[Egyptian Informatics Journal 24 (2023) 257–263](https://doi.org/10.1016/j.eij.2023.03.003)

Contents lists available at [ScienceDirect](http://www.sciencedirect.com/science/journal/11108665)

Egyptian Informatics Journal

journal homepage: [www.sciencedirect.com](http://www.sciencedirect.com/)

[](http://crossmark.crossref.org/dialog/?doi=10.1016/j.eij.2023.03.003&domain=pdf)Study on trust evaluation and service selection for Service-Oriented E- Commerce systems in IoT environments

Xu Wu [⇑](#_bookmark2),[a](#_bookmark0),[b](#_bookmark1), Junbin Liang [a](#_bookmark0)

a *School of Computer, Electronics and Information, Guangxi University, University East Road, Nanning 530000, China*

b *School of information science and technology, Hainan Normal University, Longkun South Road, Haikou 571158, China*

# a r t i c l e i n f o

*Article history:*

Received 3 April 2022

Revised 10 March 2023

Accepted 19 March 2023

Available online 1 April 2023

*Keywords:*

Trust computing Service selection Internet of Things

E-Commerce systems

# a b s t r a c t

Trust-based service management in IoT systems, a promising research direction provides an intelligent solution for the identification of appropriate and trustworthy service providers from a huge of number smart nodes providing similar services. An efficient trust-based service ranking scheme (TBSRS) is pro- posed. The novelty of our design lies in providing accurate trust evaluation and service ranking in the absence of assessment data or presence of untrustworthiness recommendations. TBSRS also addresses the issue about the trustworthiness evaluation of a new service. Service providers are ranking based on the binary fruit fly optimization algorithm in TBSRS. The experimental results demonstrate desirable convergence, accuracy, and resiliency properties of TBSRS, and also demonstrate that TBSRS outperforms Adaptive IoT Trust and IoT-HiTrust in terms of the precision of service selection and other a few perfor- mance metrics.

© 2023 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intel-

ligence, Cairo University. This is an open access article under the CC BY-NC-ND license ([http://creative-](http://creativecommons.org/licenses/by-nc-nd/4.0/)

[commons.org/licenses/by-nc-nd/4.0/](http://creativecommons.org/licenses/by-nc-nd/4.0/)).

1. Introduction

As there are many E-Commerce Systems which can provide the similar services, it is hard for the nodes to identify the appropriate and trustworthy service providers from these similar service alter- natives. Applying a trust model to the study of service selection has been proved to be an effective approach. Trustworthiness of nodes is considered as a service quality metric which reflects the perfor- mance characteristics of the services. The approach helps a service requester to decide whether the service provided is trustworthy or not.

Most of trust based service selection approaches assess the trustworthiness of service providers based on the direct service experiences or indirect recommendations. In general, if a node has not enough interaction experiences with service providers, then recommendations would be needed for decision making. These recommendations may include a number of untrustworthy or unfair users’ feedbacks. Various recommendation filtering meth- ods have been proposed in the area. One method is to use trust threshold to filter untrustworthy recommendations [[1–3]](#_bookmark16). How- ever, it neglects the most critical service requirements of requester. This greatly impacts on the results of recommendation. Another

\* Corresponding author.

*E-mail address:* [xrdz2006@163.com](mailto:xrdz2006@163.com) (X. Wu).

method is to compute social similarity to filter untrustworthy rec- ommendations [[4–7]](#_bookmark17). But it is impractical to build an accurate social network graph for all nodes in an IoT network where the number of nodes is too large, and many nodes often join in or leave the network due to their mobility.

How to evaluate the trustworthiness of a new services in Service-Oriented E-Commerce Systems. For a new service, it is dif- ficult to evaluate the trustworthiness due to data sparsity. To the best of our knowledge, one possible solution used by most of trust models is to assign an initial trust value to the new service. How- ever, this leads to another problem how to determine the initial trust value. In this paper, we propose an efficient trust-based ser- vice ranking scheme given as TBSRS which can provide accurate trust evaluation and service ranking in the absence of assessment data or presence of untrustworthiness recommendations. The key contributions of this paper are as follows:

1) A service requirement similarity algorithm based on distance correlation coefficient was proposed for filtering out the recom- menders who have a low similarity with the service requester; 2) A novel trust evaluation algorithm is proposed based on combining subjective and objective data. The algorithm solves trustworthi- ness assessment problem of a new service; 3) A service ranking method is proposed based on the binary fruit fly optimization algo- rithm, which provides the optimal ranking for service providers by

<https://doi.org/10.1016/j.eij.2023.03.003>

1110-8665/© 2023 THE AUTHORS. Published by Elsevier BV on behalf of Faculty of Computers and Artificial Intelligence, Cairo University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

considering both service provider’s trustworthiness and service requester’s benefit.

The remainder of the paper is arranged as follows: Section II discusses the previous work. The proposed scheme TBSRS is pre- sented in Section III. In Section IV, we conduct extensive experi- ments to evaluate the proposed scheme. Conclusions and our future work are discussed in Section V.

1. Related work

With the development of IoT technology, more and more E- Commerce applications are running on top of it, such as smart health, smart car, smart home and smart city [[9,10]](#_bookmark18). A large of number smart nodes can request and provide these similar appli- cations on behalf of the owners. In such a scenario, it is crucial to select the appropriate and trustworthy service providers for max- imally satisfying the service requester. Trust is viewed as an effec- tive method for selecting trustworthy service providers [[11,12,18]](#_bookmark18). A noteworthy point is that the traditional trust models for P2P net- works, social networks and service computing system cannot be directly applied for service selection in IoT systems due a huge number of IoT nodes, varied user requirements and complex con- text environments [[13]](#_bookmark18). Designing an effective and efficient trust

computation method is still an urgent and important issue in

(SOEs) consisting of service providers (SPs) and service requesters (SRs). In this SOE application, TBSRS is based on an assumed sce- nario, where a SR (service requester) requests a service, and multi- ple SPs (service providers) with similar service quality are competing for the requested service. The system framework is shown in [Fig. 1](#_bookmark3). The entire framework of TBSRS comprises of three components, namely (i) Filtering component, (ii) Trustworthiness assessment component, and (iii) Ranking component.

1. Filtering component

The filtering progress includes two steps:

Step one: Filtering based on service requirement similarity.

Service requirement is a subject description of user own idea about the most critical metrics of service performance. All features of requirement are be normalized to the interval [0,1]. Suppose

}

*S* = {*si*|*i* ∈ {1, ..., *m*}} is the set of *m* services. *N* = *nj*|*j* ∈ {1, ..., *p*}

n o

is the set of *p* nodes. *F* = *Fk*|*k* ∈ {1, ..., *l*} is the set of *l* features of service requirement. *Fk* represents the *kth* feature value of *nj*’s

*i*,*j*

*i* ∈ {1, ..., *m*},*j* ∈ {1, ..., *p*} and *k* ∈ {1, ..., *l*}. According to different service requirement with service *si*, where features (‘‘benefit” or ‘‘cost”), when *Fk* –, The normalized feature

*i*,*j*

value *Fk* is given by:

*i*,*j*

8> *Fkj* —*Fk k*

*i*,

<

*F Fk*

min

—*Fk*

*i*,*j*

*is benefit*

## 1

, *F*

=

Service-Oriented E-Commerce Systems.

Ing-Ray Chen et al. [[8]](#_bookmark18) propose a distributed IoT trust manage-

ment protocol given as Adaptive IoT Trust. In order to solve the rec-

*k*

*i*,*j*

*F*

—*F k*

*k*

max

*k*

>: max

—*F*

min

*k*

max

*k*

min

*i*,*j*

*F*

min ( )

*i*,*j* , *F is* cos *t*

ommendation collecting issue in Adaptive IoT Trust, Ing-Ray Chen et al. propose a 3-tier cloud-cloudlet device hierarchical trust- based service management protocol called IoT-HiTrust [[5]](#_bookmark19), where recommendations are acquired in the cloud. Although IoT- HiTrust is a scalable solution, the trustworthiness computation of

service providers still must rely on the existence of enough friend-

where *Fk* and *Fk* are the minimum and maximum features val- ues, respectively. To support service selection, multiple features are composed on the basis of their weights Fi,j is the composite feature value, and it is defined as:

*l*

max

X

ship social relationship data in nature. Yating Wang et al. [[1]](#_bookmark16) pro- pose a context-aware trust management model for service- oriented IoT networks. This paper pays attention to predict the probability of making satisfactory service instead of service qual-

*Fi*,*j* = *wk* × *Fk*

*k*=1

*i*,*j*

where (*wk wk* ∈ [0, 1] P*l*

*k*=1

(2)

*wk* = 1)is the weight of the *kth* feature.

ity. Al-Hamadi Hamid et al. [[6]](#_bookmark18) discuss the trust management prob- lem in a smart service community. The trustworthiness of service providers is assessed based on service requester’s own experiences

and other witnesses’ experiences. Zhiting Lin et al. [[2]](#_bookmark20) propose a

Pearson Correlation Coefficient (PPC) [[16]](#_bookmark18), is used to measure the user similarities. Given the value *Fi*,*j* and *Fi*,*c*, the similarity

*Fsim*(*j*,*c*) between *nj* and *nc* is obtained based on PPC formula:

comprehensive model of trust for social IoT. Relative to [[1,4-6,8]](#_bookmark16),

*F*

P*si* ∈*Sj*,*c*

—

*Fi*,*j* — *Fj F*

—

*i*,*c* — *Fc*

## 3)

the work in [[2]](#_bookmark20) focuses on using objective assessment data to eval-

## *sim*( *j*,*c*) = sﬃﬃPﬃﬃﬃﬃﬃﬃﬃﬃ ﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃ—ﬃﬃﬃ ﬃﬃﬃ2ﬃﬃsﬃﬃPﬃﬃﬃﬃﬃﬃﬃﬃ ﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃﬃ—ﬃﬃﬃ ﬃﬃﬃ2ﬃﬃ (

uate the trustworthiness of service providers. Li et al. [[14]](#_bookmark18) propose a trust model to identify trusted service providers in a dynamic IoT environment. The trust of service providers was evaluated based

*si* ∈*Sj*,*c*

— —

*Fi*,*j* — *Fj*

*si* ∈*Sj*,*c*

*Fi*,*c* — *Fc*

on the objective historical information relating to a service’s previ- ous negotiations and its monitored run-time performance. Wang et al. propose a method of Integrating modified cuckoo algorithm and creditability evaluation for QoS-aware service composition [[15]](#_bookmark18). In an open Internet environment, services attribute values will dynamically change along with the different context environ- ments, so the service selection methods based on service attribute values are still have limitations. Binsi et al. [[21]](#_bookmark21) propose a trust inference model for service recommendation in IoT. The model incorporated the direct and indirect subjective data for rating pred- ication. Our work is inspired by the above existing research works, different from these methods, our work focuses on providing accu- rate trust evaluation and service ranking in the absence of assess- ment data or presence of untrustworthiness recommendations.

1. System model

The section provides the details about the proposed scheme. TBSRS is proposed for Service-Oriented E-Commerce Systems

where *Fj* and *Fc* are average feature values of *nj* and *nc* respectively.

each service requester is used. Only when the similarity *Fsim*( *j*,*c*) is In this paper, a dynamic threshold d which differs with respect to bigger than the threshold d, the recommendation from *nc* can enter

the step two.

Step two: Filtering based on the trustworthiness of recommender.

To filter out untrustworthiness recommendations from step

one, a threshold parameter *Tth* is used. Only when *nc*’s trustworthi-

ness is bigger than the threshold parameter *Tth*, its recommenda- tions will be accepted.

1. Trustworthiness assessment component

The details of trustworthiness assessment are expressed in the following:

* 1. Subjective evaluation

The subjective trustworthiness of SPs reflects SR’s subjective confidence level of service.

It is assumed that a service *si* provided by *nq* has *n* indirect rec- ommendations from filtering component, which is denoted as

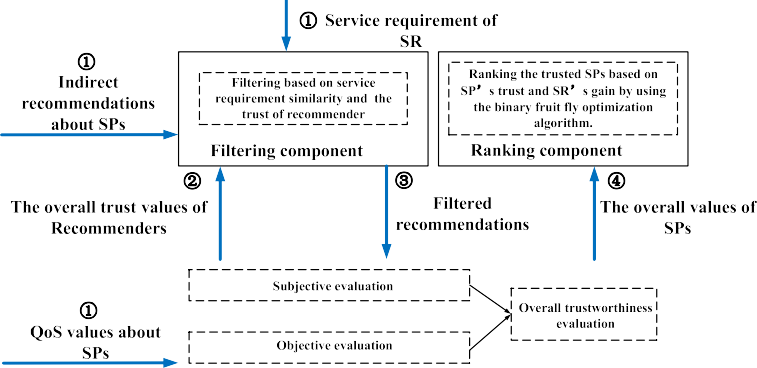


Fig. 1. The system framework of TBSRS.

*R*1, *R*2, ..., *Rn*(*Rh* ∈ [0, 1]). Bayesian estimation of the trust value of a service is used to evaluate the subjective trustworthiness of *nq*

appearing in the *xth* level. Similar to the literature [[19]](#_bookmark22), we choose

a Dirichlet prior over e, i.e., *p* →e = *Dir*(b1, ..., b*X* ). According to the

P*n Rh* + *n*w*j*

*Tsubjective* = *h*=1 *q*,*i*

property of the Dirichlet distribution, the posterior assessment e

*q*,*i* 2*n*

*j*

(4)

becomes

*Yvx* + b*x*

where w*q*,*i* denotes the prior direct service experiences of requester

E(e ) = *q*,*i*

(7)

*j x* P*X*

*nj* about *si* provided by *nq* . If *nj* has no prior service experiences, w*q*,*i*

*x*=1

*x*

*x*=1

*q*,*i*

b + P*X*+1*Yvx*

is set to 0, that is to say, the subjective trustworthiness value

*Tsubjective* is obtained only based on the recommendations.

*q*,*i*

* 1. Objective evaluation

The objective trustworthiness is to predict the probability of completing its commitment of a service provider by comparing the difference between actual provisioned value and the promised

Equation [(8)](#_bookmark4) shows the probability of a certain attribute appears in the *xth* trust level. The objective trustworthiness value of *Qv* is

denoted as the overall probability of excellent, good, and satisfac- tory level which is given by:

*q*,*i*

*Tobjective* = X E(e ) (8)

3

value.

It is assumed that *v* ∈ {1, ..., *V* }. Let Qv

qi

and Qv

qi

present *nq*’s

*v*

*q*,*i*

*Q*

*x*

*x*=1

actual provisioned value and the promised value about the *vth* attri- *Tobjective* is the composite trustworthiness of *nq*’s multiple attributes

*q*,*i*

bute *Qv*

*q*,*i*

*q*,*i*

for service *si*. *Yv*

is denoted as *nq*’s service completing

for service *si*, and it is defined as the objective trustworthiness value

extent of *Qv* . The bigger *Yv*

is, the better service completing extent.

of service provider *nq* for service *si*:

*q*,*i q*,*i*

*Yv* is calculated as follows: *V*

*q*,*i*

8 *Tobjective* = X c*v Tobjective*

*Qv*'

*Q*

*Yv*

><

*Qv*' —*Qv*'

*q*,*i q*,*i* , *q is benefit*

*q*,*i*

5)

*q*,*i*

*v*=1

*v*

*q*,*i*

*q*,*i*

3) Overall trustworthiness evaluation

(9)

*q*,*i* = *Qv*' —*Qv*''

*Q*

*q*,*i*

*q*,*i*

*q is* cos *t*

*v*

*v*

*v*=1 *v*

:

*v*'

*q*,*i*

,

>

( where c

(c ∈ [0, 1] P*V*

c = 1X) is the weight of *Qv* .

where there are two types of service attributes: benefit and cost. Based on *Yv* , the objective trustworthiness level for the *vth* attribute is defined as five levels [[19]](#_bookmark22):

*q*,*i*

The overall trustworthiness of a SP can be evaluated by aggre- gating both subjective trustworthiness and objective trustworthiness:

*Tq*,*i*

j*Tsubjective* + 1 — j *Tobjective*

## (10)

8> 1 (*excellent*) *if* 0.5 6 *Yv* < 1

*q*,*i*

= *q*,*i*

( ) *q*,*i*

2 (*good*) *if* 0 < *Yv* < 0.5

*q*,*i*

>

*Lv* = < 3 (*satisfactory*) *if Yv* = 0

*q*,*i*

*q*,*i*

(6)

The tunable parameter j is used to balance objective and sub-

jective trustworthiness.

If *s*

is a new service, *Tsubjective* and *Tobjective* calculated by the

4 (*bad*) *if* — 0.5 6 *Yv* < 0

>

*i q*,*i*

*q*,*i*

*q*,*i*

>: 5 (*very bad*) *if* — 1 6 *Y* < —0.5

*v*

*q*,*i*

Here, Bayes learning theory is applied to measure the objective

above Equations will be zero due to the data sparsity problem. It is obviously unfair for a new service. Therefore, to overcome the data sparsity problem, our TBSRS will infer the trustworthiness

*T* based on the previous services provided by *n* . It is assumed

*v* —→*v*

trustworthiness value of *Qq*,*i* . Let *Yq*,*i* = *Yq*,*i* , *Yq*,*i* , ..., *Yq*,*i*

represent

n *v*1 *v*2

*vX* o

*q*,*i q*

*v*

that a service *si* provided by *nq* has *V* attributes, and *Qq*

,*i*

is the *vth*

the service completing extent information for the attribute *Qv* ,

*q*,*i*

attribute,*v* ∈ {1, ..., *V* }. If the attribute *Qv*

is included in the previ-

where *X* is the number of levels. *YvX* represents the times of *Qv*

ous service *se* and is the *gth* attribute of *se*, that is to say *Qv*

and *Qg*

*q*,*i*

*q*,*i*

*q*,*i*

*q*,*i*

*q*,*e*

is the same attribute. The objective trustworthiness value of *Qv*

*q*,*i*

position of the fruit fly with high fitness value and the position is

can be inferred as *Tobjective*. If the attribute *Qv*

is not included in

a seed in the next iteration. The fitness of each fruit fly is calculated

*g q*,*e*

*Q*

*q*,4

with Equation [(11)](#_bookmark5).

the previous services, the objective trustworthiness value of *Qv*

*q*,4

can be given as 0.5. For example, service *s*4 is a new service, which has three attributes:*Q* 1 , *Q* 2 and *Q* 3 . Their weights are 0.2, 0.6

*fitness* = r*Tp*,*i* + (1 — r)*Gj*,*i* (11)

*q*,4

*q*,4

*q*,4

where *Tp*

denotes the trustworthiness of service provider *nq* for

and 0.2, respectively. *Q* 1 is included in the previous experienced

*q*,4

,*i*

the service *si*. r is a weight value. *Gj*,*i* denotes the gain of a service

service *s*1 and trustworthiness in service *s*1 is 0.6. *Q* 2

is included

requester *n* using the service provided by *n* . In experimental sec-

*q*,4 *j q*

in the previous experienced service *s*2 and trustworthiness in ser- tion, the gain of a service requester is randomly set as a value of

vice *s*1 is 0.8. *Q* 3 isn’t included in the previous experienced ser-

*q*,4

vices, so its trustworthiness is set to 0.5. Based on the above inferring method, the trustworthiness *Tq*,4 is:

0.6 × 0.2 + 0.8 × 0.6 + 0.5 × 0.2 = 0.7.

1. Ranking component

To rank the trustworthy service providers, our scheme uses the binary fruit fly optimization algorithm [[20]](#_bookmark23) shown in [Fig. 2](#_bookmark7). The process includes two steps: Initialization and Iteration.

Step one:

The algorithm firstly initializes population size (*popsize* ), maxi- mum number of generations (*gen*max), local best smell concentra-

tion (*smellbest*), global best smell concentration (*gsmellbest*), best position (*posbest*), global best position (*gposbest*), fitness value (*fitness*) and random position of ‘‘*m*” fruit flies with appropriate values, shown from line 1 to line 12. The position of a certain fruit fly is denoted as ‘‘*z*” tuple vectors. ‘‘*z*” is the number of trustworthy service providers. If the binary position of fruit fly *js* is

(0, 0, 1, 1, 0, 0), it shows *n*3, *n*4 are present and *n*1, *n*2, *n*5, *n*6 are

absent on the position. Global best position (*gposbest*) stores the

[[0,1]](#_bookmark16).

Step two:

The random position in the current iteration is generated in the initialization step. Then, the fitness value of each fruit fly is evalu- ated based on current position. *smellbest* and *posbest* are updated with the fitness value and position of the fruit fly with high fitness value respectively. The new *smellbest* is compared with the last

*gsmellbest*. If *smellbest*>*gsmellbest*, then *gsmellbest*← *smellbest* ; *gposbest*←*posbest*. Subsequently, the new *gsmellbest* and *gposbest* are set as a seed for the next generation. In order to obtain the optimal

service ranking result, the algorithm will check whether the value of fitness is 1 or not, shown from line 13 to line 23. In addition, if the current global best solution is the same with the solution from the last iteration, the Equation [(12)](#_bookmark6) [[12]](#_bookmark18) will be used to update the position of fruit flies, shown from line 24 to line 26.

*p*(*t* + 1) = *Mutation*(*p*(*t*)) (12)

tions (*fitness* = 1 or *gen*max) is met. The iteration process is completed until one of the two condi-

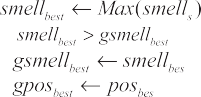
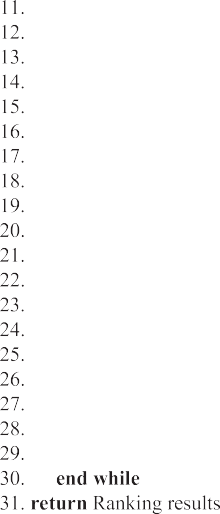
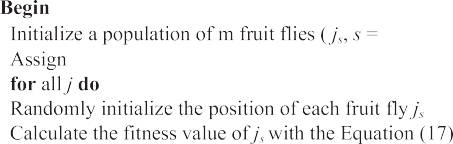


Fig. 2. The binary fruit fly optimization algorithm.

1. Experimental analysis
   1. *Experiment setup*

We simulate a service-oriented network system with *Nn* nodes. The experimental data come from realistic dataset (Epinions Trust Network Datasets). We slight modify them in the experi- ments. [Table 1](#_bookmark8) lists the parameters and their values/ ranges used

in the performance validation.

* 1. *Performance metrics*

The main performance metrics are shown as follows:

1. The difference between predicted trust value and actual trust value: The smaller the difference, the higher accuracy of trustworthiness computation.
2. The percentage of malicious nodes selected as SPs for a good SR: The smaller the number, the higher the capacity of filter- ing out malicious recommendations. The percentage is expressed as follows:

tation method. Two approaches and our TBSRS are both trust-based service selection methods. In addition, the two approaches outper- form existing trust-based service selection ones for SOEs.

* 1. *Performance validation*
     1. *TBSRS performance*

In the first experiment, the trustworthiness of a malicious SP and a good SP is calculated by our TBSRS from the perspective of a good SR as time progresses. [Fig. 3](#_bookmark9) shows the experimental results. When the experiment begins, the trustworthiness of malicious SP and good SP goes down and rises up, respectively. The main reason is that TBSRS effectively filter out untrustworthy assessment data based on the proposed recommendation filtering algorithm.

In the second experiment, the trust difference of a SP’s pre- dicted trustworthiness and the actual trustworthiness is measured from the perspective of a good SR as time progresses. [Fig. 4](#_bookmark10) shows the experimental results. One can observe that the trust difference firstly goes down slowly, then goes down quickly, finally converges to 0. The main reason is that when the experiments start, the trust-

*Pm*,*sp*

=  *Nm*,*sp* × 100% (13)

worthiness assessment data is sparse in which case the malicious recommendations would have a great influence on the trustwor- thiness computation, so the predicted trustworthiness only slowly

*Nsp* is the number of SPs selected to provide service for a good SR.

*Nsp*

*Nm*,*sp* is the number of malicious nodes in *Nsp*.

1. The precision of service selection: The bigger the number, the higher the precision of service selection. The precision is expressed as follows:

*precision* = *Nsatisfaction* × 100% (14)

*Nsp*

*Nsp* is the number of SPs selected to provide service for a good SR.

*Nsatisfaction* is in *Nsp*, and it is the number of SPs providing the satisfied service.

1. The percentage of good nodes providing new service selected as SPs for a good SR: The bigger the number, the higher the capacity of assessing a new service. The percentage is expressed as follows:

closes to the actually trustworthiness. As time passes, more trust- worthy assessment date is gathered in which case the malicious recommendations would have a little influence on the trustworthi- ness computation, so the predicted trustworthiness quickly closes to the actually trustworthiness until it is equal to the actual trust- worthiness. The third experiment shows the impact of different value of Similarity weight factor k on the precision of service selec- tion. Top-13% SPs are selected in the experiment. The results are shown in [Fig. 5](#_bookmark11). We are able to see that when k equals to 0.5, the value of precision of service selection reaches the highest point under the same simulation condition. Thus, we can get the conclu-

tion of k = 0.5. sion that the algorithm can achieve better result under the condi-

* + 1. *Comparative analysis*

*P*  *Nsp*,*new*

## 100

The first experiment compares the three methods in selecting

## 15

*sp*,*new* =

*Nnew* ×

% ( )

malicious nodes as SPs for a good SR. [Fig. 6](#_bookmark14) shows the percentage of malicious SPs selected by a good SR as time progresses. The pink

*Nnew* is the number of good nodes providing new service.*Nsp*,*new* is

the number of good nodes providing new service selected as SPs in *Nnew*. The performance of our TBSRS is compared against: Adap- tive IoT Trust [[17]](#_bookmark24) and IoT-HiTrust [[3]](#_bookmark25). The reason we select Adap- tive IoT Trust and IoT-HiTrust is that their SP’s trustworthiness evaluation method is similar with our SP’s trustworthiness compu-

Table 1

Parameter list for performance evaluation.

Symbols Meaning Default Range

*Nn* Number of nodes 100 [50–300]

*Na* Number of service attributes 3 [1–5]

*Ns* Number of service types 2 [2–5] *Nf* Number of user requirement’s feature 3 [2–5] *Tq*,*i* Initial trustworthiness of any node 0.5 [0,1] *Gj*,*i* Initial gain of any node 0.5 [0,1]

i Service request rate 5 / hr [2–10]

*Pm* Percentage of malicious nodes 10% [10%-70%]

k Similarity weight factor 0.5 [0–1]

curve expresses Adaptive IoT Trust. The green curve expresses IoT- HiTrust. The blue curve expresses our TBSRS. The trustworthiness of all SPs is initially set to 0.5, so malicious SRs initially could have the chances selected as SPs to provide the service. Under our TBSRS, the percentage of malicious nodes selected is the lowest in comparison with Adaptive IoT Trust and IoT-HiTrust.

The second experiment compares the three methods in the pre- cision of service selection. The Top-1%, Top-4%, Top-7%, Top-10% and Top-13% SPs are selected respectively and the selection results by three methods will be compared and shown in [Fig. 7](#_bookmark15). One can observe that TBSRS outperforms both Adaptive IoT Trust and IoT- HiTrust in terms of the precision performance metric of service



j Weight factor of objective and subjective trustworthiness

r Weight factor of trustworthiness and

gain

0.5 [0–1]

0.5 [0–1]



*Nsc* Number of selected candidate SPs Top-4% [Top-1%-

Top-13%] Fig. 3. Trustworthiness of a good SP and a malicious SP vs. time.



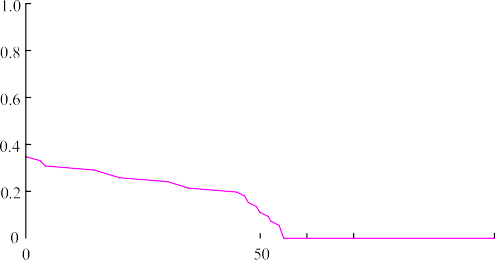


Fig. 4. Trust difference of a SP’s predicted trustworthiness and the actual trustworthiness.

Fig. 8. Percentage of good nodes providing new service selected for service over time under Adaptive IoT Trust, IoT-HiTrust and TBSRS.



Fig. 5. The influence of k on precision of service selection.







Fig. 6. Percentage of malicious nodes selected for service over time under Adaptive IoT Trust, IoT-HiTrust and TBSRS.



Fig. 7. The precision of service selection under Adaptive IoT Trust, IoT-HiTrust and TBSRS.

selection. In addition, when selecting the top-13% candidate SPs, TBSRS has a very high precision, which is close to 100%. This obser- vation implies that, Top-13% candidate SPs are recommended by us to the SR.



Fig. 9. The influence of *Pm* on precision of service selection.

The third experiment compares the three methods in the per- centage of good nodes providing new service selected as SPs. The experimental results are shown in [Fig. 8](#_bookmark12).

One can observe that TBSRS outperforms both Adaptive IoT Trust and IoT-HiTrust in terms of the percentage of good nodes providing new service selected as SPs. The experiments results show that more new services are selected by SRs due the accurate trustworthiness of new service in TBSRS as time processes. The fourth experiment shows the impact of different value of Percent- age of malicious nodes *Pm* on the precision of service selection. Top-13% SPs are selected in the experiment.

One again observes that TBSRS outperforms Adaptive IoT Trust and IoT-HiTrust. An important observation from [Fig. 9](#_bookmark13) is that, even when malicious recommenders add to 70%, the precision of service selection of TBSRS keep also remarkably more than 0.75. The rea- son is that our TBSRS provides the optimal ranking for SPs by con- sidering both service provider’s trustworthiness and service requester’s benefit.

1. Conclusion

In the paper, an efficient trust-based service ranking scheme (TBSRS) is proposed for providing accurate trust evaluation and service ranking in the absence of assessment data or presence of untrustworthiness recommendations. The entire framework of TBSRS comprises of three components, namely (i) Filtering compo- nent (ii) Trustworthiness assessment component (iii) Ranking component. The convergence, accuracy and resiliency properties of TBSRS is analyzed and validated via simulation. A comparative analysis of TBSRS is also performed against Adaptive IoT Trust and IoT-HiTrust. The experimental results validate by simulation demonstrate that TBSRS outperforms these existing approaches in terms of the precision of service selection and other a few per- formance metrics. TBSRS will be applied to mobile social IoT appli-

cations, where the mobility of nodes is considered. In service rank- ing component, how to measure the gain of a service requester is not discussed in our paper, so it will be furtherly researched. Lastly, TBSRS will be further tested in complicated multi-domain scenar- ios, and will extend our work in terms of dealing with more sophis- ticated attack behaviors such as opportunistic, collusion, and insidious attacks.

Declaration of Competing Interest

The authors declare that they have no known competing finan- cial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The work in this paper has been supported by National Natural Science Foundation of China (62062006, 71501156, 62062008, 62067001, 61762008), Natural Science Basis Research Plan in Guangxi Province of China (2018JJA170028, 2019JJA170045, 2018JJA170194), Special Funds of Guangxi Bagui Scholars and National Key Research and Development Program of China (2018YFB1404404).

References

1. Yating Wang, Ing-Ray Chen, Jin-Hee Cho, et al., ‘‘CATrust: Context-Aware Trust Management for Service-Oriented Ad Hoc Networks, IEEE Trans Services Comput 2018; 11(6): 908–221.
2. [Lin Z, Dong L. Clarifying trust in social internet of things. IEEE Trans Knowl](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0010) [Data Eng 2018;30(2):234–48](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0010).
3. [Cho JH, Swami A, Chen I-R. Modeling and analysis of trust management with](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0015) [trust chain optimization in mobile Ad hoc networks. J Netw Comput Appl](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0015) [2012;35(3):1001–12](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0015).
4. [Nitti M, Girau R, Atzori L. Trustworthiness management in the social Internet](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0020) [of Things. IEEE Trans Knowl Data Manag 2014;26(5):1253–66](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0020).
5. [Chen I-R, Guo J, et al. Trust-based service management for mobile cloud IoT](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0025) [systems. IEEE Trans Netw Service Manage 2019;16(1):246–63](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0025).
6. Hamid A-H, Chen I-R, Cho JH. Trust management of smart service communities. IEEE Access 2019. doi: [https://doi.org/10.1109/](https://doi.org/10.1109/ACCESS.2019.2901023) [ACCESS.2019.2901023](https://doi.org/10.1109/ACCESS.2019.2901023).
7. [Wu X, Cheng B, Chen J. Collaborative filtering service recommendation based](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0035) [on a novel similarity computation method. IEEE Trans Services Comput](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0035) [2017;10(3):352–65](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0035).
8. [Chen IR, Guo J, Bao F. Trust management for SOA-based IoT and its application](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0040) [to service composition. IEEE Trans Services Comput 2016;9(3):482–95](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0040).
9. [Guo J, Chen I-R, Tsai JJP. A survey of trust computation models for Internet of](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0045) [Things systems. Comput Commun 2017;97:1–14](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0045).
10. Wang Y, Chen IR, Cho JH, Swami A, Chan K. Trust-based service composi- tion and binding with multiple objective optimization in service-oriented mo- bile Ad Hoc networks. IEEE Trans Serv Comput 2016. doi: [https://doi.org/10.1109/](https://doi.org/10.1109/TSC.2015.2491285) [TSC.2015.2491285](https://doi.org/10.1109/TSC.2015.2491285). in press.
11. [Li YY, Huang YS, et al. Service selection mechanisms in the Internet of Things](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0055) [(IoT): a systematic and comprehensive study. Clust Comput 2020;23:1163–83](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0055).
12. [Adewuyi AA, Cheng H, Shi Q, Cao J, Wang X, Zhou B. SC-TRUST: a dynamic](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0060) [model for trustworthy service composition in the internet of things. IEEE](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0060) [Internet Things J 2022;9(5):3298–312](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0060).
13. Xia H, Li Z, Zheng Y, Liu A, Choi Y, Sekiya H. A novel lightweight subjective trust inference framework in MANETs. IEEE Trans Sustain Comput doi: 10.1109/ TSUSC.2018.2817219.
14. [Fan L, Gary W, et al. A trust model for SLA negotiation candidates selection in a](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0070) [dynamic IoT environment. IEEE Trans Services Comput 2022;15(5):2565–78](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0070).
15. [Wang H, Yang D, et al. Integrating modified cuckoo algorithm and creditability](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0075) [evaluation for QoS-aware service composition. Knowl-Based Syst](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0075) [2019;140:64–81](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0075).
16. [Adomavicius G, Zan H, Tuzhilin A. Personalization and recommender systems.](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0080) [INFORMS Tutorials Operations Res 2014;14(1):55–107](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0080).
17. Ding S, Xia CY, Zhou KL, Yang SL, Shang JS. Decision support for personalized cloud service selection through multi-attribute trustworthiness evaluation. PLoS One 2014;9(6):e97762. doi: [https://doi.org/10.1371/journal.](https://doi.org/10.1371/journal.pone.0097762) [pone.0097762](https://doi.org/10.1371/journal.pone.0097762). PMID: 24972237.
18. [Viriyasitavat W, Xu LD, Bi ZM. User-oriented selections of validators for trust](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0090) [of internet-of thing services. IEEE Trans Ind Inform 2022;18:4859–67](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0090).
19. [Wang HB, Yang DR, Yu Q, Ta Y. Integrating modified cuckoo algorithm and](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0095) [creditability evaluation for QoS-aware service composition. Knowl-Based Syst](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0095) [2018;140:64–81](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0095).
20. Shen L, Chen H, Yu Z, Kang W, Zhang B, Li H, Yang B, Liu D. Evolving support vector machines using fruit fly optimization for medical data classification. Knowl-Based Syst 2016;96:61–75. doi: [https://doi.org/10.1016/j.knosys.2016.](https://doi.org/10.1016/j.knosys.2016.01.002) [01.002](https://doi.org/10.1016/j.knosys.2016.01.002).
21. [Cai B, Li XY, et al. A reliable and lightweight trust inference model for service](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0105) [recommendation in SIoT. IEEE Internet Things J 2022;9(13):10988–1003](http://refhub.elsevier.com/S1110-8665(23)00018-X/h0105).