A Computational Model to Evaluate Honesty in Social Internet of Things

Upul Jayasinghe
Department of Computer Science
Liverpool John Moores University
Liverpool, United Kingdom
u.u.jayasinghe@2015.ljmu.ac.uk

Hyun-Woo Lee
Hyper-connected Communication
Research Laboratory, ETRI
Daejeon, Korea
hwlee@etri.re.kr

Gyu Myoung Lee
Department of Computer Science
Liverpool John Moores University
Liverpool, United Kingdom
g.m.lee@ljmu.ac.uk

ABSTRACT

Trust in Social Internet of Things has allowed to open new horizons in collaborative networking, particularly by allowing objects to communicate with their service providers, based on their relationships analogy to human world. However, strengthening trust is a challenging task as it involves identifying several influential factors in each domain of social-cyber-physical systems in order to build a reliable system. In this paper, we address the issue of understanding and evaluating honesty that is an important trust metric in trustworthiness evaluation process in social networks. First, we identify and define several trust attributes, which affect directly to the honesty. Then, a subjective computational model is derived based on experiences of objects and opinions from friendly objects with respect to identified attributes. Based on the outputs of this model a final honest level is predicted using regression analysis. Finally, the effectiveness of our model is tested using simulations.

Keywords

Social Networks, SIoT, Trust Metric, Trust Attributes, Trust Computation, Knowledge, Subjective Models, Regression.

1. INTRODUCTION

With the technological advancement in present information and communication infrastructures, users and owners of them (objects) generate significant amount of social information like followers, friends, communities, etc. as well as counterpart of network level interactions. Based on this, Social Internet of Things (SIoT) concept is formalized, which creates social networks between all parties (humans and objects) and among them like in online social networks (OSN) [4; 14]. Objects in SIoT autonomously generate relationships among them in order to solve common problems in cyber-physical-social systems (CPSS) including service, resource and network discovery [17].

However, heterogeneity of the devices, networks and social relationships makes CPSS vulnerable to threats. To control these kind of situations the concept of trust is introduced [3]. So far, many proposals have been presented on evaluating and managing trust in SIoT but yet prototypes lacks the basic explanations on how the information or behavioral data from CPSS is collected, processed and obtain meaningful result in the decision making process. However, authors in [9] and [18] explain about a trust model and trust computation techniques which are more relevant to our work here. Particularly, in this paper we focus on evaluating one specific trust attribute (TA) “Honesty” of objects in SIoT which helps to get an insight about “Knowledge” trust metric (TM) in our model [18]. We propose a subjective model to evaluate honesty in SIoT environment considering many aspects like object relationships, spatial and temporal properties of objects and their history of behaviors. The major contributions of this paper are to: (i) identify attributes, which affect to honesty, (ii) present a numerical model to analyze them, and (iii) evaluate the effectiveness of the numerical results on real world data set. To the best of our knowledge, we are the first to propose a subjective method to evaluate honesty in SIoT.

The remainder of the paper is organized as follows. In Section 2, we investigate current contributions on trust modeling, management and computation methods. Sections 3 provides a basic idea about SIoT environment and a brief introduction about our past contributions, which provide foundation for this research. Based on the definitions, development of numerical model is presented in Section 4 and simulation results based on the numerical model is discussed in Section 5. Finally, Section 6 concludes the paper with a summary and future work.

2. RELATED WORK

Basic underlying issues in trust assessment in IoT are the lack of concrete definition of trust, impact of relationships and context awareness on trust properties and objective of trust management in CPS environment. In this regard, authors in [21] and [16] have provided a comprehensive survey on trust management in IoT and presented a strong research model with current challenges on trust evaluation. A holistic view of trust in several application domains including TMs and usability in decision making process is explained in detail in [6].

A preliminary idea of establishing social relationships is firstly introduced in [7] and a more comprehensive description is presented in [3]. On the other hand, [8] and [14] are discussed about trust assessment of social networks based on concepts like community of interest, friendship, followers as well as frequency, duration and behavior of the objects, which provides a foundation for this research. Once the TAs are evaluated, a mechanism that combine these TAs must be investigated. In this regard, a simple arithmetic average based model is described in [11] and models which based on adaptive weights can be found in [20] and [5]. Contrast to weighted summation, regression based trust aggregation method is presented in [19] and [10].

3. BACKGROUND

3.1 Social Internet of Things

The idea of SIoT is to combine both human and objects (human or service objects) together to build an OSN while preserving their unique characteristics in their own social world. This allows different objects to establish social relationships based on their experiences, preferences and requirements without underlying network protocols. We identify several basic relationship profiles based on the SIoT architectures defined in [4] and [9]. The *parental object relationship (POR)* that is defined among homogeneous objects, which are originated at the same period of time and in the same objection creation process. The *ownership object relationship (OOR)* is observed among heterogeneous objects that belong to the same parental object. These two relationships show fairly fix relationship compared to other social relationships.

The *co-location object relationship (CLOR)* can be observed when the objects are used and operated in the same environment such as in smart home. However, cooperativeness among objects are not considered here and objects who work with each other belongs to *co-work object relationship* (CWOR) category analogy to an office where people collaborate each other. On the other hand, objects who collaborate with each other frequently and not necessarily in same location or workspace is defined as *friendship object relationship (FOR).* It has more relaxed but reliable relationship compared to others analogy to human friendships. Lastly, *community of interest (CoI)* relationships can be identified when objects follow common standards and share their knowledge and experience on achieving a common goal analogy to local community groups in a particular country area.

3.2 Trust model and Trust Metrics

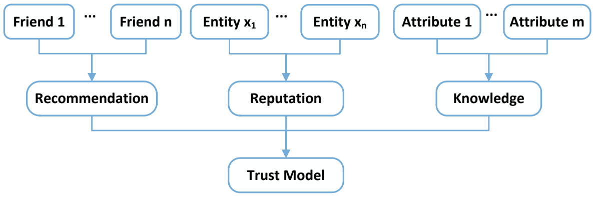


Figure 1: A Trust acquisition model.

Formally, trust can be defined as qualitative or quantitative property of a trustee measured by a trustor for a given task in a specific context and in a specific time period. In general, these properties are known as TMs and number of TMs must be taken in to account at a time in order to evaluate correct trust level of the trustee by the trustor object. These can be direct observations, indirect observations and also subjective and objective attributes. An example model of trust acquisition is shown in Figure 1 [18]. However, our objective of this paper to evaluate honesty in social environment and hence evaluating indirect TMs (recommendations and reputations) are omitted here.

The knowledge TM in the social domain is derived from many TAs including honesty, context awareness, integrity, similarity, protection, and service availability. However, we assume that honesty plays an important role on trust assessment as if there is no honesty the trust cannot be genuine and relationships would not be strong enough for reliable service provisioning analogy to sociology concepts. In SIoT, honesty TA represents whether or not a particular object is honest worthy with respect to a trustor.

4. COMPUTATIONAL MODEL

4.1 Composition of Honesty

In SIoT, we have chosen the trust property honesty, mainly because dishonest objects can severely obstruct the trust management procedures and there by smooth operation of service delivery, compared to other properties. Having a strong idea about honesty enables many positive outcomes including, ability to detect false recommendations, identify misbehaving objects, adaptively associate with future conversations based on past behaviors, resilience against threats, reduce risk associated when having conversations with strangers and ultimately assurance of trustworthy service delivery. To evaluate honesty in our trust computational model, we identify several key TAs after careful consideration among several properties as shown in Figure 2.

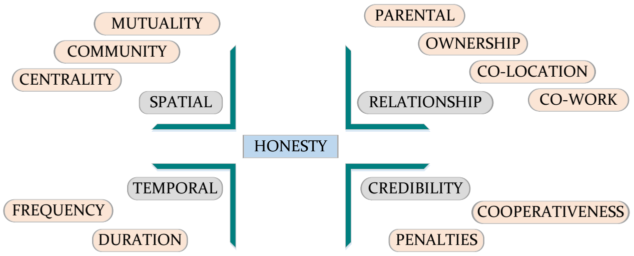


Figure 2: TAs affects Honesty.

In human world, intimacy towards other members is heavily depended on the status of their relationships. Analogy to this social phenomenon, honesty of the trustee objects can be assessed based on the relationship having among them. CLOR emphasizes how close the objects are located in physical environment as in building or city center. Often we can find common purposes among objects in close proximity in terms of their interests, required services etc. On the other hand, CWOR shows a closer relationship compared to CLOR in terms of content and context additionally to the objectives of CLOR. Hence, it is rational to consider CLOR and CWOR in order to provide valuable input in evaluating honesty.

When it comes to trustworthy service delivery, consistency in providing such a service is vital. In this regard, efforts taken to maintain the reputation, history of misbehaviors situations, following standards and keeping confidentialities are important factors when it comes to evaluating honesty. We identify these properties to represent the credibility of an object. In order to measure them, it is sensible to consider measurable aspects like cooperativeness and penalty. Cooperativeness represents the degree of the social cooperation from a trustee towards a trustor. If they are unbiased then honest worthy symmetric conversation should be taken place. Penalty is an attribute introduced by the system in order to track the misbehavior situation or the dishonesty of the trustee like not following standards, leaking confidential information etc. It can be used to discourage the future communication with misbehaved objects.

This defines the how often and how long the both a trustor and a trustee interacts with each other. Analogy to human relationships, it can be assumed that the association among parties are increased depending on the duration and frequency of the meetings. On the other hand, high frequent but small duration or longer interactions but less frequent interaction are considered as selfish dealings in order to fulfill their service requests (SR) only. As an example, in whitewashing attacks, a dishonest object can vanish for some time and rejoin the service in order to clear his bad reputation However, if a trustor can keep a record of the consistency of interested trustees then it can avoid such situations.

On the other hand, the place of a trustee in social space relative to a trustor gives meaningful contributions in evaluating honesty of a trustee. It shows how well both a trustor and a trustee are connected in social space. We consider three parameters related to spatial diversity that are mutuality, community, and centrality. Mutuality measures the degree of similar interest on other objects by both a trustee and a trustor. Community attribute defines the distance between communities. Centrality measures, how reputed the trustee is among other objects in a particular context.

4.2 Numerical Formulation

The model which analyzes honesty is a prolong process and it requires aggregation of past information as well as new information in order to predict the next honesty level. The assessment of honest towards object *j* by object *i* at time *t* is presented by $H_{ij}^{X}(t)$ where 'X' represents the attributes in Figure 2. First, we numerically model the attributes based on social layer conversations. Then based on these inputs, we perform multiple regression analysis in order to generate a prediction of honesty level in each object instead weighted summation. We consider n number of objects in the social layer as p = {p_1…,pi,…,p_j,…,p_n} where p_i represents the identity of a common object. Let N_i be the friends of the p_i and M_{ij} be the set of mutual friends between p_i and p_j.

4.2.1 Relationship Factors

4.2.1.1 CLOR

As explained in the previous section, CLOR measures the user similarity based on the environment where objects are distributed. If certain objects are visible in a particular area for considerable amount of time that indicates a common interest of activities, which yields to a measurement of honesty among participants in terms of sharing the services in that area.

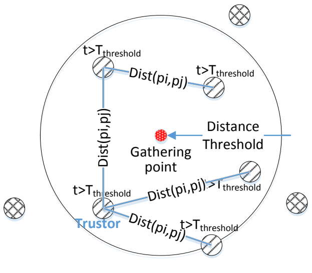


Figure 3: Spatial Similarity among Objects.

In order to find the point of gathering of these devices, maximum distance from approximate central location and a time threshold is defined as shown in Figure 3. Then the objects, which are with in this, distance boundary and who exceed the time threshold in this region is used to calculate CLOR as in equation (1).

$$H_{ij}^{CLOR}\ (t) = \frac{1}{dist(p_i, p_j)} \frac{G_{p_i} G_{p_j}}{\left\| G_{p_i} \right\| \left\| G_{p_j} \right\|} \qquad (1)$$

Here, G_{p_i} and G_{p_j} are the GPS coordinates of objects i and j respectively. The second term is the cosine similarity between two objects and it is normalized by geo distance factor $dist(p_i, p_j)$ which can be calculated as in [13].

4.2.1.2 CWOR

Objects who collaborate with other to achieve common goals can be categorized as CWOR. However, compared to CLOR the interested similarity is not the physical closeness but the work related intimacy that they share with each other in the working or service domain. In order to measure CWOR as a numerical value we compare the multicast conversations of a trustor and a trustee as shown in Figure 4. Based on this CWOR between p_i and p_j that is how much they are related as co-workers can be calculated as in (2).

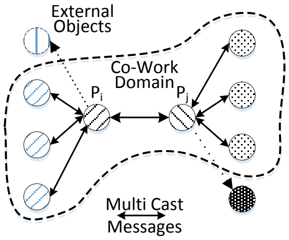


Figure 4: Co-Work Relationship among Objects.

$$H_{ij}^{CWOR}\ (t) = \frac{\left| C_{ij}^{MC} \right|}{\left| C_{i}^{MC} \right|} \qquad (2)$$

where C_{ij}^{MC} are the multicast conversations (MC) among p_i and p_j, , C_i^{MC} are the total number of MC originated at p_i respectively. However, compared to above relationships POR and OOR show a fixed relationship and hence we omitted using them for our numerical model which counts more dynamic nature of the relationships.

4.2.2 Credibility and Temporal (CT) Factors

It can be anticipated that the more frequent and longer the conversation among objects, more honesty from each party can be expected. Furthermore, interactions that are more or less balanced show how well they cooperate with each other making either party happy about their service requests and responds.

4.2.2.1 Cooperativeness, Frequency and Duration

Let consider set of conversations C = {c_1,c_2,……..c_n} over some period which trustor is interested. Then based on this, an honesty level between p_i and p_j can be calculated as in equation (3).

$$H_{ij}^{CT}\ (t) = \sum_{m=1}^{n} \frac{|c_m|}{|t_m|} E(c_m) \qquad (3)$$

where n is the number of conversations, i.e. how frequent they interact with each other, c_m is the length of the m^th successful conversation, t_m is the total conversation length and $E(c_m)$ is the entropy function which measures the balance in the conversation or the cooperativeness which can be calculated as in equation (4) [1].

$$E(c_m) = -plogp - (1-p)\log(1-p) \qquad (4)$$

where, p is the fraction of conversation that is sent by a trustor (p_i) to a trustee (p_i).

4.2.2.2 Penalty System

In here, we identify the importance of having a penalty coefficient as a feedback mechanism or as a measurement of dishonesty to downgrade the honesty level of a particular object, which has past misbehaving experiences. It is always critical to maintain the social relationships at maximum trustworthy level and hence we use exponential downgrading system as shown in equation (5).

$$H_{penalty}(t) = \frac{\|C\| - \|C_p\|}{\|C\|} e^{\left(-\frac{\|C_p\|}{\|C\|}\right)} \quad (5)$$

where ||C|| is the number of total conversations have taken place at time t and $\|C_p\|$ is the unsuccessful or suspicious conversations.

4.2.3 Spatial Factors

4.2.3.1 Mutuality and Centrality

It is logical that honesty between a trustor and a trustee is depended on how many common friends distributed among them. Higher the number of mutual friend among them higher the reliability of a conversation between them. Using this fact, the credibility of the trustee can be calculated as in (6).

$$H_{ij}^{centrality}(t) = \frac{\|M_{ij}\|}{\|N_i\|} \quad (6)$$

where M_{ij} be the set of common friends of p_i and p_j, and N_i is the friends of the trustee.

4.2.3.2 CoI

Community of interest evaluates the common interest or capabilities among objects. In mathematical form, let us define the communities that both a trustor and a trustee are involved as M_{ij}^{coi} among "D" number of communities and N_{ij}^{coi} is the number of communities of a trustee. Please note that both a trustor and a trustee can be a member of several communities and hence the honesty level of a trustee based on CoI is calculated as in (7).

$$H_{ij}^{CoI}(t) = \frac{\|M_{ij}^{coi}\|}{\|N_i^{coi}\|} \quad (7)$$

4.3 Prediction Model

In order to have a final honest level of a trustee, the factors calculated in (1),(2),(3),(6) and (7) can be combined together as in (8) such that α+β+γ+δ+η=1. Depending on the importance of the criteria, weight of each commonest must be adjacent. At the same time, a trustor must keep track on $H_{penalty}(t)$ in order to avoid conversations which are below a predefined threshold level.

$$H_{ij}(t) = \alpha H_{ij}^{CLOR}(t) + \beta H_{ij}^{CWOR}(t) + \gamma H_{ij}^{CT}(t) + \delta H_{ij}^{centrality}(t) + \eta H_{ij}^{CoI}(t) \quad (8)$$

However, linear addition may not be suitable candidate for this kind of application. Hence, we perform *multiple regression (MR)*, based on the several predictors (attributes) in order to evaluate a subsequent honest level as in (9) [12].

$$H_{ij}(t) = b_0 + \sum_{l=1}^{n} b_l H_{ij}(t) + \epsilon(t) \quad (9)$$

where H(t) is the series under investigation, and n is the order (length) of the model and b_0 is the estimated constant and b_i are the prediction coefficient of the i^{th} independent variable (attribute). ε(t) is the error term and ignored for the simplicity in our model which results the estimated model.

Table 1: Simulation Parameters.

Parameter	Value	Parameter	Value
Nodes	76	Interactions	18226
Objects	5776	Communities	711
Messages	899	Message Type (UC/MC/BC)	266/57/576

5. EXPERIMENTS AND RESULTS

5.1 Environment Setup

In order to evaluate our model, we would need mobility traces of large number of objects, which is not available at the moment for SIoT. Hence, we have used mobility traces taken at *SIGCOMM-2009* conference which is available in CRAWDAD [2] [15]. However, the model basically contains the tracers of device proximity, activity logs, friendship information, interested groups, application level message logs and data layer transmission logs. Therefore, we map these information to match with SIoT concepts as described in [4]. The parameter settings and scenario is explained the Table 1. Among 76 nodes, the parties (Trustor and Trustee) who have a conversation between them as considered as objects in order to match with SIoT concepts.

5.2 Simulation Results

In this section, we present the simulation results with the analysis of numerical results obtained in Section 4. The simulation complexity is based on the number of interactions among objects and the number of nodes. For our numerical models that take around 18000 interactions as input shows good performance as shown in Figure 5 with an average running time of 3 seconds.

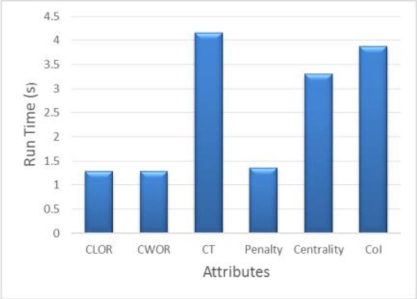


Figure 5. Simulation run time of each attribute.

First, we analyzed the data based on our CLOR model and the simulation results clearly shows how well connected the each object in the physical space as presented in Figure 6 where the arrow length show the relationship level. It can be seen that all the 76 nodes can be dispersed around major four clusters. Among them 3 clusters are in co-location relation in three different places and remaining one shows the objects who are not in close proximity to have a relationship hence low level of honesty among them.

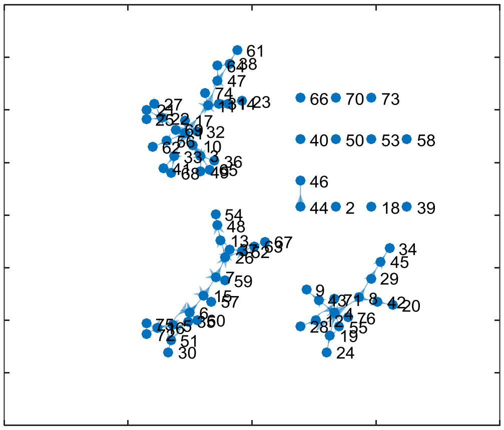
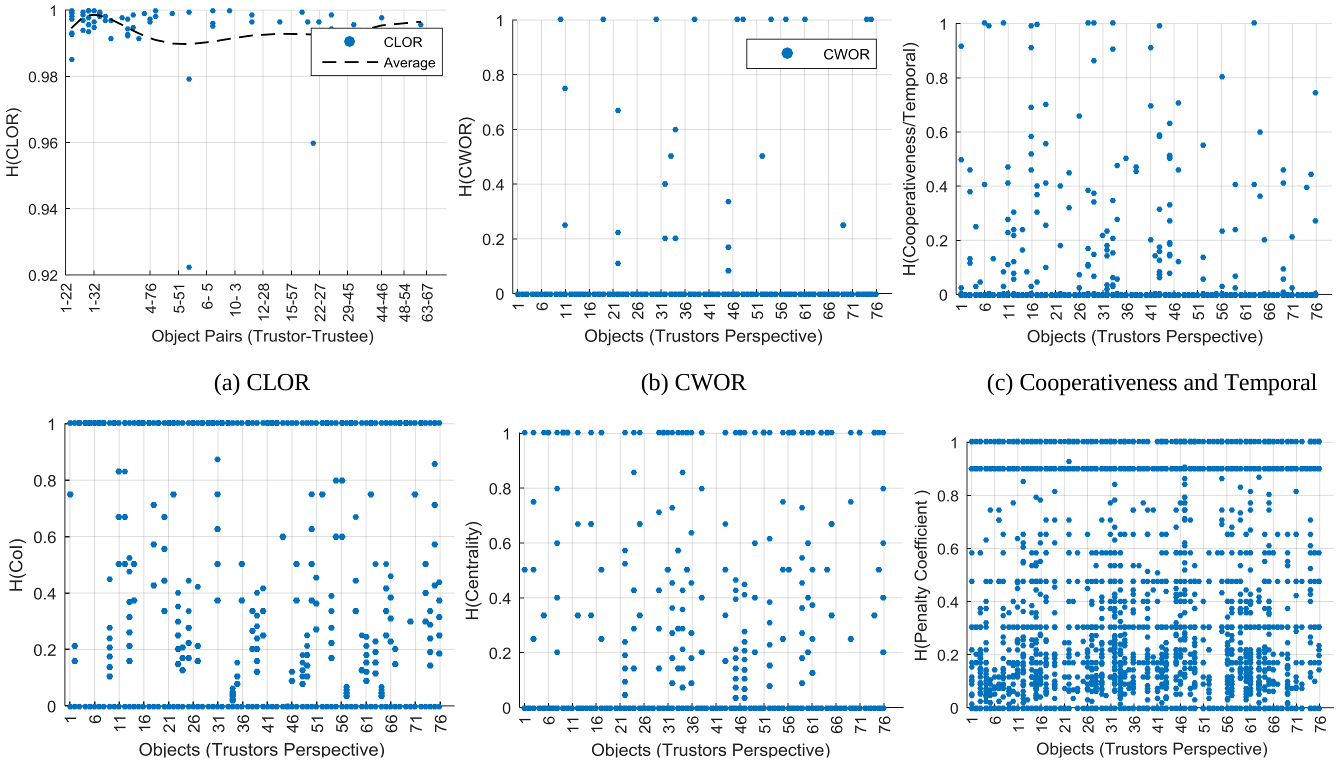


Figure 6. Co-Location Relationship.



(a) CLOR

(b) CWOR

(c) Cooperativeness and Temporal

(d) CoI

(e) Centrality

(f) Penalty Coefficient

Figure 7. Impact of Attributes on Honesty.

The numerical result obtain for H_{ij}^{CLOR} using equation (1) is show in Figure 7(a). X axis shows the Trustor (1st number) –Trustee (2nd number) pairs and Y axis shows how the honestly level changes based on the CLOR. As the data set is based on the conference location, CLOR value is quite similar in each object pair as they are created at the close proximity. Consequently, Figure 7(b), shows the effect of CWOR which is based on the MC conversations analogy to data layer multi cast messages. It can be observed that significantly lesser number of pairs willing to create co-work relationship among them.

Figure 7(c) shows how the honesty changes with cooperativeness among objects and also their frequency and duration of the conversation. It is visible that cooperativeness is distributed in the middle of the graph as often RF communication is limited to asymmetric as well as short duration of message exchanges. Similar manner, we have evaluated the honesty level based on CoI and centrality of the trustee object for trustor as shown in Figure 7(d) and Figure 7(e). However, Figure 7(f) shows that most of the penalty coefficients distributed at the low end of the graph i.e. low level of honesty. This is mainly due to the unsuccessful or misbehaviors happened in the past conversations.

In order to analyze the honest level of trustees with respect to a particular trustor we arbitrary choose node 45 and then impact of each attribute to the conversation success rate is presented in Figure 8. It clearly shows that higher the honesty level more the success rate of a conversation. Here, we define success rate as successful conversations over total number of conversation with respect to arbitrary selected node "45". As a final part of our numerical model, we have done a multiple regression analysis in order to predict future honest levels based on the values of current attributes as an alternative to simple weighted summation.

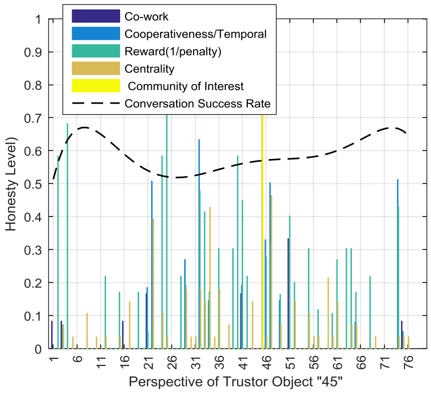


Figure 8. The view of node "45" on others.

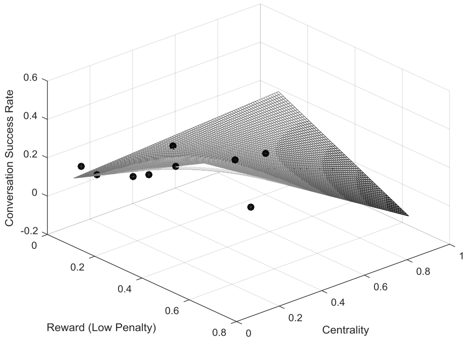


Figure 9. Prediction of Honest using MR.

In order to show the result clearly, the impact of penalty (or the reward) and centrality vs honesty is shown in Figure 9. Based on this, trustor can predict what would be the next possible success rate for specific values of attributes or the values, which must satisfy to achieve certain level of honesty.

6. CONCLUSION AND FUTURE WORK

This paper focuses on evaluating "honesty" which is a vital TM in trust assessment in SIoT. We select honesty mainly because dishonest trustees can severely damage the smooth operation at the application level processes compared to other TMs. First, we identify several attributes after careful consideration, which directly affects the honesty TM. Then based on the SIoT concepts we present a numerical as well as subjective approach to estimate individual TAs. To demonstrate the usefulness of our model, we have considered a real world scenario and analyzed the impact of each parameter on honesty in a simulation environment. Finally, we propose a prediction technique in order to find future values of honesty based on multiple regression method that is an effective alternative to weighted summation of attributes. For future work, we intend to develop a holistic trust evaluation scheme considering other major TMs as well as third party recommendations. It may include distinguishing key properties that effect on the major TMs and evaluating them based on SIoT concepts. Moreover, methods of combing TAs and TMs together, which provide the universal idea of trust levels, are also important and hence several other prediction mechanisms including machine learning techniques will be investigated.

7. ACKNOWLEDGMENTS

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].

8. REFERENCES

[1] Adali, S., Escriva, R., Goldberg, M.K., Hayvanovych, M., Magdon-Ismail, M., and Williams, G., 2010. Measuring behavioral trust in social networks. In *Proceedings of the Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on* (23-26 May 2010), 150-152.

[2] Anna-Kaisa, P. and Christophe, D., 2012. CRAWDAD dataset thlab/sigcomm2009 (v. 2012-07-15).

[3] Atzori, L., Iera, A., and Morabito, G., 2014. From "smart objects" to "social objects": The next evolutionary step of the internet of things. *IEEE Communications Magazine 52*, 1, 97-105.

[4] Atzori, L., Iera, A., Morabito, G., and Nitti, M., 2012. The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization. *Computer Networks 56*, 16, 3594-3608.

[5] Bin, Y., Singh, M.P., and Sycara, K., 2004. Developing trust in large-scale peer-to-peer systems. In *Proceedings of the Multi-Agent Security and Survivability, 2004 IEEE First Symposium on* (30-31 Aug. 2004), 1-10.

[6] Cho, J.-H., Chan, K., and Adali, S., 2015. A Survey on Trust Modeling. *ACM Comput. Surv. 48*, 2, 1-40.

[7] Holmquist, L.E., Mattern, F., Schiele, B., Alahuhta, P., Beigl, M., and Gellersen, H.-W., 2001. Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts. In *Proceedings of the Proceedings of the 3rd international conference on Ubiquitous Computing* (Atlanta, Georgia, USA2001), 741340, 116-122.

[8] Hu, Y., Wang, D., Zhong, H., and Wu, F., 2014. SocialTrust: Enabling long-term social cooperation in peer-to-peer services. *Peer-to-Peer Networking and Applications 7*, 4, 525-538.

[9] Jayasinghe, U., Truong, N.B., Lee, G.M., and Um, T.-W., 2016. RpR: A Trust Computation Model for Social Internet of Things,. In *Proceedings of the 2016 Intl IEEE Conference on Smart World Congress* (Toulouse, France2016), IEEE.

[10] Li, Z., Li, X., Narasimhan, V., Nayak, A., and Stojmenovic, I., 2011. Autoregression Models for Trust Management in Wireless Ad Hoc Networks. In *Proceedings of the Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE* (5-9 Dec. 2011), 1-5.

[11] Liang, Z. and Shi, W., 2005. Enforcing cooperative resource sharing in untrusted P2P computing environments. *Mob. Netw. Appl. 10*, 6, 971-983.

[12] MathWorks. "Interpret Linear Regression Results," 2016; https://uk.mathworks.com/help/stats/understanding-linear-regression-outputs.html.

[13] Movable Type Ltd. "Calculate distance, bearing and more between Latitude/Longitude points," 2016; http://www.movable-type.co.uk/scripts/latlong.html.

[14] Nitti, M., Girau, R., Atzori, L., Lera, A., and Morabito, G., 2013. A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things. In *Proceedings of the IEEE International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC* (Australia 2013), 18-23.

[15] Pietil, A.-K., Oliver, E., LeBrun, J., Varghese, G., and Diot, C., 2009. MobiClique: middleware for mobile social networking. In *Proceedings of the Proceedings of the 2nd ACM workshop on Online social networks* (Barcelona, Spain2009), ACM, 49-54.

[16] Sherchan, W., Nepal, S., and Paris, C., 2013. A survey of trust in social networks. *ACM Comput. Surv. 45*, 4, 1-33.

[17] Sheth, A., Anantharam, P., and Henson, C., 2013. Physical-Cyber-Social Computing: An Early 21st Century Approach. *IEEE Intelligent Systems 28*, 1, 78-82.

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

[19] Wang, Y., Lu, Y.-C., Chen, I.-R., Cho, J.-H., Swami, A., and Lu, C.-T., 2014. LogitTrust: A Logit Regression-based Trust Model for Mobile Ad Hoc Networks. In *Proceedings of the In Proceedings of the 6th ASE International Conference on Privacy, Security, Risk and Trust* (Cambridge, MA2014).

[20] Wang, Y. and Vassileva, J., 2003. Bayesian Network-Based Trust Model. In *Proceedings of the Proceedings of the 2003 IEEE/WIC International Conference on Web Intelligence* (2003), IEEE Computer Society, 946986, 372.

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