

Research Article

Structural Balance of Social Internet of Things Networks with Ambiguous Relationships

Hongfei Zhang ¹, Li Zhu ¹, Haifeng Du ², Li Zhang,³ Kaiqi Zhang ⁴, Yutian Yan,² and Chaobo Wang⁵

¹School of Software Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi Province 710049, China

²Center for Administration and Complexity Science, Xi'an Jiaotong University, Xi'an, Shaanxi Province 710049, China

³Xi'an Physical Education University, Xi'an, Shaanxi 710068, China

⁴School of Economics and Management, Chang'an University, Xi'an, Shaanxi 710054, China

⁵Shaanxi Labor College, Xi'an, Shaanxi Province 716000, China

Correspondence should be addressed to Li Zhu; zhuli@xjtu.edu.cn

Received 29 April 2021; Accepted 25 June 2021; Published 1 August 2021

Academic Editor: Wei Wang

Copyright © 2021 Hongfei Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the social Internet of Things, social networks can be built among smart objects or between smart objects and people just like human beings. One of the factors that determines the effect and efficiency of service matching in SIoT is the structure of social networks. In this paper, we exploit the theory of structural balance in signed networks to optimize SIoT network structures to provide a friendly and stable environment as well as a solid foundation for service matching of social Internet of Things. Next, besides being friends or enemies, which are traditional relationships of structural balance or structural changes in signed networks, in our research, we introduce the ambiguous relationship which is the certain state between the hostile and the friendly status and we discuss the meaning and significance of ambiguous relationship in dynamical changes of structural balance in SIoT networks. Based on previous studies, we apply an enhanced objective function and a modified approach concerning the ambiguous relationship towards the dynamical change process. Experiments show that our approach is more effective and efficient than former studies in optimizing dynamical evolution of structural balance in signed networks of SIoT.

1. Introduction

Social Internet of Things (SIoT) originates from the intention of integrating and applying the concept of social network to the solution of Internet of Things. Since then, Internet of Things has evolved from primitive interaction between smart entities to integrated intelligent cross-correlation with human elements. With the participation of people, the essence of Internet of Things is combined with the substance of social networks.

In IoT or SIoT networks, one of the most important issues is how to match people with smart devices or the services provided by them perfectly. However, the collaboration among people and things in social Internet of Things contributes to greater complexity than either social networks or

Internet of Things alone. In addition, the heterogeneous nature of Internet of Things and large-scale context data also make computing and matching more sophisticated [1]. Due to the attributes of free alternation and open network circumstances, when we regard people and smart things in SIoT networks as nodes, users will face a lot of risks in choosing the nodes they want to communicate with.

Thus, a trust mechanism is proposed to solve the dishonesty such as fraud, and trust itself has become a kind of judgment basis to evaluate whether the interactive node is credible. Nevertheless, with the development of social Internet of Things, the number of nodes connected to the network increases exponentially, which leads to a huge search space [2]. As a result, traditional service matching methods based on computing the trust value and matching degree between

each pair of nodes will lead to a more complicated calculation and high cost.

Because of these difficult challenges, we consider new solutions from a higher dimension. That is, we can improve the efficiency and environmental friendliness of people-things or people-services matching by adjusting the overall state of the network.

Obviously, the hostile and unbalanced network environments will damage the interests of nodes within the network. Apart from this, network balance is a key issue in traditional social networks [3] and Internet of Things in which trust can be sustained and the environment can be stable. Then, it is necessary to develop a balanced environment evaluation mechanism to suppress these unfriendly or uncoordinated behaviors and ensure a more stable and secure network environment. Thus, the balance problem in the social Internet of Things is worthy of our serious study.

Because things are essentially operated by human beings, the concept of relationship in social networks can be integrated into the conceptual structure of Internet of Things. Trust is the foundation of interaction between nodes, and it exists in any pair of nodes reflecting the reputation and behavior of nodes in the network. People's interaction is based on trust. Trust in the network can be equivalent to whether it is a relationship of friends or not. As we all know, friendship represents trust and vice versa. There are large numbers of locally interacting agents connected by social and economic relationships which include like or dislike and respect or disrespect for people in human societies [4]. Some social relations are assigned as positive or negative [5]. The classic structural balance theory has always been a focus for social psychologists and sociologists [3]. It is a fundamental social process and the structure of affective relations of social actors towards one another [6].

We use the theorems of structural balance as the foundation for all kinds of signed social networks to firstly construct the partitions through some optimized criterion functions towards the balanced state; secondly, we measure the extent of how the structure is balanced; and thirdly, we find the factors that can shift the network to balanced states [3]. The points or vertices in social networks denote people, and the lines or edges represent acquaintance [7]. The interplay which consists of positive and negative interactions defines the smooth functioning of society [8].

Due to the fact that most of the signed networks in the real world are unbalanced, amounts of approaches are proposed to ascertain the level or degree of unbalance in signed networks; Marvel et al. introduced a numerical model to indicate the potential function [9] in which the negative products of triangles are summed up and divided by the quantity of trigons. In [8], the subsection of unbalanced triangles is related to the feature values of the adjacency matrix of the networks, and a spectral algorithm is provided to compute social balance. With that efficient algorithm above, the top- n eigenvalues instead of all of them are used to calculate the subsection of the disequilibrium trilateral. In [10], the lopsidedness of the meshwork is surveyed by the magnitude of the rims in the disequilibrium trigons, cycles, or networks. An energy function is presented in [11] to reckon overall

equilibration in the signed meshwork. The lowest value of the energy function equals to the minimal quantity of negative signs making the network unbalanced, that is to say, the meshwork is trim when the value of energy function is zeroth. Finally, amid [12], an effectual heuristic approach appeared to improve the energy function, in which the obvious chaos in the network is deleted through the metamorphosis; meanwhile, the scalar of nonpositive edges is reduced correspondingly.

We also focus on the approach a network evolves to the balanced state. Among dynamical evolvement of signed networks, the positive edges transform to the negative ones or vice versa to make unbalanced ones balanced. In [13], Antal et al. produced some discontinuous models for the dynamic state in which the sign of the edge remains as it is unless it increases the number of balanced triangles. But there are the processes called "jammed states," in which the model may be trapped in unbalanced local minimums [13]. Recently, Marvel et al. [14], Traag et al. [15], and Summers and Shames [16] have studied continuous-time models. For instance, the model in [14] converges to the balanced state in finite time. However, the conclusion does not cover cases for nonsymmetric initial conditions. Therefore, in [15], a general model is proposed, which leads to the state of social balance. Besides that, the active external influence in dynamical models is studied in [16].

Social networks can evolve in convoluted ways. Friends can become enemies and vice versa [17]. Thus, all the methods above originated from this hypothesis.

However, we have noted that there are three flaws with them in SIoT networks.

Firstly, in the real world social network, the ties between individuals are complicated, and it is quite probable to imagine that two strangers are neither friends nor enemies, so we can get the conclusion definitely that not being friends does not lead to being an enemy inevitably and vice versa. Especially in the social Internet of Things, whether the two sides are really friends does not determine whether they can share the understanding, concept, and use of intelligent devices or services.

Secondly, in traditional social networks, people may encounter completely unfamiliar users who have no previous interaction experience with them before [18]. The existence of these users threatens the feeling of safety to some extent, but from the perspective of social Internet of Things, it also expands the scope of interaction of people, so that people in the same field or with the same interests establish more and stronger trust relations. For example, the novel corona virus pneumonia spreads throughout the world during this period and people in most countries of the world have been affected by city bans and home quarantine orders. Economic growth may decline and cultural exchanges may be suspended, but the use of the Internet, social media, and intelligent objects has not subsided yet has grown strongly. Massive data obtained from the selection, evaluation, and application of various intelligent objects by people who are related to various attributes contribute to the stability and connectivity of the social network. However, in the real world, these people do not have to be friends. It is even possible that they will

not meet for the rest of their lives. Of course, they are not hostile at all. Therefore, this absolute binary-like, strict distinction between friends and enemies does not make much sense in SIoT.

Finally, even if traditional methods are capable of shifting unbalanced signed networks into balanced states theoretically, but in practice, it is not convenient in realities. Sometimes, it is even impossible to convert the signs of edges in signed networks to their opposite directions.

The innovation of this paper is as follows:

- (1) Originating from the flaws above, we introduce the third kind of connection in SIoT networks which is called the ambiguous relationship
- (2) We suggest that the forms of structural balance of SIoT networks stem from how the ambiguous relationship shifts the state of balance in the network
- (3) By applying the concept of structural balance in signed networks into SIoT networks, through establishing the dynamical evolving mechanism of structural balance in SIoT networks which is more complete and more efficient than that in the mode of traditional social networks, we provide a more amicable and stable environment in order to build a solid foundation for service matching of social Internet of Things for further studies

2. Background

2.1. Trust in SIoT. Each node has its own credibility just as everyone has his reputation, and here comes the concept of trust. The existence of trust is the basis for the delegator to judge whether the entity which provides the information or service is trustworthy. In social networks, the trust degree of an object to another entity providing a specific service is calculated according to the behavior of the service provider in a specific stage and in a designated environment related to the service [19].

In the network of social Internet of Things, each node plays the role of trustor or trustee and establishes social relations independently, so as to carry out service-based interaction. The trustor generates and delegates the task, and the trustee receives the task and provides services for the successful completion of it. In detail, the trustor is a conscious subject with its own goals, needs, and attitudes towards other objects and their behaviors. Based on the trust of other objects, the cognition of the specific environment, and the prediction of the results, the trustor can generate and delegate the task as well as evaluate the related results. The trustee is a cognitive object or device equipped with some information or abilities that can produce a certain effect on the results of its behavior. In a sense, the trustee is not under the direct control of the trustor. The actions of both the trustor and the trustee must be consistent with their trust relationship. Both sides establish the cooperation relationship based on trust and complete the whole process from task initialization to service acceptance throughout with the element of trust.

However, how to find the most suitable trustee to perform the corresponding task is the key problem when the trustor assigns the task. Traditionally, trust degree or trust value is generally used as a measure to select a suitable trustee. Trust values are usually normalized to $[0,1]$, and it concludes two parts called capability and honesty which determine two fundamental aspects of trustworthiness of both the trustor and the trustee. The trustor can use these two parts to evaluate the qualification of trustee and judge whether the cooperation can be obtained. For the trustee, capability refers to the hardware conditions such as the number of related devices equipped, the performance of each device, and the involved information or intelligence, while for the trustor, it refers to the ability of the subject to use the object or device and to provide the resources available for the trustee. A competent trustor (or trustee) may also deceive the other side and behave badly or even maliciously, and an incompetent candidate may also claim to be qualified for the job. Therefore, it is necessary to have an honest index to evaluate the authenticity of the trustor and the trustee, as well as the importance they attach to the cooperative relationship. To summarize, we need to combine the capability and honesty element to constitute the trust value.

There is another important issue that the trust value is task related. When the same pair of trustor and trustee handles different tasks, there will be different trust values. The most important reason for the above conclusion is that each task has its unique attributes and specific targets only belonging to this service. To achieve the task goal, different equipment and different activities will be used.

In SIoT, trust is a process in which a trustor entrusts a task with a certain degree of risk to a trustee equipped with appropriate devices or abilities in a specified context based on the positive expectation for credibility. The trustee acts and evaluates the trustor, while the trustor also assesses the other side during the same period. Finally, results of the service and the trust evaluation of the whole process will in turn affect the attitudes of both sides.

SIoT ensures the scalability of the network and can effectively help the discovery of services [20]. The trust management of nodes in the SIoT network can be achieved by the interaction experience of smart objects. Although trust seems to have nothing to do with intelligence, the realization of intelligence must be realized through a strict trust management mechanism.

As we discussed earlier in the introduction section, the level of trust in the SIoT network is based on the propagation of trust. In addition to the length of trust propagation route, it is also affected by different aggregation strategies of trust values of multiple trust propagation paths. Although evaluating trust values based on all trust propagation paths provides more accurate trust inference values, it is excessively time-consuming in large-scale SIoT or social networks.

Besides, trust can be divided into direct trust and indirect trust [21]. To evaluate the entity trust in the SIoT network, both direct trust and indirect trust should be considered comprehensively. The direct trust is stored locally by the trustor, and the indirect trust value can be obtained from the third-party node. Therefore, when we need to obtain an

indirect trust value, it is necessary to query the relative information of the IoT service provider, and this process will cause network congestion.

In the process of interaction, nodes often encounter unfamiliar ones. In this case, the cooperation needs to be introduced by the middleman, i.e., the intermediate node who plays the role of trust messenger. Therefore, the transitivity of trust makes more cooperation possible in SIoT networks. As it happens, in the balanced network state, friend relationships are also transitive, because if one person's friend is the mate of another, they will all become compadres.

To sum up, there are many problems and limitations to optimize the network structure performance of social Internet of Things purely through a trust management system. Therefore, we introduce the idea of a network structural balance with the relations of friends and enemies to utilize the essence and significance of the trust management mechanism to provide a more favorable network environment for matching people with smart devices or the services through improving optimization performance and efficiency of dynamical evolving of structural balance in SIoT networks.

2.2. Structural Balance. From the structural balance theory of Heider, there are four situations in a signed network which conclude three nodes and three edges between them, as shown in Figure 1. Each network in the triangle form must have 1 or 3 positive edges to be balanced. The state of Figures 1(a) and 1(c) is balanced, while the situation of Figures 1(b) and 1(d) is unbalanced. Generously speaking, in a balanced basic network composed of three nodes, there must be even negative edges, while in an unbalanced basic network, there are odd negative edges.

Based on the classic balance theory of Heider, the state of a signed network is balanced when all the triangular basic networks of nodes within it are balanced. Another definition is that the network is structural balanced only if it does not contain cycles of negative product.

Furthermore, Iacono et al. demonstrated that the definition of the triangle- and cycle-based theory is equivalent [12]. That is, the structure of a signed network is in equilibrium, when any edges in it is positive, or all the nodes can be partitioned into two cliques where nodes in the identical clique can be seen as friends. Meanwhile, nodes come from different cliques can be tagged as enemies. We can briefly describe this definition in Figure 2.

Based on our theory, besides hostile or friendly relationships in SIoT networks, there is a mild or neutral mode, and we call it the ambiguous relationship. It is between the hostile and the kindness situation, and it has the opportunity to be altered towards any of the two standard bipolar states when external forces or elements are exerted. So far, the so-called ambiguous relationship has not caught too much attention in this field of research. However, an ambiguous relationship counts much in SIoT, making it possible to predict temporary trust between unfamiliar nodes without interaction experience. If an ambiguous relationship cannot be defined, strangers will never be able to evaluate whether the other side is trustworthy at least in information, experience or advice, and strangers will always remain unfamiliar, and

they cannot form new interactions. This will lead to low connectivity of the SIoT network, and tasks and services among the network cannot be handled properly and effectively. Therefore, ambiguous relations are fundamental for social Internet of Things.

Furthermore, we can classify the conversion process into two kinds: friendly relationship to none friendly (hostile) and vice versa. Each kind mentioned above may spend too much cost such as resources, time, energy, or power in reality. Although nothing is impossible in this world, in the real world, anything could be done only with the right prize.

Moreover, according to [22], when dealing with the relationship between the owners of IoT nodes sharing similar social interests, there are three kinds of social relations: friendship, social association, and interest group communication, which are used to measure social similarity and to filter trust feedback based on them. This theorization proves that in social Internet of Things networks, in addition to friend relationships, there are two other kinds of relationships between nodes that can be exploited. Besides, if we suspect whether the new relationship dimension exists or not, in some deeper level, the comprehensive meaning of the combination of the two other relations can correspond to the ambiguous relationship we proposed in this paper.

Therefore, it is improper to sign the relation between two individuals just as a friendly or a hostile relationship and deny the existence of the third connection which is neither friendly nor hostile in reality. Consistent with the traditional theory that "1" indicates friendly relationship and "-1" denotes hostile connection, we introduce "0" to represent ambiguous relationship, which makes our model match the real world system more appropriately.

However, according to the hypothesis of Heider, structural balance makes sense only with fully connected networks. We suggest that the "0" edge represents the edge which cannot be defined as "1" or "-1" state, rather than having no edge at all. Once we appreciate the existence of the "0" relationship, we see how this mechanism can establish structural balance other than simply shifting "1" to "-1" or vice versa.

In this essay, with the introduction of the "0" edge, we transform the unbalanced signed networks of SIoT to balanced states only by one step, which makes our method more economical, efficient, and realistic. The "0" edge signifies the ambiguous relationship of nodes in SIoT networks that is neither friendly nor hostile but falls in between the two extreme relations.

3. Structural Balance Evolving with Ambiguous Relationships

3.1. Energy Function. The generally accepted relationship types in social Internet of Things can be divided into three categories: human-object relationship, object-object relationship, and human-human relationship. In the human-object relationship, users search for services provided by smart objects. In the next step, a new search mode will naturally arise, that is, in order to meet the needs of human users, intelligent objects will actively search for other objects that can

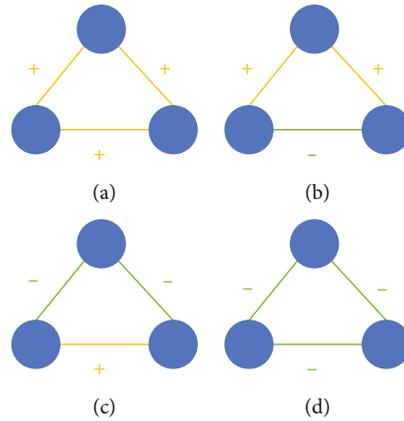


FIGURE 1: Four modes of basic signed networks.

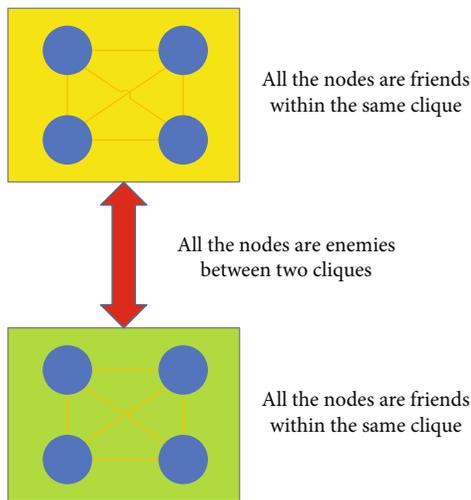


FIGURE 2: Same clique: friends. Different cliques: enemies.

provide relevant composite services. From this perspective, all intelligent objects in social Internet of Things can cooperate with other people or things and establish social relationships, just as human groups do. Therefore, the services and information provided by each intelligent object can be automatically processed by any node in the whole social Internet of Things system.

In the process of node interaction, the two sides will judge whether the other party is trustworthy or the specific value of its trustworthiness, respectively, according to their own experience and the amount of resource reserves. The availability of empirical data may affect the trustworthiness of a node persistently. Moreover, even if they have experienced the same events, there will be differences in all kinds of benefits obtained by both nodes, which leads to a dissimilar evaluation value of the two sides. In other words, trust has the natural attribute of asymmetry.

Next, trust can be divided into two types: identity trust and behavior trust. Identity trust, also known as static trust, at the technical level, refers to the application of encryption, authentication, and other traditional security mechanisms to authorize and verify the validity of entities or nodes in

the network. From the perspective of social networks, identity trust is the historical performance of the subject, which makes it have the corresponding word-of-mouth figure in a certain field. High credibility is the performance of their own identity trust. Behavioral trust, also known as dynamic trust, refers to persistent adjustment of trust relationship based on past interaction experiences. This is the cumulative result of the historical evaluation given by the service user according to the behavior of the service provider. In the trust relationship, it includes the trustor who enjoys the service and the trustee who performs the service relative operation. After the end of the service, both sides will evaluate the other party based on the implementation process and the final results of this cooperation. The evaluation situation will in turn affect the trust value between the two sides and the external credibility of both entities. Therefore, the degree of trust is not static and fixed.

The result of the trustee's action can be described in further detail as it includes not only the expected harvest but also a series of negative effects and the price that must be paid regardless of success or failure. Only by comprehensively calculating the cost of task execution, benefits brought by the action, and the completion degree of expected results can we determine whether the service results are positive or negative.

In addition, the mutual trust between two nodes of the interaction and the trustworthiness of a node in the whole group changes dynamically. If a pair of nodes cooperates with each other frequently, the trust evaluation value of each node will increase gradually. But if the two sides lack interaction or contact and have stopped cooperation for a period of time for some reasons, the trust value will decrease with the passage of time. One of the main reasons is that the judgment data of each node is still in the memory of the past, and there are no real-time source data to help judge the credibility of both nodes, resulting in the decrease of the trust value.

Thus, we can find out that the energy function to calculate the trust value between nodes must be an accurate and complex model with typical and prominent dynamic characteristics.

However, in social Internet of Things, because we do not need to strictly calculate the degree of trust and distinguish

the level of trust, so the excessive accurate and complex trust calculation and management model has become a great burden for the service matching process of social Internet of Things.

Therefore, in SIoT, we use the network of friends and hostility relation of the network structural balance theory to replace the traditional trust relationship network. The relational network between friends and enemies can clearly express the meaning of trust and distrust, and at the same time, it does not focus on detailed trust values. Therefore, the application of the network balance theory in this field is equivalent to the directional abstraction and fuzzification of the trust relationship network, which retains the elements we need and avoids the part of the trust network that is not suitable for social IoT service matching.

In [11], an energy function is presented to calculate the degree of overall balance towards signed networks. By assigning “+1” or “-1” to all the nodes in social IoT, we could compute global balance through the energy function as follows:

$$H(s) = \sum_{i,j} \frac{1 - E_{ij}s_i s_j}{2}, \quad (1)$$

where $H(s)$ equals to the summation of the number of edges leading to the unbalanced state or the unbalanced energy value in the whole SIoT network and it traverses all the couples of nodes in adjacency. $E_{ij} \in \{+1, -1\}$ presents the edge between nodes s_i and s_j . $S = [s_1, \dots, s_n]^T$ ($s_i \in \{+1, -1\}$) signifies the nodes in the network. When E_{ij} presents friendship, if nodes s_i and s_j share the same sign (positive or negative), every corresponding determined value of (1) equals zero, and it means that there is no unbalanced or discordant energy between nodes of SIoT in this area. However, when E_{ij} presents hostility, every term in (1) is “+1,” and the degree of unbalance increases. Likewise, when the signs of s_i and s_j seem opposite to each other, every corresponding determined value is “0” under the condition that E_{ij} presents rivalry and the value is “+1” otherwise. In the end, if the summation value of (1) is still “0,” the whole network of SIoT correlated can be seen as balanced.

Nonetheless, with the introduction of our method with “0” value edge, problems arise. The fatal defect of (1) lies in the fact that when one edge which causes the unbalance of the network is fuzzily processed, the value of E_{ij} equals to 0, but at the same time, the term in $H(s)$ comes to 0.5, and this number conflicts with the theory that $H(s)$ suggests that the number of edges which arouse the whole system becomes unbalanced in that there are no half edges amid the SIoT network background.

Therefore, in order to present the degree of overall balance of SIoT networks, we can take advantage of the formula in [23] to upgrade the optimization approach to

$$H(s) = \sum_{i,j} \frac{|E_{ij}| - E_{ij}s_i s_j}{2}. \quad (2)$$

TABLE 1: Detailed data related to the experiment of each signed network.

Network for experiments	Number of nodes	Number of edges	Number of positive edges	Number of negative edges
SPPN	10	45	18	27
EGN	330	779	515	264
MN	697	1425	947	478

In comparison, when the fuzzy processing is proposed, $E_{ij} = 0$, and meanwhile, $|E_{ij}| = 0$, the term in the equation is “0” too. Under this circumstance, value “0” represents that since the edge stands for ambiguous or neutral relationship now, there is nothing it can do to make the whole SIoT network unbalanced.

3.2. Quantifying in Dynamical Evolution. We want to locate the set of edges containing the edges that should be made ambiguous to make the SIoT network balanced in dynamical evolution, and we want to keep the number of these edges to a minimum value. So a standard is necessary to ensure that the signed SIoT network can evolve to balanced states.

Equation (2) is adopted as the criterion since we can check whether the SIoT network is balanced by computing the energy function to find out if the final value equals zero. In addition, a parameter $\lambda \in [0, 1]$ is introduced into (2) to show that different edges with related signs are processed with different probabilities [24]. Via shifting the numeric value of λ , varying amount of edges involved in neutralization can be obtained and processed.

The formula of the optimization problem of dynamical evolving of structural balance in SIoT networks is shown below:

$$\begin{aligned} \min F(x) &= \lambda x_+ + (1 - \lambda)x_-, \\ \text{s.t. } H(s) &= 0. \end{aligned} \quad (3)$$

According to the previous definition, λ is the parameter to adjust the probability of neutralization towards edge signs, while x_+ is the number of positive signs involved in the ambiguous state of the sign direction and x_- indicates the amount of negative ones. $H(s)$ in (3) and (2) are identical.

3.3. Objective Function and Representation. To optimize (3), an algorithm which comes from [24] is utilized in this section. The algorithm includes the following steps: firstly, the initial population is generated by initialization function, and then, the corresponding population is selected from the parent and child population. The next step is mutation, cross-selection, and population regeneration. Finally, the termination condition function is used to determine when the algorithm can be terminated. In this thesis, the evolutionary algorithm based on MAs (memetic algorithms) is modified and reused to change unbalanced SIoT networks into balanced states dynamically with an enhanced mode.

TABLE 2: Results of 10 runs of variant values of λ and μ . “NPP” denotes the number of the positive edges being neutralized while “NNP” is the number of negative ones. “VA” denotes the value of the object function and “EN” is the result of the energy function.

Networks	Index	$\mu = 0.1$		$\mu = 1$		$\mu = 5$		$\mu = 10$		$\mu = 100$	
		$\lambda = 0.3$	$\lambda = 0.6$								
SPP	NPP	0	0	0	0	0	0	0	0	0	0
	NNP	0	0	2	2	2	2	2	2	2	2
	VA	0.2	0.2	1.4	0.8	1.4	0.8	1.4	0.8	1.4	0.8
	EN	2	2	0	0	0	0	0	0	0	0
	NPP	140.8	134.2	158.5	163.3	169.9	171.7	151.7	169.1	170.2	170.7
EGN	NNP	59	75.1	136.4	136.8	133.9	135.6	144.3	135.4	135.4	133.1
	VA	105.8	132	143	152.7	144.7	156.5	146.5	155.6	145.8	155.7
	EN	223	214.9	0	0	0	0	0	0	0	0
	NPP	319.7	305.9	252	267	281.8	281.1	284.7	277.8	277.8	286.5
MN	NNP	137.7	161.8	270.7	255.9	260.8	257.5	260.1	260.7	261.7	249.6
	VA	232.4	287.3	265	264.2	267.1	271.7	267.5	271	266.5	271.7
	EN	401.2	390.6	0	0	0	0	0	0	0	0

The object is to minimize the value of the objective function in (3). We use the function

$$\min f(x) = \lambda x_+ + (1 - \lambda)x_- + \mu H(s). \quad (4)$$

λ is the weighting parameter, and μ works as the penalizing factor for forming the constraint.

In this algorithm, every individual is encoded as a string: $X = \{X1, X2, X3\}$, where $X1$ denotes positive edges, $X2$ represents negative edges, and $X3$ indicates notes. Their assignment all lies in $\{-1, +1\}^N$ in which N stands for the number of edges and notes. When $Xi \in \{X3\}$, Xi represents the sign of the i th node, and when $Xi \in \{X1\}$ or $\{X2\}$, $Xi = -1$ indicates that the direction of the sign for the edge is neutralized while $Xi = 1$ means that the direction of the sign keeps the same state as before. Node $n1$ is one of the neighbors of $n2$ when they are linked by a positive edge, and the sign of every gene in the individual is designated “+1” or “-1” with a random chance.

The initialization process and the operating measure which consist of the crossover and mutation operation can be found in [24].

3.4. Modified Local Search Procedure. Local search procedures including hill climbing [25] and simulated annealing [26] are usually combined with evolutionary algorithms to prevent the algorithm from falling into the local-best solution. In this procedure, every gene is searched by selecting and neutralizing the sign randomly. When the changing leads to the decrease of the value in (3), the sign of the gene is neutralized permanently. The algorithm is described in [24] in which we only process the best samples in the group based on the modified process after the crossover conduct and mutation operation.

4. Experiments

We test our approach on three real signed network datasets, and the experimental outcome demonstrates that our

method has a better effect in optimization towards the dynamical evolving of edge signs than the algorithm from [24].

4.1. Experimental Setup. Our model and approaches are realized through MATLAB. We conduct the experiments on a 3.8 GHz computer with 8 GB RAM. The OS on the computer is Windows 10 of Microsoft. The parameters used in the experiment are identical as [24] so that we can make sure that the contrast is accurate and persuasive. The parameters include the number of iterations, sizes of population, mating pool, the tournament, and probabilities of the crossover and mutation operations. They all are fundamental parameters in memetic algorithms.

4.2. Experimental Result. The effect of the model in our paper is examined on three real signed network datasets: Slovene Parliamentary Party Network (SPPN), EGFR (EGN), and Macrophage (MN). These three datasets are all used as experimental networks in [23–25] which have strong correlation with the model and experiment in this paper, so they are more suitable for the experimental scenario. The detailed data related to the experiment of each signed network are shown in Table 1.

Slovene Parliamentary Party Network (SPPN): a group of experts on parliamentary activities created the SPPN dataset in 1994 [27]. The network presents the relationship between different network subsets. Nodes represent the subnetworks, while edges represent the hostile or friendly relationship between subnetworks.

EGFR (EGN): created by [28] with the epidermal growth factor receptor pathway. Edges can be considered as transcription factors. The positive and negative of edges represent the positive and negative of control in the physical sense, respectively.

Macrophage (MN): obtained by [26], and the data came from the molecular reciprocity map focusing on a macrophage. Edges are used to describe the interaction of macrophage molecules in the field of biology. The positive edge

shows activation action, while the negative edge indicates translocation or segregation operation.

There are two variable parameters of λ and μ in order to determine the variation. First, we explore the impact of μ in the goal function. In Table 2, we calculate the average values of the algorithm for $\mu = 0.1, 1, 5, 10,$ and 100 .

In Table 2, we find that when $\mu = 0.1$, the energy function $H(s) = 0$ can never be achieved on all the networks. The unbalanced network cannot evolve to the balanced one, i.e., the results of the objective function (3) do not satisfy what we need in dynamical changes of structural balance. And for $\lambda = 0.3$ and $\lambda = 0.6$, our algorithm can always get the minimum value of the function on three signed networks when $\mu = 1$. We run the algorithm 10 times for different parameter values of λ for each network.

In our approach, every solution represents a kind of balanced structure of the signed network evolved from the unbalanced state. According to the approach and results in [24], we find that although the processes in the two systems are all alike except the fact that we exclusively change the target sign into “0” instead of shifting it to “+1” or “-1,” the effect and result of the dynamical evolution looks better in our data, which means that there are less edges to be changed under the same circumstance compared with that in [24].

5. Conclusion

In SIoT, social networks can be established among intelligent objects or between intelligent objects and human beings. How to get the most appropriate service efficiently and accurately is a fundamental problem for intelligent objects, applications, and users in SIoT networks. Among many factors that can determine the effect and efficiency of service matching in SIoT, the structure attribute of SIoT networks is seldom considered yet. While structural balance is a significant issue in traditional studies of signed networks, in this paper, we exploit the theory of structural balance to optimize SIoT network structures to provide a friendly and stable environment for the service matching of social Internet of Things. Then, based on the nature and features of SIoT, we introduce the ambiguous relationship which is the certain state between the hostile and the friendly status, and we discuss the meaning and significance of an ambiguous relationship in the dynamical shifting of structural balance in SIoT networks. Furthermore, we take advantage of the optimized dynamical evolution of structural balance to shift the SIoT network structure by neutralizing the sign of edges. Based on previous studies, we apply an enhanced objective function and a modified approach concerning the ambiguous relationship towards the dynamical change process. Experiments show that our approach is more effective and efficient than former studies in optimizing the dynamical evolution of the structural balance in signed networks of SIoT. In the future, we will continue to explore and study other elements and methods in the network structure that can enhance the efficiency and effectiveness of SIoT service matching.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

The work is supported by the National Key Research and Development Program, China (No. 2019YFB2102500), and the Natural Science Basic Research Program, Shaanxi (No. 2020JQ-855, No. 2019-JQ.531).

References

- [1] D. Hussein, S. Park, S. N. Han, and N. Crespi, “Dynamic social structure of things: a contextual approach in CPSS,” *IEEE Internet Computing*, vol. 19, no. 3, pp. 12–20, 2015.
- [2] M. Nitti, L. Atzori, and I. P. Cvijikj, “Friendship selection in the social internet of things: challenges and possible strategies,” *IEEE Internet of Things Journal*, vol. 2, no. 3, pp. 240–247, 2015.
- [3] P. Doreian and A. Mrvar, “A partitioning approach to structural balance,” *Social Networks*, vol. 18, no. 2, pp. 149–168, 1996.
- [4] M. Szell, R. Lambiotte, and S. Thurner, “Multi-relational organization of large-scale social networks in an online world,” *Proceedings of the National Academy of Sciences*, vol. 107, no. 31, pp. 13636–13641, 2010.
- [5] P. Doreian and A. Mrvar, “Partitioning signed social networks,” *Social Networks*, vol. 31, no. 1, pp. 1–11, 2009.
- [6] N. P. Hummon and P. Doreian, “Some dynamics of social balance processes: bringing Heider back into balance theory,” *Social Networks*, vol. 25, no. 1, pp. 17–49, 2003.
- [7] M. E. Newman, “The structure of scientific collaboration networks,” *Proceedings of the National Academy of Sciences*, vol. 98, no. 2, pp. 404–409, 2001.
- [8] E. Terzi and M. Winkler, “A spectral algorithm for computing social balance,” in *Algorithms and Models for the Web Graph*, pp. 1–13, Springer, 2011.
- [9] S. A. Marvel, S. H. Strogatz, and J. M. Kleinberg, “Energy landscape of social balance,” *Physical Review Letters*, vol. 103, no. 19, article 198701, 2009.
- [10] P. Anchuri and M. Magdon-Ismael, “Communities and balance in signed networks: a spectral approach,” in *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 235–242, Istanbul, Turkey, 2012.
- [11] G. Facchetti, G. Iacono, and C. Altafini, “Computing global structural balance in large-scale signed social networks,” *Proceedings of the National Academy of Sciences*, vol. 108, no. 52, pp. 20953–20958, 2011.
- [12] G. Iacono, F. Ramezani, N. Soranzo, and C. Altafini, “Determining the distance to monotonicity of a bio-logical network: a graph-theoretical approach,” *IET Systems Biology*, vol. 4, no. 3, pp. 223–235, 2010.

- [13] T. Antal, P. Krapivsky, and S. Redner, "Dynamics of social balance on networks," *Physical Review E*, vol. 72, no. 3, article 036121, 2005.
- [14] S. A. Marvel, J. Kleinberg, R. D. Kleinberg, and S. H. Strogatz, "Continuous-time model of structural balance," *Proceedings of the National Academy of Sciences*, vol. 108, no. 5, pp. 1771–1776, 2011.
- [15] V. A. Traag, P. Van Dooren, and P. De Leenheer, "Dynamical models explaining social balance and evolution of cooperation," *PloS One*, vol. 8, no. 4, article e60063, 2013.
- [16] T. H. Summers and I. Shames, "Active influence in dynamical models of structural balance in social networks," *EPL (Europhysics Letters)*, vol. 103, no. 1, article 18001, 2013.
- [17] T. Antal, P. L. Krapivsky, and S. Redner, "Social balance on networks: the dynamics of friendship and enmity," *Physica D: Nonlinear Phenomena*, vol. 224, no. 1-2, pp. 130–136, 2006.
- [18] C. Jiang, S. Liu, Z. Lin, G. Zhao, R. Duan, and K. Liang, "Domain-aware trust network extraction for trust propagation in large-scale heterogeneous trust networks," *Knowledge-Based Systems*, vol. 111, pp. 237–247, 2016.
- [19] D. Olmedilla, O. F. Rana, B. Matthews, and W. Nejdl, "Security and trust issues in semantic grids," in *Semantic Grid: The Convergence of Technologies*, Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2006.
- [20] L. Atzori, A. Iera, and G. Morabito, "SIoT: giving a social structure to the internet of things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, 2011.
- [21] F. Azzedin and M. Maheswaran, "Evolving and managing trust in grid computing systems," in *IEEE CCECE2002. Canadian Conference on Electrical and Computer Engineering. Conference Proceedings (Cat. No.02CH37373)*, Winnipeg, MB, Canada, 2002.
- [22] I.-R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, 2016.
- [23] D. Haife, H. Xiaochen, W. Shanfeng, G. Maoguo, and W. Feldman Marcus, "Optimizing transformations of structural balance in signed networks with potential relationships," *Physica A: Statistical Mechanics and its Applications*, vol. 465, pp. 414–424, 2017.
- [24] S. Wang, M. Gong, D. Haifeng, L. Ma, Q. Miao, and W. Du, "Optimizing dynamical changes of structural balance in signed network based on memetic algorithm," *Social Networks*, vol. 44, pp. 64–73, 2016.
- [25] M. Gong, B. Fu, L. Jiao, and H. Du, "Memetic algorithm for community detection in networks," *Physical Review E*, vol. 84, no. 5, article 056101, 2011.
- [26] K. Oda, T. Kimura, Y. Matsuoka, A. Funahashi, M. Muramatsu, and H. Kitano, "Molecular interaction map of a macrophage," *AfCS Research Reports*, vol. 2, no. 14, pp. 1–12, 2004.
- [27] A. Ferligoj and A. Kramberger, "An analysis of the Slovene parliamentary parties network," *Developments in Statistics and Methodology*, vol. 12, pp. 209–216, 1996.
- [28] K. Oda, Y. Matsuoka, A. Funahashi, and H. Kitano, "A comprehensive pathway map of epidermal growth factor receptor signaling," *Molecular Systems Biology*, vol. 1, no. 1, 2005.