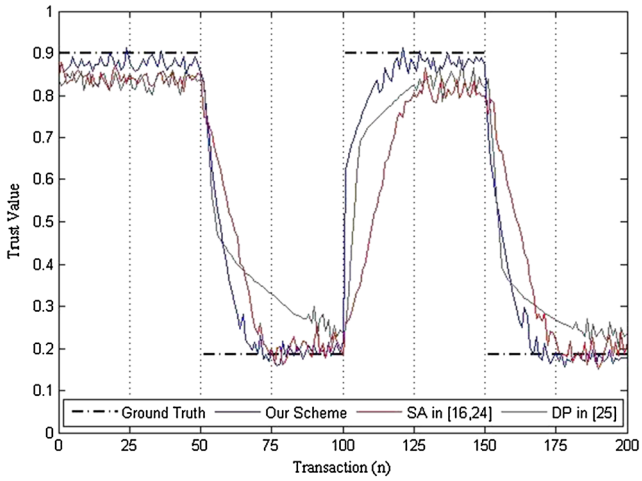


Figure 8. Comparison of changeable behavior performance. SA, subjective approach; DP, direct protocol.

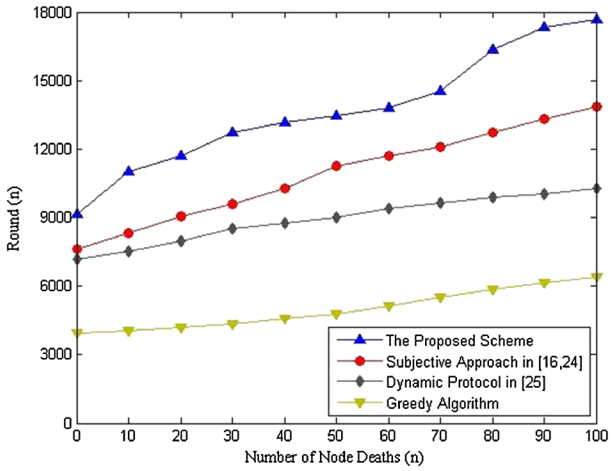


Figure 9. Comparison of energy consumption.

energy in route detection and information sharing; another important reason is that the energy consumption factor being considered by our scheme significantly affects the death rate of nodes and balances the energy status of the entire network.

6. CONCLUSIONS

In this paper, an access service recommendation scheme for efficient service composition and malicious attacks resistance in SIoT environments has been proposed. To address the critical issues in trustworthiness evaluation of SIoT services/devices including vulnerability, dynamic behavior, and resource restriction, we presented a coherent recommendation metric which integrated the timeliness properties of transactions and the social relationships between devices into the evaluation of access service in dynamic environment. Moreover, an energy aware mechanism was also considered for workload balancing and network stability. In order to verify the effectiveness of our scheme, a set of in-depth simulation experiments was conducted in three aspects including rating accuracy, dynamical response rate, and network stability. Results demonstrated that the proposed scheme can effectively provide the access to quality services and achieve better performance coping with dynamic node behavior and unstable network status compared with related methods.

DOI: 10.1002/dac

In future research, we plan to study the strategies for implementing our proposed scheme to actual networks in a distributed and secure manner. We also intend to explore the mutual promotion between social relationship and access service recommendation systems in SIoT environment.

ACKNOWLEDGEMENT

This work is supported by Project U1301253 of NSFC and Project 201202032 of Liaoning Provincial Natural Science Foundation of China.

REFERENCES

1. Atzori L, Iera A, Morabito G. The internet of things: a survey. *Computer Networks* 2010; **54**(15): 2787–2805.
2. Xia F, Yang LT, Wang L, Vinel A. Internet of Things. *International Journal of Communication Systems* 2012; **25**(9): 1101–1102.
3. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: vision, applications and research challenges. *Ad Hoc Networks* 2012; **10**(7): 1497–1516.
4. Ning H, Sha H. Technology classification, industry, and education for future Internet of Things. *International Journal of Communication Systems* 2012; **25**(9): 1230–1241.
5. Lin H, Labiod H. Aggregation methods for integrated services. *International Journal of Communication Systems* 2011; **24**(8): 978–1001.
6. Yen NY, Huang R, Ma J, Jin Q, Shih TK. Intelligent route generation: discovery and search of correlation between shared resources. *International Journal of Communication Systems* 2013; **26**(6): 732–746.
7. Liu CX, Liu Y, Zhang ZJ, Cheng ZY. High energy-efficient and privacy-preserving secure data aggregation for wireless sensor networks. *International Journal of Communication Systems* 2013; **26**(3): 380–394.
8. Ning H, Wang Z. Future internet of things architecture: like mankind neural system or social organization framework? *IEEE Communications Letters* 2011; **15**(4): 461–463.
9. Ding L, Shi P, Liu B. The clustering of internet, internet of things and social network. *Knowledge Acquisition and Modeling (KAM), 2010 3rd International Symposium on. IEEE*, 2010; 417–420.
10. Guo B, Zhang D, Wang Z, Yu Z, Zhou X. Opportunistic IoT: exploring the social side of the internet of things. *Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on. IEEE*, 2012; 925–929.
11. Atzori L, Iera A, Morabito G. Siot: giving a social structure to the internet of things. *IEEE Communications Letters* 2011; **15**(11): 1193–1195.
12. Luigi A, Ierab A, Morabitoc G, Nitti M. The Social Internet of Things (SIoT)–when social networks meet the Internet of Things: concept, architecture and network characterization. *Computer Networks* 2012; **56**(16):3594–3608.
13. Bao F, Chen I-R, Guo J. Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems. *Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE*, 2013; 1–7.
14. Chen D, Chang G, Sun D, Li J, Jia J, Wang X. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things. *Computer Science and Information Systems* 2011; **8**(4): 1207–1228.
15. Bao F, Chen R. Trust management for the internet of things and its application to service composition. *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a. IEEE*, 2012; 1–6.
16. Nitti M, Girau R, Atzori L, Iera A, Morabito G. A subjective model for trustworthiness evaluation in the social Internet of Things. *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on. IEEE*, 2012; 18–23.
17. Roman R, Najera P, Lopez J. Securing the Internet of Things. *Computer* 2011; **44**(9): 51–58.
18. Ou S, Pan H, Li F. Heterogeneous wireless access technology and its impact on forming and maintaining friendship through mobile social networks. *International Journal of Communication Systems* 2012; **25**(10): 1300–1312.
19. Liu Y, Chen Z, Xia F, Lv X, Bu F. An integrated scheme based on service classification in pervasive mobile services. *International Journal of Communication Systems* 2012; **25**(9): 1178–1188.
20. Wang Q, Wang J, Yu J, Yu M, Zhang Y. Trust-aware query routing in P2P social networks. *International Journal of Communication Systems* 2012; **25**(10): 1260–1280.
21. Wang Y, Shi P, Li K, Chen Z. An energy efficient medium access control protocol for target tracking based on dynamic convey tree collaboration in wireless sensor networks. *International Journal of Communication Systems* 2012; **25**(9): 1139–1159.
22. Hamad F, Smalov L, James A. Energy-aware security in M-commerce and the Internet of Things. *IETE Technical Review* 2009; **26**(5): 357–362.
23. Bao F, Chen I-R. Dynamic trust management for internet of things applications. *Proceedings of the 2012 international workshop on Self-aware internet of things. ACM*, 2012; 1–6.
24. Nitti M, Girau R, Atzori L. Trustworthiness management in the Social Internet of Things. *IEEE Transactions on Knowledge and Data Engineering* 2013; **26**(5): 1253–1266.
25. Yu Y, Li K, Zhou W, Li P. Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. *Journal of Network and Computer Applications* 2012; **35**(3): 867–880.
26. Pietilainen AK, Diot C. CRAWDAD data set thlab/sigcomm2009(v. 2012-07-15), 2012.

DOI: 10.1002/dac