Paper 2019-2-16 http://dx.doi.org/10.29056/jsav.2019.12.16

Trust Evaluation Metrics for Selecting the Optimal Service on SOA-based Internet of Things

Yukyong Kim*†

Abstract

In the IoT environment, there is a huge amount of heterogeneous devices with limited capacity. Existing trust evaluation methods are not adequate to accommodate this requirement due to the limited storage space and computational resources. In addition, since IoT devices are mainly human operated devices, the trust evaluation should reflect the social relations among device owners. There is also a need for a mechanism that reflects the tendency of the trustor and environmental factors. In this paper, we propose an adaptable trust evaluation method for SOA-based IoT system to deal with these issues. The proposed model is designed to minimize the confidence bias and to dynamically respond to environmental changes by combining direct evaluation and indirect evaluation. It is expected that it will be possible to secure trust through quantitative evaluation by providing feedback based on social relationships.

keywords : IoT, SOA, service quality, trustworthy service, trust assessment

1. Introduction

The Internet of Things (IoT) is a technology for connecting intelligent devices with context-awareness and learning capabilities, to a huge network such as the Internet and bundling into a single frame to provide services with optimal useful value to users. The IoT environment consists of numerous heterogeneous IoT devices such as RFID tags, sensors and smart objects, that can provide services on demand. Service-Oriented Architecture (SOA) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network. The basic principles of SOA are independent of vendors, products and technologies. A service is a discrete unit of functionality that can be accessed remotely and acted upon and updated independently. The service in SOA is a black box for its consumer and logically represents a business activity with a specified outcome. Because SOA is a flexible service-based model for construction, assembly and deployment of networks of services, it enables posting, retrieval, selection, and configuration of services provided by extremely numerous IoT devices. In a SOA-based IoT system, each

* Division of Basic Engineering, Sookmyung Women's University
† Corresponding Author : Yukyong Kim (email: ykim.be@sookmyung.ac.kr)
Received: 2019.11.30. Revised: 2019.12.17. Accepted: 2019.12.20.

device is a service consumer, and at the same time can be a service provider that interacts with a service consumer through compatible service APIs. In general, each service not only has a specific function, but also has a set of Quality of Service (QoS) attributes such as response time, availability and reliability. In fact, many service providers can provide similar functionality, but each QoS attribute is different. Trust is another QoS attribute. In the IoT environment, QoS is a critical issue for service consumers because there are huge amounts of heterogeneous devices. Since not only the QoS of the service itself but also the trust level of the service provider is varied, it is difficult to select a service provider of the desired quality. The user has to worry about the level of trust of the service provider. It is very important to know if other IoT services can be trusted when IoT devices request services [1]. The explosive growth of the IoT environment has increased the frequency of interactions among new objects, but some IoT devices may have malicious purposes, such as personal information hijacking or service quality degradation. Therefore, trustworthiness is an important service selection factor in SOA-based IoT systems.

IoT device users can be socially connected via social networks such as Facebook, Twitter, and Google. Especially, social network is easy to produce information and easy to share with friends who have friendship, so the spread and reproduction speed of information is very fast. However, there is a problem of trustworthiness of services provided in the IoT environment, and there is a demand for not only trust of the information itself but also the malfunction of the information generating device, because there are lots of indisputable information that can not be trusted [2].

Evaluating trust in SOA-based IoT systems is a challenging task. In the IoT environment, there is a huge amount of heterogeneous devices with limited capacity. Existing trust evaluation methods are not adequate to accommodate this requirement because of the limited storage space and computational resources. In addition, since IoT devices are mainly human operated devices, the trust evaluation should reflect the social relations among device owners. Since trust is essentially based on human social relations, the subjective view for individual things on social interactions should not be ignored. There is also a need for a mechanism that reflects the tendency of the trustor and environmental factors for the trust model. In a social IoT environment, trustee and trustor are people, devices, systems, applications, and services, and trust measures may be relative. The trust target may be an action to be performed by the trustee and may be information provided by the trustee.

This paper proposes an adaptable trust evaluation method for SOA-based IoT system to deal with these issues. In the SOA-based IoT environment, the proposed model is designed to minimize the confidence bias and to dynamically respond to environmental changes by combining direct evaluation and indirect evaluation. The purpose of this study is to provide a framework for selecting the

optimal trustworthy service from the viewpoint of users by evaluating and predicting the trust of services satisfying the functional requirements. A more objective and systematic approach can be made by formalizing the problem of service selection.

Despite the fact that trust is a key factor of service selection, there is a lack of research on trust evaluation in a IoT environment. We will survey and compare as well as contrast our approach with existing work

The remainder of this paper is organized as follows. In Chapter 2, we discuss issues related to SOA-based IoT environment and describe existing trust evaluation methods. In Section 3, we define the problem of trust evaluation, and in Chapter 4, we propose a trust evaluation method together with a trust model, and formulate the trust evaluation problem in SOA-based IoT. In Section 5, the proposed evaluation method is validated through experiments. Chapter 6 concludes with future works.

2. Related Works

2.1 Features of SOA-based IoT systems

The biggest feature of IoT systems is the heterogeneity of the devices. There is a huge amount of heterogeneous devices such as RFID tags, sensors, smart phones and laptops. These devices are also connected to the network in a variety of ways, such as cable, Wi-Fi, Bluetooth or NFC. SOA technology can be a good alternative for dealing with these problems.

Guinard proposed an SOA-based IoT architecture in which each device provides functionality through a SOAP-based Web service or a RESTful API [1]. A web-based smart space framework is proposed. The framework applies REST to support pervasive applications such as resource sharing on a variety of devices [3].

Recently, IoT system has been developed as social IoT (SIoT) which is a fusion of social networks. Doddy and Shields applied reality mining, a data mining technique that is applied to understand human behavior and relationships, to the IoT system. They identified patterns and interactions among smart objects, and analyzed the issues that need to be addressed in order to implement the proposed method [4]. Kranz explored the possibility of combining social and technical networks to provide joint services to users and technical systems in IoT systems [5]. Atzori proposed the concept of SIoT and analyzed social relationships among objects such as parent-to-person relationships, social contact relations, collaborative relations, and ownership relationships among similar objects [6].

The current SIoT system is characterized by cooperative devices that can be connected to a social network that plays a role of connecting people with existing IoT devices. In such a SIoT environment, each device can provide information through the API of the existing SNS, acquire information of another person, and be influenced by the social relation of the

owner. For example, through SIoT, A's audio can access to the music database of a friend B, and he can continuously receive new music that B acquires. Thus, devices of SIoT distribute and acquire information based on the owner's social relations and have access privileges of other devices. In SIoT, a device is an autonomous agent that can request and provide information and services while maintaining personality as a social entity. In this paper, we discuss the problem of trust in the SIoT system based on SOA.

The SIoT network structure is evolving to ensure mobility and scalability, such as human social networks. Achieving an effective social network of intelligent objects needs socialization of various forms between things similar to human social networks. This socialization should be written and updated according to the functions and activities of objects, and the establishment and management of relationships should be done without human intervention. Human beings are responsible for defining the rules for the social interaction of things, and use the service resulting from such interactions. Therefore, when designing a SIoT network structure, it should be based on social networks and take into account both the social relationships between objects and object owners.

Based on the characteristics of SIoT, this paper considers the user-centric SIoT environment where each device is physically connected through the network and socially connected through the user's social network as defined in [6].

2.2 Trust Evaluation of IoT System

Currently, trust management research on IoT is at an early stage. In the IoT environment, trust concepts, trust models, and evaluation mechanisms have been proposed. However, most of them focused on establishing a reputation system for social networks for e-commerce services or developing a trust management mechanism in distributed systems such as WSN or P2P networks. Those methods have a problem that information is not sufficient because it relies mainly on direct observation information or third party information [7].

Some trust models introduce an evaluation mechanism associated with trusted agents (TA) to assess trust levels. However, in some environments, such as mobile networks, there is a limitation that only a direct observation information can be obtained because a centralized system must be maintained to manage third party information. Another approach is to apply a modified Bayesian model using different weights for the information obtained through direct observation [8]. Chen proposed a trust management model based on fuzzy reputation for IoT [9]. However, the proposed trust management model considers a specific IoT environment composed of wireless sensors with QoS trust metrics, such as transmission rate and energy consumption for packet forwarding, and does not consider important social relationships in the SIoT system.

Some trust models also mimic human

cognitive processes to form belief values, taking into account different types of trust measures such as reputation, recommendation, and observation. This model is proposed for trust management of P2P networks, social networks, IoT and SIoT, and is based on interactions among individuals in social networks to assess trust [10].

In this paper, we focus on trust management of SOA-based IoT system relatively more than previous studies. Unlike traditional social networks, IoT networks have numerous entities and devices, and the storage capacity of each device is very limited. Taking these constraints into account, we design to dynamically adjust the trust variable settings to choose trust feedback from nodes that share similar social interests, and to minimize bias to confidence estimates.

3. Problem Definition

IoT devices that provide services are primarily human operated devices, so they mimic human social behavior when they find and provide information. As seen in most IoT architectures, the device owner will control the services that the device provides and social interactions. In other words, when an IoT device receives a service request, the device requests the owner for authorization for a specific service or information provisioning, and the owner authorizes the device to allow the service to be provided. This process is performed when the first interaction occurs, but the next transaction will be learned and operational. In this scenario, the response of the device owner to the service request is strongly dependent on the direct or indirect relationship with the service requester.

In this paper, we design a dynamic trust model for evaluating the trust level of service and information providers and requestors in SOA-based IoT environment. For a more systematic approach, the trust evaluation problem is formulated as a generalized shortest distance problem on a weighted non-directional graph. To do this, we first define a trust model and explain the trust evaluation method.

In the IoT environment, each node has an identifiable URI. As shown in Figure 1, there is no authorized authority defined in the centralized trust management method, and there are two types of nodes: user and device owner(or device itself). The relationship between the user and the device owner is a one-to-many relationship. In the trust management, the trustor is the user and the trustee is the device owner (or the owned device). The trust evaluation information is calculated for each user and stored in the designated device owned by the user.

Trust is evaluated based on a direct user experience of past interactions and recommendations from others. We consider social relationships to select trust feedback from nodes that share similar social interests. That is, the weight of the recommendation is determined using the social relationship between the trustor and the trustee. This is because users who share similar social

relationships tend to have a similar subjective trust view on the service.

This social relationship is represented by a experience list that include friends lists, direct interaction devices (or services) that can be identified based on the current location. Each user stores these lists in a user profile, and other devices of the same user have permission to access the profile. Friends list and experience list are accumulated in the profile and used for trust evaluation. However, it is not efficient to utilize all information for analysis, so we limited the proximity range that can provide service based on location information. Since the work is done only when changes occur, the cost to maintain these lists is negligible as it is very small.

In an SOA-based environment, each device provides or uses services using SOAP-based technologies or RESTful APIs. For example, when the device d1 of the user u1 requests the service of the device d1 of the user u2, the device d1 of u1 updates the experience list including the device d1 of u2 in the user profile of u1. The experience list that the user has gained from experience with interacting with other devices has information about transactions and satisfaction values. The device d1 of u1 can also look at the transaction information or feedback information for the device d1 of u2 in the user profile of u1. The proposed model uses a user profile because the storage space of the devices can not accommodate the entire trust value for all other devices.

4. Trust Evaluation

The basic components of an SOA-based IoT environment for defining trust evaluation models are service providers and service requestors. In addition, the trust evaluation model has two components : Service Discovery Component (SDC) and Trust Evaluation Component (TEC). SDC is defined as a system that provides a list of service provision candidates who can receive a request from the IoT device and provide the service. TEC is a system that evaluates trust level of nodes and provides trust information. Based on these components, the trust graph is defined as follows to formulate the trust evaluation.

Definition 1. Trust Graph(TG)

The trust graph TG is a weighted non-directional graph. In general, trust relationships tend to be directional. However, non-directional graph TG is defined by recognizing only two-way trusts as friends. In the trust graph TG, IoT devices that are both service and information providers and requestors are represented by nodes. The set of nodes is $V = \{v_1, v_2, ..., v_n\}$. $E \subseteq \{V \times V\}$ is a set of edges that connect pairs of nodes. The edge between nodes means that they have social relations as friends.

Assuming that any node on the graph TG provides a service, the user requesting the service tries to acquire the trust information of the node directly or indirectly. Direct trust information can be obtained on the basis of social relations formed between two nodes, while indirect information can be derived from

friendships as a kind of reputation value.

The elements required for the trust evaluation on the graph TG are defined as follows :

- $AD_i = \{v_j \in V | (v_i, v_j) \in E\}$ is a set of nodes adjacent to the node v_i, and each element in AD_i has a friend relationship with v_i.
- $CF_{i,j} = \{v_k \in V | v_k \in AD_i \cap AD_j\}$ is a set of common neighbors that have a relationship with both nodes v_i and v_j.
- S_i is a set of services provided by the node v_i.
- $SP_k = \{v_j \in V | s_k \in S_j\}$ is a set of nodes that can provide the service s_k, and is generated by SDC.

SDC provides path $P_{i,j}$ for one node v_j in SP_k where $P_{i,j}$ is a path from the service requestor v_i to the service provider v_j. The path $P_{i,j}$ is a sequence of edges representing social relations. The TEC evaluates the trust level of nodes on the path $P_{i,j}$ and provides the trust information.

Figure 1 shows an example of a simple trust graph. $V = \{v_1, v_2, v_3, ..., v_{10}\}$ and each node in V can provide one or more services. The service is represented by a square label on each node. The node v_1 requests the service s_{10}, and $SP_{10} = \{v_7\}$ is the set of nodes that can provide the requested service s_{10}.

$P_{1,7} = \{(v_1, v_4), (v_4, v_6), (v_6, v_7)\}$ is the set of edges going through from v_1 to v_7 and is the path provided by the service discovery process of the SDC. In Figure 1, $AD_1 = \{v_2, v_3, v_4\}$ is the set of adjacent nodes forming the social relationship with v_1. $CF_{1,4} = \{v_2, v_3\}$ is the set of common neighbors between v_1 and v_4, and is represented as blue nodes.

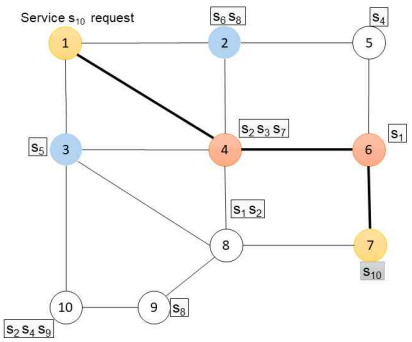

Fig. 1. Trust graph example

Suppose that any one node on TG provides some service. Then, users who need the service will want to obtain trust information of the node, either directly or indirectly. It can be evaluated based on direct interaction or indirectly based on social relations.

Definition 2. Trustworthiness

The trust level T of the node v_j evaluated by the node v_i is defined as follows :

$$T_{i,j} = \alpha \times t_{i,j}^{d} + (1-\alpha) \times t_{i,j}^{r} \quad \cdots\cdots\cdots \text{(Eq. 1)}$$

In Equation 1, α is an empirical factor and has a range of $0 \leq \alpha < 1$. The empirical factor can reflect the situation by recalculating each time a new experience occurs. A larger value of α means that the experience gained from direct interactions will be considered more when evaluating the level of trust.

The trust-related experience grows as the quantity of interaction between the two nodes increases. However, it is assumed that when the amount of interaction reaches a certain level, it will not show a large change. In the

proposed model, a simple exponential function is used to express the value of the empirical factor. The empirical factor can be obtained based on the direct interaction and social relations of the two nodes, and is defined as Equation 2. In this equation, φ is a very small number used as a factor to model the change in confidence over time and $\triangle t$ is the time interval at which trust information is updated. If there is no direct interaction, $\alpha = 0$. Information about the interaction is stored in the experience list of the profile, and each time a transaction occurs, it sets the user satisfaction experience to binary values (0 or 1).

$$\alpha = e^{-\varphi \triangle t} \quad \cdots\cdots\cdots\cdots \text{(Eq. 2)}$$

In Equation 1, $t_{i,j}^{d}$ and $t_{i,j}^{r}$ are the confidence derived from the social relations. They are to compute the trust level for each node v_i belonging to AD_i based on its own experience and experience of its friends. $t_{i,j}^{d}$ represents the degree of trust that the node v_i directly evaluates to the node v_j. In service-oriented computing, a service requester can evaluate the functional and non-functional characteristics of a service provider based on direct interactions. Non-functional properties include response time, failure probability, price, and so on. When $P_{i,j} = \{(v_i, v_j)\}$, $t_{i,j}^{d}$ is defined as the following Equation 3. In Equation 3, $A_{i,j} = A_{i,j}^{(old)} + \beta_{i,j}$ and $B_{i,j} = B_{i,j}^{(old)} + (1 - \beta_{i,j})$, where $\beta_{i,j}$ is a value indicating whether the node v_i is satisfied with respect to the node v_j, and it is 1 if satisfied and 0 when it is not satisfied.

$$t_{i,j}^{d} = \frac{A_{i,j}}{A_{i,j} + B_{i,j}} \quad \cdots\cdots\cdots\cdots \text{(Eq. 3)}$$

The term $t_{i,j}^{r}$ used in Equation 1 is calculated based on the recommendation value through the social relation when the two nodes v_i and v_j are not adjacent. Then $t_{i,j}^{r}$ is defined as the Equation 4.

For $P_{i,j} = \{(v_i, v_{i_1}), \ldots, (v_{i_{n-1}}, v_{i_n}), (v_{i_n}, v_j)\}$,

$$t_{i,j}^{r} = \Sigma(w_k \times \gamma_k) \quad \cdots\cdots\cdots\cdots \text{(Eq. 4)}$$

In Equation 4, γ_k is the recommended value referenced in the user profile of the nodes belonging to $P_{i,j}$ and w is a weight value and is calculated as $w_k = l - (k-1)/L_l$, where $l = |P_{i,j}|$ and $L_l = l(l+1)/2$ for $1 \le k \le l$.

If two nodes are not adjacent, $t_{i,j}^{r}$ is computed based on the recommendation value through the social relations.

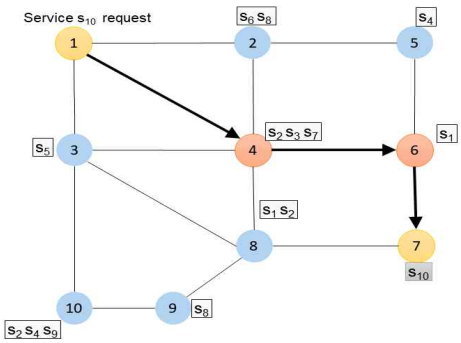

Fig. 2. Request of the recommendation value

It is intended to give a larger weight, since it may be more important for a friend to have a direct relationship or close friendship. In other words, in the case of a friend relationship, a larger weight is given since it is more reliable than a friend's friend relationship.

For example, calculating $t_{1,7}^{r}$ between two nodes v_1 and v_7 is $t_{1,7}^{r} = w_4\gamma_4 + w_6\gamma_6 + w_7\gamma_7$ as shown in Figure 2.

When the recommended value referenced through the node belonging to $P_{1,7}$ is transmitted as shown in Figure 3, $t_{1,7}^{r} = 3/6\gamma_4 + 2/6\gamma_6 + 1/6\gamma_7$ where $l = 3$ and $L_l = 6$ for $1 \le k \le 3$. At the end of the transaction, node v_1 provides feedback to all nodes belonging to AD_1 and v_k which is an element of $\{v_k | v_k \in CF_{i,k} \text{ for } \forall v_i \in P\}$, and this feedback is accumulated in the user profile. It is 1 if positive feedback, or 0 if negative feedback. The initial value is set to 0.

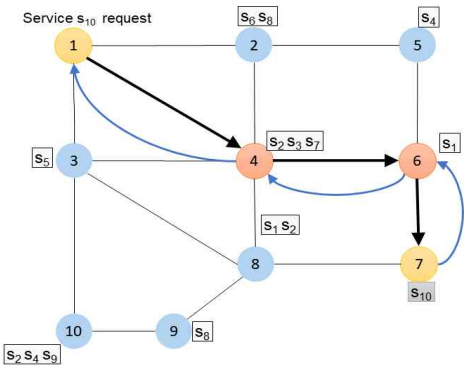

Fig. 3. Computation of the trust value

Even in the same context as the same trustee, trust can vary depending on the evaluator. Trust assessments are highly subjective and personalized, and in some cases they may be symmetric, but they are inherently non-reciprocal. Trust is not transitive, but it is propagated. For example, if A trusts B highly, and B trusts C very much, A can not necessarily trust C. However, when A judges whether he can trust C, he tends to be highly dependent on the trust relationship between B and C [7]. Another characteristic of trust is composability. For an unknown object in which social relations are not formed, it is judged whether or not to trust by combining opinions of many people rather than evaluation of specific individuals. Instead of relying on a friend's recommendation, it may be more accurate to collect opinions from a number of friends and evaluate it using the reputation of the subject [11]. Since the proposed trust evaluation method is based on direct interactions and social relations, it can be said that this characteristic of trust is well reflected. If devices between two users can exchange trust information with profiles created based on direct transactions or social relations, trust can be estimated using recommendation or reputation for devices that do not have social relations.

5. Experimental results and analysis

In order to validate the proposed trust model, a total of 150 different IoT devices are created on the social network based on actual data, and the services s_1 to s_{100} are defined. At least one to at most 10 services are randomly assigned to each device. The social network used in the experiment is Dept3 of email-EuCore [12], which is composed of 68 people. The generated IoT devices were randomly assigned to users with a limit of at least 1 and a maximum of 5. For each user, a

profile containing a list of owned devices was created, and since a small number of communities were targeted, no community centered on the area was set. The transactions between IoT devices are performed 2,000 times in total, and binary feedback is provided for service requests. When each transaction starts, the simulator randomly selects the node requesting the service, and randomly chooses not to exceed 50 nodes (10% of the total nodes) that can provide the service. It is implemented in Java on Intel Core i7 3.40GHz / 8GB desktop including SDC and TEC module.

The purpose of the experiment is to demonstrate that the proposed trust model is useful for selecting the best service by comparing and analyzing the results of service selection based on trust evaluation. A profile of 100 nodes was arbitrarily set up to have the best service quality for each service of s_1 to s_{100}, and a list of trustworthy devices was constructed. For a specific service request, we compared the hit ratio against the list of trusted devices with a case where a service is selected based on a trust value by the proposed model, and a case where a provider is arbitrarily selected. When a request for an arbitrary service occurs, $T_{a,b1}$, $T_{a,b2}$, ..., and $T_{a,bn}$ of Equation 1 is calculated for the node v_a requesting the service and the nodes v_{b1}, v_{b2}, ..., and v_{bn} providing the service, and then the service provider having the highest trust value is selected.

In the case of random selection, the hit rate distribution has a relatively constant level, while the trust based selection tends to increase slightly as the number of interactions increases. Figure 4 is a summary graph centered around the selection value every 100 times. In the study of [13], according to the result of the survey on the level of user satisfaction with the actual user's web service call, the trust and quality satisfaction are formed at about 83% level. In the absence of a history of transactions, it is not far below the 83% level. However, as the number of interactions increases, trust information accumulates, so trustworthy service selection is made and user satisfaction level is increased.

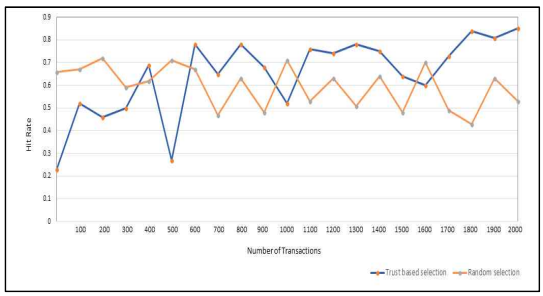

Fig. 4. Summary of hit rate

We also randomly selected a node to apply the trust measure for comparison with the proposed trust model and the most known trust models EigenTrust and PeerTrust [14][15]. In the same environment as the previous experiment, we selected the arbitrary node forming a lot of trust relationships, calculated trust values, and compared the distribution of values. Figure 5 shows a comparison of the calculated trust values. Since the proposed trust model shows a high trust value for the node from the beginning of the transaction, it is more likely to select the trustworthy node more accurately than the other models.

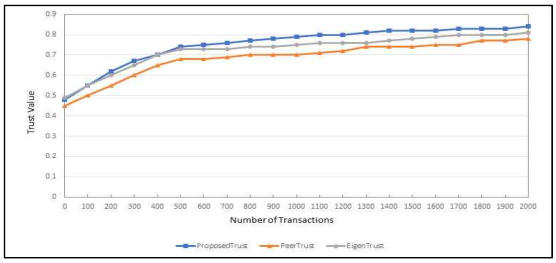

Fig. 5. Comparison of trust values

6. Conclusion and future works

Trust is a complex concept with many different meanings. In an IoT environment where heterogeneous entities exist, trust information can provide very important value as a basis for how trustworthy a service is and how useful it is. In an IoT environment, not all information is valuable, and malicious users are likely to exist. Therefore, there is a need to consider the trust of the service provider, and determination by poor information can lead to unacceptable negative consequences.

This paper considers the limited storage capacity of each device on the IoT network for trust evaluation in SOA-based IoT environment. It is designed to dynamically adjust the variable settings for trust in order to receive trust feedback from nodes sharing similar social interests and to minimize bias on confidence estimates. And to provide a conceptual framework for evaluating the trust of service providers quantitatively. Trust evaluation is a method to judge the trust level of services provided by information providers and devices distributed online such as social networks. The proposed trust evaluation method is expected to be used as a predictor of the trend of social trust formation in the rapidly expanding IoT environment.

The experiments on the proposed model should be improved considering the various relational characteristics in social networks and information of the center of location and community. Since the concept of trust is very relative, it is necessary to consider the characteristics of social relations that can emerge with the rapid change of the IoT environment and to improve it as a realistic evaluation method that reflects the problems of malicious users.

References

[1] Guinard, D., V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, “Interacting with the SOA-Based Internet of Things : Discovery, Query, Selection, and On-Demand Provisioning of Web Services,” IEEE Transactions on Services Computing, Vol.3, No.3 (2010), 223 - 235. DOI : https://doi.org/10.1109/TSC.2010.3.

[2] Kim, Y. K., E. W. Jhee, and Y. T. Shin, “Development of The Korean Trust Index for Social Network Services,” Journal of Internet Computing and Services, Vol.15. No.6 (2014), 35 - 45. http://kiss.kstudy.com/thesis/thesis-view.asp?key=3505159

[3] Prehofer, C., J. V. Gurp, V. Stirbu, S. Sathish, P. P. Liimatainen, C. D. Flora, and S. Tarkoma, “Practical web-based smart spaces,” IEEE Pervasive Computing, Vol.9, No.3 (2010) 72 - 80. DOI: https://doi.org/10.1109/MPRV.2009.88

[4] Doody, P., and A. Shields, “Mining network relationships in the internet of things,” Proceedings of the 9th ACM International Workshop of Self-Aware

IoT, (2012), 7-12. DOI: https://doi.org/10.1145/2378023.2378026
[5] Kranz, M., L. Roalter, and F. Michahelles, "Things that twitter: Social networks and the internet of things," Proceedings of the CIoT Workshop at the 8th International Conference on Pervasive Computing (2010), 1-10. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.395.1105&rep=rep1&type=pdf
[6] Atzori, L., A. Iera, and G. Morabito, "SIoT: Giving a social structure to the internet of things," IEEE Communication Letters, Vol.15, No.11 (2011), 1193 - 1195. DOI: https://doi.org/10.1109/LCOMM.2011.090911.111340
[7] Truong, N. B., H. Lee, B. Askwith and G. Lee, "Toward a Trust Evaluation Mechanism in the Social Internet of Things," Sensors (Basel), Vol.17, No.6 (2017), Article 1346. DOI: https://doi.org/10.3390/s17061346
[8] Li, J., R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," IEEE Communication Magazine (2008), Article 46. DOI: https://doi.org/10.1109/MCOM.2008.4481349
[9] Chen, D., G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," Computer Science and Information System, Vol.8, No.4 (2011), 1207 - 1228. http://eudml.org/doc/253429
[10] Nitti, M., R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social internet of things," Proceedings of the 23rd IEEE International Symposium on Personal Indoor and Mobile Radio Communications (2012), 18-23. DOI: https://doi.org/10.1109/PIMRC.2012.6362662
[11] Song, H., "Is Trust Transitive and composable in Social Networks ?," Journal of Information Technology Application & Management, Vol.20, No.4 (2013), 191-205. http://www.kdbs.or.kr
[12] Leskovec, J., Stanford Large Network Dataset Collection, 2008. Available at http://snap.stanford.edu/data/ (Downloaded 15 December, 2018)
[13] Zheng, Z., Y. Zhang, and M. R. Lyu, "Investigating QoS of realworld web services," IEEE Transactions on Service Computing, Vol.7, No.1 (2014), 32 - 39. DOI: https://doi.org/10.1109/TSC.2012.34
[14] Kamvar, S., M. Schlosser, and H. Molina, "The eigen-trust algorithm for reputation management in P2P Networks," Proceedings of the 12th International World Wide Web Conference (2003), 640-651. DOI: https://doi.org/10.1145/775152.775242
[15] Xiong, L. and L. Liu, "PeerTrust: Supporting reputation based trust for peer-to-peer electronic communities," IEEE Transactions on Knowledge and Data Engineering, Vol.16, No.7 (2004), 843-857. DOI: https://doi.org/10.1109/TKDE.2004.1318566

Authors

Yukyong Kim

2001.8 Ph.D. in Computer Science from Sookmyung Women's University.
2005.9 - 2006.8 Post-doc. in University of California at Davis.
2006.9 - 2013.9 Research professor in Dept. of Computer Engineering at Hanyang University.
2018.2 - present. Faculty member in Division of Basic Engineering at Sookmyung Women's University.

<Research interests> Web services, QoS Evaluation, Trust Assessment on SOA based IoT, Software Quality Metrics