

From Personal Experience to Global Reputation for Trust Evaluation in the Social Internet of Things

Nguyen B. Truong*, Tai-Won Um†, Bo Zhou*, Gyu Myoung Lee*

* Department of Computer Science, Liverpool John Moores University, Liverpool, L3 3AF, UK

Email: {n.b.truong@2015., b.zhou@, g.m.lee@}ljmu.ac.uk

† Department of Information and Communication Engineering, Chosun University, Gwangju, Korea

Email: twum@chosun.ac.kr

Abstract—Trust has been exploring in the era of Internet of Things (IoT) as an extension of the traditional triad of security, privacy and reliability for offering secure, reliable and seamless communications and services. It plays a crucial role in supporting IoT entities to reduce possible risks before making decisions. However, despite a large amount of trust-related research in IoT, a prevailing trust evaluation model has been still debatable and under development. In this article, we clarify the concept of trust in the Social Internet of Things (SIoT) ecosystems and propose a comprehensive trust model called REK that incorporates third-party opinions, experience and direct observation as the three Trust Indicators. As the convergence of the IoT and social network, the SIoT enables any types of entities (physical devices, smart agents and services) to establish their own social networks based on their owners relationships. We leverage this characteristic for inaugurating Experience and Reputation, which are originally two concepts from social networks, as the two paramount indicators for trust. The Experience and Reputation are characterized and modeled using mathematical analysis along with simulation experiments and analytical results. We believe our contributions offer better understandings of trust models and evaluation mechanisms in the SIoT environment, particularly the two Experience and Reputation models. This paper also opens important trust-related research directions in near future.

Index Terms—Trust; Social Internet of Things; REK Trust Model; Reputation; Experience; Knowledge

I. INTRODUCTION

Recently the Internet of Things (IoT) has been deploying in the real world, however, it still needs a variety of technologies to flourish. In the IoT infrastructure, billions of electronic devices are connected to the Internet. These devices are normally equipped with sensors that observe or monitor various aspects of human life for supporting ubiquitous and smart applications and services. As about 50 billion devices are estimated to be connected to the Internet by 2020 with the amount of data transaction sets to grow 10-fold in the next 5 years [1], there will be a critical need for a more reliable infrastructure upon the current networking infrastructure. In the last few years, the Social Internet of Things (SIoT) concept, which enables characteristics of social networks to the IoT, has attracted many researchers as a prospective approach for boosting applications and services as well as for dealing with some vigorous challenges in IoT [2], [3]. In the SIoT environment, physical objects, software components and humans are strongly inter-operated, which is considered as a breakthrough of a Cyber-Physical-Social System (CPSS) that connects the Cyber-Social

Webs with physical world objects [4]. In this complex networked world, applications and services are able to make use of people to deal with a variety of challenges, and people can rely on machines to support their daily lives. This introduces new concerns for risks, privacy and security at both computer system level and human society level. Consequently, managing risks and securing SIoT are broader in scope and pose greater challenges than the traditional privacy and security in the physical and cyber domains. The large-scale of data collection and analysis from the SIoT environment will impose difficulties ranging from the risks of data management to the potential discrimination enabled by data aggregation and analytic over personal sensitive information such as locations, interests and activities [5]. In this regard, trust is as a prospective solution for supporting both humans and services to overcome the perception of uncertainty as well as to lower down potential risks before making any decisions. Therefore, a trust service platform could minimize the unexpected risks and maximize the predictability; and it could assist the SIoT infrastructure to operate in a controlled manner and to avoid unpredicted conditions and service failures.

An important component of a trust service platform is trust evaluation; and despite the large amount of research on trust, a complete trust evaluation mechanism in the IoT is still under investigation [6], [7]. Normally, a trust evaluation model is based on a set of trust indicators (TIs) to evaluate trust between a trustor and a trustee. In social and cognitive psychology, indicators of trust are principally from the three sources: (i) what the trustor hear about the trustee from other people (trustee's reputation, recommendations on the trustee); (ii) trustor's experiences on the trustee based on previous interactions; and (iii) understandings of the trustor on the trustee based on direct observations (knowledge) [6]–[8]. This human cognitive process is the catalyst for our trust evaluation model in the SIoT by considering trust is as a composite of three main TIs namely Reputation, Experience and Knowledge.

Experience and Reputation TIs as social features are extracted based on previous interactions among entities in the SIoT. After each interaction, a trustor is aware of how a trustee has behaved (i.e., accomplished a given task). By aggregating the trustor's awareness after each interaction, Experience TI can be obtained. In other word, the Experience TI is an

interrelation between a trustor and a trustee that reflects the perception of the trustor to the trustee about how the trustor trusts the trustee to accomplish a task. The Reputation TI, instead, is a property of the trustee itself which reflects the global perception about the trustee by incorporating all experiences of entities in a society with the trustee. In this paper, we would like to present the Experience and Reputation TIs in detail by characterizing the meanings and their roles in evaluating trust as well as proposing mathematical models and analytical results for clarifying the two TIs. The Knowledge TI is out of scope of this paper since it has been studied in our previous research [9], [10]. The main contributions of our paper are three-fold:

- A trust evaluation model called REK imitating the human cognitive process in the SIoT environment.
- An experience model that counterfeits the evolution of human intelligence respecting to the trust relationship.
- A reputation model based on the ideas of Google *PageRank*TM that leverages the proposed Experience model.

The rest of the paper is organized as follows. Section II provides important understandings about trust concept, relevant work, and the REK trust evaluation model. Section III describes experience concept in trust with related work, and the proposed model including mathematical formulations and analytical results. Section IV presents the reputation concept, the computational model and analysis. The last section concludes our work and outlines future research directions.

II. BACKGROUND AND REK TRUST EVALUATION MODEL IN THE SIoT

Trust is widely understood as ‘*belief*’ of a trustor in a trustee that the trustee is going to perform a specific task in an expected manner. In this regard, the trustor might somewhat recognize potential risks when the trustee accomplishes the task, thus trust also reflects the trustor’s willingness to be vulnerable under conditions of risks and interdependence [11].

A. Trust Concept and Definition

Trust is a multi-faceted concept used in many disciplines including human society and computer science. Trust is as an underlying psychological measurement assisting an entity (as a trustor) to make up a decision that whether it should interact with a trustee and take the risk that might turn out to be misplaced by the trustee and harm the trustor. There are plenty of trust definitions, and a widely accepted definition in the field of social science and psychology considers trust as ‘*belief*’ [11], [12]. Authors in these articles have pointed out that a belief of a human in another is not only influenced by that human’s perspective and the counterpart’s characteristics, but also other factors such as period of time and their surroundings. They have used some belief models to evaluate trust, however, found it hard to port those models to computer science areas. Nevertheless, trust is an original aspect of human social relations, and it still inherits intrinsic factors when porting trust to the SIoT environment.

Therefore, judging trust requires to characterize the triad of trustor’s viewpoint, trustee’s characteristics and environmental influences. We identify the three influential factors of trust in more detail by specifying them as *trustor’s propensity*, *trustee’s trustworthiness* and *environment risks*.

To avoid confusions of trust which can be found in several articles, it is worth mentioning that trust is neither a property of a trustee (such as its trustworthiness and reputation) nor a properties of a trustor (such as its requirements and preferences). It is interrelation between the trustor and the trustee as a relationship and derived from the triad of the trustee’s trustworthiness, the trustor’s propensity and the environment risks. We finally come up with a definition of trust in the SIoT as following:

Trust is the perception of a trustor on a trustee’s trustworthiness to accomplish a trust goal under a particular environment (within a period of time).

In other words, trust can be roughly defined as the perceived trustworthiness regarding to a particular trustee and a specific environment as interpreted in the conceptual model (Fig. 1). Evaluating trust, thus, is as valuating the trustworthiness of a trustee that respects to the trustor’s propensity and the environmental influences.

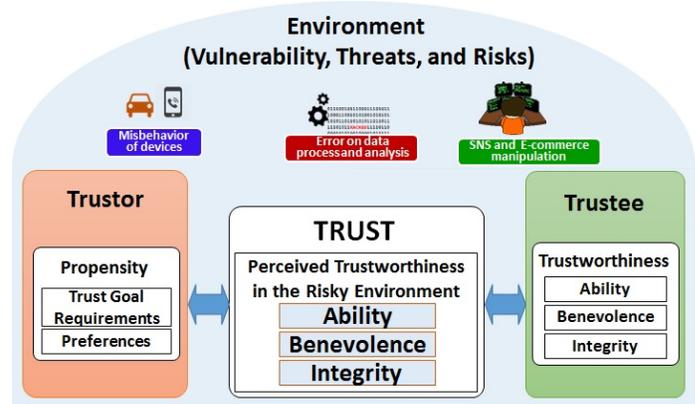


Fig. 1: Conceptual Model of Trust in the SIoT environment

Trustworthiness of a trustee is a composite of a variety of trustworthiness attributes (TAs) that represent various characteristics of the trustee. A canonical classification for TAs in the field of social organization settings can be found in [12] which considers three categories: Ability, Benevolence and Integrity. This article has listed variety of TAs belonged to the three dimensions. We believe it is also appropriate for consideration of trustworthiness of any entities in the SIoT environment (Fig. 1). Trustor’s propensity consists of the requirements for the trust goal and preferences about the trustee’s trustworthiness. The environment risks are the reflection of vulnerabilities, threats and risks in the considering environment. The requirements and the environment risks are factors for specifying a set of necessary TAs whereas the preferences are for combining the TAs to reason an overall trust value as the final goal. For example, preferences could be weights of TAs indicating the importance of the TAs

when deriving the trustworthiness. Detailed explanation and examples of trust and TAs can be found in [13].

In the SIoT, the trustor and the trustee can be humans or devices. The given task can be defined as a service in a specified environment. The trust value might be absolute (e.g., probability) or relative (e.g., level of trust). For instance, we have envisaged trust between users (trustors) and vehicles (trustees) in the Smart City (environment) for the Car Sharing service (trust goal) in [10]. We also investigated trust relationship between data stakeholders (trustors) and data consumers (trustees) for the Data Sharing service (trust goal) in Smart City (environment) [9].

B. REK Trust Evaluation Model

It is impossible to accurately evaluate trust absolutely due to a huge range of factors contributing to trust relationship and some of them are unable to obtain or greatly challenging to measure. Instead of trying to completely evaluate trust, an appropriate approach for any trust evaluation model is to find a set of TIs that are achievable to obtain and are effectively used as trust in most of cases. As mentioned before, the proposed REK evaluation model imitates the cognitive trust in social science consisting of the three TIs namely Reputation, Experience and Knowledge. These TIs can spread a wide range of trust as depicted in Fig. 2; and by synthesizing them, the REK hopefully consolidates trust with high accuracy in most scenarios in the SIoT environment.

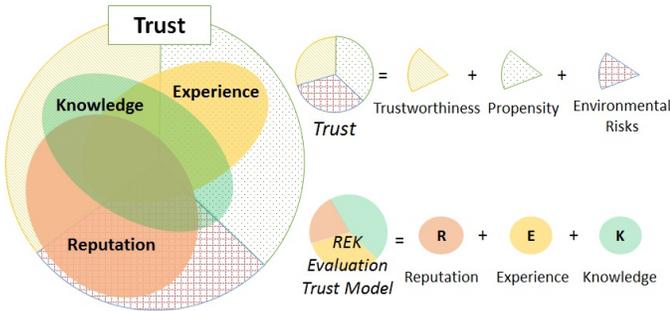


Fig. 2: Three TIs Reputation, Experience and Knowledge in the REK Trust Evaluation Model and their coverages of trust

The Reputation and Experience TIs are original concepts from social science as two of the foundational aspects of trust in human society. Both are obtained by incorporating previous interactions between entities over time. The Experience TI is personal perception of a trustor to a trustee, thus, the Experience TI covers more about the trustor’s propensity portion of trust. The Reputation TI, instead, represents global perception about an entity by aggregating all previous experiences with that entity. Thus, the Reputation TI tends to cover the trustee’s trustworthiness and the environment risks; but not about any specific trustor’s propensity (Fig. 2). The Knowledge TI represents direct observation of a trustor toward a trustee by breaking down characteristics of the trustee respecting to a specific environment. The Knowledge TI indicates a partial of trust due to limited available information about the trustee as well as the environment. In this article, we focus

on evaluation models for the two Experience and Reputation TIs because they are correlated to each other and are attained using mathematical models. The Knowledge TI as the direct observation of trust usually uses different methodology to obtain and has already been investigated in our previous articles [9], [10].

III. EXPERIENCE AS AN INDICATOR OF TRUST

A. Experience concept under the perspective of trust

Experience is a social concept that represents personal knowledge of an entity to another in a particular context gained from previous interactions between the two. Experience is a type of asymmetric relationship between two entities that high Experience values represent strong ties whereas low values express weak ties. If the trustor has Experience with the trustee, it has some cues for evaluating trust at the moment for the next interaction. Two questions might be raised: ‘why do not use Experience as trust?’ and ‘why do we need Reputation and Knowledge TIs besides Experience?’. This is because Experience is obtained based only on previous activities whereas trust is evaluated for the future interactions, thus, there is a possibility that the trustee will behave differently due to changes or occurrences of trust-related factors such as TAs, environment risks and propensity, especially in a dynamic environment like the SIoT. The Knowledge and Reputation TIs are introduced because they could reflect these factors and consolidate trust. Consequently, Experience can be used just as a TI to represent a portion of trust.

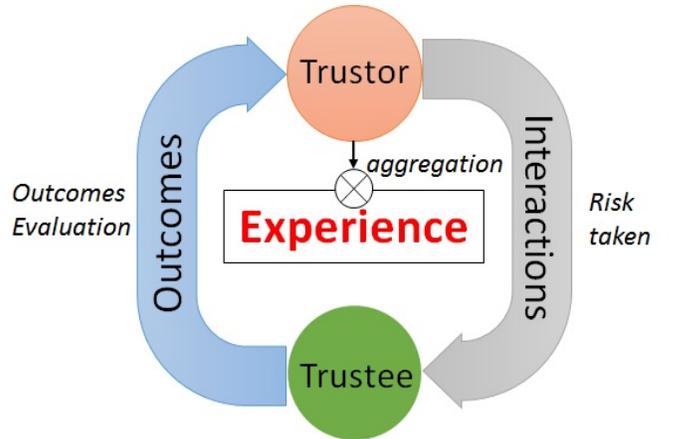


Fig. 3: Experience conceptual model in the REK Trust Evaluation

There are two essential elements in an Experience TI mechanism as illustrated in Fig. 3: (i) an evaluation scheme for valuating outcomes of interactions between two entities; and (ii) an Experience model for combining the outcomes to obtain the Experience value. Several mechanisms have been proposed to evaluate the outcomes of interactions between a trustor and a trustee. A popular scheme uses a feedback mechanism in which outcomes are evaluated by a trustor as satisfaction ratings. This scheme usually depends upon human participants which is biased and requires huge effort to attract users to participate. Another outcome evaluation scheme can be found

in some networking protocols that use an ACK message to trace whether an interaction successfully accomplished or not. Drawback of this approach is that outcomes are interpreted in two values only: successful (as 1) or unsuccessful (as 0). This approach can be found in several reputation-based mechanisms in Wireless Sensor Networks (WSNs), for instance, package transmissions between two nodes are considered as interactions; and if a transmission is successful, then the outcome is 1, and vice versa [14]. Another example is file transfer transactions as interactions in peer-to-peer networks (P2P) [15]. If a file is successfully transferred, then the outcome is 1; otherwise it is 0. Another form of interactions and associated outcomes can be found in web-pages ranking literature in which a hyperlink is considered as an interaction between a source page and a destination page with the outcome is 1. If there is no hyperlink between two web-pages, then there is no interactions [16]. The trust platform can use one of these approaches for evaluating interactions depending on particular use-cases.

B. Experience Model in the REK Trust Evaluation

Experience tends to follow the assumptions from many trust-related sociological literature [17], [18]: Experience develops due to cooperative interactions and is decreased by uncooperative interactions. It also decays over time if it is not maintained. The increase, decrease and decay values depend on three major factors: intensity of the interactions, values of the interactions (cooperative, neutral or uncooperative), and current state of the relationship (reflected by the Experience value). Thus, mathematical difference equations can be used for modeling the three trends of the Experience TI.

• Development (due to cooperative interactions)

Let ϑ be the outcome value of a considering interaction which is in the range $[0, 1]$. If the interaction is cooperative then ϑ must be greater than a threshold called $\theta_{cooperative}$. The development trend is modeled using a linear difference equation as follows:

$$Exp_{t+1} = Exp_t + \Delta Exp_{t+1} \quad (1)$$

$$\Delta Exp_{t+1} = \alpha - \alpha \frac{Exp_t}{max_{Exp}} \quad (2)$$

where Exp_t is the Experience TI value at the time t . At the beginning state, we specify a parameter called $init_{Exp}$ which is the initial value for Experience TI. α is the maximum increase value of Experience. max_{Exp} is the maximum Experience TI value, and obviously $\alpha < max_{Exp}$.

• Loss (due to uncooperative interactions)

An uncooperative interaction is when ϑ smaller than a threshold called $\theta_{uncooperative}$. The mathematical model for the Experience Loss is as following:

$$Exp_{t+1} = Max(min_{Exp}, Exp_t - \beta \Delta Exp_{t+1}) \quad (3)$$

where ΔExp_{t+1} is determined by Equation (2); β is a parameter for controlling the rate of loss. β can be fixed or dynamic but it should be always greater than 1 because

TABLE I: PARAMETERS SETTINGS FOR THE EXPERIENCE TI SIMULATION

Parameters	Values	Parameters	Values
max_{Exp}	1	γ	0.005
min_{Exp}	0	δ	0.005
$init_{Exp}$	0.3	$\theta_{uncooperative}$	0.3
α	0.1	$\theta_{cooperative}$	0.6
β	2		

Experience is difficult to gain but easy to loose. min_{Exp} is the minimum Experience TI which guarantees that the experience value cannot go lower than that.

• Decay (due to no or neutral interactions)

Empirical studies in the sociology field have figured out that most of social relationships decay over time if participants do not interact, although decay rate may vary depending on the strength of the relationships [19]. We follow this social fact so that Experience TI decays if there is no interaction after a period of time or interactions are neutral. The latter is when the interactions cannot be specified as cooperative or uncooperative (i.e., $\theta_{uncooperative} \leq \vartheta \leq \theta_{cooperative}$). Decay is assumed to be inversely proportional to current Experience values, thus strong ties exhibit less decay than weak ties. A mathematical model for the Experience Decay is proposed as follows:

$$Exp_{t+1} = Max(init_{Exp}, Exp_t - \Delta decay_{t+1}) \quad (4)$$

$$\Delta decay_{t+1} = \delta \left(1 + \gamma - \frac{Exp_{t-1}}{max_{Exp}} \right) \quad (5)$$

where δ is the minimal decay value of Experience TI which guarantees that even strong ties still get decreased. γ is the decay rate that can be fixed or dynamic depending on particular use-cases.

C. Analytical Results and Discussion

We simulate the proposed Experience TI model in Matlab. For convenience and consistency, Experience TI values are normalized to the range $[0, 1]$ (i.e., $min_{Exp} = 0$ and $max_{Exp} = 1$). Consequently, Equation (1) and (2) can be rewritten as either:

$$Exp_{t+1} = Exp_t + \alpha(1 - Exp_t) \quad (6)$$

$$Exp_{t+1} = (1 - \alpha)Exp_t + \alpha \quad (7)$$

The source code for the simulation can be found here¹. Parameters settings are explained in Table 1. As shown in Equation (2) and (6), the increase value $\Delta Exp_{t+1} = \alpha(1 - Exp_t)$ is relatively large when the current value Exp_t is small and vice versa. The mathematical solution of such linear difference equation (7) is simple that the Experience TI will reach to 1 in a log scale. This is also proven using the simulation illustrated in Fig. 4 in which the Experience TI development curve is an asymptote to 1. The loss model and decay model also form log curves which make the Experience TI less susceptible if a relationship is strong tie and vice versa. Therefore, in order to achieve high Experience TI value

¹https://github.com/nguyentb/REK/blob/master/Experience_model.m

(strong tie between two entities), it is required to have many cooperative interactions consecutively; and when it gets high, it is not easy to decay as time goes by. As can be seen in Fig. 4, decay values depend on current status of a relationship: a strong tie decays much slower than the weak tie. Hence, the relationship is assumed to require periodic maintenance but strong ties tend to persist longer even without reinforcing cooperative interactions. However, uncooperative interactions

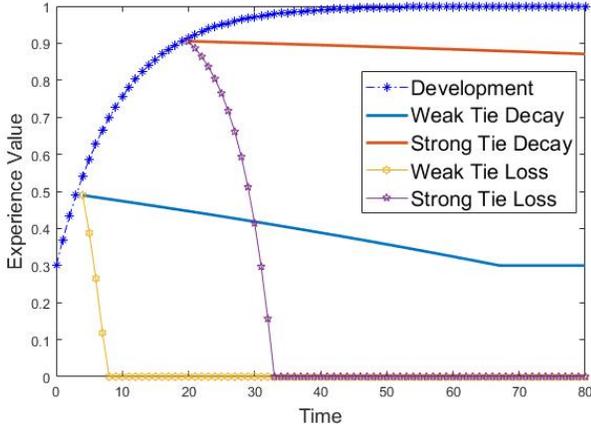


Fig. 4: Experience Model with Development, Loss and Decay trends

can severely damage the relationship even with a strong ties. The loss rate $\beta = 2$ means that Experience TI loses *twice* (due to an uncooperative interaction) compared to what it has gained (due to a cooperative interaction) (Fig.4). This is similar to what happens in the real human world, thus, we believe the proposed Experience TI model can effectively migrate the experience relationship from human sociology environment to entities in the SIoT.

IV. REPUTATION AS AN INDICATOR OF TRUST

A. Reputation concept under the perspective of trust

Reputation is a social concept corresponds to a public understanding about entity's characteristics. Reputation systems have been intensively explored in both computer sciences and information sciences in last two decades [20], [21]. The primary goal of a reputation system is to accurately provide information about trustworthiness of an entity (as a trustee) to others (as trustors), thus, encourages the trustors to participate in online transactions without first-hand knowledge. Most reputation systems are based on a feedback mechanism for managing opinions of participants after transactions, in both positive and negative forms. Difference between Experience TI and Reputation TI is that experience is a subjective relationship built on interactions from a specific trustor to a specific trustee; whereas reputation is an objective property of the trustee by considering interactions from all entities to that trustee. According to the Experience TI model proposed in Section III, entities have interacted with a trustee hold their opinions about the trustee as experiences. Therefore if these entities share their opinions (the shared opinions is as *recommendations* on the trustee), an aggregation model can be leveraged to combine

these recommendations to finalize a unique value as reputation (Fig. 5). In the SIoT environment with billions of entities, only a small number of entities that have been interacted with one another, and there is very high possibility that two entities in SIoT are new to each other, thus, no experience between the two. Therefore, Reputation TI is a crucial indicator for trust, especially in case there is no prior experience; and any reputation system should develop incentive schemes to encourage entities to share their experiences, resulting in better reputation results.

B. Reputation TI Model in the REK Trust Evaluation

A necessary consideration when designing a reputation model is that each recommendation differently contributes to the reputation of an entity. The weight a recommendation from entity x to entity y depends on both experience value $Exp(x, y)$ as well as reputation value of the entity x itself $Rep(x)$. It is understandable because that besides experience values, recommendations from high reputation entities (illustrated as big circles in Fig. 5) are more valuable than the lower ones (small circles in Fig. 5). Moreover, a recommendation could be supportive or unsupportive specified by a threshold parameter θ . That is, if $Exp(i, X) \geq \theta$ the recommendation from entity i to entity X is supportive, resulting in increasing X 's reputation whereas if $Exp(j, X) \leq \theta$ the recommendation is unsupportive, resulting in reputation decrease. Based on these two observations, and inspired by *GooglePageRankTM* idea, we have proposed a novel mathematical model for Reputation TI as following:

$$Rep_{Pos}(X) = \frac{1-d}{N} + d \left(\sum_{\forall i} Rep_{Pos}(i) x \frac{Exp(i, X)}{C_{Pos}(i)} \right) \quad (8)$$

$$Rep_{Neg}(X) = \frac{1-d}{N} + d \left(\sum_{\forall i} Rep_{Neg}(i) x \frac{1-Exp(i, X)}{C_{Neg}(i)} \right) \quad (9)$$

$$Rep(X) = \max(\min_{rep}, Rep_{Pos}(X) - Rep_{Neg}(X)) \quad (10)$$

- $Rep(i)$ is the reputation of the entity i that we are interested. Equation (10) guarantees that Reputation TI values are not below \min_{Rep} (i.e., 0).
- N is total numbers of entities in the networks.
- $d = 0.85$ is the damping factor which was intensively investigated on web-pages ranking area.
- $Exp(i, X)$ is the Experience TI from the entity i toward the entity X described in Section III.
- $Rep_{Pos}(i)$ is positive reputation of the entity i which considers only supportive recommendations.
- $C_{Pos}(i) = \sum_{Exp(i,j) > \theta} Exp(i, j)$ is the total values of all experiences in supportive recommendations that the entity i is currently sharing.
- $Rep_{Neg}(i)$ is negative reputation of the entity i which considers only unsupportive recommendations.
- $C_{Neg}(i) = \sum_{Exp(i,j) < \theta} (1 - Exp(i, j))$ is total compliments of experiences in all negative recommendations that the entity i is currently sharing.

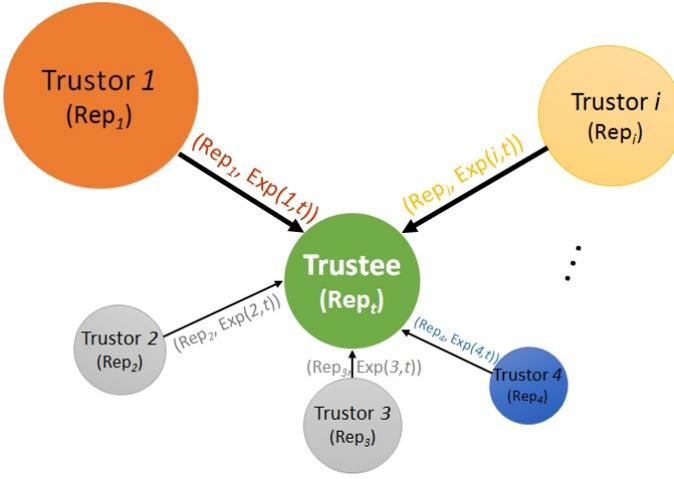


Fig. 5: Reputation of an entity is calculated based on both Experience and Reputation from/of other entities that have interacted with this entity

C. Mathematical Analysis

According to Equation (8), let M is the $N \times N$ diagonal matrix where the diagonal element $m_i = C_{Pos}(i) \forall i = \overline{1, N}$. Let Exp_{Pos} is a $N \times N$ matrix that:

$$Exp_{Pos}(i, j) = \begin{cases} Exp(i, j) & \text{if } Exp(j, i) \geq \theta \\ 0 & \text{otherwise } (Exp(j, i) < \theta) \end{cases} \quad (11)$$

And let Rep_{Pos} is the vector of the positive reputation $Rep_{Pos}(i) \forall i = \overline{1, N}$. Then, recall Equation (8) we come up with the formula in matrix notation:

$$Rep_{Pos} = \left(\frac{1-d}{N} \times E + d \times Exp_{Pos} \times M^{-1} \right) \times Rep_{Pos} \quad (12)$$

where E is $N \times N$ matrix of 1s. Let $A = \frac{1-d}{N} \times E + d \times Exp_{Pos} \times M^{-1}$, then the equation (11) is rewritten as:

$$Rep_{Pos} = A \times Rep_{Pos} \quad (13)$$

Thus, Rep_{Pos} an *eigenvector* of matrix A with *eigenvalue* = 1. We now have to prove that Rep_{Pos} is *existed* and *unique* (i.e., it is not *ambiguously defined*), resulting in the positive reputation of any entity $Rep_{Pos}(X)$ is successfully determined. Equations (12) and (13) remind of the stationary distribution of a Markov chain of random process moves among the set of states numbered 1 to N with an $N \times N$ transition matrix P where $P(\text{go from state } i \text{ to state } j) = P(i, j)$. Thus, consider a Markov chain that the states are as the N entities with the transition matrix P as the transpose matrix of A , thus:

$$P(i, j) = A^T(i, j) = A(j, i) = \frac{1-d}{N} + d \frac{Exp_{Pos}(j, i)}{m(j)} \quad (14)$$

Consequently the Markov chain can be defined as following:

$$P(i, j) = \begin{cases} \frac{1-d}{N} + d \frac{Exp_{Pos}(j, i)}{m(j)} & \text{if } Exp(j, i) \geq \theta \\ \frac{1-d}{N} & \text{otherwise } (Exp(j, i) < \theta) \end{cases} \quad (15)$$

Fortunately, this turns to a model of *random suffer* with *random jumps*. This leads to the Markov chain is strongly

connected, and the Rep_{Pos} vector, which is the *stationary distribution* of the Markov chain, is *unique* [16], [22], [23]. Similarly, the Rep_{Neg} vector from Equation (9) is *existed* and *unique*. Therefore the Reputation TI defined in Equation (10) is also *existed* and *unique*.

D. Simulation and Results

The Reputation TI for all entities in a network can be calculated using Equation (8), (9) and (10) either algebraically or iteratively. Using the algebra traditional method to solve the matrix equations (8) and (9) takes roughly N^3 operations which is a big concern when size of a network dramatically increases. We, therefore, use the iterative methods which is much faster [31]. Our source code implemented in Matlab for the Reputation TI model can be found here². Equations (8), (9), and (10) form a normalized probability distribution after conducting a number of iterations throughout the network; reputation values for all entities in the network are updated after each iteration. For a clear visualization of the algorithm convergence, we do not normalize the reputation values to the range $[0, 1]$, instead the reputation values will be in the range of the network size. Fig. 6 depicts the convergence rate for the network size $N = 100, 400$ and 800 with the tolerance = 10^{-3} which is accurate enough for ranking of entities in the range $[0, N]$. The tolerance is defined as the 2-norm vector of the difference between Rep vectors in two consecutive iterations. As can be seen from the graph in Fig. 6,

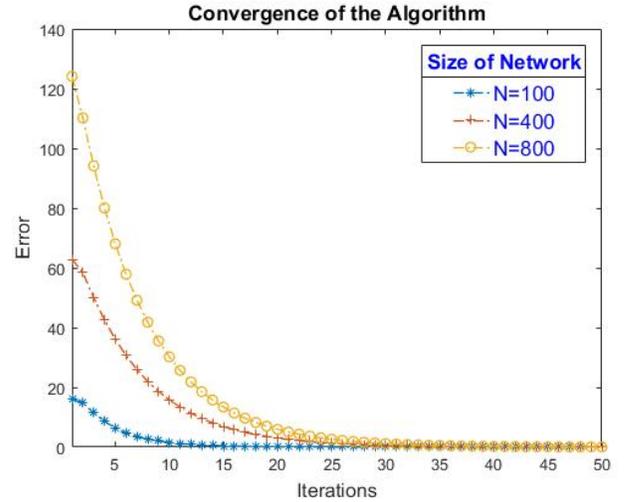


Fig. 6: Convergence of the proposed Reputation TI algorithm with several network sizes the Reputation TI model converges to a reasonable tolerance (i.e., 10^{-3}) in 50 iterations. The convergences on half and one eighth of the data take 42 and 38 iterations, respectively. This graph suggests that this reputation model will well scale even for a large network size as the scaling factor is roughly linear in \log_n . Therefore, the reputation model can be implemented in a centralized system to calculate reputation values for all of the entities in a social network. Similar mechanisms

²https://github.com/nguyentb/REK/blob/master/Reputation_model.m

for calculating rankings can be found in various related-literature [16], [22], [23]. However, the implementation might be challenged when the size of a network is extremely high (i.e., SIoT network with billions of entities) due to memory size requirements for managing all experiences among entities. This could be solved by using classification algorithms with an appropriate semi-distributed architecture so that a network can be divided into smaller sub-populations, resulting in the feasibility of conducting the proposed reputation model.

V. CONCLUSIONS AND FUTURE WORK

In this article, we have provided the comprehensive trust evaluation model called REK in the SIoT which incorporates the three indicators namely Reputation, Experience and Knowledge. We more focus on the first two indicators which are the original concepts from social and psychological sciences. The characteristics of each concept are characterized and based on that, associated mathematical models are then proposed in order to illustrate such concepts into the SIoT environment. We leverage the sociological behaviors of human relationships in the real world for modeling Experience TI and we adapt the original Google *PageRank*TM algorithm in the web-page ranking area to Reputation TI mechanism. Finally, the two models are simulated, analyzed and discussed for showing that the Experience TI and Reputation TI also inherit some important characteristics of the original concepts from human society. Consequently, the two TIs can be used for evaluating trust of any entities in the SIoT environment effectively.

This article opens a some research directions to fulfill the proposed REK model. The first direction is related to the third Knowledge TI that requires to figure out a set of TAs for evaluating direct trust. The second direction is the adaptation of the Experience TI model and the Reputation TI model to a specific use-case which requires more investigation on appropriate parameters in the models. Here, these parameters can be dynamically changed in a context-aware manner. The third direction could be more advanced mathematical models for the Experience and Reputation TIs which not only base on intensity and outcomes of interactions but also other complicated features such as the mutuality and difference among entities extracted from social contexts.

ACKNOWLEDGMENT

This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT). [2015-0-00533, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system] and the EU funded Horizon 2020 Wise-IoT project [The EC Grant Agreement No. 723156, Worldwide Interoperability for Semantics IoT].

REFERENCES

[1] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, no. 2011, pp. 1–11, 2011.

[2] L. Atzori, A. Iera, and G. Morabito, "Siot: Giving a social structure to the internet of things," *IEEE communications letters*, vol. 15, no. 11, pp. 1193–1195, 2011.

[3] 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, no. 16, pp. 3594–3608, 2012.

[4] G. Xiong, F. Zhu, X. Liu, X. Dong, W. Huang, S. Chen, and K. Zhao, "Cyber-physical-social system in intelligent transportation," *IEEE/CAA Journal of Automatica Sinica*, vol. 2, no. 3, pp. 320–333, 2015.

[5] P. Barnaghi, M. Bermudez-Edo, and R. Tönjes, "Challenges for quality of data in smart cities," *Journal of Data and Information Quality (JDIQ)*, vol. 6, no. 2-3, p. 6, 2015.

[6] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 279–298, 2012.

[7] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

[8] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, 2008.

[9] N. B. Truong, Q. H. Cao, T.-W. Um, and G. M. Lee, "Leverage a trust service platform for data usage control in smart city," in *Global Communications Conference (GLOBECOM), 2016 IEEE*. IEEE, 2016, pp. 1–7.

[10] N. B. Truong, T.-W. Um, and G. M. Lee, "A reputation and knowledge based trust service platform for trustworthy social internet of things," in *Innovations in Clouds, Internet and Networks (ICIN), Paris, France*. IEEE, IFIP, 2016.

[11] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Academy of management review*, vol. 23, no. 3, pp. 393–404, 1998.

[12] F. D. Schoorman, R. C. Mayer, and J. H. Davis, "An integrative model of organizational trust: Past, present, and future," *Academy of Management review*, vol. 32, no. 2, pp. 344–354, 2007.

[13] N. B. Truong, H. Lee, B. Askwith, and G. M. Lee, "Toward a trust evaluation mechanism in the social internet of things," *Sensors*, vol. 17, no. 6, p. 1346, 2017.

[14] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of network and computer applications*, vol. 35, no. 3, pp. 867–880, 2012.

[15] S. Kraounakis, I. N. Demetropoulos, A. Michalas, M. S. Obaidat, P. G. Sarigiannidis, and M. D. Louta, "A robust reputation-based computational model for trust establishment in pervasive systems," *IEEE Systems Journal*, vol. 9, no. 3, pp. 878–891, 2015.

[16] S. Brin and L. Page, "Reprint of: The anatomy of a large-scale hypertextual web search engine," *Computer networks*, vol. 56, no. 18, pp. 3825–3833, 2012.

[17] R. F. Baumeister and M. R. Leary, "The need to belong: desire for interpersonal attachments as a fundamental human motivation," *Psychological bulletin*, vol. 117, no. 3, p. 497, 1995.

[18] D. L. Oswald, E. M. Clark, and C. M. Kelly, "Friendship maintenance: An analysis of individual and dyad behaviors," *Journal of Social and Clinical Psychology*, vol. 23, no. 3, pp. 413–441, 2004.

[19] S. G. Roberts, R. I. Dunbar, T. V. Pollet, and T. Kuppens, "Exploring variation in active network size: Constraints and ego characteristics," *Social Networks*, vol. 31, no. 2, pp. 138–146, 2009.

[20] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th international conference on World Wide Web*. ACM, 2003, pp. 640–651.

[21] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision support systems*, vol. 43, no. 2, pp. 618–644, 2007.

[22] N. Tyagi and S. Sharma, "Weighted page rank algorithm based on number of visits of links of web page," *International Journal of Soft Computing and Engineering (IJSCE) ISSN*, pp. 2231–2307, 2012.

[23] L. Backstrom and J. Leskovec, "Supervised random walks: predicting and recommending links in social networks," in *Proceedings of the fourth ACM international conference on Web search and data mining*. ACM, 2011, pp. 635–644.