Social Internet of Tings Trust Management Based on Implicit Social Relationship

Hongbin Zhang[1,2], Fan Fan[1], Dongmei Zhao[2(✉)], Bin Liu[3,4], Yanxia Wang[5], and Jian Liu[1]

[1] School of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang 050000, China

[2] Hebei Key Laboratory of Network and Information Security, Hebei Normal University, Shijiazhuang 050024, Hebei, China
zhaodongmei666@126.com

[3] School of Economics and Management, Hebei University of Science and Technology, Shijiazhuang 050000, China

[4] Research Center of Big Data and Social Computing, Hebei University of Science, Shijiazhuang, China

[5] Hebei Geological Workers' University, Shijiazhuang 050081, China

Abstract. The "Social Internet of Things (SIoT)" is a combination of the Internet of Things (IoT) and social networks to form a new paradigm. The SIoT promotes the development of smart cities, smart transportation, and many other fields. In SIoT, the openness and mobility of objects are enhanced. However, this tends to lead to network data sparsity problems. By distinguishing explicit and implicit social relationships, we introduce an implicit social relationship-based trust management model (IRTM) for reliable service delivery in SIoT. IRTM establishes implicit social relationships among nodes by mining their latent characteristics and trust transitivity. It models SIoT by creating sub-networks for each social relationship as a way to fuse the impact of different types of social relationships on trust management. To address the problem of malicious attacks by malicious nodes in the network to protect their interests, it considers two metrics, node relationship strength, and recommendation reliability, to filter malicious recommendations. Experiments conducted in the presence of data sparsity and malicious objects show that IRTM can improve the accuracy and convergence of trust evaluation compared to other methods that ignore implicit social relationships when computing trust. In addition, our scheme can improve resistance to trust-related attacks.

Keywords: Social Internet of Things · Trust Management · Malicious Attack · Implicit Social Relationship · Multiple Social Relationships

1 Introduction

Information and intelligence are important features of modern development, and the realization of "interconnection of all things and intelligent interoperability" is an important goal of modern development. To further promote the "Internet of Everything", a

Q. Jiang et al. (Eds.): SPNCE 2022, LNICST 496, pp. 129–139, 2023.
https://doi.org/10.1007/978-3-031-30623-5_9

new paradigm, the Social Internet of Things, has been proposed. The Social Internet of Things (SIoT) will further promote the development of health care (telemedicine, e-health, etc.), smart cities (connected cars, smart weather, etc.), smart homes (home lighting control systems, home security systems, etc.) and other fields by establishing social networks among smart devices [1–3]. However, in this environment where frequent interactions occur, some bad nodes can maliciously attack other nodes. The service request process of good nodes will be disturbed. Therefore, trust plays a crucial role in ensuring reliable service delivery [4–6]. The concept, metrics, and assessment methods of trust are not uniform in different fields [7]. For example, in real life, trust represents the intimacy between people, and trust also indicates recognition of people's abilities in some specific scenarios, etc. In SIoT, trust represents the reliability of the services provided by objects. Therefore, trust management in SIoT is essential for a more reliable and satisfactory service to the principals.

It is important to note that in traditional IoT, the location of smart objects is relatively fixed. However, in SIoT, the mobility of smart objects becomes stronger. And mobility tends to lead to dense nodes in some areas and sparse nodes in others. Objects can build social relationships autonomously is the characteristic of SIoT. The social relationship is an important evaluation metric in SIoT trust management. When the data where the nodes are located is sparse, it means that there is a lack of information about the social relations of the nodes, which leads to the inability to accurately evaluate trust. Therefore, we propose an implicit social relationship-based trust management model (IRTM). The model extends the social relationship network by mining the implicit social relationships among nodes, making its scheme applicable in sparse networks as well. Two metrics, node relationship strength, and recommendation reliability are considered to filter malicious recommendations so that its model is still robust in a hostile environment. An example diagram for seeking the most reliable service using trust management is given in Fig. 1. And the detailed part of the IRTM trust management model we will discuss in detail in Sect. 4.

The remainder of this paper is organized as follows. Section 2 reviews the related work. Section 3 describes the preparatory work. In Sect. 4, we detail the design of an implicit social relationship-based trust management model (IRTM) for SIoT. In Sect. 5, we verify the effectiveness of the model through experimental simulations. Finally, we summarize the work in this paper and outline future work in Sect. 6.

2 Related Work

This section reviewed and analyzed the related work on trust management of the Social Internet of Things in recent years.

M. Nitti et al. [8] model subjective trust management based on social network characteristics; an objective trust model was built based on P2P related approach and using some characteristics of social networks. In Ref [9], multiplicative attribute maps were used to quantify predefined social relationships and calculate the trust strength between nodes in the context of SIoT. The Ref [10] considers four attributes of closeness, service feedback, sociality, and transaction importance for the trust management of nodes. Fang-Yu Gai [11] introduced the theory of social networks in in-vehicle networks so that

they can better serve the trust model. The accuracy of trust assessment models can be improved by quantifying social relationships. In Ref [12], context-aware trust quantification methods based on feature-attribute matching methods were proposed. And ability, willingness, and social relationship elements were used to measure trust. In Ref [13], a differentiated perceptual trust management model is proposed. This model introduces social relations in the computation of trust to better understand some discriminatory behaviors. However, the above references are more homogeneous in considering social relationships and only use the social similarity between nodes to represent the strength of ties. It is not possible to integrate the impact of multiple social relationships on trust management.

The Ref [14] considers trust attributes such as honesty, collaboration, community interest, and node energy of trust and calculates trust based on direct observation, indirect recommendation, the centrality of nodes, and reliability factors. In Ref [15], an adaptive trust management protocol under SIoT is proposed. In Ref [16], the authors propose a temporal similarity-based trust model for social IoT that incorporates the impact of three attributes, namely the community interest attribute, friend attribute, and collaborative work attribute, on trust assessment. However, the above references only exploit explicit social relationships and completely ignore implicit social relationships. It is not able to effectively solve the network sparsity problem.

Therefore, this paper effectively alleviates the network data sparsity problem and the cold start problem by establishing implicit social relationships. Inspired by the subnet composite approach in Ref [17] and Ref [18], the multi-subnet composite complex network idea is used to model the SIoT. In the following, the system model will be elaborated.

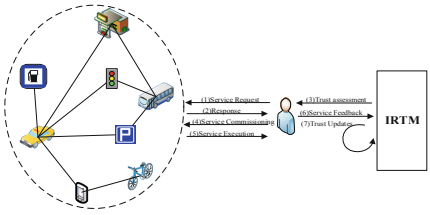


Fig. 1. SIoT trust management process

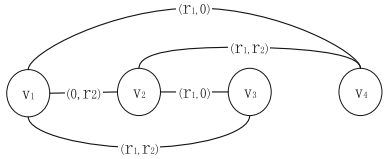


Fig. 2. Composite network example diagram

3 Preliminaries

3.1 Types of Social Relationships

The SIoT enhances the navigability of the network. Each type of social relations has a different impact on navigability and represents a different level of trust [18, 19]. According to the object-specific socialization model of SIoT defined in Ref [20], objects create different types of social relationships. The initial trust value of social relationships is set according to the definition of social relationships and the analysis of the type of navigability and importance of social relationships in SIoT by Ref [21] and [22].

In this paper, the trust value range is set within (0, 1), when the higher trust value indicates that the more reliable the smart object is, the higher the interaction success rate. When objects such as cell phones and laptops belong to the same owner, they will have a higher probability of having similar behaviors. Therefore, we set the highest initial trust value of 0.9 to the Ownership Object Relationship (OOR). There is a higher similarity between objects produced by the same manufacturer in the same period. Therefore, we set a higher initial trust value of 0.8 for the Parental Object Relationship (POR). There is a high probability of interaction and collaboration between objects such as sensors and actuators used in the same environment such as a smart home or smart city to accomplish tasks. Therefore, we give a slightly higher initial trust value of 0.7 to Co-Location Object Relationship (C-LOR). Co-Work Object Relationship (C-WOR) are established between objects that are far away from each other according to the task type, such as telemedicine. Since the longer distance makes the objects more likely to suffer from malicious attacks, we give a low initial trust value of 0.6 to the Co-Work Object Relationship. The initial trust value between objects without social relations is 0.5.

3.2 Implicit Social Relationship

In most of the previous studies on trust management in SIoT, only explicit social relationships between nodes have been utilized, and the role of implicit social relationships in trust management has been completely ignored. Explicit social relationships are explicitly establishable social relationships between nodes. The types of explicit social relationships in SIoT are described in Sect. 3.1. Implicit social relationships are implicit social links established through the transferability of trust between two nodes that do not have social relationships. For example, in real life, people tend to trust their friends and will trust their friends' friends. This implies that there may be potential implicit social links between people who do not have direct social relationships. Therefore, to overcome the network sparsity and cold start problems and to maximize the use of online social information, we classify social relationships into explicit and implicit social relationships. Inspired by Ref [24], we mine and establish implicit social relationships between nodes based on trust transferability and potential features between nodes. Among them, the type and strength of implicit social relationships are determined by the type of explicit social relationships that exist between nodes and the number of common neighbors. Thus many nodes may be related to each other through implicit social relationships.

Based on the explicit social relationship types described in Sect. 3.1, we can establish implicit parent-object relationships, implicit collaborative location relationships, etc. Objects have both explicit and implicit social relationships with each other, and there may be multiple social relationships. And different types of explicit and implicit social relationships have different impacts on trust evaluation. Considering one type of social relationship alone will affect the accuracy of the evaluation results. Therefore, we use the idea of the composite network to build a composite SIoT network with explicit and implicit social relationships by loading multiple explicit and implicit single-relationship sub-networks. The composite network is introduced as described in Sect. 3.3.

3.3 Multi-relationship Composite Network

Smart objects are abstracted as nodes, and the relationships between smart objects are abstracted as connected edges in SIoT. The SIoT composite network model can be represented by a quadruplet $G = (V, E, R, F)$, and an example diagram is shown in Fig. 2.

- $V = \{v_1, v_2, v_3, \ldots, v_m\}$ represents the set of nodes, which is the number of nodes in the set.
- $E = \{\langle v_h, v_l \rangle | v_h, v_l \in V\}$ denotes the set of connected edges between nodes.
- $R = \{r_1, r_2, r_3, ..., r_n\}$ denotes the set of social relations between nodes, and is the number of types of relations in the set.
- F denotes the function to calculate the degree of multiple social relations.

4 The Proposed Trust Management Model

The Implicit Social Relationships (IRTM) based social IoT trust management model consists of six components: SIoT composite network construction, trust propagation, trust aggregation, filtering mechanism, outcome processing, and trust evaluation. Honesty, cooperativeness, and community interest are considered to be the most prominent indicators for characterizing SIoT systems [15]. The trust management model is elaborated below using the community interest attribute as an example and describing the attribute in terms of POR and C-LOR between nodes, as shown in Fig. 3 below.

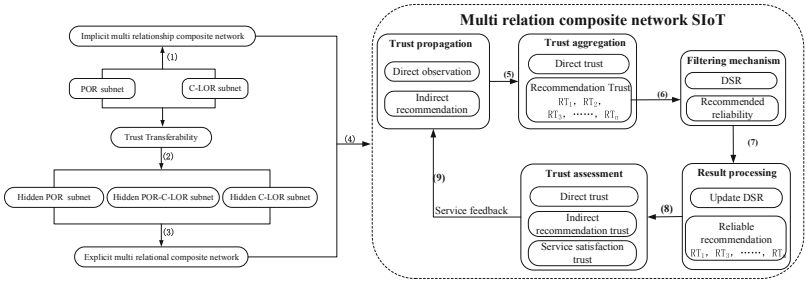


Fig. 3. IRTM model

1. Based on the social relationship matrix ES and the corresponding initial trust values, we obtain the dominant relationship trust matrix E_DSR_1 and E_DSR_2. The relationship trust values of both social relationships are calculated by Eq. (1), and the dominant multi-relationship composite network is constructed.

$$F\_DSR_E(i,j) = \max(E\_DSR_1(i,j), E\_DSR_2(i,j)) + |E\_DSR_1(i,j) - E\_DSR_2(i,j)|^{\eta} \times \sigma \quad (1)$$

where the parameter σ controls the trust value within the range, $\sigma = 0.01$ in this paper; The size of the parameter η depends on the type of the node social relationship and takes values in the range (0, 1);

2. The relational strength of implicit social relationships decays from the strength of explicit social relationships and evolves according to the type of social relationships and the number of indirect friends. Thus, the implicit social relationship matrix is calculated as shown in (2):

$$IS = ES \otimes ES \cdot RM \tag{2}$$

where $\otimes$ denotes the outer product operation and $\cdot$ denotes the inner product operation; the regularization matrix RM is used to exclude the node from establishing an implicit trust relationship with itself; in the implicit social relationship matrix, the value 0 indicates that there is no implicit social relationship between two nodes, and other values indicate the number of times the node appears as an indirect friend;

The calculation of the strength of implicit social relations between nodes is given in Eq. (4):

$$I\_DSR(i,j) = (1-r) \times E\_DSR(i,j) - (r \times E\_DSR(i,j))^{IS(i,j)^{\eta}} \tag{3}$$

where $IS(i,j)$ denotes the number of times the node j appears as an indirect friend of the node i; the parameter r is the trust decay factor, and the value range is (0, 1);

3. We give the calculation of the relationship trust level with both implicit social relationships as shown in Eq. (5):

$$F\_DSR_I(i,j) = \max(I\_DSR_1(i,j), I\_DSR_2(i,j)) + |I\_DSR_1(i,j) - I\_DSR_2(i,j)|^{\eta} \times \sigma \tag{4}$$

To prevent the establishment of implicit social relationships from leading to too dense network links, this paper sets the threshold of implicit social relationship degree as 0.4, that is, when $F\_DSR_I(i,j) > 0.4$, the implicit social relationship is established between node i and node j;

4. Explicit social relationships between nodes are more important than implicit social relationships, so the strength of relationships with both explicit and implicit social relationships is calculated by the following Eq. (6):

$$DSR(i,j) = E\_DSR(i,j) + |E\_DSR(i,j) - I\_DSR(i,j)|^{\eta} \times \sigma \tag{5}$$

5. Trust management is performed in the composite network. The IRTM forms direct trust DT_{ij}^{CI} through direct observation and indirect trust RT_{kj}^{CI} through indirect recommendation.

6. To prevent malicious nodes from making dishonest recommendations, this paper sets up a filtering mechanism in the IRTM model. The recommendation trust is filtered according to the degree of social relationship between node i and node k and the reliability of node k' recommendation values. The relationship degree threshold is set to 0.5, which means that node i only accepts recommendations from recommenders whose relationship trust degree is higher than 0.5. We calculated the reliability of the recommended values by considering the difference between the mean and median of the recommended values. Assuming that the node i has n recommenders, the calculation formula is as follows:

$$RT_{rel}(k) = 1 - \frac{\left|2n \times RT_{kj}^{CI} - \sum_{k=1}^{n} RT_{kj}^{CI} - 2n \times RT_{med}\right|}{\sum_{k=1}^{n} RT_{kj}^{CI} + n \times RT_{med}} \tag{6}$$

7. Based on the results of the filtering mechanism, m reliable recommendation values are obtained. Thus, a reliable indirect trust can be formed.
8. At the end of the interaction at moment t, node i will rate the satisfaction of the service provided by node j to provide feedback for the next interaction, which is calculated as follows:

$$S_{ij}(t) = \begin{cases} T_{ij}^{CI}(t - \Delta t) \times 1, \ \textit{if satisfied} \\ T_{ij}^{CI}(t - \Delta t) \times (-1), \ \textit{if dissatisfied} \end{cases} \tag{7}$$

9. The three trust measures of direct trust, indirect referral trust, and service satisfaction are considered for a comprehensive assessment of trust values, calculated as follows:

$$TT_{ij}^{CI} = \begin{cases} (1-\mu) \times DT_{ij}^{CI}(t) + \frac{\mu}{2} \times RT_{ij}^{CI}(t) + \frac{\mu}{2} \times S_{ij}(t - \Delta t), \ \textit{if } j == k \\ \mu \times RT_{ij}^{CI}(t) + (1-\mu) \times S_{ij}(t - \Delta t), \ \textit{if } j! = k \end{cases} \tag{8}$$

where μ ($0 \leq \mu \leq 1$) used to balance the contribution of direct trust, indirect trust, and service satisfaction to trust.

We will conduct experiments and analyze the accuracy, convergence, and resilience of the IRTM model in detail in Sect. 5.

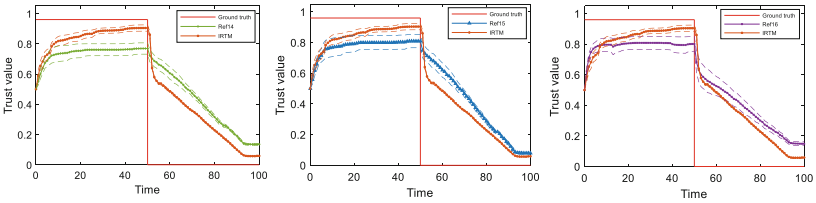
5 Experimental Results and Analysis

In this section, we compare the IRTM model in detail with the approaches in Ref [14, 15], and [16]. Experiments show that the IRTM model improves accuracy, convergence, and resistance to attacks. In this paper, simulations are performed in MATLAB using the dataset from Ref [22]. This dataset is based on a real IoT dataset provided by the city of Santan-der. We randomly selected 30 users from this dataset and constructed SIoT networks for 100 objects owned by their users. The total experimental simulation time was 100 h.

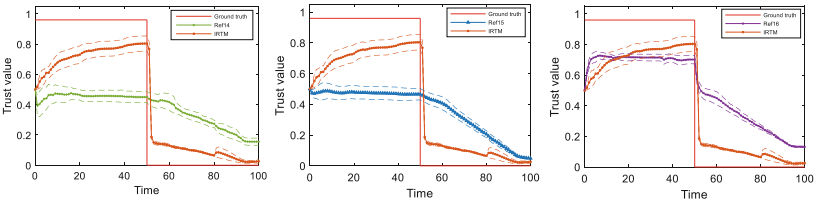
5.1 Trust Evaluation of Nodes in the Good Condition

To verify that the IRTM model improves the accuracy of trust assessment, multiple groups of dynamic nodes are randomly selected in a good environment for trust assessment comparison experiments. The network environment in which half of the nodes are located exhibits obvious sparse characteristics. Sparse networks are a common and not negligible application scenario for SIoT. Therefore, we compare the convergence properties of trust evaluation algorithms in general non-sparse scenarios and sparse network scenarios. The evaluated nodes perform well for the first 50 h, after which they are transformed from good to malicious nodes. Ideally, the good node trust evaluation value tends to be 1 and the malicious node tends to be 0. The IRTM model is compared with the methods Ref [14, 15], and [16]. The results are shown in Fig. 4. The dashed line shows the empirical confidence interval at a 90% confidence level.

In Fig. 4(a), the trust value evaluated by the IRTM model proposed in this paper for good nodes in the normal network environment is closer to the true value1 than the trust



(a) Non-sparse environment



(b) Sparse environment

Fig. 4. Trust evaluation of a randomly selected malicious node

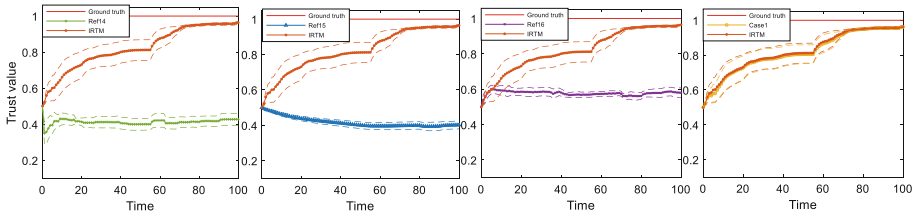
values evaluated by the methods in Ref [14, 15], and [16]; the trust value evaluated for malicious nodes is closer to the true value 0 and converges faster. This indicates that the IRTM model improves the accuracy of node trust assessment. This is because on the one hand the IRTM model incorporates service feedback trust in the trust evaluation, and on the other hand the trust between nodes is dynamically updated. When the nodes provide good services, the trust in the degree of relationship between nodes increases; when the nodes provide malicious services, the trust between nodes dynamically decreases.

As can be seen in Fig. 4(b), the IRTM model differs significantly from the evaluated values of the methods in Ref [14] and Ref [15]. This is due to the sparse data of the network environment in which the nodes are located, which affects the evaluation of the trust value of the nodes by comparing the methods of Ref [14] and Ref [15]. Compared with the evaluation results of the three comparative kinds of literature, it can be seen that the IRTM model is still close to the true value of the node trust value evaluation in the sparse network environment. This is because this paper solves the problem that the node trust cannot be evaluated correctly due to network sparsity by establishing implicit social relationships between nodes to populate the network. In addition, IRTM can converge to the new true value faster when the node becomes a malicious node. Comparing Fig. 4(a) and Fig. 4(b), we can see that IRTM improves the convergence speed and accuracy of trust evaluation regardless of whether the nodes are in the non-sparse or sparse scenario.

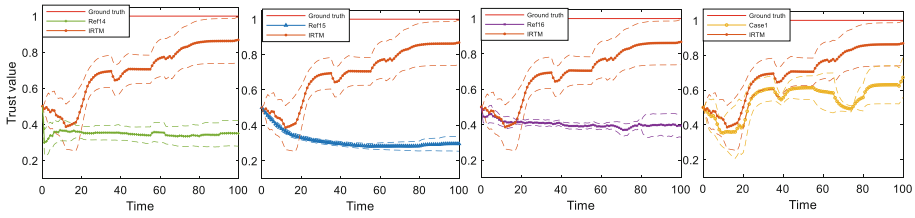
5.2 Trust Management in the Dynamic Hostile Change Conditions

To further validate the resilience of the IRTM model to trust attacks in SIoT environments with different levels of hostility. We consider two different malicious environments with a high malicious node percentage of 50% and a low malicious node percentage of 20%. In the experiments, the optimal parameter weights are set for the methods of Ref [14, 15], and [16]. In addition, to verify the importance of the degree of relationship between nodes in the trust management model, it is also compared with the case where

malicious recommendations are filtered only by the reliability of the recommendation value without considering the degree of relationship in the model of this paper. For the sake of comparison and analysis, the above Case is referred to as "Case 1". The trust evaluation results of different models on randomly selected good nodes when malicious nodes launch attacks under two malicious node percentages, high and low, are shown in Fig. 5.



(a) 20% percentage of malicious nodes



(b) 50% percentage of malicious nodes

Fig. 5. Trust evaluation of randomly selected nodes under malicious attacks

From Fig. 5(a), it can be seen that the result curves of trust evaluation of good nodes at low malicious node percentage for method case 1 in this paper are consistent. It is closer to the true value than the results of Ref [14, 15], and [16]. This indicates that this paper's model filters malicious recommendations and has a better stability. In contrast, the evaluation results of Ref [14] and Ref [15] differ more from the true value. On the one hand, it is because these two methods cannot filter malicious recommendations under defamation attack, which leads to lower trust value; on the other hand, it is because the network environment in which the nodes are located is more sparse, which makes the evaluation accuracy lower.

From Fig. 5(b), we can see that the evaluation result curves of this paper's model and "Case 1" are above the other three methods and closer to the true value 1. This indicates that the IRTM model has a strong ability to resist malicious attacks. The evaluation result curve of Case 1 fluctuates more and is below the curve of this paper's model. This is because under the high malicious node percentage, due to the increase in the number of malicious nodes, filtering malicious recommendations only by recommendation reliability will filter normal recommendations incorrectly as malicious recommendations, making the evaluation accuracy lower. In contrast, the evaluation result curve of the model in this paper is still smoother and closer to the true value than the evaluation result of Case 1. This indicates that introducing the degree of social relationship into trust management effectively improves the accuracy of evaluation results.

6 Conclusion

Autonomous social relationships between objects are a characteristic of SIoT. In this paper, we propose a SIoT trust management model based on implicit relationships, namely IRTM. Unlike other approaches, this paper introduces implicit social relationships in trust computation to better overcome network sparsity and cold start problems. It makes the model equally applicable in a sparse network environment. In addition, we also consider the degree of social relationship and the reliability index of recommendation value in the model to set a filtering mechanism to filter malicious recommendations. According to the results, IRTM can filter dishonest recommendations very well. The simulations also confirm that the proposed model works well even if the percentage of malicious objects in the network increases compared to the other three trust models. In future work, we hope to make IRTM resilient to more sophisticated attacks through learning studies. In addition, we will consider introducing social relationships into multidimensional trust management to build a trust management model that is context-aware.

References

1. Khan, W.Z., Arshad, Q. -u. -A., Hakak, S., et al.: Trust management in social internet of things: architectures, recent advancements, and future challenges. IEEE Internet Things J. **8**(10), 7768–7788 (2021)
2. Mi, B.T., Liang, X., Zhang, S.S.: Review of social internet of things. J. Comput. Sci. **41**(07), 1448–1475 (2018)
3. Xiong, J.B., Bi, R.W., Tian, Y.L., et al.: Mobile swarm intelligence perceives security and privacy: models, progress and trends. J. Comput. Sci. **9**, 1949–1966 (2021)
4. Khanfor, A., Hamrouni, A., Ghazzai, H., at al.: A trustworthy recruitment process for spatial mobile crowdsourcing in large-scale social IoT. In: 2020 IEEE Technology & Engineering Management Conference (TEMSCON), pp. 1–6. IEEE, Novi (2020)
5. Thirukkumaran, R., Muthu Kannan, P.: Survey: security and trust management in internet of things. In: 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp. 131–134. IEEE, Lonavala (2018)
6. Wen, Y.Y., Xu, Z., Jiao, R.X.: A social IoT trust prediction model using deep learning. Telecommun. Technol. **61**(03), 269–275 (2021)
7. Artz, D., Gil, Y.: A survey of trust in computer science and the semantic web. J. Web Seman. **5**(2), 58–71 (2007)
8. Nitti, M., Girau, R., Atzori, L.: Trustworthiness management in the social internet of things. IEEE Trans. Knowl. Data Eng. **26**(5), 1253–1266 (2014)
9. Premarathne, U.S.: MAG-SIoT: a multiplicative attributes graph model based trust computation method for social internet of things. In: 2017 IEEE International Conference on Industrial and Information Systems (ICIIS), pp. 1–6. IEEE, Peradeniya (2017)
10. Ekbatanifard, G., Yousefi, O.: A novel trust management model in the social internet of things. J. Adv. Comput. Eng. Technol. **5**(2), 57–70 (2019)
11. Gai, F.Y.: Research on trust management based security mechanism in Internet of Things. National University of Defense Technology (2017)
12. Wei, L., Wu, J., Long, C.: On designing context-aware trust model and service delegation for social internet of things. IEEE Internet Things J. **8**(6), 4775–4787 (2021)

13. Jafarian, B., Yazdani, N., Haghighi, M.S.: Discrimination-aware trust management for social internet of things. Comput. Netw. **178**, 107254 (2020)
14. Meena Kowshalya, A., Valarmathi, M.L.: Dynamic trust management for secure communications in social internet of things (SIoT). Sādhanā **43**(9), 1–8 (2018). https://doi.org/10.1007/s12046-018-0885-z
15. Chen, I., Bao, F., Guo, J.: Trust-based service management for social internet of things systems. IEEE Trans. Dependable Secure Comput. **13**(6), 684–696 (2016)
16. Sagar, S., Mahmood, A., Kumar, J., et al.: A time-aware similarity-based trust computational model for social internet of things. In: GLOBECOM 2020 Global Communications Conference, pp. 1–6 (2020)
17. Zhou, S., Bin, S., Shao, F.J.: Material diffusion recommendation algorithm based on multi-subnet composite complex network model. Complex Syst. Complex. Sci. **15**(04), 77–84 (2018)
18. Sui, Y.: Study on multi-subnet complex network model and its related properties. Qingdao University (2012)
19. Nitti, M., Atzori, L., Cvijikj, I. P.: Network navigability in the social internet of things. In: 2014 IEEE World Forum on Internet Of Things (WF-IoT), pp. 405–410, IEEE. Seoul (2014)
20. Atzori, L., Iera, A., Morabito, G.: The social internet of things (siot)–when social networks meet the internet of things: concept, architecture and network characterization. Comput. Netw. **56**(16), 3594–3608 (2012)
21. Ouechtati, H., Nadia, B.A., Lamjed, B.S.: A fuzzy logic-based model for filtering dishonest recommendations in the social internet of things. J. Ambient Intell. Humanized Comput. 1-20 (2021).
22. Marche, C., Atzori, L., Nitti, M.: A dataset for performance analysis of the social internet of things. In: 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1–5. IEEE, Bologna (2018)
23. Marche, C., Atzori, L., Iera, A., et al.: Navigability in social networks of objects: the importance of friendship type and nodes' distance. In: 2017 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. IEEE, Singapore (2017)
24. Qin, Q., Zhang, H.R.: Three-branch recommendation based on trust transfer mechanism. Pattern Recogn. Artif. Intell. **33**(07), 600–609 (2020)