*future internet*

MDPI

*Article*

# A Bidirectional Trust Model for Service Delegation in Social Internet of Things

**Lijun Wei [1], Yuhan Yang [1], Jing Wu [1], Chengnian Long [1,*] and Yi-Bing Lin [2,3,*]**

[1] Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China; sjtu_weilijun@sjtu.edu.cn (L.W.); yuhanyang@sjtu.edu.cn (Y.Y.); jingwu@sjtu.edu.cn (J.W.)
[2] Department of Computer Science, National Yang Ming Chiao Tung University, Hsinchu 30010, Taiwan
[3] College of Humanities and Sciences, China Medical University, Taichung 406, Taiwan
* Correspondence: longcn@sjtu.edu.cn (C.L.); liny@csie.nctu.edu.tw (Y.-B.L.)

**Abstract:** As an emerging paradigm of service infrastructure, social internet of things (SIoT) applies the social networking aspects to the internet of things (IoT). Each object in SIoT can establish the social relationship without human intervention, which will enhance the efficiency of interaction among objects, thus boosting the service efficiency. The issue of trust is regarded as an important issue in the development of SIoT. It will influence the object to make decisions about the service delegation. In the current literature, the solutions for the trust issue are always unidirectional, that is, only consider the needs of the service requester to evaluate the trust of service providers. Moreover, the relationship between the service delegation and trust model is still ambiguous. In this paper, we present a bidirectional trust model and construct an explicit approach to address the issue of service delegation based on the trust model. We comprehensively consider the context of the SIoT services or tasks for enhancing the feasibility of our model. The subjective logic is used for trust quantification and we design two optimized operators for opinion convergence. Finally, the proposed trust model and trust-based service delegation method are validated through a series of numerical tests.

**Keywords:** trust model; social internet of things; service delegation



**Citation:** Wei, L.; Yang, Y.; Wu, J.; Long, C.; Lin, Y.-B. A Bidirectional Trust Model for Service Delegation in Social Internet of Things. *Future Internet* **2022**, *14*, 135. https://doi.org/10.3390/fi14050135

Academic Editor: Christoph Stach

Received: 9 April 2022
Accepted: 26 April 2022
Published: 29 April 2022



## 1. Introduction

As the 4th industrial revolution and the development of future social interconnection technology, internet of things (IoT), following the internet, brings tremendous changes in people's lives [1–3]. With the continuous intelligence of hardware devices and the maturity of edge computing technology, IoT will have greater scalability [4,5]. Integrating the concept of socialization into the IoT system, the social internet of things (SIoT) [6,7], as a new service paradigm, improves the interoperability among IoT objects and enhances the service efficiency in industry applications. The objects will establish the relationship with each other and collaborate on services without human intervention, which make the objects more autonomous in the process of IoT service. Moreover, the structure of SIoT boosts the network navigability and scalability, which enhances the service discovery and resource acquisition. Currently, the SIoT paradigm has been widely applied in various application scenarios, such as vehicular social networks [8–11], mobile crowdsensing [12–16], data-driven smart city [17–20], etc.

In SIoT, each object (e.g., intelligent sensors, smartphone, and video camera) can be a service requester (SR) or service provider (SP), according to its own motivations. The SR will broadcast the service request, such as collecting sensing tasks or urban noise data, and provide some rewards to the SP. On the other hand, the SP will provide the specific service, such as sharing information or computation resources to the SR, to receive some rewards from the SR. Each IoT object can autonomously determine which service to initiate and which object to delegate within a given set of candidate objects. By this method, the service discovery, interaction, and execution will be optimally implemented.

Although the SIoT paradigm will improve the quality of services to a certain extent, it also may suffer from various types of attacks due to the presence of malicious objects [21]. Some malicious objects may launch bad-mouthing or cheating attacks to affect the decision process of service delegation [22]. To address this issue, in recent years, some works in the literature have presented various trust models to solve the problems of trust establishment and relationship maintenance among objects in SIoT [23,24]. Trust is a complex and comprehensive concept in SIoT [25,26]. Specifically, trust not only reflects the security and reliability at the IoT system level, but also reflects the degree of cooperation between two IoT objects when establishing an interactive relationship. The establishment of trust will stimulate cooperation and improve security in the process of service [27–29]. Castelfranchi and Falcone introduced a systematic socio-cognitive trust theory [27]. They proposed a layered model for trust, which consists of five basic ingredients: trustor, trustee, task, goal, and context. They also proposed and analyzed the important characteristics, including integrated, socio-cognitive, multi-factor and multi-dimensional, dynamic, non-prescriptive, etc. The proposed trust theory can be used as a theoretical foundation for analyzing the trust issue of SIoT. Xia et al. combined the fuzzy logic method to solve the trustworthiness convergence issue and proposed a lightweight mechanism for service discovery based on directed acyclic graph (DAG) [28]. On this basis, Xia et al. proposed a trustworthiness inference framework which combines a kernel-based nonlinear multivariate grey prediction model and fuzzy logic method to quantify the trust [29]. Amin et al. presented a classified catalog of friendliness and trust in SIoT. They described the key ingredients and challenges of friendliness- and trust-based approaches, which contributes to the analysis of the effectiveness of the trust model [30]. Narang and Kar proposed a hybrid trust management framework based on probabilistic neighborhood overlap, which considers the resource-constrained IoT devices [31]. Moreover, they analyzed the various attack scenarios, such as slandering/bad-mouthing attack, Sybil attack, self-promoting attack, and ballot stuffing attack to demonstrate the effectiveness of the proposed model. Chen et al. proposed an integrated trust evaluation model which combines direct and indirect trustworthiness [32,33]. Moreover, they further proposed a series of new metrics, such as friendship similarity, social contact similarity, and community of interest similarity to quantify the indirect trust evaluation. They also applied the typical application scenarios, including air pollution detection and augmented map travel assistance, to illustrate the feasibility of the proposed model. In order to comprehensively compare the recent studies along with advantages and disadvantages, we presented detailed comparison of various works in the literature on the SIoT trust model in our previous work [34].

However, the current research on trust model in SIoT still faces three important challenges. First, most works focus on the unidirectional trust evaluation from the SR to the SP. The evaluation of the trustworthiness of SR is ignored, which may cause the trust crisis from the SPs to the SR. The SPs may gradually lose enthusiasm if they suffer prejudiced treatment of the malicious SR. Second, the trust model and service delegation are context- or environment dependent. The properties of the same task are different in different contexts or environments. Third, the decision of service delegation should not only consider the trust of SPs, but also the utility of the SR. In addition, the correlation between trust and utility is ambiguous.

To address the above challenges, we propose a bidirectional trust model and trust-based service delegation approach by comprehensively considering the trust and utility of service requesters and providers. We combine the social trust theory and characteristics of IoT tasks to formalize the trust evaluation and service delegation model. The main contributions of this paper are as follows:

- In order to improve the quality of the IoT service, we propose the bidirectional evaluation and selection model between the SRs and SPs to formulate the process of service or task in SIoT, thus preventing the malicious behaviors of SRs and SPs.

- A context-aware trust model which comprehensively considers the task properties in the specific environment is presented. We employ the subjective logic to construct the opinion-based and evidence-based trust quantification method.
- We present a trust-based service delegation approach that optimizes the utility of the SR while effectively isolating the malicious SPs. Since the service delegation problem in SIoT seldom considers the trust and utility issue at the same time, this paper explores the correlation of trust and utility and their impacts on the service delegation.
- In order to validate the feasibility of our proposed trust model and service delegation method, we present a series of vital experiments to explain the operation of our model. Our results show that the proposed model can effectively assist the IoT object to make the decision of the service delegation.

The remainder of the paper is organized as follows: the system overview and problem statement are presented in Section 2. On this basis, we present the trust and service delegation model, including the trust quantification method and integrated service delegation mechanism in Section 3. In Section 4, in order to demonstrate the feasibility of proposed trust model, we present a series of experiments. In Section 5, we conclude the paper and summarize the contributions. Moreover, some pending research issues are discussed for further research.

## 2. System Overview and Problem Statement

We consider a general system model in SIoT which consists of five ingredients: (1) service requester (SR), (2) service provider (SP), (3) intermediate object, (4) the context, and the (5) service/task. The life cycle of a task or service is shown in Figure 1. The first step that the SR will perform is to determine the content of the task, including the context, property and goal. It will also publish the task request information. Then, after receiving the message of the task request, the SPs will determine whether to respond to the request by evaluating the trustworthiness of the SR. If the SR is trustworthy from the perspective of the SP, the SP will send a respond message which contains the task price, which is calculated by considering the cost of the task performance. After receiving some response, the SR will delegate the task to the specific SP based on the trust model and the consideration of utility. Then, the delegated SP will perform the task and submit the result. After receiving the result of the task from the delegated SPs, the SR and SP will evaluate each other about their behaviors and update the trust model.

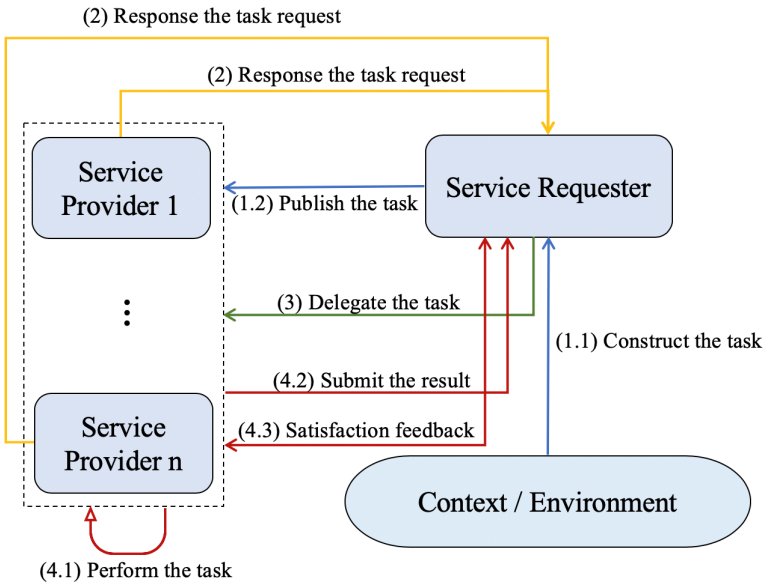



**Figure 1.** The operation framework of the task/service cycle.

Different from the traditional trust-based service delegation model in SIoT, we combine the bidirectional evaluation to construct the trust model and adopt the utility optimization to formulate the service delegation problem. On the one hand, most of the current literature assumed that SR is reliable, which means the trust between the SR and SP is unidirectional. This assumption may be reasonable and useful in the small-scale network or SR-centric situation. However, in the open and large-scale SIoT scenarios, the SR may not be reliable. If there is no bidirectional evaluation, a malicious SR may damage the SP's privacy, or it may delay a payment after the SP submits the task results. On the other hand, the current literature often employs trustworthiness to determine which SP should be delegated, but there is a lack of consideration for utility issues. To this end, we design the trust-based utility formulation for service delegation.

In order to facilitate the formal description, we divide the entire process into four steps, focusing on the decision-making problem of the object in the process of IoT tasks or services.

### *2.1. Step 1: The SR Determines the Content of the Task in the Specific Context*

In the first step, the SR $u_i$ will comprehensively consider the goal of task and the context to construct the content of the task. A task includes the several necessary properties, which reflect the SR requirements. Formally, the task is denoted by $\varphi = \{p_\varphi = \{p_\varphi^1, p_\varphi^2, \ldots, p_\varphi^m\} | G_\varphi\}_C$, where $C$ is the context of the task $\varphi$. $p_\varphi$ represents the properties of task $\varphi$ in the context $C$, and $G_\varphi$ is the goal of the SR $u_i$ for publishing the task $\varphi$.

### *2.2. Step 2: The SPs Determine Whether to Response the Task Request of the SR*

After receiving the request from the SR $u_i$, the SPs will evaluate the trustworthiness of the SR $u_i$ based on the direct interaction records and some recommendation opinions from several intermediate objects. The set of SPs is denoted by $V = \{v_1, v_2, \ldots, v_n\}$. The set of intermediate objects, which have some interactions with the SR, is denoted by $IN_{SR} = \{r_1, r_2, \ldots\}$. The trustworthiness of the SR $u_i$ from the viewpoint of the SP $v_j$ is formulated as

$$\overrightarrow{T}_{u_i \leftarrow v_j}(\varphi) = f_{ct}(\overrightarrow{T}^{d}_{u_i \leftarrow v_j}(\varphi), \{\overrightarrow{T}^{rec}_{u_i \leftarrow r_k}(\varphi)\}_{k=1,2,\ldots}), \tag{1}$$

where $\overrightarrow{T}^{d}_{u_i \leftarrow v_j}(\varphi)$ denotes the direct trust vector of the SR $u_i$ from the viewpoint of the SP $v_j$. Additionally, $\overrightarrow{T}^{rec}_{u_i \leftarrow r_k}(\varphi)$ denotes the recommendation trust of the SR $u_i$ from the viewpoint of the intermediate object $r_k$. The function $f_{ct}$ is the convergence function of the trust opinions from the different sources. Based on the evaluation result of the SR trust, the SP will determine whether to respond to the task request by solving the following formulation:

$$Response_{u_i \leftarrow v_j}(\varphi) \begin{cases} \psi_{v_j}(\varphi), & g(\overrightarrow{T}_{u_i \leftarrow v_j}(\varphi)) \geq th_v(\varphi) \\ null, & g(\overrightarrow{T}_{u_i \leftarrow v_j}(\varphi)) < th_v(\varphi). \end{cases} \tag{2}$$

where $th_v(\varphi)$ is a response threshold set by $v_j$ for the task $\varphi$, and $\psi_{v_j}(\varphi)$ denotes the price that SR $u_i$ needs to pay to the SP $v_j$ if $u_i$ delegates $v_j$ to perform task $\varphi$. $g(\cdot)$ denotes the function of the trustworthiness calculation.

### *2.3. Step 3: The SR Delegates the Task to the SP*

After receiving several responses, the SR $u_i$ will consider the factors of trust and utility to make a decision of service delegation. Similar to the process of trust evaluation of the SR from the viewpoint of the SP in step 2, the trust of the SP $v_j$ from the viewpoint of the SR $u_j$ is formulated as

$$\overrightarrow{T}_{v_j \leftarrow u_i}(\varphi) = f_{ct}(\overrightarrow{T}^{d}_{v_j \leftarrow u_i}(\varphi), \{\overrightarrow{T}^{rec}_{v_j \leftarrow s_k}(\varphi)\}_{k=1,2,\ldots}), \tag{3}$$

where $s_k$ denotes the intermediate objects which have some interactions with the SP $v_j$. Based on the trust analysis, the SR will determine the delegated SP by solving the following formulation:

$$\begin{aligned} DSP &= \arg\max_{v_j} \ f_{tu}(\overrightarrow{T}_{v_j \leftarrow u_i}(\varphi), \psi_{v_j}(\varphi)), \\ s.t. \quad & g(\overrightarrow{T}_{v_j \leftarrow u_i}(\varphi)) \geq th_u(\varphi) \end{aligned} \tag{4}$$

where $f_{tu}$ is the delegation function that calculates the integrated index for service delegation. $th_u(\varphi)$ is a trust threshold set by $u_i$ for the task $\varphi$.

### *2.4. Step 4: The Delegated SP Performs the Task and Submits the Result, and Then the SR and SP Will Mutually Comment Each Other*

After receiving the delegation message from the SR, the delegated SP (we assume $v_j$) will perform the task and submit the result. After that, the SR will evaluate the result according to the accuracy, real-time, etc., of the task performance to decide the success or failure of the task. The SR's evaluation of the task is denoted by $Y^{t_\varphi}_{v_j \leftarrow u_i}(\varphi)$, where $t_\varphi$ is the occurred time of the task $\varphi$. If the SR is satisfied according to the SP's performance, the $Y^{t_\varphi}_{v_j \leftarrow u_i}(\varphi)$ will be set 1, and it will be set $-1$ if the SR is unsatisfied. Similarly, the SP will also evaluate the SR's behavior in the process of the task, which is denoted by $Y^{t_\varphi}_{u_i \leftarrow v_j}(\varphi)$. If the SP is satisfied, then the $Y^{t_\varphi}_{u_i \leftarrow v_j}(\varphi)$ will be set 1, and it will be set $-1$ if the SP feels unsatisfied.

### *2.5. Problem Statement*

According to the previous description, we can find that in the entire service delegation process, the most important part lies in the rules for mutual trust evaluation between objects, and how to use the trust evaluation information to make decisions. The first important problem is the structuralization of the interactions and the calculation of the direct trust.

***Problem Statement 1:*** *Based on historical interaction records between object A and object B, how does object A determine the direct trust of object B?*

The recommended trust opinions from intermediate objects can be great references for object A to evaluate the trust of object B. However, trust opinions from different sources should have different degrees of confidence. For example, we usually believe in information from reliable sources. Therefore, how to effectively quantify the confidence of information from different sources will be the second important problem.

***Problem Statement 2:*** *When intermediate object C provides A with trust opinions about object B, how will A integrate the opinions of C?*

The success of task execution is seriously related to the delegation decision of the SR, so in the process of service delegation, the SR must carefully evaluate the reliability of SPs. Establishing trust is a suitable way to evaluate the reliability of an object. However, the SR will not only consider trust, but also its own benefits in the delegation process. Therefore, how to comprehensively consider both trust and utility so as to ensure that a relatively reliable SP is selected and optimize the utility of SR is the third important problem.

***Problem Statement 3:*** *According to the trust of the candidate objects, how does object A delegate the task?*

In summary, *Problem 1* corresponds to the quantitative calculation of $T^{d}_{v_j \leftarrow u_i}(\varphi)$. *Problem 2* corresponds to the formulation of Equation (1). In addition, *Problem 3* corresponds to the formulation of Equation (4).

## 3. Trust and Service Delegation Model

### *3.1. Trust Model*

In our trust model, the direct interactions and indirect opinions are comprehensively considered. We employ subjective logic for the trust analysis. The results of the trust analysis and utility analysis are integrated for the decision of the service delegation. The whole design framework is shown in Figure 2. Next, we detail the entire trust analysis and service delegation process.

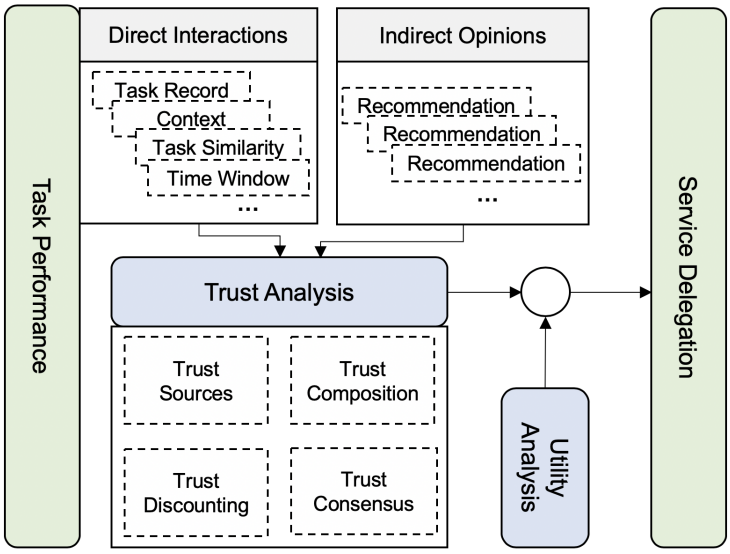



**Figure 2.** The design framework of the trust model and service delegation.

#### 3.1.1. Subjective Logic

Subjective logic is an uncertain probabilistic logic that was initially introduced by Audun Jøsang to address formal representations of trust [35]. The subjective logic constructs a bijective mapping between opinion space and evidence space, which can help SR to form its own opinion based on the existing direct evidence, and to integrate the recommendation opinions from others to form a comprehensive opinion.

**Definition 1** (Opinion Space)**.** *A's direct opinion about object B for the task $\varphi$ is a vector:*

$$\overrightarrow{T}_{B \leftarrow A}(\varphi) = (b_{B \leftarrow A}(\varphi), d_{B \leftarrow A}(\varphi), u_{B \leftarrow A}(\varphi), a_{B \leftarrow A}(\varphi)), \tag{5}$$

*where $b_{B \leftarrow A}(\varphi)$ represents the degree to which A believes B will successfully perform the task $\varphi$, and $d_{B \leftarrow A}(\varphi)$ represents the degree to which A disbelieves that B will successfully perform the task $\varphi$. $u_{B \leftarrow A}(\varphi)$ represents the degree to which A is uncertain about whether B will successfully perform the task $\varphi$, and $a_{B \leftarrow A}(\varphi)$ is the base rate. The opinion satisfies the additivity requirement as follows:*

$$b_{B \leftarrow A}(\varphi) + d_{B \leftarrow A}(\varphi) + u_{B \leftarrow A}(\varphi) = 1, \tag{6}$$

*and the projected probability of the opinion $\overrightarrow{T}_{B \leftarrow A}(\varphi)$ is defined as*

$$\hat{T}_{B \leftarrow A}(\varphi) = b_{B \leftarrow A}(\varphi) + a_{B \leftarrow A}(\varphi) u_{B \leftarrow A}(\varphi). \tag{7}$$

In our trust model, we use $\overrightarrow{T}^{d}_{B\leftarrow A}(\varphi)$ to represent the direct trust vector of object B from the viewpoint of object A for the task $\varphi$. $\hat{T}^{d}_{B\leftarrow A}(\varphi)$ is used for representing the projected trustworthiness of object B.

Evidences are fundamental for forming opinions, which can be presented as a series of the binary comments such as "satisfaction" and "dissatisfaction". The amount of evidence will affect the certainty of the opinion. In subjective logic, the Beta function is used for constructing the evidence space. The probability density function is as follows:

$$Beta(p_x, \alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p_x^{\alpha-1}(1-p_x)^{\beta-1}, \tag{8}$$

where $\Gamma()$ is the gamma function. The beta function can be used to represent the probability distribution of binary events. Therefore, the evidence space can be defined as follows:

**Definition 2** (Evidence Space)**.** *An evidence space can be depicted by a beta probability distribution:*

$$Beta(\overrightarrow{T}'^{d}_{B\leftarrow A}(\varphi), \alpha_{B\leftarrow A}(\varphi), \beta_{B\leftarrow A}(\varphi)), \tag{9}$$

*where* $\overrightarrow{T}'^{d}_{B\leftarrow A}(\varphi)$ *represents the direct trust vector of B from the viewpoint of A in evidence space.* $\alpha_{B\leftarrow A}(\varphi)$ *and* $\beta_{B\leftarrow A}(\varphi)$ *are defined as:*

$$\begin{cases} \alpha_{B\leftarrow A}(\varphi) = \gamma_{B\leftarrow A}(\varphi) + 2a_{B\leftarrow A}(\varphi) \\ \beta_{B\leftarrow A}(\varphi) = \overline{\gamma}_{B\leftarrow A}(\varphi) + 2(1 - a_{B\leftarrow A}(\varphi)) \end{cases} \tag{10}$$

*where* $\gamma_{B\leftarrow A}(\varphi)$ *and* $\overline{\gamma}_{B\leftarrow A}(\varphi)$ *are the evidence strength which is based on the historical interactions between objects A and B.* $\gamma_{B\leftarrow A}(\varphi)$ *denotes the positive evidence strength, which indicates that the B is trustworthy.* $\overline{\gamma}_{B\leftarrow A}(\varphi)$ *denotes the negative evidence strength, which indicates that B is untrustworthy.*

*The expected probability* $E(\overrightarrow{T}'^{d}_{B\leftarrow A}(\varphi))$ *is defined as the projected trustworthiness in evidence space, which is expressed as follows:*

$$\begin{aligned} \widetilde{T}^{d}_{B\leftarrow A}(\varphi) = E(\overrightarrow{T}'^{d}_{B\leftarrow A}(\varphi)) &= \frac{\alpha_{B\leftarrow A}(\varphi)}{\alpha_{B\leftarrow A}(\varphi) + \beta_{B\leftarrow A}(\varphi)} \\ &= \frac{\gamma_{B\leftarrow A}(\varphi) + 2a_{B\leftarrow A}(\varphi)}{\gamma_{B\leftarrow A}(\varphi) + \overline{\gamma}_{B\leftarrow A}(\varphi) + 2} \end{aligned} \tag{11}$$

The bijective mapping between the trust vector in opinion space and the trust vector in the evidence space emerges from the intuitive requirement $\hat{T}^{d}_{B\leftarrow A}(\varphi) = \widetilde{T}^{d}_{B\leftarrow A}(\varphi)$, which is defined as follows.

**Definition 3** (Mapping between opinion space and evidence space)**.**

$$\begin{cases} b_{B\leftarrow A}(\varphi) = \frac{\gamma_{B\leftarrow A}(\varphi)}{\gamma_{B\leftarrow A}(\varphi)+\overline{\gamma}_{B\leftarrow A}(\varphi)+2} \\ d_{B\leftarrow A}(\varphi) = \frac{\overline{\gamma}_{B\leftarrow A}(\varphi)}{\gamma_{B\leftarrow A}(\varphi)+\overline{\gamma}_{B\leftarrow A}(\varphi)+2} \\ u_{B\leftarrow A}(\varphi) = \frac{2}{\gamma_{B\leftarrow A}(\varphi)+\overline{\gamma}_{B\leftarrow A}(\varphi)+2} \end{cases} \tag{12}$$

$$\begin{cases} \gamma_{B\leftarrow A}(\varphi) = \frac{2b_{B\leftarrow A}(\varphi)}{u_{B\leftarrow A}(\varphi)} \\ \overline{\gamma}_{B\leftarrow A}(\varphi) = \frac{2d_{B\leftarrow A}(\varphi)}{u_{B\leftarrow A}(\varphi)} \end{cases} \tag{13}$$

#### 3.1.2. Direct Trust

In this paragraph, we introduce the direct trust which is based on the direct interaction records between objects A and B.

- **Task Similarity**

Due to the different context of each task, the importance of different past interaction comments to the current task is different and should be decided by the task similarity. To this end, we use the Jaccard Similarity Index to estimate the similarity of two task in the different context, which is expressed as follows.

$$Sim(\varphi, \varphi') = J(p_\varphi, p_{\varphi'}) = \frac{|p_\varphi \cap p_{\varphi'}|}{|p_\varphi \cup p_{\varphi'}|} \tag{14}$$

For a simple example, we assume there are, in total, four properties, such as {"High Definition", "Least Memory", "Location Range", "Real-Time", and "Measurement Accuracy"}. If the property is required in the task, then the corresponding value of the property vector is set to "1" and otherwise "0". If the $\varphi$ is a video monitoring task, then the $p_\varphi$ may be equal to {1, 1, 1, 1, 0}. If the $\varphi'$ is crowdsensing noise monitoring, then the $p_{\varphi'}$ may be equal to {0, 1, 1, 0, 1}. Then the similarity between $\varphi$ and $\varphi'$ is equal to 2/5.

- **Time Window**

The evidence is time dependent. Recent task performance has a greater effect than the older task on the trust evaluation of the object. The time window is presented for the time-dependent strength of single evidence, which is shown in Figure 3.

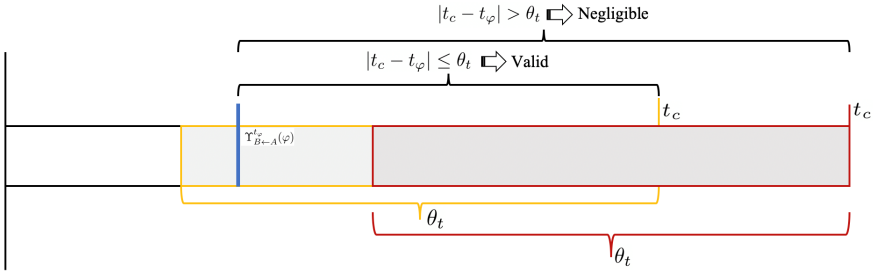



**Figure 3.** The design of time window for trust evaluation.

Based on the time window, the strength of single evidence can be expressed as follows:

$$\hat{\Upsilon}^{t_\varphi}_{B\leftarrow A}(\varphi) = \begin{cases} \Upsilon^{t_\varphi}_{B\leftarrow A}(\varphi) e^{-\lambda(t_c - t_\varphi)}, & |t_c - t_\varphi| \leq \theta_t. \\ 0, & |t_c - t_\varphi| > \theta_t. \end{cases} \tag{15}$$

where $t_c$ denotes the current time and $\lambda$ denotes the decay factor, which affects the rate of decay of the evidence strength.

- **Evidence Strength**

By aggregating the valid direct interaction records, that is, a batch of valid single evidence, we can calculate the total strength of direct evidences as follows:

$$\gamma^d_{B\leftarrow A}(\varphi) = \sum_{\hat{\Upsilon}^{t_\varphi}_{B\leftarrow A}(\varphi')>0} \hat{\Upsilon}^{t_\varphi}_{B\leftarrow A}(\varphi') Sim(\varphi, \varphi'), \tag{16}$$

$$\overline{\gamma}^d_{B\leftarrow A}(\varphi) = -\sum_{\hat{\Upsilon}^{t_\varphi}_{B\leftarrow A}(\varphi')<0} \hat{\Upsilon}^{t_\varphi}_{B\leftarrow A}(\varphi') Sim(\varphi, \varphi'). \tag{17}$$

- **Direct Trust Calculation**

By combining the methods of task similarity, time window, and evidence strength, we can calculate the direct trust vector $\overrightarrow{T}^d_{B\leftarrow A}(\varphi)$ of the object B from the viewpoint of A for the task $\varphi$ by substituting Equations (16) and (17) into (12). Therefore, the *problem 1* is addressed through the above design and analysis.

3.1.3. Indirect Trust

In addition to direct trust evaluation, A will also ask C and D for relevant opinions about B. This paragraph solves the fusion problem of recommendation opinions by designing the discounting and consensus operators. The recommendation opinions from objects C and D are expressed as follows, respectively.

$$\overrightarrow{T}^{rec}_{B\leftarrow C}(\varphi) = (b_{B\leftarrow C}(\varphi), d_{B\leftarrow C}(\varphi), u_{B\leftarrow C}(\varphi), a_{B\leftarrow C}(\varphi)) \tag{18}$$

$$\overrightarrow{T}^{rec}_{B\leftarrow D}(\varphi) = (b_{B\leftarrow D}(\varphi), d_{B\leftarrow D}(\varphi), u_{B\leftarrow D}(\varphi), a_{B\leftarrow D}(\varphi)) \tag{19}$$

The objective in this part is to construct the suitable function $f_{ind}(\cdot)$ to integrate the $\overrightarrow{T}^{rec}_{B\leftarrow D}(\varphi)$ and $\overrightarrow{T}^{rec}_{B\leftarrow C}(\varphi)$, which is formulated as follows:

$$\overrightarrow{T}^{ind}_{B\leftarrow A}(\varphi) = f_{ind}(\overrightarrow{T}^{rec}_{B\leftarrow C}(\varphi), \overrightarrow{T}^{rec}_{B\leftarrow D}(\varphi)), \tag{20}$$

and $\overrightarrow{T}^{ind}_{B\leftarrow A}(\varphi) = (b^{ind}_{B\leftarrow A}, d^{ind}_{B\leftarrow A}, u^{ind}_{B\leftarrow A}, a^{ind}_{B\leftarrow A})$.

- **Discounting and Consensus Operator**

In the subjective logic framework, the discounting rule does not have a natural interpretation of evidence handling [36]. To this end, we use the trust in opinion space to discount the trust in evidence space. The ideas and principles are shown in Figure 4. We use the symbol $\otimes$ to represent the discounting operator. Thus we have $\overrightarrow{T}^{ind}_{B\leftarrow C\leftarrow A}(\varphi) = \overrightarrow{T}^{rec}_{B\leftarrow C}(\varphi) \otimes \overrightarrow{T}^{d}_{C\leftarrow A}(\varphi)$.

The specific discounting rule $\otimes$ in evidence space is shown as follows.

$$\begin{cases} \gamma^{ind}_{B\leftarrow C\leftarrow A}(\varphi) = \hat{T}^{d}_{C\leftarrow A}(\varphi)\gamma^{rec}_{B\leftarrow C}(\varphi) \\ \overline{\gamma}^{ind}_{B\leftarrow C\leftarrow A}(\varphi) = \hat{T}^{d}_{C\leftarrow A}(\varphi)\overline{\gamma}^{rec}_{B\leftarrow C}(\varphi) \end{cases} \tag{21}$$

Based on Equations (12) and (21), we can calculate the indirect trust vector $\overrightarrow{T}^{ind}_{B\leftarrow C\leftarrow A}(\varphi)$, which is shown as follows.

$$\begin{cases} b^{ind}_{B\leftarrow C\leftarrow A}(\varphi) = \frac{\hat{T}^{d}_{C\leftarrow A}(\varphi)b^{rec}_{B\leftarrow C}(\varphi)}{\hat{T}^{d}_{C\leftarrow A}(\varphi)b^{rec}_{B\leftarrow C}(\varphi)+\hat{T}^{d}_{C\leftarrow A}(\varphi)d^{rec}_{B\leftarrow C}(\varphi)+u^{rec}_{B\leftarrow C}(\varphi)} \\ d^{ind}_{B\leftarrow C\leftarrow A}(\varphi) = \frac{\hat{T}^{d}_{C\leftarrow A}(\varphi)d^{rec}_{B\leftarrow C}(\varphi)}{\hat{T}^{d}_{C\leftarrow A}(\varphi)b^{rec}_{B\leftarrow C}(\varphi)+\hat{T}^{d}_{C\leftarrow A}(\varphi)d^{rec}_{B\leftarrow C}(\varphi)+u^{rec}_{B\leftarrow C}(\varphi)} \\ u^{ind}_{B\leftarrow C\leftarrow A}(\varphi) = \frac{u^{rec}_{B\leftarrow C}(\varphi)}{\hat{T}^{d}_{C\leftarrow A}(\varphi)b^{rec}_{B\leftarrow C}(\varphi)+\hat{T}^{d}_{C\leftarrow A}(\varphi)d^{rec}_{B\leftarrow C}(\varphi)+u^{rec}_{B\leftarrow C}(\varphi)} \\ a^{ind}_{B\leftarrow C\leftarrow A}(\varphi) = \hat{T}^{d}_{C\leftarrow A}(\varphi)a^{rec}_{B\leftarrow A}(\varphi) \end{cases} \tag{22}$$

The consensus operator is designed for integrating the recommendation opinions from different sources. We use the weighted sum method to design the consensus operator. Similar to the design idea of discounting operator, we use the trust in opinion space as weight parameters. The symbol $\oplus$ represents the consensus operator, and thus we have $\overrightarrow{T}^{ind}_{B\leftarrow A}(\varphi) = \overrightarrow{T}^{ind}_{B\leftarrow CD\leftarrow A}(\varphi) = \overrightarrow{T}^{ind}_{B\leftarrow C\leftarrow A}(\varphi) \oplus \overrightarrow{T}^{ind}_{B\leftarrow D\leftarrow A}(\varphi)$. The specific consensus operator in evidence space is shown as follows.

$$\begin{cases} \gamma^{ind}_{B\leftarrow A}(\varphi) = \frac{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))\gamma^{ind}_{B\leftarrow C\leftarrow A}(\varphi)+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))\gamma^{ind}_{B\leftarrow D\leftarrow A}(\varphi)}{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))} \\ \overline{\gamma}^{ind}_{B\leftarrow A}(\varphi) = \frac{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))\overline{\gamma}^{ind}_{B\leftarrow C\leftarrow A}(\varphi)+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))\overline{\gamma}^{ind}_{B\leftarrow D\leftarrow A}(\varphi)}{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))} \end{cases} \tag{23}$$

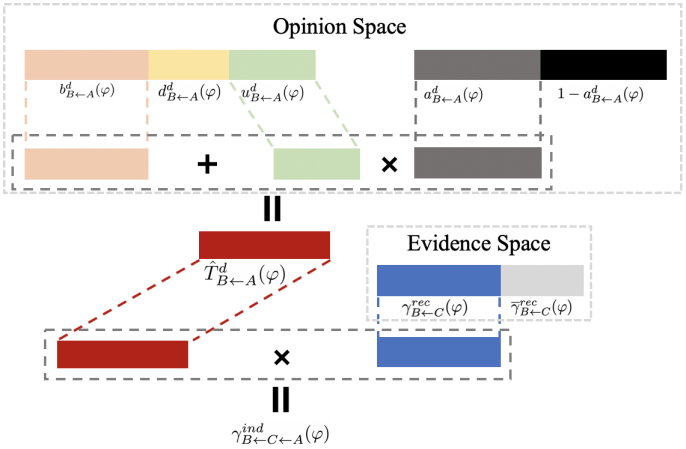



**Figure 4.** The design of discounting operator.

- **Indirect Trust Calculation**

From Equations (12) and (23), we obtain the indirect trust vector $\overrightarrow{T}^{ind}_{B\leftarrow A}(\varphi)$:

$$\begin{cases} b^{ind}_{B\leftarrow A}(\varphi) = \frac{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))u^{ind}_{B\leftarrow D\leftarrow A}(\varphi)b^{ind}_{B\leftarrow C\leftarrow A}(\varphi)+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi)))b^{ind}_{B\leftarrow C\leftarrow A}(\varphi)b^{ind}_{B\leftarrow D\leftarrow A}(\varphi)}{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))u^{ind}_{B\leftarrow D\leftarrow A}(\varphi)+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))u^{ind}_{B\leftarrow C\leftarrow A}(\varphi)} \\ d^{ind}_{B\leftarrow A}(\varphi) = \frac{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))u^{ind}_{B\leftarrow D\leftarrow A}(\varphi)d^{ind}_{B\leftarrow C\leftarrow A}(\varphi)+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))u^{ind}_{B\leftarrow C\leftarrow A}(\varphi)d^{ind}_{B\leftarrow D\leftarrow A}(\varphi)}{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))u^{ind}_{B\leftarrow D\leftarrow A}(\varphi)+(1-u^{ind}_{B\leftarrow D\leftarrow A})(\varphi)u^{ind}_{B\leftarrow C\leftarrow A}(\varphi)} \\ u^{ind}_{B\leftarrow A}(\varphi) = \frac{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))u^{ind}_{B\leftarrow C\leftarrow A}(\varphi)u^{ind}_{B\leftarrow D\leftarrow A}(\varphi)+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))u^{ind}_{B\leftarrow C\leftarrow A}(\varphi)u^{ind}_{B\leftarrow D\leftarrow A}(\varphi)}{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))u^{ind}_{B\leftarrow D\leftarrow A}(\varphi)+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))u^{ind}_{B\leftarrow C\leftarrow A}(\varphi)} \\ a^{ind}_{B\leftarrow A}(\varphi) = \frac{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))a^{ind}_{B\leftarrow C\leftarrow A}(\varphi)+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))a^{ind}_{B\leftarrow D\leftarrow A}(\varphi)}{(1-u^{ind}_{B\leftarrow C\leftarrow A}(\varphi))+(1-u^{ind}_{B\leftarrow D\leftarrow A}(\varphi))} \end{cases} \tag{24}$$

Therefore, we have the indirect trust calculation function

$$\begin{aligned} &f_{ind}(\overrightarrow{T}^{rec}_{B\leftarrow C}(\varphi), \overrightarrow{T}^{rec}_{B\leftarrow D}(\varphi)) = \\ &(\overrightarrow{T}^{rec}_{B\leftarrow C}(\varphi) \otimes \overrightarrow{T}^{d}_{C\leftarrow A}(\varphi)) \oplus (\overrightarrow{T}^{rec}_{B\leftarrow D}(\varphi) \otimes \overrightarrow{T}^{d}_{D\leftarrow A}(\varphi)). \end{aligned} \tag{25}$$

#### 3.1.4. Compositive Trust

The compositive trust is the fusion of direct trust and indirect trust. We also use the consensus operator to fuse them. From Equations (3) and (25), we have

$$\begin{aligned} \overrightarrow{T}_{B\leftarrow A}(\varphi) &= f_{ct}(\overrightarrow{T}^{d}_{B\leftarrow A}(\varphi), \overrightarrow{T}^{rec}_{B\leftarrow C}(\varphi), \overrightarrow{T}^{rec}_{B\leftarrow D}(\varphi)) \\ &= \overrightarrow{T}^{d}_{B\leftarrow A}(\varphi) \oplus \overrightarrow{T}^{ind}_{B\leftarrow A}(\varphi) \\ &= \overrightarrow{T}^{d}_{B\leftarrow A}(\varphi) \oplus [(\overrightarrow{T}^{rec}_{B\leftarrow C}(\varphi) \otimes \overrightarrow{T}^{d}_{C\leftarrow A}(\varphi)) \oplus (\overrightarrow{T}^{rec}_{B\leftarrow D}(\varphi) \otimes \overrightarrow{T}^{d}_{D\leftarrow A}(\varphi))]. \end{aligned} \tag{26}$$

Therefore, *problem 2* is addressed through the above design and analysis.

### *3.2. Service Delegation Mechanism*

After calculating the trust vector of the SP $v_j$ based on the method proposed at last subsection, we further study the issue of service delegation. In SIoT, the SR $u_i$ will not only consider the trust of the SP $v_j$, but also concern the utility. Therefore, we present the trust-based service delegation method to solve the *Problem 3*. We define the decision function of service delegation as follows:

$$\begin{aligned} U_{v_j\leftarrow u_i}(\varphi) &= f_{tu}(\overrightarrow{T}_{v_j\leftarrow u_i}(\varphi), \psi_{v_j}(\varphi)) \\ &= \hat{T}_{v_j\leftarrow u_i}(\varphi)(\zeta_{u_i}(\varphi) - \psi_{v_j}(\varphi)) + (d_{v_j\leftarrow u_i}(\varphi) + (1 - a_{v_j\leftarrow u_i}(\varphi))u_{v_j\leftarrow u_i})(-\overline{\zeta}_{u_i}(\varphi)), \end{aligned} \tag{27}$$

where $\psi_{v_j}(\varphi)$ denotes the benefit value when the task is successful and $\overline{\zeta}_{u_i}(\varphi)$ denotes the lost value when the task is failed. Therefore, the decision of the service delegation (e.g., Equation (4)) can be rewritten as follows:

$$\begin{aligned} DSP &= \arg\max_{v_j} \ U_{v_j \leftarrow u_i}(\varphi) \\ s.t. \quad & \hat{T}_{v_j \leftarrow u_i}(\varphi)) \geq th_u(\varphi) \end{aligned} \tag{28}$$

Through the proposed decision-making method for service delegation, the SR can make a plan to maximize its own utility under the consideration of trust of SPs. For the entire SIoT system, on the one hand, our proposed method can guarantee a high task success rate based on trust analysis. On the other hand, we can improve the overall social welfare and boost the cooperation.

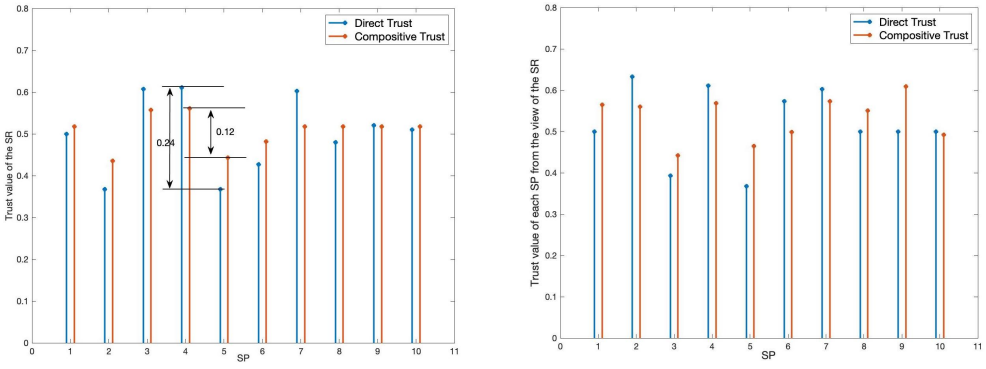
## 4. Simulation and Results

In order to verify the validity of the subjective logic-based trust model proposed in this section, this study conducts experiments based on the Netlogo experimental platform [37]. NetLogo is an agent-based programming language, which is useful to simulate the interaction among objects and monitor the state changes in a simulative SIoT environment. The construction of the experimental platform is based on our previous work [38]. The trust evaluation mechanism module and service delegation module are adjusted based on the aforementioned bidirectional model. The experiments are divided into the following parts: First, after the interactive experiment, the results of the bidirectional trust evaluation of SPs to SR and SR to SPs are observed to test the effectiveness of subjective logic in the process of trust evaluation. On this basis, the impact of similarity of the services/tasks and positive evaluation rates on trust evaluation results are analyzed. Then, the influence of the number of recommenders on the compositive trust evaluation results is analyzed, and finally the benefits of SR and the changes in the number of responding SPs are measured.

This study defines the rate of positive evidence (RPE) as the proportion of the number of simulated service results that are rated as "positive—that is, satisfied" in the total number of service evaluations. Similarity, the rate of task similarity (RTS) is the similarity of the attributes among the services. For example, when the similarity is 40%, it means that 40% attributes of randomly generated services in the network are consistent. In this experiment, a total of 110 virtual nodes are deployed for service interaction, of which 10 nodes are employed as SRs and 100 nodes are employed as SPs. At the same time, the above virtual nodes will also serve as intermediate nodes in the process of trust evaluation to provide recommendations.

### *4.1. Comparison of SR and SPs' Basic Bidirectional Trust Evaluation Results*

In this part of the experiment, the positive evaluation rate is set to 50%, and the task similarity is 40%. The experiment runs 500 ticks, and one service/task is executed in each tick. In addition, 10 SPs and 1 SR were randomly selected for observation. Figure 5a,b shows the trust evaluation results of 10 SPs and SR. As shown in Figure 5a, compared with the direct trust evaluation results of each SP, the compositive trust evaluation results for SR have less difference and more comprehensive opinions, which reflects that the evaluation method based on subjective logic can better integrate the recommendations from different sources so that most SPs can have a more consistent evaluation for SR. Similarly, as shown in Figure 5b, after the SR obtains the recommendations of other intermediate nodes in the network, it obtains the integrated evaluation results of each SP's trust. It can be seen that the recommendations of other intermediate nodes will facilitate the SR to make a more accurate evaluation on the trustworthiness of SPs.

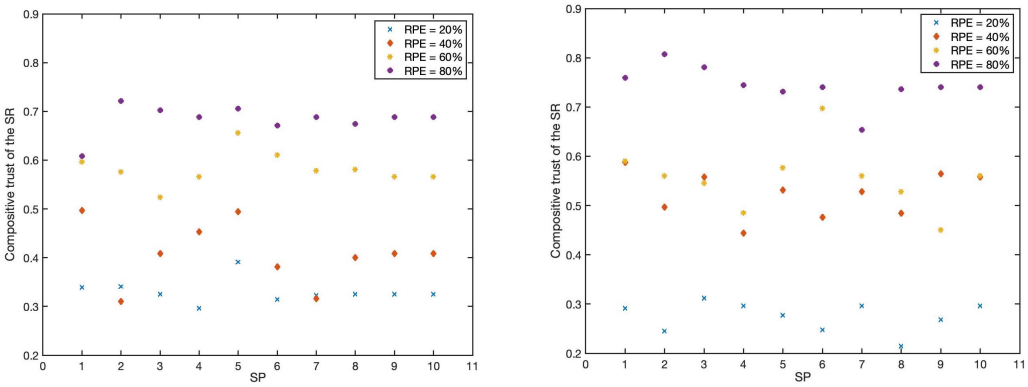



(**a**) Trust evaluation of SR. (**b**) Trust evaluation of SPs.

**Figure 5.** Bidirectional trust evaluation of SR and SPs.

*4.2. The Influence of RPE and RTS on the Results of Trust Evaluation*

This part of the experiment analyzes the impact of RPE and RTS on the evaluation of SR's trust. As shown in Figure 6a, with the increase in the positive evaluation rate, the trust evaluation result of the object will be improved to a certain extent. However, this improvement still has certain limitations. The evaluation results of some SPs for SR may decrease with the increase in RPE. The main reason is that due to the low similarity of tasks. Although some service evaluation opinions are positive or satisfactory, the evidence strength is slight.




(**a**) Trust evaluation of SR when RTS = 40%. (**b**) Trust evaluation of SR when RTS = 80%.

**Figure 6.** Trust evaluation of SR with different RPE and RTS.

As shown in Figure 6b, compared with the case where the task similarity is 40%, when the task similarity is 80%, the attributes between tasks are more similar. Therefore, the evidence strength of a single evidence will be increased, which will make the formation of the trust evaluation more accurate and reliable. Compared with Figure 6a, the upper and lower boundaries in Figure 6b are larger, and the differences among different RPE groups are more obvious. It can be demonstrated that when the task similarity is greater, the object can provide more accurate recommendations, thereby forming a more accurate trust evaluation result.

*4.3. The Influence of the Number of Recommenders on the Trust Evaluation*

In the process of trust evaluation for a certain SP, the SR needs to collect the recommendation opinions from the intermediate nodes to form a more accurate trust point of view. As shown in Figure 7, when the number of the recommenders is 0, it indicates that the trust value of SP to form the viewpoint of the SR is completely evaluated based on direct experience. Along with the number of recommenders gradually increasing, the SR

can collect more recommendation opinions. From the experimental results of this group, it can be seen that when the number of recommendation opinions is equal to or greater than 6, the SR's trust evaluation opinion on SP tends to be stable, and the SR can more accurately identify the honest and trustworthy SP while avoiding wrongly delegating malicious or negative SPs. Therefore, in order to better evaluate the trustworthiness of the SP, the SR needs to obtain as many recommendations from intermediate nodes as possible during the service delegation process.

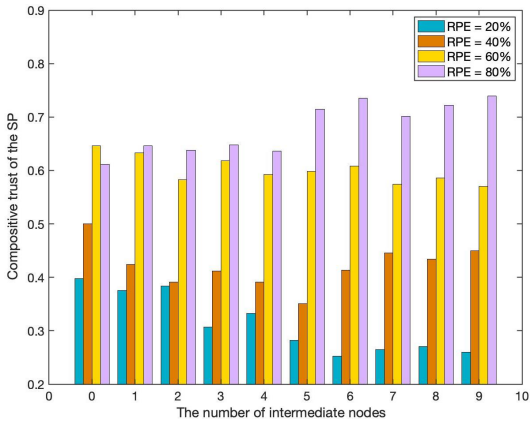
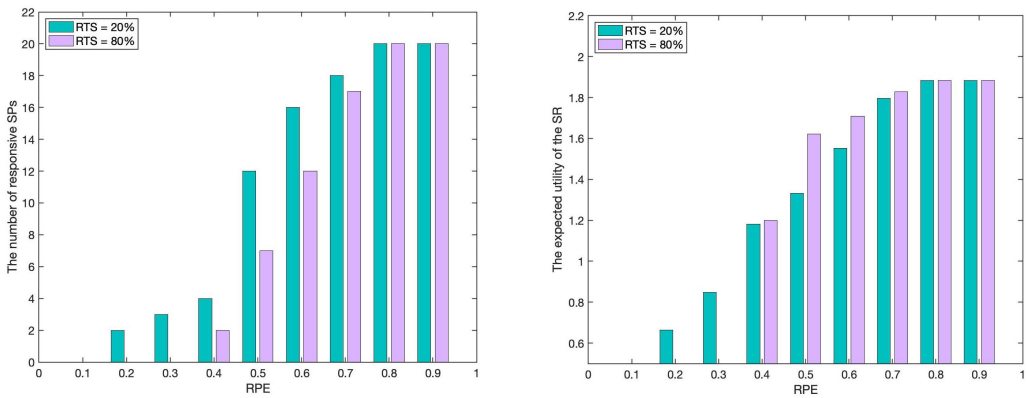



**Figure 7.** Trust evaluation of the SP with different number of intermediate nodes.

### *4.4. Quantity of Responsive SPs and Benefit Analysis of the SR under the Bidirectional Trust Evaluation*

Figure 8 shows the number of responsive SPs and benefits of the SR when the RPE is from 10% to 90% for a certain task. It can be seen that when the RPE is less than 0.5 and the RTS is large, there are more negative opinions referenced. Therefore, the trust evaluation result of SR from the viewpoint of SPs is generally low, and few SPs respond. Therefore, the SR cannot select a suitable SP, and the income is low. With the increase in RPE, the trustworthiness of the SR increases and the number of responding SPs gradually increases, so the SR can obtain a better delegation scheme, which improves the overall revenue. In addition, in the case of small RPE, although the expected benefit of SR is higher when the RTS is lower (the reason is that some SPs cannot correctly estimate the trustworthiness of SR, resulting in a wrong response to the service), it may lead to lower service quality of SPs and failure to guarantee the benefits of SPs. Higher RTS will lead to more accurate bidirectional evaluation results, and more SPs choose not to respond to the service request when RPE is low. On the other hand, in the case of higher RPE, higher RTS will make the bidirectional evaluation between SPs and SR more accurate, so the overall benefit of the SR will be higher.




(**a**) The number of responsive SPs with different RPE. (**b**) Expected utility of the SR with different RPE.

**Figure 8.** The number of responsive SPs and the SR's utility with different RPE.

## 5. Conclusions and Discussions

In this article, we studied the trust-based service delegation problem in SIoT. Considering the bidirectionality of trust, we design a framework of the trust model and service delegation. On this basis, we propose a bidirectional trust evaluation method based on subjective logic. We have shown that by using this formulation, the SR and SP can quantitatively evaluate the trust of each other in a reasonable way. In addition, we consider the context of the task to ensure the feasibility of our model in the SIoT scenario. The task similarity and time window are presented for the calculation of evidence strength. The convergence operators including discounting and consensus operator are constructed for compositive trust quantification. The decision-making approach of the service delegation with comprehensive consideration of trust and utility is proposed to ensure the success of the task while improving the utility of the SR.

However, the current work is in infancy. First, considering the computational complexity, the proposed model simplifies the condition setting to a certain extent. The evidence composition in evidence space only includes service attributes, bidirectional service evaluation information, service time, etc., without considering the relationships between device characteristics of IoT objects and service properties. Therefore, our proposed model is more suitable for the scenarios where the degree of heterogeneity and differentiation of IoT devices is low. The evidence-based descriptions of the characteristics of IoT devices and the relationship between these evidence-based descriptions and opinions will be our important future work. Second, with the development of the Internet of Things, some new architectures, such as multiple internets of things, are proposed. Therefore, we will further evaluate whether our model can be feasible and adaptive for various paradigms [39–41]. Moreover, we plan to extend this model and configure a real-world application scenario in order to make it more capable. The task simulations at different network scales will be carried out in the following research process to validate the effectiveness and practicability of our trust model and service delegation method. Furthermore, testing under different attack environments will be also further provided.

**Author Contributions:** Conceptualization, L.W., C.L. and Y.-B.L.; Methodology, L.W. and J.W.; Software, L.W. and Y.Y.; Validation, L.W., Y.Y., J.W., C.L. and Y.-B.L.; Formal Analysis, L.W. and C.L.; Investigation, L.W., Y.Y. and J.W.; Writing—original Draft Preparation, L.W., Y.Y. and Y.-B.L.; Writing—review and Editing, L.W., J.W. and Y.-B.L.; Supervision, C.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the National Natural Science Foundation of China under Grants 62136006, 62073215 and 61873166.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
2. Li, S.; Da Xu, L.; Zhao, S. The internet of things: A survey. *Inf. Syst. Front.* **2015**, *17*, 243–259. [CrossRef]
3. Tan, L.; Wang, N. Future internet: The internet of things. In Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), Chengdu, China, 20–22 August 2010; Volume 5, pp. 376–380.
4. Chen, T.; Barbarossa, S.; Wang, X.; Giannakis, G.B.; Zhang, Z.L. Learning and Management for Internet of Things: Accounting for Adaptivity and Scalability. *Proc. IEEE* **2019**, *107*, 778–796. [CrossRef]
5. Silva, J.d.C.; Rodrigues, J.J.P.C.; Al-Muhtadi, J.; Rabêlo, R.A.L.; Furtado, V. Management Platforms and Protocols for Internet of Things: A Survey. *Sensors* **2019**, *19*, 676. [CrossRef]
6. Atzori, L.; Iera, A.; Morabito, G. SIoT: Giving a Social Structure to the Internet of Things. *IEEE Commun. Lett.* **2011**, *15*, 1193–1195. [CrossRef]
7. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [CrossRef]
8. Vegni, A.M.; Loscrí, V. A Survey on Vehicular Social Networks. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2397–2419. [CrossRef]
9. Jain, B.; Brar, G.; Malhotra, J.; Rani, S.; Ahmed, S.H. A cross layer protocol for traffic management in Social Internet of Vehicles. *Future Gener. Comput. Syst.* **2018**, *82*, 707–714. [CrossRef]

10. Zia, K.; Shafi, M.; Farooq, U. Improving Recommendation Accuracy Using Social Network of Owners in Social Internet of Vehicles. *Future Internet* **2020**, *12*, 69. [CrossRef]
11. Schurgot, M.R.; Comaniciu, C.; Jaffres-Runser, K. Beyond traditional DTN routing: Social networks for opportunistic communication. *IEEE Commun. Mag.* **2012**, *50*, 155–162. [CrossRef]
12. Wang, J.; Wang, F.; Wang, Y.; Zhang, D.; Wang, L.; Qiu, Z. Social-Network-Assisted Worker Recruitment in Mobile Crowd Sensing. *IEEE Trans. Mob. Comput.* **2019**, *18*, 1661–1673. [CrossRef]
13. Chen, P.Y.; Cheng, S.M.; Ting, P.S.; Lien, C.W.; Chu, F.J. When crowdsourcing meets mobile sensing: A social network perspective. *IEEE Commun. Mag.* **2015**, *53*, 157–163. [CrossRef]
14. Nie, J.; Luo, J.; Xiong, Z.; Niyato, D.; Wang, P. A Stackelberg Game Approach Toward Socially-Aware Incentive Mechanisms for Mobile Crowdsensing. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 724–738. [CrossRef]
15. Wei, L.; Wu, J.; Long, C. A Blockchain-Based Hybrid Incentive Model for Crowdsensing. *Electronics* **2020**, *9*, 215. [CrossRef]
16. Hu, X.; Li, X.; Ngai, E.C.H.; Leung, V.C.; Kruchten, P. Multidimensional context-aware social network architecture for mobile crowdsensing. *IEEE Commun. Mag.* **2014**, *52*, 78–87. [CrossRef]
17. Manogaran, G.; Rodrigues, J.J.P.C.; Kozlov, S.A.; Manokaran, K. Conditional Support-Vector-Machine-Based Shared Adaptive Computing Model for Smart City Traffic Management. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 174–183. [CrossRef]
18. Amin, F.; Choi, G.S. Hotspots Analysis Using Cyber-Physical-Social System for a Smart City. *IEEE Access* **2020**, *8*, 122197–122209. [CrossRef]
19. Azeroual, O.; Jha, M.; Nikiforova, A.; Sha, K.; Alsmirat, M.; Jha, S. A Record Linkage-Based Data Deduplication Framework with DataCleaner Extension. *Multimodal Technol. Interact.* **2022**, *6*, 27. [CrossRef]
20. Rehman, A.U.; Naqvi, R.A.; Rehman, A.; Paul, A.; Sadiq, M.T.; Hussain, D. A Trustworthy SIoT Aware Mechanism as an Enabler for Citizen Services in Smart Cities. *Electronics* **2020**, *9*, 918. [CrossRef]
21. Huang, Z.; Zeng, D.; Chen, H. A comparison of collaborative-filtering recommendation algorithms for e-commerce. *IEEE Intell. Syst.* **2007**, *22*, 68–78. [CrossRef]
22. Guo, J.; Chen, R.; Tsai, J.J. A survey of trust computation models for service management in internet of things systems. *Comput. Commun.* **2017**, *97*, 1–14. [CrossRef]
23. Chahal, R.K.; Kumar, N.; Batra, S. Trust management in social Internet of Things: A taxonomy, open issues, and challenges. *Comput. Commun.* **2020**, *150*, 13–46. [CrossRef]
24. Khan, W.Z.; Arshad, Q.u.A.; Hakak, S.; Khan, M.K.; Saeed-Ur-Rehman. Trust Management in Social Internet of Things: Architectures, Recent Advancements, and Future Challenges. *IEEE Internet Things J.* **2021**, *8*, 7768–7788. [CrossRef]
25. Roopa, M.S.; Pattar, S.; Buyya, R.; Venugopal, K.R.; Iyengar, S.S.; Patnaik, L.M. Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions. *Comput. Commun.* **2019**, *139*, 32–57. [CrossRef]
26. Nitti, M.; Girau, R.; Atzori, L. Trustworthiness Management in the Social Internet of Things. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 1253–1266. [CrossRef]
27. Castelfranchi, C.; Falcone, R. *Trust Theory: A Socio-Cognitive and Computational Model*; John Wiley & Sons: Hoboken, NJ, USA, 2010; Volume 18.
28. Xia, H.; Xiao, F.; Zhang, S.S.; Cheng, X.G.; Pan, Z.K. A reputation-based model for trust evaluation in social cyber-physical systems. *IEEE Trans. Netw. Sci. Eng.* **2018**, *7*, 792–804. [CrossRef]
29. Xia, H.; Xiao, F.; Zhang, S.S.; Hu, C.Q.; Cheng, X.Z. Trustworthiness inference framework in the social Internet of Things: A context-aware approach. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 838–846.
30. Amin, F.; Ahmad, A.; Sang Choi, G. Towards Trust and Friendliness Approaches in the Social Internet of Things. *Appl. Sci.* **2019**, *9*, 166. [CrossRef]
31. Narang, N.; Kar, S. A hybrid trust management framework for a multi-service social IoT network. *Comput. Commun.* **2021**, *171*, 61–79. [CrossRef]
32. Chen, R.; Guo, J.; Bao, F. Trust management for SOA-based IoT and its application to service composition. *IEEE Trans. Serv. Comput.* **2014**, *9*, 482–495. [CrossRef]
33. Chen, R.; Bao, F.; Guo, J. Trust-based service management for social internet of things systems. *IEEE Trans. Dependable Secur. Comput.* **2015**, *13*, 684–696. [CrossRef]
34. Wei, L.; Yang, Y.; Wu, J.; Long, C.; Li, B. Trust Management for Internet of Things: A Comprehensive Study. *IEEE Internet Things J.* 2021, Early Access. [CrossRef]
35. Jøsang, A. *Subjective Logic: A Formalism for Reasoning Under Uncertainty*; Springer: Cham, Switzerland, 2016.
36. Škorić, B.; de Hoogh, S.J.A.; Zannone, N. Flow-based reputation with uncertainty: Evidence-based subjective logic. *Int. J. Inf. Secur.* **2016**, *15*, 381–402. [CrossRef]
37. Wilensky, U. *NetLogo. Center for Connected Learning and Computer-Based Modeling*; Northwestern University: Evanston, IL, USA, 1999. Available online: http://ccl.northwestern.edu/netlogo/ (accessed on 16 February 2022).
38. Wei, L.; Wu, J.; Long, C.; Li, B. On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 4775–4787. [CrossRef]
39. Baldassarre, G.; Lo Giudice, P.; Musarella, L.; Ursino, D. The MIoT paradigm: Main features and an "ad-hoc" crawler. *Future Gener. Comput. Syst.* **2019**, *92*, 29–42. [CrossRef]

40. Cauteruccio, F.; Cinelli, L.; Fortino, G.; Savaglio, C.; Terracina, G.; Ursino, D.; Virgili, L. An approach to compute the scope of a social object in a Multi-IoT scenario. *Pervasive Mob. Comput.* **2020**, *67*, 101223. [CrossRef]
41. Ursino, D.; Virgili, L. An approach to evaluate trust and reputation of things in a Multi-IoTs scenario. *Computing* **2020**, *102*, 2257–2298. [CrossRef]