Trust information network in social Internet of things using trust-aware recommender systems

Juyeon Son¹, Wonyoung Choi² and Sang-Min Choi¹

Abstract
Social Internet of things is one of the most up-to-date research issues in the applications of Internet of things technologies. In social Internet of things, accuracy and reliability are standard features to discerning decisions. We assume that decision support systems based on social Internet of things could leverage research from recommender systems to achieve more stable performance. Therefore, we propose a trust-aware recommender systems suitable for social Internet of things. Trust-aware recommender systems adapt the concept of social networking service and utilize social interaction information. Trust information not only improves recommender systems from opinion spam problems but also more accurately predicts users’ preferences. We confirm that the performance of a recommender system becomes more improved when implicit trust is able to satisfy the properties of trust in the social Internet of things environment. The structure and amount of social link information are context-sensitive, so applying the concept of trust into social Internet of things environments requires a method to optimize implicit and explicit trust with minimal social link information. Our proposed method configures an asymmetric implicit trust network utilizing user–item rating matrix and transforms trust propagation metrics for a directional and weighted trust network. Through experiments, we confirm that the proposed methods enable higher accuracy and wider coverage compared to the existing recommendation methods.

Keywords
Internet of things, recommender systems, social network, trust-aware, implicit trust, trust asymmetry, trust propagation

Date received: 1 November 2019; accepted: 3 February 2020

Handling Editor: Pascal Lorenz

Introduction
The basic concept of the Internet of things (IoT) is that various things or objects are interconnected with each other and achieve their common purpose.¹ Various things or objects can be interconnected with addressing wireless communication, such as radio frequency identification (RFID) or near-field communication (NFC).²,³ For example, in the logistics domain, researchers examined the reduction of logistics by addressing the purchasing of materials, transportation, and storage using the IoT.⁴ In other domains, such as composite structures, researchers address sensor networks to model methods.⁵–⁷ People also considered of efficient methods that analyze personal information, such as social or historical activities on the web using smart devices in the IoT.⁸

As IoT is recognized as a new paradigm of modern wireless communication in several fields,² research on...
social IoT is actively underway to magnify the great potential. A variety of devices are connected, communicated, and shared, and actions can be determined by the information.\textsuperscript{9} IoT technologies send and share information among various devices utilizing wireless sensor networks. To establish IoT environments, we first need to build reliable wireless sensor networks. To build the networks, we can utilize methods for detecting selective forwarding attacks as well as robust methods for identifying outliers and data gaps.\textsuperscript{10,11}

There are studies for effectively building wireless sensor networks as well as reliability. Chi and Chen\textsuperscript{12} have proposed the feasible method for physical communication and link optimization in wireless communication. Liu et al.\textsuperscript{13} have proposed the subtractive clustering algorithm to select cluster heads and build optimal clusters.

To provide various IoT services, we apply smart devices, such as mobile, and concept of social relationships to IoT.\textsuperscript{14,15} In the case of IoT using social concepts, we can use recommendation services by addressing data from IoT devices.\textsuperscript{16} We can also discover the social relationships among physical objects utilizing the spatial–temporal attributes for the devices.\textsuperscript{17} In addition, there is research applying social concepts to IoT for vehicles.\textsuperscript{18}

There is a trade-off between scalability and reliability in the social IoT.\textsuperscript{19} Namely, if we build a social network based on more devices, the reliability of the data is compromised. Because of this reason, the accuracy and reliability of the information are considered as the important factors in social IoT. Each factor is an act of criteria to determine the decision. We assumed that a decision support system in social IoT could produce more reliable results by adopting the research of the recommendation system on the web. Therefore, we first introduce recommender systems on the web and propose a trust-aware recommender system suitable for social IoT.

As the volume of online information grows rapidly, huge amounts of information lead information inefficiency in information retrieval. As a solution to reduce the information overload problems, “recommender system” has become an important research topic. Recommender systems analyze the preference of users with users’ past record or attributes and then provide personalized suggestions that users might be interested in. Depending on the various information channels, such as smartphones and wearable devices, recommender systems have extended application area into music, product, video, and social connections.\textsuperscript{20} Initial recommender systems are focused on utilizing raw data from database, including users’ ratings and demographic features, and properties of items to predict the preference of users.\textsuperscript{21–24}

The conventional recommender systems are divided into three types: content-based filtering, collaborative filtering (CF), and hybrid recommender systems.\textsuperscript{25–30} Content-based recommender systems are based on calculating item similarity with properties. CF-based systems recommend items that other users with similar preferences liked in the past. Hybrid recommender systems combine the techniques of content-based filtering and the CF. However, such conventional recommender systems suffer from problems, such as data sparsity, cold start, and opinion spam problems.\textsuperscript{31,32}

Trust-aware recommender systems reduce the problems in conventional recommender systems by adapting the concept of the social network service into recommender systems.\textsuperscript{33–37} Trust in recommender systems means one’s belief toward the ability of others in providing valuable ratings.\textsuperscript{38–40} Information representing social interaction among users is the main source to find other users having similar tendencies, which is under the assumption that user behaviors are affected by other users whom they trust.\textsuperscript{41}

In trust-aware recommender systems, there are two types of trust: explicit and implicit trust.\textsuperscript{42,43} Explicit trust is pre-established social links among users in social network and it is defined directly by users. Explicit trust-aware recommender systems provide a function for users to mark other users whom they trust. Explicit trust information is separately saved in user–user trust matrix database. However, implicit trust is not specified by users but inferred from a user–item rating matrix.

While explicit trust information reduces the shortcomings of traditional recommender systems, there are still drawbacks to the way of incorporating explicit trust into recommender systems.\textsuperscript{42,44,45} First of all, the lower the density of the dataset, the more likely trust sparsity issues arise which leads to degrade the prediction performance. The user–user trust matrix is generally less dense than user–item rating matrices because users tend to be more reluctant to provide personal information to systems. Second, most recommender systems in the real world do not have features for explicit trust. Third, explicit trust datasets used in research are based on research-oriented datasets that follow a binary form to protect privacy. Finally, there is a trust tendency problem where each user expresses degree of trust at different levels.

Since such problems degrade the quality of recommendations, it becomes an important matter to develop implicit trust methods to reflect properties of trust: transitivity, asymmetry, dynamicity, and context dependence.\textsuperscript{42} Trust transitivity means that trust must be propagated.\textsuperscript{46,47} Trust asymmetry is that the structure of a trust network should be a directional and weighted graph like in the real world. Trust dynamicity is that the level and the state of trust change over time. Context dependence means that degrees of trust on
others may vary depending on areas. However, current implicit trust metrics only satisfy transitivity. Therefore, we configure an asymmetric implicit trust network from user–item rating matrix and then additionally infer latent trust relations utilizing trust propagation property. The proposed method requires only user–item rating dataset and it is adaptable to most recommender systems in the real world. Also, we reduce the trust tendency problem by considering the general assessment of each item in calculating trust values between two users.

We evaluate our method with the fivefold cross validation and compare our method with three existing methods: (1) CF with a threshold of Pearson’s correlation coefficient (PCC), (2) Shambour’s implicit trust method, and (3) Moradi and Ahmadian’s reliability-based recommendation method. Through experiments, the proposed method enables relatively high accuracy and a wide range compared to the existing recommendation studies. The study improves the existing implicit trust-aware recommender system without additional trust databases.

In section “Background,” we briefly review the background and the related works on the trust-aware recommender systems. In section “Relative-trust recommendation models,” we introduce our recommendation methods. Then, we compare our proposed method with three other related methods using FilmTrust in section “Experiments.” Finally, we discuss the conclusion and the future work in section “Conclusion.”

Background

Trust-aware recommender systems

Trust-aware recommender systems have a network of trust relationship among users like in social networking sites (SNS). When user A registers user B into a trust list, user A becomes a “truster” and user B is a “trustee” in the trust relationship. A review is a main factor when a “truster” decides whether to trust on “trustee” or not. A trust network is described as a weighted directed graph $G$ with a set $V$ of vertices and a set $E$ of trust relations. A vertex represents a single user and a directed edge represents trust relationship between two users. Trust recommender systems analyze interest, preferences, and social behavior of users utilizing the trust information.

In recommender systems, trust means one’s belief toward the ability of others in providing valuable ratings. Trust network has the following properties: asymmetry, transitivity, dynamicity, and context dependence. Asymmetry is that a trust value $T_{u,v}$ from user $u$ to user $v$ and a trust value $T_{v,u}$ from user $v$ to user $u$ can be different. It is because each one has a different standard to mark the degree of trust. For instance, if user $u_2$ trusts user $u_1$ with 2 out of 10, there is no guarantee that user $u_1$ also trusts user $u_2$ to the same extent. Transitivity means that trust can be propagated. Transitivity is used to reduce trust data sparsity problem with extracting latent trust relations. For example, if user $u_1$ trusts user $u_2$ and user $u_2$ trusts user $u_3$, we expect the latent relationship from user $u_1$ to user $u_3$. Dynamicity is that the level and the state of trust change over time. Also, trust relation is easy to be damaged, but difficult to be created. Context dependence is that levels of trust on others may vary depending on areas. For example, a user $u_1$ may trust user $u_2$ in Electronics, but it does not guarantee that a user $u_1$ trusts user $u_2$ in Kitchenware to the same extent.

There are two general approaches to assort trust: explicit and implicit trust. Explicit trust is a pre-established social link between users in a social network and it is explicitly defined by users. Explicit trust methods configure explicit trust networks as directional and unweighted graphs because explicit trust dataset for research is formed in binary. A user–user matrix contains sets of user IDs of truster and trustee, and the trust values. A trust relation exists only when trust value $T_{u,v}$ is 1 where user $u$ is truster and user $v$ is trustee. Table 1 and Figure 1 show the dataset and an explicit trust network. In the example, user $u_1$ trusts user $u_2$ with 1.

| Truster | Trustee | Weight |
|---------|---------|--------|
| 1       | 2       | 1      |
| 2       | 4       | 1      |
| 2       | 3       | 1      |
| 3       | 4       | 1      |

Figure 1. An example of an explicit trust network based on Table 1.
However, implicit trust is inferred from the rating dataset. An implicit trust network is denoted as a weighted and undirected graph. If two users have ratings on common items, there is likely to be a latent implicit trust statement between two users.42,52,53 The concept of implicit trust is hardly distinguishable from user-based recommender system.54

Table 2 and Figure 2 show an example of an implicit trust network inferred from rating dataset. Recommender systems compute implicit trust values utilizing the user–item rating matrix. In Table 2, trust relation $T_{u_1u_2}$ from user $u_1$ to user $u_2$ is computed based on the ratings of item $i_4$ which user $u_1$ and user $u_2$ commonly rate on. In other words, user $u_1$ has ratings for items $i_3$ and $i_4$. User $u_2$ rated items $i_1$, $i_2$, and $i_4$. In this case, user $u_1$ and $u_2$ have only one common rated item $i_4$. We use the common rating of $i_4$ as trust reaction $T_{u_1u_2}$.

### Related works

Implicit trust metrics reduce shortcomings in explicit trust metrics.42,44,55 Guo et al.42 incorporate the same methods, which compared, to the matrix factorization techniques. The implicit trust metrics in both studies satisfy the only transitivity among trust properties.42,44 Wang et al.55 employ implicit trust relationships to overcome the disadvantage of explicit trust relationships. They propose two neural network models addressing both implicit and explicit trust relationships.

Reliability measurements are methods to filter unnecessary information that is expected to cause a negative effect on the performance of recommendations.48,54 Hernando et al.54 propose reliability measurements for CF. The proposed reliability measurements filter unnecessary neighbors before predicting ratings. However, it is unadaptable for recommender systems having explicit trust networks. So, Moradi and Ahmadian48 improve reliability measurements suitable for recommender systems having explicit trust networks. Wang et al.55

Even though explicit trust information improves the performance of traditional recommender systems, there are still limitations in explicit metrics.42,44,45 All the techniques for explicit trust are available only when recommender systems have the explicit trust dataset. However, most recommendation systems in the real world do not have additional explicit trust datasets.

Also, explicit trust values of the publicly available dataset are scaled in a different way than real-world recommender systems. Although trust value in real-world recommender systems is scaled with real numbers, trust value in most publicly available datasets is binary because of user privacy. Moreover, there is a tendency issue that each user has a different standard to express the degree of trust. In addition, trust sparsity problem is more serious than in rating information because it is difficult to encourage users to rate trust values of others into systems. It becomes more important to improve implicit trust methods to overcome the disadvantages found in existing methods for explicit trust network. However, current implicit trust metrics also have problems that these metrics only satisfy transitivity among properties of trust. The structure of implicit trust network configured by existing metrics is a symmetry graph, which is unrealistic. Moreover, there is no consideration of dynamicity or context dependence. Although implicit trust value decreases trust tendency problem more than explicit trust value, implicit trust value is also risky on trust tendency problem because of no consideration on the general assessment of each item.

We expect the performance of recommendations to be improved if implicit trust further satisfies trust properties. Therefore, our proposed method configures trust implicit network as an asymmetric structure like in the real world. Also, we reduce trust tendency problem by considering the general assessment of items.
**Relative-trust recommendation models**

We follow the definition of trust as one’s belief toward the ability of others in providing valuable ratings. Trust-aware recommender systems presume that there is high correlation between trust and similarity of preference. Therefore, the core procedure is to identify neighbors who might have similar preference.

Our proposed method is based on implicit measurement with following reasons. First of all, implicit trust is more easily obtained in recommender systems than explicit trust. Implicit trust value is calculated from user-item rating matrix and explicit trust value is obtained from user-user trust matrix. However, user-user trust matrix is not commonly used in recommender systems yet. It is because additional functions and datasets for user-user trust datasets require more memory space and computation. Also, users tend to be reluctant to provide their personal information to the system.

Second, the density of the dataset is important than the amount. When density of dataset is high, there are many single users or items with historical data. However, low-density datasets have many single users or items with little or no historical data. In general, user-item dataset is denser than user-user dataset. Therefore, our method configures a user-user network from user-item datasets and predicts users’ preferences for reducing trust sparsity.

Third, implicit trust is more directly related with users’ purchase behavior. When a user A decides to mark to trust another user B, the user A may trust user B for IT matters, but not fashion. Then, the explicit trust value becomes a latent risk factor to produce prediction error when predicting user A’s preference. However, an explicit trust value is not distinguishable about the contextual reason why user A decides to trust user B. However, there are data sparsity and tendency problems even in implicit trust metrics. Our proposed metrics suggest three following steps to alleviate such problems in implicit trust measurements:

1. **Constructing asymmetric trust networks**: we calculate the relative similarity between trustee and trustor to obtain an implicit trust network in the form of a directional and weighted graph like in the real world. We utilize the average rating of each item as a representative factor of the qualities of items to reduce the user tendency problem.

2. **Inferring latent trust networks**: we utilize a trust propagation metric to compensate for the rating sparsity problem. We transform the existing trust propagation metric for explicit trust networks to be suitable for our trust network formed in a directional and weighted graph.

3. **Prediction**: we make predictions for recommendations based on the trust network.

Figure 3 shows the overall process of the proposed method.
**Constructing asymmetric trust networks**

The first step is to calculate the relative similarity between the truster and trustee using the user–item rating dataset. The proposed implicit trust value has two main differences from existing methods. First, we utilize the average rating of an item as an indicator representing the general assessment of each item. Existing methods derive implicit trust values with the similarity of their ratings and the average rating of a user is a representative of personal tendency. Therefore, when a user A gives the best rating for all the purchased items, the user A is categorized as a generous consumer. However, it leads to false predictions in the case that he gave generous items because he purchased only good quality items, not because he is a generous customer. In the situation, we cannot guarantee that he is willing to give the best rating again for the next purchase. Thus, if both users give the highest rating even to the worst rated items in the past, then implicit trust between the two users should be weighted more.

Second, our proposed method calculates implicit trust value as relative and asymmetry relation. We argue that the quality of products is the primary factor to consider the rating tendency of each user, not the average rating. Implicit trust value between two users is symmetry following to existing implicit trust methods. That means, if there is a trust relationship between two users, both users must believe that other users provide valuable ratings to the same extent. Considering trust relationships, in reality, such symmetry trust relations hardly exist.

In the sense, we concentrate on the phenomenon that consumers review other’s ratings to pre-estimate the quality of an item before making orders. Our proposed method first derive relative similarity value \( a_{u,v} \) from user \( u \) to user \( v \) from all the items commonly rated by both users. Each trust relation has a truster and a trustee and it is in a form of directional and asymmetry edge.

This step uses equation (1)

\[
a_{u,v} = \begin{cases} 
    \frac{r_{max} - |r_{ui} - r_{vi}|}{r_{max} - \bar{r}_i} & \text{if } |I| > 0 \\
    0, & \text{otherwise}
\end{cases}
\]

where \( r_{ui} \) is a rating by user \( u \) for item \( i \), \( r_{max} \) is the maximum value of the rating in the recommender system, \( \bar{r}_i \) is the average rating about item \( i \) except \( r_{ui} \) and \( r_{vi} \), \( |I| \) is the number of ratings about item \( i \) except \( r_{ui} \) and \( r_{vi} \).

Then, we total up a set of \( a_{u,v} \) to derive the relative similarity value \( b_{u,v} \) from user \( u \) to user \( v \) for all the items user \( u \) and user \( v \) purchased in common using equation (2)

\[
b_{u,v} = \frac{1}{|I_{u,v}|} \sum_{k \in I_{u,v}} (a_{u,v})_k
\]

where \( |I_{u,v}| \) is the number of common items purchased by user \( u \) and user \( v \).

Table 3 is an example of rating dataset to help the explanation above. Following to existing implicit trust methods, \( I_{Sophia,Alice}, I_{Alice,Sophia}, I_{Alice,Michael}, I_{Michael,Sophia} \) are all same where \( I_{A,B} \) is an implicit trust value from user \( A \) to user \( B \). It is because implicit trust relations by existing methods are unidirectional. However, following to the proposed method, \( I_{Sophia,Alice} \) is bigger than \( I_{Sophia,Michael} \) and \( I_{Sophia,Alice} \) is bigger than \( I_{Alice,Sophia} \).

**Inferring latent trust networks**

After constructing an asymmetric trust network, we identify latent trust relations through the trust propagation metric. Propagation metrics infer latent relationships between users and alleviates the data sparsity problem. However, existing propagation methods are adaptable only for a directional and unweighted graph with explicit trust information or a unidirectional graph with implicit trust values. Since our method configures a trust network as a directional and weighted graph, existing trust propagation is not adoptable. So, we transform the existing propagation metric to be suitable for our trust network with calculating the final relative similarity \( I_{u,v} \) between user \( u \) and user \( v \). Figure 4 shows an example of implicit trust
propagation. The trust network is configured following the proposed method, which is clearly different from a trust network with implicit trust information.

Even though there is no directional implicit trust value from user $a$ to user $b$ in Figure 4, it is possible to calculate $t_{a,b}$ through equation (3). In a trust network configured by the proposed method, each edge is weighted with real value. In the example, we can find two shortest paths user $a$ to user $b$: shortestpath $(A \rightarrow m_1 \rightarrow b)$ and shortestpath $(A \rightarrow m_2 \rightarrow b)$. In the case, $t_{a,b}$ utilizing shortestpath $(A \rightarrow m_1 \rightarrow b)$ is bigger than $t_{a,b}$ utilizing shortestpath $(A \rightarrow m_2 \rightarrow b)$

\[ t_{u,v} = \max_{p \in S_{uv}} \sum_{i=1}^{k} \frac{k-i+1}{k} \cdot b_{u,a_i} \]  

(3)

where $P = \{u, a_1, a_2, \ldots, a_k, v\}$ is a set of users in a shortest path from user $u$ to user $v$, $S_{uv}$ is a set of all the shortest paths from user $u$ to user $v$ in $d_{max}$ hops, $i$ is the smallest number of hops from user $u$ to user $v$.

Since the relative similarity value $a_{u,v}$ for an item is a ratio of the difference between $r_{u,i}$ and $\bar{r}_i$ to the difference between $r_{u,i}$ and $r_{v,i}$, we regulate the final relative similarity value $t_{u,v}$ with the medium relative similarity value $\bar{t}_{u,v}$ of all relative similarity values in the system. The finalized weight $w_{u,v}$ is calculated as $t_{u,v}$ divided with $\bar{t}_{u,v}$.

We consider that $t_{u,v}$ is valuable information for making recommendations. The important difference is to find all the shortest paths in $d_{max}$ hops from user $u$ to user $v$. $d_{max}$ is distance threshold from user $u$ to $v$ to save computation complexity. Therefore, we consider users who have less distance from the target user $u$ than the threshold.

**Prediction**

Then, we predict ratings of unseen items for a target user through Resnick’s prediction formula.\(^{60}\) The predicted rating $p_{u,i}$ of item $i$ for user $u$ is derived as follows

\[ p_{u,i} = \bar{r}_u + \frac{\sum_{v \in N_{u,i}} w_{u,v}(r_{v,i} - \bar{r}_i)}{\sum_{v \in N_{u,i}} W_{u,v}} \]  

(4)

where $\bar{r}_u$ is the average ratings by user $u$, $r_{v,i}$ is the rating of item $i$ by user $v$, $N_{u,i}$ is a set of neighbors who have a rating of item $i$ and $w_{u,v}$.

We select $K$ nearest neighbors of the target user $u$ among $N_{u,i}$. Also, only $w_{u,v}$ bigger than threshold $\theta$ is considered in prediction because low $w_{u,v}$ value degrades the quality of recommendations. Finally, we suggest $Top - N$ recommendations that user might be interested in.

**Experiments**

**Dataset**

We analyze FilmTrust dataset crawled by Guo et al.\(^{42,61,62}\) FilmTrust is a movie recommender website where users evaluate movies and also add other users to the trust list. The user–item rating data consist of the total 35,497 ratings of 2071 different items by 1508 users. The trust network data contain 1853 directed trust edge information from 609 trusters to 732 trustees without trust weights. The summary of the FilmTrust dataset is in Tables 4 and 5.

We verify the performance of the proposed method with the fivefold cross validation.\(^{42,44}\) We evaluate the accuracy of rating prediction with the following metrics—mean absolute error (MAE) and root mean square deviation (RMSE). We also utilize rating coverage (RC) and user coverage (UC) to test the available coverage of rating prediction.

MAE is the average difference between predicted rates and real rates, and the definition of MAE for user $u$ is

\[ MAE = \frac{\sum_{i} |p_{u,i} - r_{u,i}|}{k} \]  

(5)

where $u$ is a target user, $i$ is a target item, $r_{u,i}$ means a real rating by a user $u$ for item $i$. $p_{u,i}$ is the predicted rating by methods and $k$ is the number of predicted ratings. The lower MAE values means the higher accuracy of rating prediction because the evaluated method is able to calculate the predicted rating $p_{u,i}$ close to the actual rating by a target user $u$.

RMSE shows the contributions of the absolute errors between the predicted and actual rates. Low RMSE value means positive high accuracy of recommendation and the definition is as follows

\[ RMSE = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (r_i - p_i)^2} \]  

(6)

| Table 4. Rating dataset. |
|--------------------------|
| No. of users | No. of items | No. of ratings |
| 1508 | 2071 | 35,497 |

| Table 5. Trust dataset. |
|--------------------------|
| No. of trusters | No. of trustee | No. of edges |
| 609 | 732 | 1853 |
where $r_i$ and $p_i$ are real and predicted ratings, $N$ is the total number of ratings that are predicted by the evaluated method. RC is used to check how many effective ratings are predicted by the proposed method. RC is an important factor to understand a trade-off between the accuracy of rating prediction and predictable RC. RC is calculated as the number of predictable ratings divided with the total number of ratings in the test set. High RC value means the more ratings are predictable with the evaluated method. If RC value is 1, all the ratings in the systems are predictable with the evaluated method within acceptable errors.

We also evaluate UC. UC measure defines the portion of users who are able to have at least one predictable rating with the proposed method. UC equals the number of predictable users divided by the total number of users in the test set. High UC value means the high performance of recommendation methods. When UC value is 1, the evaluated method can predict at least one item for all users in systems within acceptable errors.

**Result and analysis**

To evaluate the proposed method, we calculate the accuracy of rating prediction and predictable RC with the following existing methods:

1. CF with threshold
2. Shambour’s method
3. Moradi and Ahmadian’s reliability-based recommendation method

CF based on PCC with threshold shows the worst performance in the evaluation of implicit trust methods. Shambour’s method shows the best performances in the evaluation of implicit trust methods. Reliability-based recommendation method by Moradi and Ahmadian shows the best performance among trust-aware recommender systems using explicit and implicit trust statements.

We set threshold $\theta_p$ with 0.7 for PCC same with evaluations by Guo et al. So, we consider an implicit trust value between users a valid factor only when PCC is higher than 0.7. For Shambour’s method, we set $\theta_p = 0.15$ which shows the best performance. For Moradi’s method, we set threshold as $\alpha = 0.6$, $\beta = 0.5$, and $\theta_m = 0.7$ for the best performance. For the proposed method, we set threshold $\theta = 0.7$ and $d_{\text{max}}$ for implicit trust relations as 3. $K$-nearest neighbors method is used commonly and $k$ is the most valuable factor in the experiments. The performance of all methods in the experiment shows positive relation with $K$ and we set $k$ as 50 which is the biggest value used in Guo et al.

Figures 5 and 6 show the comparison results of the proposed method with other methods. As the result shown in Figure 5, the performance of the proposed method outperforms other methods. Also, explicit trust statements in the proposed method negatively effect on the performance when the density of trust statements is sparse. Since FilmTrust dataset is dense compared with other datasets, the difference among methods is relatively small.

Figure 7 shows the MAE performance of predicting item ratings over density of each test set. Since we conduct fivefold cross evaluation, each training dataset has different density. Our method shows not only the lowest MAE but also the highest RC than other methods. It shows more clearly that our proposed method is effective considering a trade-off between the coverage and accuracy of the predictions in the recommender system.

The parameter $\theta$ is an important factor in determining the results. $\theta$ is a threshold parameter to eliminate the information of other users who are relatively less relevant with target users. Figures 8 and 9 show the result of change in $\theta$. In the figures, we notice that the prediction result shows more precise but the coverage
result shows lower as \( \theta \) is increased because of the trade-off between coverage and MAE. Therefore, we set up \( \theta = 1.0 \) in our experiments for the best performance in MAE and RC.

The UC performance in Figure 10 shows that UC gets lower as threshold \( \theta \) increases, but our proposed method covers more users in systems.

We also test RMSE of change over the threshold \( \theta \). As illustrated in Figure 11, RMSE shows positive relation over threshold \( \theta \). From the performances of MAE and RC, we notice that relative similarity by our proposed method is positively related with recommendations. Also, results of RC, UC, MAE, and RMSE of change in threshold \( \theta \) show that our inferred implicit trust value is highly connected with recommendation performance. Moreover, our proposed method improves the structure of implicit trust network to reflect trust asymmetry, unlike existing implicit trust methods.

**Conclusion**

Trust-aware recommender systems utilize explicit trust and implicit trust to make better personalized recommendations in terms of correctness and coverage. Although most research about trust-aware recommender systems is focused on merging explicit trust into recommender systems, our research concentrates on improving implicit trust metrics to compensate for the limitations in explicit trust. For that, we argue that the performance of a recommender system becomes improved when implicit trust is able to explain the properties of trust better. The properties are asymmetry, trust tendency, and trust propagation. It means that we can utilize implicit trust in the environment of social IoT. Namely, we can use implicit trust in social IoT to spread more reliable information.
Therefore, we propose a method to configure an asymmetric trusted network. Also, we suggest a propagation metric for a directional and weighted trust graph. The proposed method calculates the relative similarity value based on the general assessment of each item. Through experiments, we confirm that our proposed method shows positive performance with higher accuracy and RC compared to existing methods. From our work, we provide contributions in recommender systems and social IoT:

1. We propose a method to configure an implicit trust network reflecting trust properties from a user-item rating matrix in a recommender system;
2. We propose new implicit trust metric, relative trust value;
3. We modify the explicit trust propagation method for a directional and weighted trust graph;
4. Our proposed method shows higher accuracy with higher RC compared to the existing recommendation methods;
5. It can be guaranteed that our proposed method can be utilized in social IoT environment;
6. We identify possibilities of new follow-up studies of implicit trust metrics.

As users are willing to provide less information online, the methods for predictions with less referred data should be considered. For that, we suggest novel follow-up studies based on our work: reliability measurements, and belief propagation methods for a directional and weighted trust network.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by a grant (18SCIP-C079445-05) from Architecture and Technology Development Research Program funded by Ministry of Land, Infrastructure, and Transport of Korean government.

ORCID iD
Sang-Min Choi https://orcid.org/0000-0003-0100-8269

References
1. Giusto D, Iera A, Morabito G, et al. (eds). The Internet of things: 20th Tyrrhenian Workshop on Digital Communications. Berlin: Springer, 2010.
2. Atzori L, Iera A and Morabito G. The internet of things: a survey. Comput Netw 2010; 54(15): 2787–2805.
3. Gluhak A, Krco S, Nati M, et al. A survey on facilities for experimental internet of things research. IEEE Commun Mag 2011; 49(11): 58–67.
4. Bendavid Y and Boeck H. Using RFID to improve hospital supply chain management for high value and consignment items. Proc Comput Sci 2011; 5: 849–856.
5. Xu X and Yang H. Network method for deformation analysis of three-dimensional point cloud with terrestrial laser scanning sensor. Int J Distrib Sens Netw 2018; 14(11): 1550147718814139.
6. Yang H, Xu X, Kargoll B, et al. An automatic and intelligent optimal surface modeling method for composite tunnel structures. Comp Struct 2019; 208: 702–710.
7. Yang H and Xu X. Multi-sensor technology for b-spline modelling and deformation analysis of composite structures. Comp Struct 2019; 224: 111000.
8. Welbourne E, Battle L, Cole G, et al. Building the internet of things using RFID: the RFID ecosystem experience. IEEE Int Comput 2009; 13(3): 48–55.
9. Jung J, Chun S, Jin X, et al. Quantitative computation of social strength in social internet of things. IEEE Int Thing J 2018; 5(5): 4066–4075.
10. Xu X, Yang H and Kargoll B. Robust and automatic modeling of tunnel structures based on terrestrial laser scanning measurement. Int J Distrib Sens Netw 2019; 15(11): 1550147719884886.
11. Zhang Q and Zhang W. Accurate detection of selective forwarding attack in wireless sensor networks. Int J Distrib Sens Netw 2019; 15(1): 1550147718824008.
12. Chi T and Chen M. Interconnection algorithm of a wide range of pervasive devices for the internet of things. Int J Distrib Sens Netw 2018; 14(1): 1550147718756014.
13. Liu B, Yang H, Chen Q, et al. Research on the subtractive clustering algorithm for mobile ad hoc network based on the Akaike information criterion. Int J Distrib Sens Netw 2019; 15(9): 1550147719877612.
14. Félix IR, Castro LA, Rodriguez L, et al. Mobile sensing for behavioral research: a component-based approach for rapid deployment of sensing campaigns. Int J Distrib Sens Netw 2019; 15(9): 1550147719874186.
15. Ortíz AM, Hussein D, Park S, et al. The cluster between internet of things and social networks: review and research challenges. IEEE Int Thing J 2014; 1(3): 206–215.
16. Saleem Y, Crespi N, Rehman MH, et al. Exploitation of social IoT for recommendation services. In: Proceedings of the 3rd IEEE world forum on internet of things (WF-IoT), Reston, VA, 12–14 December 2016, pp.359–364. New York: IEEE.
17. Wei D, Ning H, Qian Y, et al. Social relationship for physical objects. Int J Distrib Sens Netw 2018; 14(1): 1550147718754968.
18. Iqbal R, Butt TA, Afzaal M, et al. Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions. Int J Distrib Sens Netw 2019; 15(1): 1550147719825820.
19. Chen I, Bao F and Guo J. Trust-based service management for social internet of things systems. IEEE Trans Depend Sec Comput 2016; 13(6): 684–696.
20. Mukamakuza CP, Sacharidis D and Werthner H. Mining user behavior in social recommender systems. In: Proceedings of the 8th international conference on web intelligence, mining and semantics (WIMS), Novi Sad, 25–27 June 2018, pp.37:1–37:6. New York, NY: Association for Computing Machinery.

21. Choi K, Yoo D, Kim G, et al. A hybrid online-product recommendation system: combining implicit rating-based collaborative filtering and sequential pattern analysis. Electron Comm Res Appl 2012; 11(4): 309–317.

22. Lee SK, Cho YH and Kim SH. Collaborative filtering with ordinal scale-based implicit ratings for mobile music recommendations. Inform Sci 2010; 180(11): 2142–2155.

23. Núñez-Valdés ER, Lovelle JMC, Martinez OS, et al. Implicit feedback techniques on recommender systems applied to electronic books. Comput Human Behav 2012; 28(4): 1186–1193.

24. Gohari FS, Aliee FS and Haghighi H. A significance-based trust-aware recommendation approach. Inform Syst 2020; 87: 101421.

25. Adomavicius G and Tuzhilin A. Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions. IEEE Trans Knowl Data Eng 2005; 17(6): 734–749.

26. Bobadilla J, Ortega F, Hernando A, et al. Recommender systems survey. Knowl Based Syst 2013; 46: 109–132.

27. Burke R. Hybrid recommender systems: survey and experiments. User Model User Adapt Interact 2002; 12(4): 331–370.

28. Porcel C, Tejeda-Lorente A, Martinez M, et al. A hybrid recommender system for the selective dissemination of research resources in a technology transfer office. Inform Sci 2012; 184(1): 1–19.

29. Vozalis MG and Margaritis KG. Using SVD and demographic data for the enhancement of generalized collaborative filtering. Inform Sci 2007; 177(15): 3017–3037.

30. Zhang S, Gu Y and Yi G. A hybrid knowledge push method based on trust-aware and item-cluster oriented to product design. New Generat Comput 2019; 37(3): 339–357.

31. Reafee W and Salim N. The social network role in improving recommendation performance of collaborative filtering. In: Herawan T, Deris M and Abawajy J (eds) Proceedings of the first international conference on advanced data and information engineering (DaEng). Singapore: Springer, 2014, pp.231–240.

32. Victor P, De Cock M and Cornelis C. Trust and recommendations. In: Ricci F, Rokach L, Shapira B, et al. (eds) Recommender systems handbook. Boston, MA: Springer, 2011, pp.645–675.

33. O’Donovan J and Smyth B. Trust in recommender systems. In: Proceedings of the 10th international conference on intelligent user interfaces, San Diego, CA, 9–12 January 2005, pp.167–174. New York: ACM.

34. Parvin H, Moradi P and Esmaeili S. TCFACO: trust-aware collaborative filtering method based on ant colony optimization. Exp Syst Appl 2019; 118: 152–168.

35. Ahmadian S, Joorabioo N, Jalili M, et al. A temporal clustering approach for social recommender systems. In: International conference on advances in social networks analysis and mining (ASONAM), Barcelona, 28–31 August 2018, pp.1139–1144. New York: IEEE.

36. Pan Y, He F and Yu H. An adaptive method to learn directive trust strength for trust-aware recommender systems. In: Proceedings of the 22nd IEEE international conference on computer supported cooperative work in design (CSCWD), Nanjing, China, 9–11 May 2018, pp.10–16. New York: IEEE.

37. Yu T, Guo J, Li W, et al. Recommendation with diversity: an adaptive trust-aware model. Decision Supp Syst 2019; 123: 113073.

38. Yadav S, Kumar V, Sinha S, et al. Trust aware recommender system using swarm intelligence. J Comput Sci 2018; 28: 180–192.

39. Tong C, Qi J, Lian Y, et al. TimeTrustSVD: a collaborative filtering model integrating time, trust and rating information. Fut Generat Comput Syst 2019; 93: 933–941.

40. Wang X, Liu Y, Lu J, et al. TruGRC: trust-aware group recommendation with virtual coordinators. Fut Generat Comput Syst 2019; 94: 224–236.

41. Hassan T. Trust and trustworthiness in social recommender systems. In: Companion of the 2019 World Wide Web conference (WWW), San Francisco, CA, 13–17 May 2019, pp.529–532. New York, NY: Association for Computing Machinery.

42. Guo G, Zhang J, Thalmann D, et al. From ratings to trust: an empirical study of implicit trust in recommender systems. In: Proceedings of the 29th annual ACM symposium on applied computing. Gyeongju, South Korea, 24–28 March 2014, pp.248–253. New York: ACM.

43. Moradi P, Ahmadian S and Akhlaghian F. An effective trust-based recommendation method using a novel graph clustering algorithm. Phys A Stat Mech Appl 2015; 436: 462–481.

44. Fazeli S, Loni B, Bellogin A, et al. Implicit vs. explicit trust in social matrix factorization. In: Proceedings of the 8th ACM conference on recommender systems, San Jose, CA, 6–10 October 2014, pp.317–320. New York: ACM.

45. Ma X, Lu H and Gan Z. Implicit trust and distrust prediction for recommender systems. In: Proceedings of the 16th international conference on web information systems engineering (WISE), part I, Miami, FL, 1–3 November 2015, vol. 9418, pp.185–199. New York: Springer.

46. RahmatAbadi AF and Alizadeh SH. Effect of distrust propagation to enhance the performance of trust based recommender systems. In: Proceedings of the 9th conference on artificial intelligence and robotics and 2nd Asia-Pacific international symposium, Kish Island, Iran, 10 December 2018. New York: IEEE.

47. Pal B, Banerjee S and Jenamani M. Threshold-based heuristics for trust inference in a social network. In: Proceedings of the 11th international conference on contemporary computing (IC3), Noida, India, 2–4 August 2018, pp.1–7. IEEE Computer Society.

48. Moradi P and Ahmadian S. A reliability-based recommendation method to improve trust-aware recommender systems. Exp Syst Appl 2015; 42(21): 7386–7398.

49. Guo G. Integrating trust and similarity to ameliorate the data sparsity and cold start for recommender systems. In: Proceedings of the 7th ACM conference on recommender
50. Massa P and Avesani P. Trust-aware recommender systems. In: *Proceedings of the 2007 ACM conference on recommender systems*, Minneapolis, MN, 19–20 October 2007, pp.17–24. New York: ACM.

51. Castelfranchi C and Falcone R. Socio-cognitive model of trust: basic ingredients. In: Castelfranchi C and Falcone R (eds) *Trust theory*. Hoboken, NJ: John Wiley & Sons, 2010, pp.35–94.

52. Li YM and Kao CP. Trepps: a trust-based recommender system for peer production services. *Exp Syst Appl* 2009; 36(2): 3263–3277.

53. Park MH, Hong JH and Cho SB. Location-based recommendation system using Bayesian user’s preference model in mobile devices. In: *Ubiquitous intelligence and computing*, Hong Kong, China, 11–13 July 2007, pp.1130–1139. Berlin: Springer.

54. Hernando A, Bobadilla J, Ortega F, et al. Incorporating reliability measurements into the predictions of a recommender system. *Inform Sci* 2013; 218: 1–16.

55. Wang M, Wu Z, Sun X, et al. Trust-aware collaborative filtering with a denoising autoencoder. *Neur Process Lett* 2019; 49(2): 835–849.

56. Hwang CS and Chen YP. Using trust in collaborative filtering recommendation. In: *New trends in applied artificial intelligence*, Kyoto, Japan, 26–29 June 2007, pp.1052–1060. Berlin: Springer.

57. Lathia N, Hailes S and Capra L. Trust-based collaborative filtering. In: *Trust management II*, Trondheim, 18–20 June 2008, pp.119–134. Berlin: Springer.

58. Papagelis M, Plexousakis D and Kutsaras T. Alleviating the sparsity problem of collaborative filtering using trust inferences. In: *Trust management*, Paris, 23–26 May 2005, pp.224–239. Berlin: Springer.

59. Shambour Q and Lu J. A trust-semantic fusion-based recommendation approach for e-business applications. *Decision Supp Syst* 2012; 54(1): 768–780.

60. Resnick P, Iacovou N, Suchak M, et al. Grouplens: an open architecture for collaborative filtering of netnews. In: *Proceedings of the 1994 ACM conference on computer supported cooperative work*, Chapel Hill, NC, pp.175–186. New York: ACM.

61. Guo G, Zhang J and Yorke-Smith N. A novel evidence-based Bayesian similarity measure for recommender systems. *ACM Trans Web* 2016; 10(2): 81–830.

62. Guo G, Zhang J and Yorke-Smith N. Leveraging multi-views of trust and similarity to enhance clustering-based recommender systems. *Knowl Based Syst* 2015; 74: 14–27.