2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress

RpR: A Trust Computation Model for Social Internet of Things

Upul Jayasinghe, Nguyen B. Truong, Gyu Myoung Lee
Department of Computer Science
Liverpool John Moores University (LJMU)
Liverpool, United Kingdom
u.u.jayasinghe@2015.ljmu.ac.uk,
n.b.truong@2015.ljmu.ac.uk, g.m.lee@ljmu.ac.uk

Tai-Won Um
Hyper-connected Communication Research Laboratory
Electronics and Telecommunications Research Institute
Daejeon, Korea
twum@etri.re.kr

***Abstract*—Social Internet of Things (SIoT) is an evolutionary idea which combines traditional IoT models with social network paradigms. "Objects" in SIoT formulate social relationships with other "trusted objects" according to the relationships of their owners which deliver trustworthy services on request. From our trust platform concept to identify vital trust metrics and attributes, we propose a Recommendations plus Reputations based Trust Computational Model (RpR) that enables objects in SIoT to build associations in a trustworthy manner. A numerical model is developed to estimate trust of each object based on Recommendation and Reputation parameters. Next, both estimates are merged together and a robust algorithm is proposed. Finally, we demonstrate and validate the usefulness of RpR over prior approaches through simulations and analysis. The aim of our approach is to facilitate accurate modeling of trustworthiness in distributed SIoT environments.**

***Keywords*— Social Networks, SIoT, Trust Computation, Trust Model, Knowledge, Reputation, Recommendation.**

I. INTRODUCTION

The Social Internet of Things (SIoT) is a collection of diverse objects which are capable of establishing social relationships in order to achieve a specific goal [1]. Most importantly, the underlying working principle of SIoT is depended upon the relationship and trustworthiness between a trustee and a trustor. This allows devices to have their own social networks while allowing humans to impose rules to protect their privacy and preferences. In general, the idea of trust in SIoT can be considered as a combination of policy based trust, reputation based trust and knowledge [2]. Until now, most of the work in literature concentrated on developing definitions, architectures and protocols. Hence, there is a significant ambiguity related to trust in SIoT such as efficient usage of information provided by other parties in order to assess the behavior of other objects and implement reliable decision making.

On the other hand, [3] and [4] have identified the value of modeling, computing and reasoning of trust through many numerical and idealistic approaches. However, most of these techniques have confined to specific network environments like peer-to-peer (P2P), wireless sensor networks (WSN) and mobile ad-hoc networks (MANET). Moreover, the objectives of these investigations are more biased towards solving related security issues like Access Control in decentralized systems [5], Identity Management and Public Key Certification [6]. Also, there is not much research on trust assessment in SIoT and cloud computing [7]. Yet, many such proposals don't satisfy the requirements of SIoT in regard to many issues including complexity and scalability.

Thus, in this paper, we propose a novel trust computational model based on three trust metrics (TMs); Knowledge, Recommendations and Reputations defined in [8]. The knowledge represents more subjective properties related to trust like honesty, cooperativeness, user experience and community-interest, inspired by ideas in [9]. However, as the knowledge factor is more biased towards subjective properties, we omitted including it here but will be considered as a future work in this research. Hence, Recommendations plus Reputations (RpR) is the main concern of this paper for building a numerical model for trust computation. Along with SIoT concepts, we define Recommendations as the opinions from Friends (objects or humans) in analogy to human social networks and Reputations as opinions from other objects.

We have adapted some concepts in PageRank (PR) model in order to make the numerical approach less complex and provide more insight about the whole target environment [10]. To the best of our knowledge, there is little work on trust computation based on this concept which fulfills the requirements of SIoT. Basically PR model discusses how the incoming and outgoing link of a web page can be used to evaluate the importance of that particular page compared to its neighbors. However, PR model is not capable of assessing objects other than directly connected and shows extremely weak performance in case of fake reputations. With these issues in mind, we propose a numerical model which evaluates recommendations and reputations, and generate a collective trust value which will be identified as RpR scores. Along with the model, we present an algorithm to calculate trust scores of each object in a more robust manner. Finally, we simulate the model and demonstrate convergence, accuracy and resiliency over fake information as well as the performance improvement compared to famous PR algorithms.

The rest of the paper is organized as follows. Section II identifies some related work on reputation systems and trust computation methods. In Section III, we describe our trust model in corresponds to SIoT environment. Section IV presents the formulation of trust computation method while meeting the properties of real world scenario. Section V provides simulation results in order to validate and compare the desirable attributes

978-1-5090-2771-2/16 $31.00 © 2016 IEEE
DOI 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.129

and the performance enhancements. Finally, Section VI concludes the paper and outlines future work.

II. Related Work

There are several well-known reputation systems in the context of e-commerce systems, such as eBay and Internet-based systems such as Keynote [11]. In centralized reputation systems like eBay, both sellers and customers can rate each other and weighted average during period of time is considered as the reputation score of each partner. However, the approach is depended on the centralized system and not a good candidate for SIoT. Bao *et al.* [12] describe a trust management scheme based on QoS metrics and recommendations. However, the target environment was static and not useful for rapidly changing conditions like random number of objects, dynamic behavior changes, and handling dishonest information.

More evolved version of a reputation model called SPORAS compared to eBay™ is developed by [13] where only the most recent recommendations have been taken into the consideration. The mechanism is built in such a way that the reputation update will affect significantly for low reputed users and rarely for the users with high reputation. The underlying core principal is based on the standard deviation of reputation values. In [14] an agent based trust computation method is suggested for MANET. It uses the weighted means to measure the objects' final trust and then makes the corresponding decision. A recommendation based trust computation method for WSNs in [15] relies on confidence interval concept. In the method, directly connected objects are monitored for some time and based on that, a final trust value is derived.

An algorithm that identifies dishonest users is investigated in [3]. The algorithm works as a weighting system and lesser weights are assigned for dishonest users and hence the effect of malicious behavior is gradually reduced in future transactions. Moreover, they have analyzed the effectiveness of each honest recommendation. A more distributed version, based on threat report is studied in [16]. Authors have designed an alarming agent in each object which listens to adjacent objects and produces a trust report based on their behavior. If the agent would detect any abnormalities, it will be broadcasted to each and every other object.

Further, authors in [2] have presented a holistic trust management framework of IoT based on IoT's system model, which address three areas namely cyber-physical trust relationship, trust management objectives, and IoT trust management. A fuzzy logic based approach is proposed for reputation estimation in SIoT in [17]. Authors in [18] are proposed a P2P network based on their social trust which is based on their corporation level and common social interests. On the other hand, EigenTrust [19], PeerTrust [20], P2PTrust [21], FCTrust [22] and SecuredTrust [23] are some important contributions based on the recommendation or reputation based trust models. However, existing recommendation based trust models suffer from the limitations of slow convergence and high complexity of trust computations with the growth of the objects. Also, they are more volatile to fake recommendation as they lack the ability to downgrade the ranking based on past interactions, leading to an inaccurate evaluation of trust value.

III. Background of the Trust Model

A. Trust in the Social Internet of Things

In SIoT, objects are linked with services that they can deliver. The key objectives of such a network is to discover reputed services, active resources and publish this information over the network to be used by interested parties. To achieve this kind of behavior, navigating through a social network is done based on the relationship of objects rather than depending on typical internet discovery tools. Social relationships can be considered as human-human, human-objects and also objects-objects. Relationship based routing is far more proficient technique compared to standard routing methods due to requirements in SIoT, including, but not limited to, context awareness service delivery, trustworthiness and scalability.

Accordingly, we categorize relationships into four main categories depending on their trust level: namely Friendship, Ownership, Interaction, and Community interest. In Fig. 1, we have shown an example scenario of this classification using a *car sharing* use case. As demonstrated in the example, each object has at least one owner and which may be a friend, a part of transaction and/or a member of specific community. Also we identify the trustor and trustee relationship in which the trustor is responsible for evaluating the trust and trustee is responsible for providing necessary information upon requested by trustor.

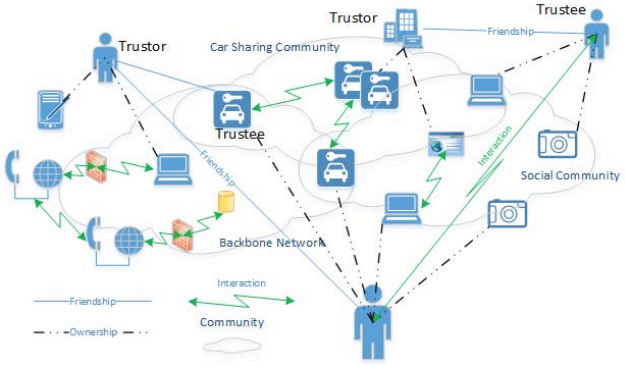

Fig. 1. Associations in a SIoT system.

Being a friend is one of the strongest relationship in SIoT and it allows to collaborate more reliably compared to others. Likewise, there can be devices which are operated to achieve certain goals or policies set by the community. Some examples are social networking, backbone services, security measures and also the community who interfere with goodness of the operation. Objects belong to the same community are likely to share their information with their member than other community members. As an example, spam community might share information or mechanisms relevant to self-promoting, bad-mouthing, good-mouthing with in their community to achieve bigger shake to the target system. Our use case example presented in Fig. 1 is a car sharing system where people can rent a car for a period of time. Normally, a customer wants a reliable car for reasonable service level and cost. At the same time a car provider and a broker need to ensure that the customer must be trustworthy. To meet these criteria, it's essential to have a system which provides assurance for every party who participates in the

transaction which is essentially establishing a estimate of trust among objects in SIoT.

B. Trust model and Trust Metrics

We develop our RpR model to measure a trust level of every object in SIoT which contributes to any type of transaction. The final outcome of the trust model is to exchange trust information depending on their relationship as discussed above, and build an intelligent system in which one knows whom to be connected with for a particular service. Following this approach, we design our trust model based on three TMs as mentioned before. Information about these TMs must be gathered from the device itself, directly connected objects as well as from the indirectly connected objects like brokers in our use case example. An example illustration of trust acquisition is shown in Fig. 2.

In general, trust is measured only using knowledge and reputation TMs. However, in this paper, we identify one additional TM called recommendations which we define as an attitude towards trustee from its directly connected objects. The reason to identify this as a separate property to reputation is in agreement to human relationship with friends. Friends are more familiar with behaviors, abilities and weakness of a particular person than others who work with him professionally. In comparison to that, we define recommendation as trust metric which is estimated with the support of its' friendly objects which can be humans or objects. Recommendation TM can provide more accurate measurement about its friends avoiding both unnecessary promoting or demoting references.

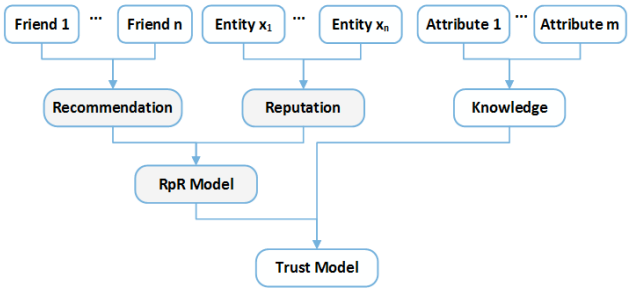

Fig. 2. A Trust model with three Trust Metrics.

Alternatively, reputation TM is calculated from third party information where objects are still in connection but not as friends. Typically this measures how good are the transactions taken place before. One important factor that must be considered is the context in which the reputation scores are calculated. As an example, a customer may trust the car sharing service provider when it comes to cars, but not for their payment service. Though it is important to maintain the context awareness, it does not affect the mechanisms which we describe here for trust computation as a system has to maintain a separate trust score for each object depending on the context. However, context awareness issue is more associated with knowledge TM and hence detail presentation is out of scope of this paper.

IV. RpR - Trust Computation Model

Our trust model is specifically suitable for a distributed environment where each and every object keeps a record of its own trust value based on a particular set of friendly and third party estimations. Yet, we have limited acquiring views with third party objects up to some extent purposefully as along the way one can receive more fake opinions rather than genuine ones. We assume that if a particular object (Trustor) is already connected or in contract with another object (Trustee), there is a relationship with these two objects regardless of trustworthiness. We apply this property to generate a weighted directed graph where vertices represent objects and edges represent the relationship in between. Fig. 3 shows a graph representaiton for the *Car Sharing* use case where user 1 ("A") has a friendly relationship with Service Provider 2 ("D") and User 2 ("E") provides some reputation on object "A" through object "B" based on their social relationship.

Moreover, it is reasonable to believe that an object would have a higher trust score if many objects were directed towards it. However, if a particular object provides an extensively high number of opinions about its neighbor, one can suspect, which is a dishonest object and tries to achieve some undesirable objectives. Therefore, filtering out opinions is also critical to have a more trustworthy score. Keeping these factors in mind, we develop our Recommendation and Reputation model. Later on we will combine these two and formulate the complete algorithm to calculate RpR trust scores.

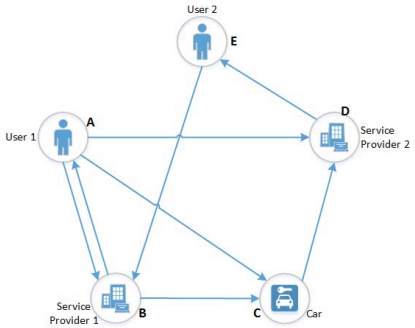

Fig. 3. A Graph Representation of the SIoT Model.

A. Recommendation Model

1) Groundwork

In this section, we formulate a basic design of the recommendation model for SIoT in comparison to PR for the web. Since our goal is to build the model on relationships but not the web links, multi-graphs and self-promoting are ignored. Let's consider an object v_j which has friendly relationship with object v_i as shown in Fig. 4. Since the number of incoming relationship corresponds to the recommendation level of a target object, we can express the recommendation value of v_i as $R_{rec}(v_i) = \sum_{j=1}^{N} 1$, for N number of total directly connected objects in relevance to a particular context. However, if the recommender has many outgoing links, it is an indication that he is a friend of many other objects and hence a recommendation score for each target object must be equally distributed along the links as in (1). In order to simplify the computational overhead and the algorithm, the factor $1/O(v_j)$ is represented in matrix from as in (2) [10].

Fig. 4. An example of Recommendation flow.

$$R_{rec}(v_i) = \sum_{j=1}^{N} \frac{1}{O(v_j)} \quad (1)$$

where $O(v_j)$ is equivalent to number of direct links from v_j.

$$T_{ij} = \begin{cases} 0 & Otherwise \\ \frac{1}{O(v_j)} & if(v_j, v_i) \in \epsilon \end{cases} \quad (2)$$

where T_{ij} represents the transition probability from object "j" towards "i" in the directed graph.

$$R_{rec}(v_i) = \sum_{j=1}^{N} T_{ij} \quad (3)$$

As the objects are distributed, the final recommendation score of each object can be calculated recursively as in (4).

$$R_{rec}(v_i) = \sum_{j=1}^{N} T_{ij}\, R_{rec}(v_j) \quad (4)$$

The equivalent matrix form is:

$$\boldsymbol{R_{rec}^{t+1}} = \boldsymbol{T}\, \boldsymbol{R_{rec}^{t}} \quad (5)$$

where $\boldsymbol{R_{rec}^{t+1}}$ is the predicted recommendation score, $\boldsymbol{T}$ is the transition matrix and $\boldsymbol{R_{rec}^{t}}$ is the current score.

2) Improved version with clustoring

Equation (5) basically represents the numerical model for SIoT environment in comparison to PR for web links. Moreover, this is developed based on the assumption that there are no dishonest objects present and initial recommendation values are uniformly distributed over the entire network. In a real environment, this is not the case and we discuss a solution for these issues in this section. First, it is essential to filter out untrustworthy objects from good objects as we assume that good objects often recommend reliable objects and dishonest objects recommend unreliable objects. This is in relation to human behavior and we adapt that concept here to develop our model discussed in (5) further.

Let's consider object A in the Fig. 3. It can be observed that object "A" provides more outgoing links to other objects, i.e. "A" has a good relationship with many other objects. If a third party user is connected to object A, that user can reach three other friends of "A" easily in order to get some information or services. Following this approach, if we can distinguish objects like "A" we can reasonably filter out dishonest objects from the environment. In order to do this clustering we adopt the inverse version of the PR algorithm discussed in [24]. In the PR model, a rank score depends on how many inwards links there are from adjacent objects. Higher the number of inward links is greater, the rank score of target object will be greater.

Let us consider our model discussed in Fig. 3, with an inverse directed graph as shown in Fig. 5, and apply the algorithm discussed in (5). Now that the graph is inverted, PR gives the ranking scores based on most outgoing links in contrast to the original PR algorithm which is based on inward links. We define inverse transition matrix **U** as in (6) where $I(v_j)$ are the input relationships in contrast to (2).

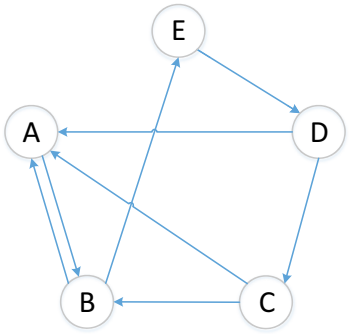

Fig. 5. An Inverse Graph of the SIoT Model.

$$U_{ij} = \begin{cases} 0 & Otherwise \\ \frac{1}{I(v_j)} & if(v_i, v_j) \in \epsilon \end{cases} \quad (6)$$

Note that $\mathbf{T}^{\mathrm{T}} \neq \mathbf{U}$. Then the inverse rank scores of each object can be calculated by substituting (6) in to (5) as shown in (7).

$$\boldsymbol{t_{r+1}} = \boldsymbol{U}\, \boldsymbol{t_r} \quad (7)$$

Equation (7) provides an idea about which object has the highest number of outgoing links and hence the most trustworthy objects. However, it is required to define a threshold value (δ) to select most trustworthy objects (K) from total N objects. After identifying most trustworthy objects, we can distribute initial rank values only for these objects, making others zero.

Let's say that the modified vector is t_r where K number of objects have a positive value and N-K number of objects are zero. Then, we combine the trust vector t_r with (5) as in (8).

$$\boldsymbol{R_{rec}^{t+1}} = \alpha\, \boldsymbol{T}\, \boldsymbol{R_{rec}^{t}} + \beta\, \boldsymbol{t_r} \quad (8)$$

Therefore, the model is biased and will get more updates from most trustworthy objects instead uniformly as before. Here α and β are decay parameters which brings the final scores in between 0 and 1.

B. Reputation Model

We defined that the reputations are opinions from objects other than friends in our proposed SIoT model. One such illustration is shown in Fig. 6, where object v_k gives his attitude towards v_i through object v_{ij}. More clearly, this can be a situation where User 1 in Fig. 3 has a relation with D through C when the direct link from A-D is not present.

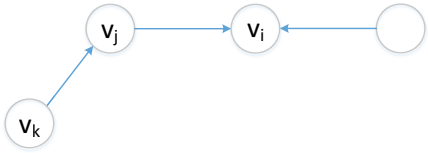

Fig. 6. An example of Recommendation flow.

In graph theory, power of transition matrix determines the paths from non-directly connected objects towards a particular object, having an edge count equal to the power of the matrix. Based on this property, we can find a number of detour relationships which contribute to the final reputation score. However, as the networks grow, there can be a large number of such paths but which are not closely associated with the targeted

object to provide valuable opinions in order to calculate a final reputation value. Hence, the number of levels that one object can pass his reputation score towards another one is limited. Furthermore, we observe through simulations that after three levels deeper in the graph, the effect of reputation score is negligible. Based on these grounds, let us calculate the reputation value passes from v_k towards v_i as modelled in (9).

$$R_{rep}^{k \to i}(v_i) = \sum_{j=1}^{N} T_{kj} T_{ji} \, R_{rep}(v_k) \qquad (9)$$

where T_{kj} is the transition matrix from v_k towards v_j and T_{ji} is the transition matrix from v_j towards v_i.

However according to graph theory, the product of above two transition matrix is the equivalent of 2-length transition matrix is given by (10).

$$\sum_{j=1}^{\cdot\cdot} T_{kj} T_{ji} = \boldsymbol{T}^2 \qquad (10)$$

Algorithm : RpR Score

function **RpR***
input
N *number of objects*
T *transition matrix*
U *inverse transition matrix*
δ *threshold value for good recommendations*
α *decay factor of recommendations*
β *decay factor of trustworthy roots*
γ *decay factor of reputations*
m *number of iterations*
output
$\boldsymbol{t}_r$ *trustworthy roots*
$\boldsymbol{R}_{rec}$ *recommendation scores of each object*
$\boldsymbol{R}_{rep}$ *reputation scores of each object*
$\boldsymbol{R}_{RpR}$ *RpR trust scores*
begin
//discover trustworthy objects
(1) $\boldsymbol{t}_r(\cdots)$
//evaluate recommendation scores
(2) $\boldsymbol{R}_{\boldsymbol{rec}}^{\boldsymbol{t}} = \boldsymbol{t}_r$
for i =1 to m do
$\boldsymbol{R}_{\boldsymbol{rec}}^{\boldsymbol{t+1}} = \alpha \boldsymbol{T} \boldsymbol{R}_{\boldsymbol{rec}}^{\boldsymbol{t}} + \beta \boldsymbol{t}_r$
return $\boldsymbol{R}_{rec}$
//evaluate reputation scores
(3) $\boldsymbol{R}_{\boldsymbol{rep}}^{\boldsymbol{t}} = \frac{\boldsymbol{1}}{\boldsymbol{N}}$
for i =1 to m do
$\boldsymbol{R}_{\boldsymbol{rep}}^{\boldsymbol{t+1}} = \boldsymbol{T}^{\boldsymbol{n}} \boldsymbol{R}_{\boldsymbol{rep}}^{\boldsymbol{t}} \qquad 1 < n < 4$
return $\boldsymbol{R}_{rep}$
//joint Repute scores
(4) return $\boldsymbol{R}_{joint} = \boldsymbol{R}_{rec} + \gamma \boldsymbol{R}_{rep}$
end

Fig. 7. The RpR Algorithm.

Substituting (10) in to (9), matrix representation of tier-2 reputation scores can be calculated as in (11).

$$\boldsymbol{R}_{\boldsymbol{rep}}^{\boldsymbol{k \to i}}(v_i) = \boldsymbol{T^2 R}_{\boldsymbol{rep}}(v_k) \qquad (11)$$

Similarly for n-length graph,

$$\boldsymbol{R}_{\boldsymbol{rep}}^{\boldsymbol{t+1}} = \boldsymbol{T}^{\boldsymbol{n}} \boldsymbol{R}_{\boldsymbol{rep}}^{\boldsymbol{t}} \qquad n>1 \qquad (12)$$

where "n" is the depth level and limited to "3" as in Fig. 8, in order to reduce the computational overhead as well as due to their negligible effect.

Fig. 8. Depth level that Reputation scores are collected.

C. RpR Model and the Algorithem

Combining two scenarios, discussed in (8) and (12), the final numerical model which aggregates Recommendations and Reputations scores is shown in (13).

$$\boldsymbol{R}_{RpR} = \boldsymbol{R}_{rec} + \gamma \boldsymbol{R}_{rep} \qquad (13)$$

where $\mathbf{R}_{rec}$ are the recommendation scores from friends and $\mathbf{R}_{rep}$ are the reputation scores who interact with the target object. Again γ is a normalization factor which satisfies the condition $\alpha+\beta+\gamma=1$, in order to maintain the final RpR score of each object in between 0 and 1.

The function RpR, shown in Fig. 7, computes the RpR trust scores for the model we presented in Section IV for a SIoT environment. The first step of the algorithm is to find most trustworthy objects by calling the function $\mathbf{t_r}$ **(⋯)**. This will create a vector in which initial scores are positive only for most trustworthy objects where scores are greater than the threshold value requested by the context. In the second step, Recommendation scores are calculated in a recursive manner as in (8) where initial conditions are set as described by trust vector $\mathbf{t_r}$. Similarly, Reputation scores are calculated where opinions are collected from nods up to the third tier, i.e. $1<n<4$. Finally, two scores are combined after normalizing with decay factors α, β, and γ.

V. Experiments and Results

In order to evaluate the model, we have conducted a simulation of a SIoT environment based on the illustration in Fig. 3. Initially, the simulation initiated with 5 objects and gradually increased it up to 100 objects to investigate the robustness of the system compared to the PR method. However, we observed that the algorithm described in Fig. 7, is capable of handling tens of thousands nodes due to simplicity of calculation model just like in PR method. The complexity of the model is constrained by the n-value which determines how far the algorithm runs to collect reputation values and by limiting the number of recursive iterations to preserve an accuracy up to 10^{-5}. With the adjustments, the algorithm converges really quickly with only about six iterations as shown in Fig. 9.

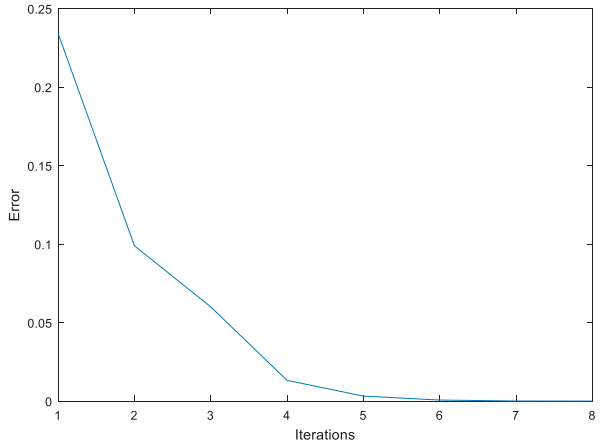

Fig. 9. Convergence Speed of the Algorithm.

The RpR ranking scores obtained for the five object model discussed before is shown in Fig. 10 for the explanatory purpose and to observe the correctness of the algorithm. The area of the circles is proportional to the trustworthiness score of a particular object. It is obvious that "B" has gained higher score compared to others as it does have many incoming and outgoing relationships with friendly neighbor objects. On the other hand, object "A" received the minimum score, as it only got one recommendation from "B" while it tries to reach three others. "C" and "D" has obtained a nearly equal amount of rank as both have two incoming recommendations and one outgoing link.

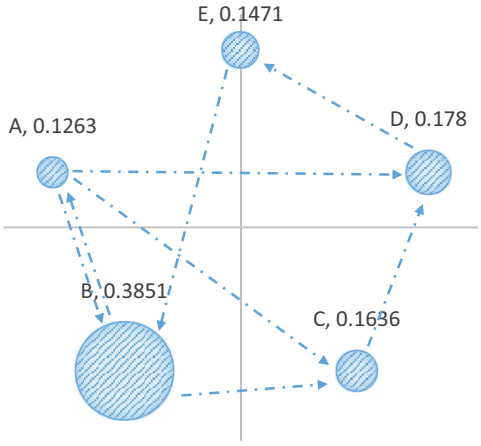

Fig. 10. Distribution of RpR Scores.

Another view of the same example is shown in Fig. 11, where RpR scores in each individual object are compared with PR model and with In Degree (ID). It shows that RpR model is more sensitive compared to others. As an example, when the trend is increasing, RpR assigns a more reasonably higher score for most trustworthy objects. Similarly, when the trend is decreasing, RpR assigns a lower value compared to others which makes the model more sensitive to dishonest behaviors. With the presence of the increment number of unreliable objects, the detection sensitivity is compared in Fig. 12. It can be observed that RpR is always a good candidate for detection of suspicious behavior in comparison to PR model.

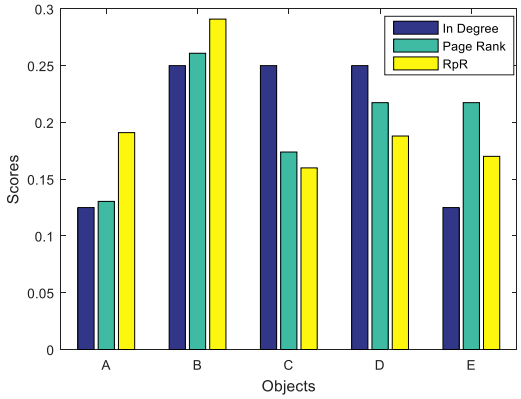

Fig. 11. Comparison of Distribution Scores: 5 Objects

One important property of a good ranking system is that it must be unbiased in extreme conditions. We experiment this scenario in our simulation and it can be observed that neither PR nor ID algorithms were able to fulfill this with the growth of network. In here, we checked whether the algorithm is capable of detecting objects which are in best 20% of trust scores as shown in Fig. 13. RpR always showed a consistent performance irrespective of the network size while PR performance was heavily degraded with the increase of object count as PR/ID models are heavily depended on opinions from old objects.

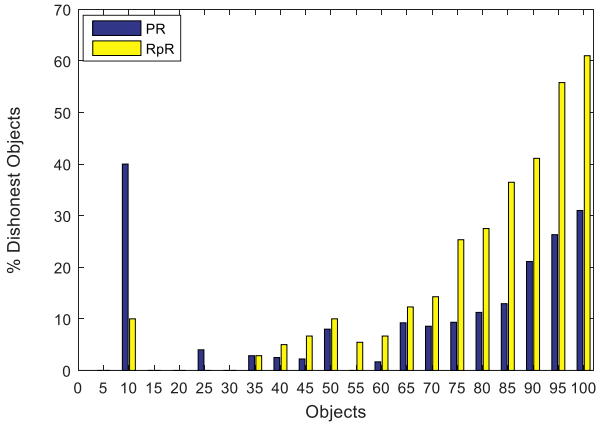

Fig. 12. Dishonest Object Detection.

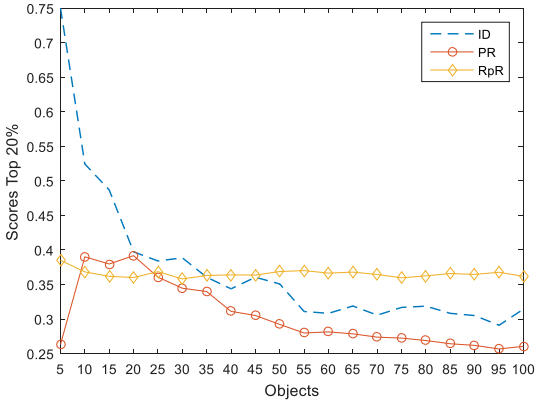

Fig. 13. Detection of top 20% of trustworthy Objects.

To clearly observe this effect, we have calculated the Kendall correlation coefficient of both PR and RpR methods compared to ID as it's the basis for both methods. According to Fig. 14, PR method always shows higher correlation compared to RpR as the effect of inward relationships plays a more dominant role in PR method to rank objects. On the other hand RpR is not depended only on inward links but also recommendations from trustworthy objects, reputations from unfriendly objects and the ability to detect least trustworthy objects.

In the model described in Fig. 3, we assumed that there are no dangling objects which have only inwards relationships but no outgoing edges, in order to avoid sinking all the trust scored to one object during the process of iteration. However, these types of objects should have good scores as it is recommended by several friends. Therefore, to be fair with dangling objects, we suggest replacing the column of the dangling object with equally distributed values. In this way, the importance of the object is equally redistributed among the other objects at the beginning, instead of being lost and at the end of iteration the true value will be transported back to the object. Furthermore, the nods which do not have any incoming links will be ignored from the index as no object would prefer to get any service from these type of objects.

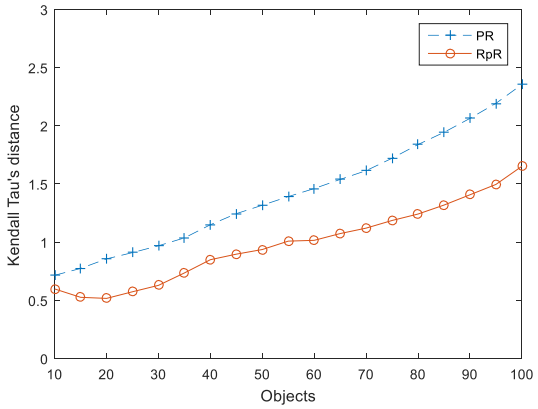

Fig. 14. Kendall Correlation with In Degree.

VI. Conclusion and Future Work

In this paper, we have proposed the trust computation model (RpR) based on Recommendations and Reputations provided by the objects in distributed SIoT environment. First, we have separated and identified the meanings of reputation and recommendations in SIoT and also the importance of these metrics when it comes to trust evaluation. Then, we have applied these concepts to the possible use case scenario and numerically assessed the trustworthiness of each object in SIoT. After that, we formally examined the key properties like convergence, accuracy and resiliency against deceitful activities through a simulation. We observe that the proposed model provide robust method to compute trust within few iteration for thousands of objects accurately specially with the downgrading feature for the untrustworthy objects over time. Finally, we demonstrated the effectiveness and performance of our algorithm over other well-known ranking systems.

However, the RpR model does not consider knowledge TM to calculate the final trust scores in this work as it is difficult to assess subjective properties in a numerical way. However, in order to provide a holistic model, a way of combining all three TMs must be considered. On the other hand, to cluster trustworthy objects we have followed an inverse PR algorithm which is totally depended on the number of outgoing links. Hence, a better method of filtering out bad recommenders is required. Moreover, the effect of decay factors on having best performance should be addressed. Even with the good recommendation system, defective objects can interfere with the feedback provided by the relations in a networking environment. Hence, a reliable way of transmitting estimations must be taken into account.

Acknowledgment

This research was supported by the ICT R&D program of MSIP/IITP [R0190-15-2027, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system].

References

[1] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization," *Computer Networks,* vol. 56, pp. 3594-3608, 2012.

[2] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications,* vol. 42, pp. 120-134, 2014.

[3] J. Audun, R. I. smail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.,* vol. 43, pp. 618-644, 2007.

[4] G. Jia and C. Ing-Ray, "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems," in *Services Computing (SCC), 2015 IEEE International Conference on*, 2015, pp. 324-331.

[5] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in internet of things," in *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2013 3rd International Conference on*, 2013, pp. 1-5.

[6] Z. Yan, *Trust Modeling and Management in Digital Environments : From Social Concept to System Development,*. Hershey, PA: IGI Global, 2010.

[7] M. Firdhous, O. Ghazali, and S. Hassan, "Trust Management in Cloud Computing: A Critical Review," *Advances in ICT for Emerging Regions (ICTer),* vol. 04, pp. 24-36, 2012.

[8] N. B. Truong, G. M. Lee, and T.-W. Um, "A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things,," in *Innovations in Clouds, Internet and Networks (ICIN)*, Paris, France., 2016.

[9] I. Chen, F. Bao, and J. Guo, "Trust-based Service Management for Social Internet of Things Systems," *IEEE Transactions on Dependable and Secure Computing,* p. 1, 2015.

[10] S. Brin and L. Page, "Reprint of: The Anatomy of a Large-Scale Hypertextual Web Search Engine,," *Computer Networks,* vol. 56, pp. 3825-3833, 2012.

[11] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, *The KeyNote Trust-Management System Version 2*: RFC Editor, 1999.

[12] F. Bao and I. Chen, "Trust Management for Internet of Things and its Application to Service Composition," *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM,* pp. 1-6, 2012.

[13] G. Zacharia and P. Maes, "Collaborative Reputation Mechanisms for Online Communities,," Dept. of Architecture., Massachusetts Institute of Technology, 2005.

[14] Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks," 2008, pp. 2129-2133.

[15] M. J. Probst and S. K. Kasera, "Statistical trust establishment in wireless sensor networks," in *Parallel and Distributed Systems, 2007 International Conference on*, 2007, pp. 1-8.

[16] L. Zhaoyu, A. W. Joy, and R. A. Thompson, "A dynamic trust model for mobile ad hoc networks," in *Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of*, 2004, pp. 80-85.

[17] D. Chen, G. R. Chang, D. W. Sun, J. J. Li, J. Jia, and X. W. Wang, "TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things," *Computer Science and Information Systems,* vol. 8, pp. 1207-1228, 2011.

[18] Y. Hu, D. Wang, H. Zhong, and F. Wu, "SocialTrust: Enabling long-term social cooperation in peer-to-peer services," *Peer-to-Peer Networking and Applications,* vol. 7, pp. 525-538, 2014.

[19] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," presented at the Proceedings of the 12th international conference on World Wide Web, Budapest, Hungary, 2003.

[20] X. Li and L. Ling, "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Transactions on Knowledge and Data Engineering,* vol. 16, pp. 843-857, 2004.

[21] P. Wu and G. Wu, "A Reputation-Based Trust Model for P2P Systems," in *Computational Intelligence and Security, 2009. CIS '09. International Conference on*, 2009, pp. 352-356.

[22] J. Hu, Q. Wu, and B. Zhou, "FCTrust: A Robust and Efficient Feedback Credibility-Based Distributed P2P Trust Model," in *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*, 2008, pp. 1963-1968.

[23] A. Das and M. M. Islam, "SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems," *IEEE Transactions on Dependable and Secure Computing,* vol. 9, pp. 261-274, 2012.

[24] J. Fei, Y. Yang, J. Shuyuan, and X. Jin, "Fast Search to Detect Communities by Truncated Inverse Page Rank in Social Networks," in *Mobile Services (MS), 2015 IEEE International Conference on*, 2015, pp. 239-246.