Trust Management for the Internet of Things and Its Application to Service Composition

Fenye Bao and Ing-Ray Chen
Department of Computer Science
Virginia Tech
{baofenye, irchen}@vt.edu

Abstract— **The Internet of Things (IoT) integrates a large amount of everyday life devices from heterogeneous network environments, bringing a great challenge into security and reliability management. Recognizing that the smart objects in IoT are most likely human-carried or human-operated devices, we propose a scalable trust management protocol for IoT, with the emphasis on social relationships. We consider multiple trust properties including *honesty*, *cooperativeness*, and *community-interest* to account for social interaction. Each node performs trust evaluation towards a limited set of devices of its interest only. The trust management protocol is event-driven upon the occurrence of a social encounter or interaction event, and trust is aggregated using both direct observations and indirect recommendations. We analyze the effect of trust parameters on trust assessment accuracy and trust convergence time. Our results show that there exists a trade-off between trust assessment accuracy vs. trust convergence time in the presence of false recommendations attacks performed by malicious nodes. We demonstrate the effectiveness of the proposed trust management protocol with a trust-based service composition application. Our results indicate that trust-based service composition significantly outperforms non-trust-based (random) service composition and its performance approaches the maximum achievable performance with global knowledge.**

Keywords - Trust management; Internet of things; social networks; performance analysis.

I. INTRODUCTION

The emerging paradigm of the Internet of Things (IoT) builds upon the ubiquitous connectivity of smart objects, including radio frequency identification (RFID) tags, sensors, actuators, PDAs, smartphones, etc. with wide applicability [1, 8]. The existing work of IoT has been focusing on the architecture of IoT and the enabling technologies for seamless cooperation among smart objects [1, 7-9, 12, 13, 20]. In addition, researchers have developed important IoT application scenarios, such as e-health [3, 11], smart-home and smart-community [15]. As the building blocks of IoT, smart objects with heterogeneous characteristics need cooperatively work together to accomplish the application tasks. Another characteristic of IoT is that most smart objects are human-carried or human-related devices. Therefore, the social relationships among the device users must be taken into consideration during the design phase of IoT applications. Atzori *et al.* [2] introduced the notion of Social Internet of Things (SIoT) and analyzed various types of social relationships, like parental object relationship, co-location and co-work relationship, ownership, etc., among objects. Further, devices in IoT very often expose to public areas and communicate through wireless. Hence, IoT objects are vulnerable to malicious attacks [17]. In this paper, we propose a trust management protocol for IoT considering both malicious and socially uncooperative nodes, with the goal to enhance the security and increase the performance of IoT applications.

Security has drawn the attention in IoT research [4, 5, 16, 17, 19]. Roman *et al.* [17] discussed the old and new threats to IoT, such as compromising botnets trying to hinder services and the domino effect between intertwined services and user profiling. Traditional approaches to protocol and network security, data and privacy management, identity management, trust and governance, and fault tolerance will not accommodate the requirements of IoT due to the scalability and the high variety of identity and relationship types [17]. Possible solutions were proposed to each security problem, but no specific protocol or analysis was given. Ren [16] proposed a compromise-resilient key management scheme for heterogeneous wireless IoT. The proposed key management protocol includes key agreement schemes and key evolution policies (forward and backward secure key evolution). The author also designed a quality of service (QoS) aware enhancement to the proposed scheme. However, the proposed scheme does not take social relationships among IoT identities into consideration. Chen and Helal [4] proposed a device-centric approach to enhance the safety of IoT. They designed a device description language (DDL) in which each device can specify its safety concerns, constraints, and knowledge. Nevertheless, their approach is specifically designed for sensor and actuator devices, and does not consider social relationships among device owners. Zhou and Chao [19] proposed a media-aware traffic security architecture for IoT. The authors first designed a multimedia traffic classification and analysis method, and then developed this media-aware traffic security architecture to achieve a good trade-off between system flexibility and efficiency. The limitation of their work is that they only considered direct observations to traffic without considering indirect recommendations.

There is little work on the trust management for IoT environments. Chen *et al.* [5] proposed a trust management model based on fuzzy reputation for IoT. However, their trust management model considers a specific IoT environment consisting of only wireless sensors with QoS trust metrics only like packet forwarding/delivery ratio and energy consumption. In contrast, in this paper we propose and analyze a trust management protocol considering both

978-1-4673-1239-4/12/$31.00 ©2012 IEEE

social trust and QoS trust metrics and using both direct observations and indirect recommendations to update trust.

Specifically, we consider three trust properties: *honesty*, *cooperativeness*, and *community-interest*. The *honesty* trust property represents whether or not a node is honest. The *cooperativeness* trust property represents whether or not the trustee is socially cooperative [14] with the trustor. The *community-interest* trust represents whether or not the trustor and trustee are in the same social communities/groups (e.g. co-location or co-work relationship [2]) or have the similar capabilities (parental object relationship [2]). We define and quantify trust using social network theory [6] and evaluate trust value with both direct observations and indirect recommendations. Finally, we analyze the effects of trust parameters on the trust convergence time and accuracy of trust evaluation and demonstrate the effectiveness by showing the utility gain of our trust management protocol in a service composition application. To the best of our knowledge [1, 8], our work is the first to consider social relationships in trust management for IoT.

The rest of this paper is organized as follows. Section II describes the IoT system model. In Section III, we present the detail of our trust management protocol. Section IV gives the numerical results of trust evaluation and the trust-based service composition application with physical interpretation given. Finally, Section V concludes the paper and discusses future work.

II. System Model

Figure 1 illustrates the social relationship in IoT environments. We consider an IoT environment with no centralized trusted authority. Every device (node) has an owner and an owner could have many devices. Each owner has a list of friends, representing its social relationships. A device is carried or operated by its owner in certain communities or working environments. Nodes belonging to a similar set of communities likely have similar interests or similar capabilities. We differentiate uncooperative nodes from malicious nodes. An uncooperative node acts for its own interest. So it may stop providing service to a service requester if it does not have a strong social tie (e.g., friendship) with the service requester. A malicious node aims to break the basic functionality of the IoT. In addition, it can perform the following trust-related attacks:

1. Self-promoting attacks: it can promote its importance (by providing good recommendations for itself) so as to be selected as the service provider, but then stop providing service or provide malfunction service.
2. Bad-mouthing attacks: it can ruin the reputation of well-behaved nodes (by providing bad recommendations against good nodes) so as to decrease the chance of good nodes being selected as service providers.
3. Good-mouthing attacks; it can boost the reputation of bad nodes (by providing good recommendations for them) so as to increase the chance of bad nodes being selected as service providers.

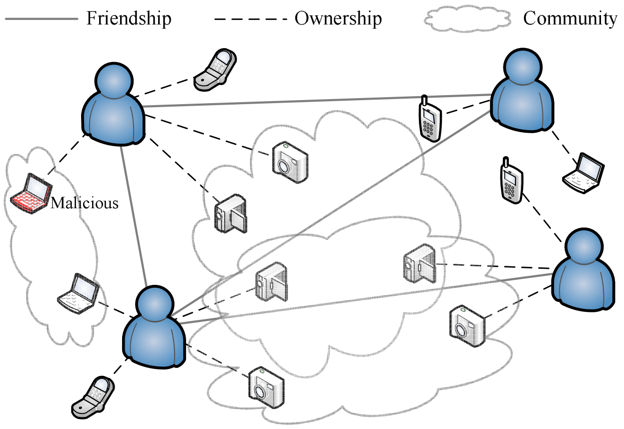

Figure 1: Social Structures of the Internet of Things.

A node's trust value is assessed based on direct observations and indirect information like recommendations. The trust of one node toward another node is updated upon encounter and interaction events. Each node will execute the trust protocol independently and will perform its direct trust assessment toward an encountered node based on specific detection mechanisms designed for assessing a trust property. Later we will discuss these specific detection mechanisms employed in our protocol.

III. Trust Management Protocol

Our trust management protocol for IoT is distributed. Each node maintains its own trust assessment towards other nodes. For scalability, a node may just keep its trust evaluation towards a limited set of nodes which it is most interested in. The trust management protocol is encounter-based as well as activity-based, meaning that the trust value is updated upon an encounter event or an interaction activity. Two nodes encountering each other or involved in a direct interaction activity can directly observe each other and update their trust assessments. They also exchange their trust evaluation results toward other nodes as recommendations.

In our trust management protocol, a node maintains multiple trust properties in *honesty*, *cooperativeness*, and *community-interest*. The trust assessment of node i evaluating node j at time t is denoted by $T_{ij}^{X}(t)$ where $X =$ *honesty*, *cooperativeness*, or *community-interest*. The trust value $T_{ij}^{X}(t)$ is a real number in the range of [0, 1] where 1 indicates complete trust, 0.5 ignorance, and 0 distrust. When node i encounters or directly interacts with another node k at time t, node i will update its trust assessment $T_{ij}^{X}(t)$ as follows:

$$T_{ij}^{X}(t) = \begin{cases} (1-\alpha)T_{ij}^{X}(t-\Delta t) + \alpha T_{ij}^{X,direct}(t), \\ \qquad if\ j == k; \\ (1-\gamma)T_{ij}^{X}(t-\Delta t) + \gamma T_{kj}^{X,recom}(t), \\ \qquad if\ j! = k; \end{cases} \quad (1)$$

Here, Δt is the elapsed time since the last trust update. If the trustee node j is node k itself, node i will use its new trust assessment toward node j based on direct observations

($T_{ij}^{X,direct}(t)$) and its old trust toward node j based on past experiences to update $T_{ij}^{X}(t)$. A parameter α ($0 \leq \alpha \leq 1$) is used here to weigh these two trust values and to consider trust decay over time, i.e., the decay of the old trust value and the contribution of the new trust value. A larger α means that trust evaluation will rely more on direct observations. Here $T_{ij}^{X,direct}(t)$ indicates node i's trust value toward node j based on direct observations accumulated over the time period $[0, t]$. Below we describe how each trust component value $T_{ij}^{X,direct}(t)$ can be obtained based on direct observations for the case in which node i and node j interacting or encountering each other within radio range:

$T_{ij}^{honesty,direct}(t)$: This refers to the belief of node i that node j is honest based on node i's direct observations toward node j. Node i estimates $T_{ij}^{honesty,direct}(t)$ by keeping a count of suspicious dishonest experiences of node j which node i has observed during $[0, t]$ using a set of anomaly detection rules such as a high discrepancy in recommendation has been experienced, as well as interval, retransmission, repetition, and delay rules as in [10, 18]. If the count exceeds a system-defined threshold, node j is considered totally dishonest at time t, i.e., $T_{ij}^{honesty,direct}(t) = 0$. Otherwise, $T_{ij}^{honesty,direct}(t)$ is computed by 1 minus the ratio of the count to the threshold. Our hypothesis is that a compromised node must be dishonest. We consider non-zero false positive probability (P_{fp}) and false negative probability (P_{fn}) for such detection mechanism.

$T_{ij}^{cooperativeness,direct}(t)$: This provides the degree of cooperativeness of node j as evaluated by node i based on direct observations over $[0, t]$. We use the social friendship [14] relationship among device owners to characterize the cooperativeness. Our hypothesis is that friends are likely to be cooperative toward each other. The cooperativeness trust of node i towards node j is computed as the ratio of the number of common friends over the number of node i's friends, i.e., $\frac{|friends(i) \cap friends(j)|}{|friends(i)|}$, where $friends(i)$ denotes the set of node i's friends. A node is included in its own friend list (i.e., $i \in friends(i)$) to deal with the case where two nodes are the only friends to each other. When node i and node j encounter and directly interact with each other, they can exchange their friend lists. Node i can validate a friend in node j's list if it is their common friend. Therefore, the direct observation of cooperativeness will be close to actual status.

$T_{ij}^{community-interest,direct}(t)$: This provides the degree of the common interest or similar capability of node j as evaluated by node i based on direct observations over $[0, t]$. The community-interest trust of node i towards node j is computed as the ratio of the number of common community/group interests over the number of node i's community/group interests, i.e., $\frac{|community(i) \cap community(j)|}{|community(i)|}$, where $community(i)$ denotes the set of node i's communities/groups. When node i and node j encounter and directly interact with each other, they can exchange their service and device profiles. Node i can validate whether node j and itself are in a particular community/group. Therefore, the direct observation of community-interest will be close to actual status.

On the other hand, if node j is not node k, then node i will not have direct observation on node j and will use its past experience $T_{ij}^{X}(t - \Delta t)$ and recommendations from node k ($T_{kj}^{X,recom}(t)$ where k is the recommender) to update $T_{ij}^{X}(t)$. The parameter γ is used here to weigh recommendations vs. past experiences and to consider trust decay over time as follows:

$$\gamma = \frac{\beta T_{ik}^{X}(t)}{1 + \beta T_{ik}^{X}(t)} \qquad (2)$$

Here we introduce another parameter $\beta \geq 0$ to specify the impact of "indirect recommendations" on $T_{ij}^{X}(t)$ such that the weight assigned to indirect recommendations is normalized to $\beta T_{ik}^{X}(t)$ relative to 1 assigned to past experiences. Essentially, the contribution of recommended trust increases proportionally as either $T_{ik}^{X}(t)$ or β increases. Instead of having a fixed weight ratio $T_{ik}^{X}(t)$ to 1 for the special case in which $\beta = 1$, we allow the weight ratio to be adjusted by adjusting the value of β and test its effect on protocol resiliency against slandering attacks such as good-mouthing and bad-mouthing attacks. Here, $T_{ik}^{X}(t)$ is node i's trust toward node k as a recommender (for node i to judge if node k provides correct information). The recommendation $T_{kj}^{X,recom}(t)$ provided by node k to node i about node j depends on if node k is a good node. If node k is a good node, $T_{kj}^{X,recom}(t)$ is simply equal to $T_{kj}^{X}(t)$. If node k is a bad node, it can provide $T_{kj}^{X,recom}(t) = 0$ when node j is a good node by means of bad-mouthing attacks, and can provide $T_{kj}^{X,recom}(t) = 1$ when node j is a bad node by means of good-mouthing attacks. In our analysis we assume this worst-case attack behavior to test our protocol resiliency.

IV. Numerical Results

In this section, we give numerical results obtained as a result of executing our proposed trust management protocol by IoT devices and demonstrate the effectiveness of our trust protocol with a service composition application.

Table 1: Default Parameter Values Used.

Param	Value	Param	Value	Param	Value
N_T	500	N_H	50	N_G	10
N_M	20	α	[0, 1]	β	[0, 8]
P_M	[20-40]%	P_{fp},P_{fn}	5%	$1/\lambda$	2 days

Table 1 lists the default parameter values. We consider an IoT environment with N_T = 500 heterogeneous smart objects/devices. These devices are randomly distributed to

N_H = 50 owners. The social cooperativeness relationship among the devices is characterized by the friendship relationship (matrix) [14] among device owners, i.e., if the owners of devices *i* and *j* are friends, then there is a 1 in the *ij* position. Devices are used by their owners in one or more social communities or groups. A device can belong to up to N_G = 10 communities or groups. The average interval that two devices encounter or directly interact with each is $1/\lambda$ = 2 days. We randomly select P_M = 20-40% out of all devices as dishonest malicious nodes. A normal or good node follows the execution of our trust management protocol, while a dishonest node acts maliciously by providing false trust recommendations (good-mouthing, bad-mouthing, and self-promoting attacks) to disrupt trust management. The initial trust value of all devices is set to ignorance (0.5).

A. *Trust Evaluation Results*

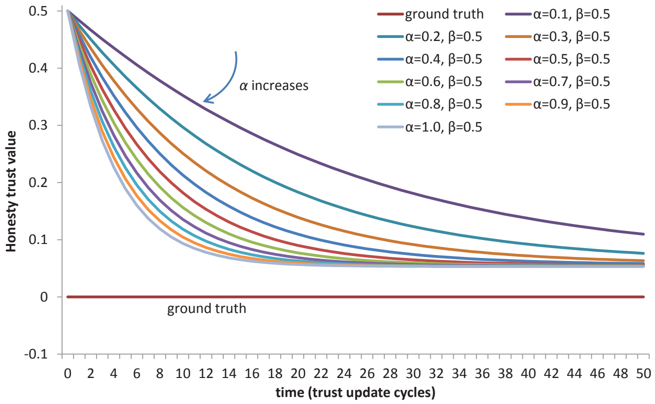

Figure 2: Effect of *α* on *Honesty* Trust Evaluation of a Malicious Node.

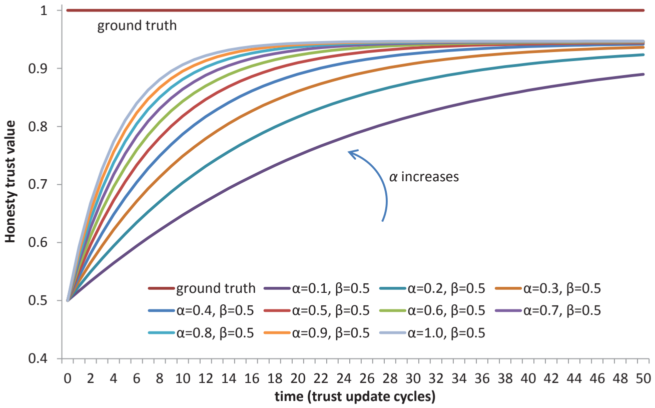

Figure 3: Effect of *α* on *Honesty* Trust Evaluation of a Good Node.

Figures 2-5 show the effect of trust parameter α on trust evaluation results for a node randomly picked. We vary the value of α in the range of [0.1, 1.0] and fix the value of β to 0.5 to isolate its effect. The horizontal straight line on each figure indicates the actual trust value derived from *ground truth*. For example, the ground truth *honesty* trust value is 1 for a good node and 0 for a malicious node. The ground truth trust values for *cooperativeness* and *community-interest* are calculated by the formulas in Section III with actual node status as input. We can see that the trust value obtained by executing our protocol approaches the ground truth value and quickly converges (with the trust update cycle being 10 hours). We observe that the trust convergence time is shorter as α increases. The reason is that new direct observations can better reflect actual node status than past trust information. The convergence value deviates from actual status because of the imperfect direct observations. Nevertheless, the accuracy is still remarkably high (with the mean square error (MSE) less than 5%).

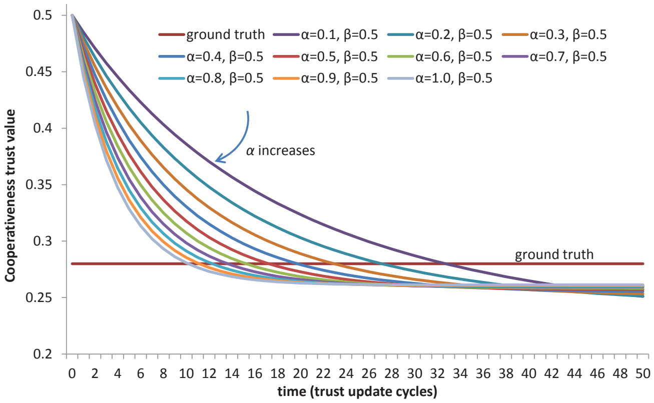

Figure 4: Effect of *α* on *Cooperativeness* Trust Evaluation.

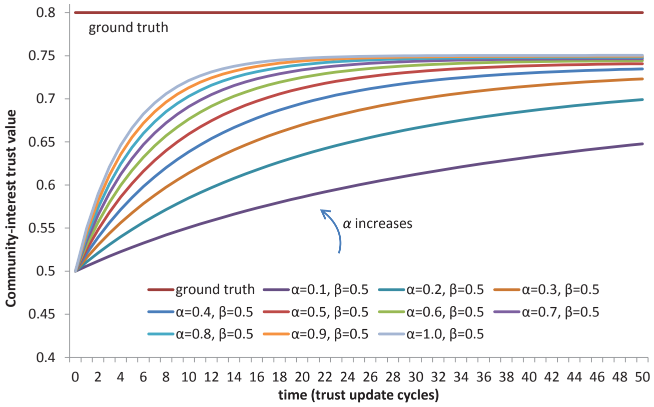

Figure 5: Effect of *α* on *Community-interest* Trust Evaluation.

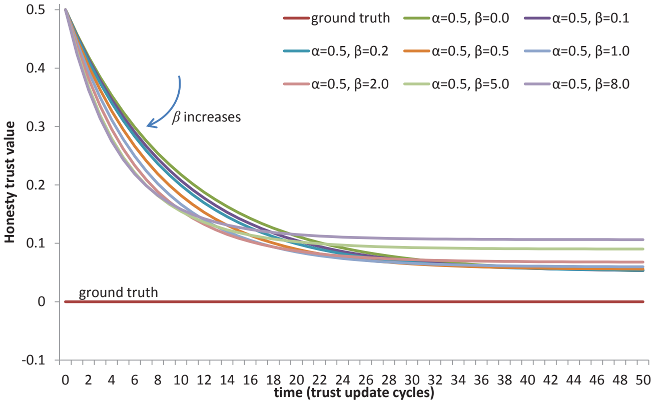

Figure 6: Effect of *β* on *Honesty* Trust Evaluation of a Malicious Node.

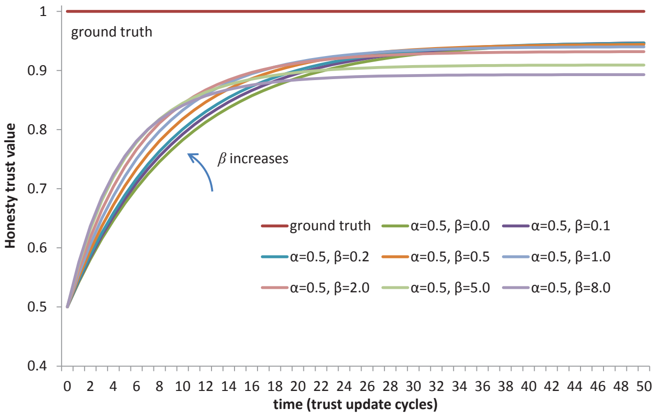

Figure 7: Effect of *β* on *Honesty* Trust Evaluation of a Good Node.

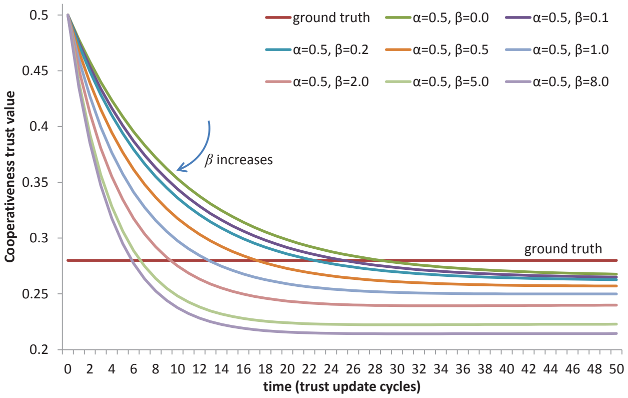

Figure 8: Effect of *β* on *Cooperativeness* Trust Evaluation.

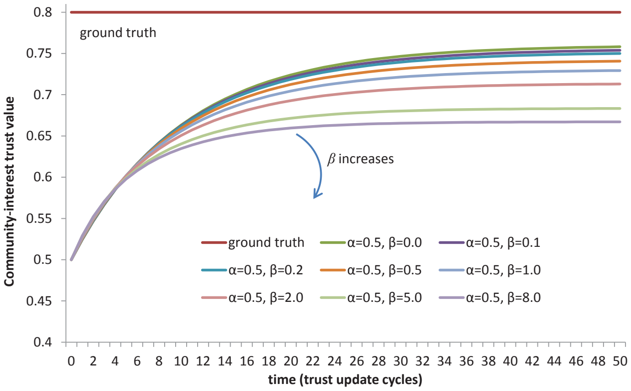

Figure 9: Effect of *β* on *Community-interest* Trust Evaluation.

Similarly, Figures 6-9 show the effect of trust parameter β on trust evaluation results for a node randomly picked. We vary the value of β in the range of [0, 8] and fix the value of α to 0.5 to isolate its effect. We observe that as β increases, the convergence time of the trust value becomes shorter, but the MSE of the trust value obtained vs. ground truth trust increases. The reason behind this is that using more recommendations in trust evaluation helps in trust convergence by propagating trust in IoT environments, but also amplifies the effect of false recommendation attacks performed by malicious nodes. However, the MSE of the trust value obtained vs. ground truth trust is still less than 10%, implying that our protocol is resilient to false recommendation attacks, including good-mouthing, bad-mouthing, and self-promoting attacks.

B. *Trust-Based Application*

To demonstrate the effectiveness of our trust management protocol, we consider a trust-based service composition application in IoT environments. In this application scenario, a node requests services (or information) from N_M service providers. The objective is to select the most trustworthy service providers such that the *utility* score representing the goodness of the service composition is maximized. Trust formation using the three trust components is application-specific. We consider the trust formation design that if a selected service provider is malicious, the returning utility score is zero; otherwise, the returning utility score equals to the smaller one of the *cooperativeness* trust value and *community-interest* trust value the node has towards the service provider. In *trust-based service composition*, a node estimates the possible returning utility of each service provider based on its own knowledge and selects N_M service providers with the highest combined returning utility. The actual returning utility score is then computed based on actual status of the service providers selected. We compare the performance of our *trust-based service composition* with two baseline approaches, *ideal service composition* which returns the maximum achievable utility score derived from global knowledge, and *random service composition* in which a node randomly selects N_M service providers without regard to trust.

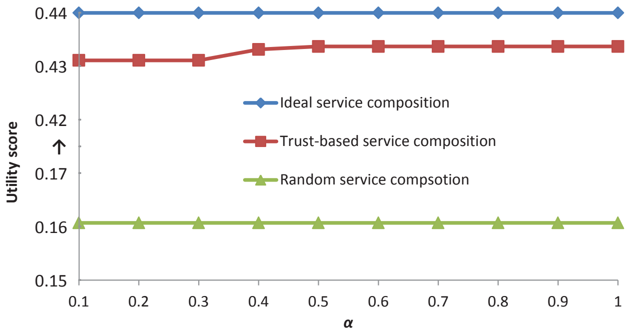

Figure 10: Effect of *α* on Trust-Based Service Composition.

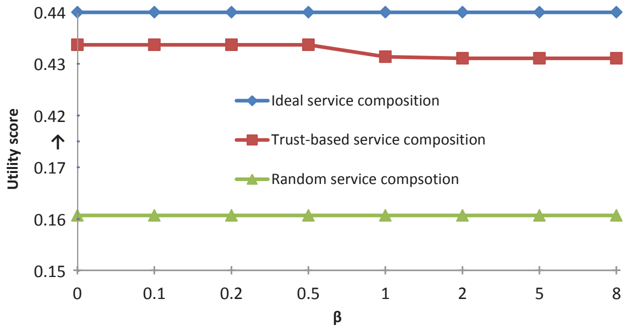

Figure 11: Effect of *β* on Trust-Based Service Composition.

Figures 10 and 11 compare the utility scores obtained from trust-based service composition vs. ideal and random service composition. We randomly pick a node as the service requester. We can see that the utility score obtained by trust-based service composition approaches the maximum achievable utility score and is significantly higher than the utility score obtained by random service composition. Figure 10 shows the effect of trust parameter α on the utility score obtained by trust-based service composition (β is fixed to 0.5 to isolate its effect). We notice that there is a cutoff point (α = 0.4) after which the utility score is higher. The reason is that using larger α value can help trust evaluation values quickly converge, so that a node could select trustworthy service providers. Figure 11 shows the effect of trust parameter β on the utility score obtained by trust-based service composition (α is fixed to 0.5 to isolate its effect). After the cutoff point (β = 0.5), the utility score becomes smaller. The reason is that using a larger β value introduces the bias of false recommendations into trust evaluation. Hence, a selected service provider might not be the most trustworthy. However, here we note that the effects of α and β on the utility score are relatively insignificant, thus demonstrating the robustness of our trust protocol.

V. Conclusion

In this paper, we designed and analyzed a scalable trust management protocol for IoT. The proposed protocol takes social relationships into account and advocates the use of three trust properties, *honesty*, *cooperativeness*, and *community-interest* to evaluate trust. The protocol is distributed and each node only updates trust towards others of its interest upon encounter or interaction events. The trust assessment is updated by both direct observations and indirect recommendations. We analyzed the effect of trust parameters (α and β) on trust evaluation. The results demonstrate that (1) using more new direct observations over pass information could increase the trust assessment accuracy and trust convergence speed, and (2) using more indirect recommendations over pass information could increase the trust convergence speed but decrease the accuracy in the presence of false recommendation attacks from malicious nodes. Our results demonstrate that our protocol provides trust assessment close to the actual node status. One can tradeoff trust assessment accuracy for trust convergence speed by adjusting trust parameters. Finally, we demonstrated the effectiveness of our trust management protocol by a service composition application in IoT environments. The results showed that trust-based service composition outperforms random service composition and approaches the maximum achievable performance from ground truth.

In the future, we plan to develop trustee-based and mission-based trust management for IoT. We also plan to consider dynamic trust management for IoT and explore new trust-based IoT applications that can adapt to changing environments such as malicious node population/activities.

References

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A Survey,” *Computer Networks,* vol. 54, no. 15, Oct. 2010, pp. 2787-2805.

[2] L. Atzori, A. Iera, and G. Morabito, “SIoT: Giving a Social Structure to the Internet of Things,” *IEEE Communication Letters,* vol. 15, no. 11, Nov. 2011, pp. 1193-1195.

[3] N. Bui, and M. Zorzi, “Health Care Applications: A Solution Based on The Internet of Things,” *4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, Barcelona, Spain, Oct. 2011, pp. 1-5.

[4] C. Chen, and S. Helal, “A Device-Centric Approach to a Safer Internet of Things,” *2011 International Workshop on Networking and Object Memories for the Internet of Things*, Beijing, China, Sep. 2011, pp. 1-6.

[5] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, “TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things,” *Computer Science and Information Systems,* vol. 8, no. 4, Oct. 2011, pp. 1207-1228.

[6] E. M. Daly, and M. Haahr, “Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs,” *IEEE Transactions on Mobile Computing,* vol. 8, no. 5, May 2009, pp. 606-621.

[7] K. Dar, A. Taherkordi, R. Rouvoy, and F. Eliassen, “Adaptable Service Composition for Very-Large-Scale Internet of Things Systems,” *8th Middleware Doctoral Symposium*, Lisbon, Portugal, Dec. 2011, pp. 1-6.

[8] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, “A Survey on Facilities for Experimental Internet of Things Research,” *IEEE Communications Magazine,* vol. 49, no. 11, Nov. 2011, pp. 58-67.

[9] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, “Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-Demand Provisioning of Web Services,” *IEEE Transaction on Services Computing,* vol. 3, no. 3, July-Sep. 2010, pp. 223-235.

[10] M. S. Islam, R. H. Khan, and D. M. Bappy, “A Hierarchical Intrusion Detection System in Wireless Sensor Networks,” *Computer Science and Network Security,* vol. 10, no. 8, August 2010, pp. 21-26.

[11] A. J. Jara, M. A. Zamora, and A. F. G. Skarmeta, “An Internet of Things-Based Personal Device for Diabetes Therapy Management in Ambient Assisted Living (AAL),” *Personal and Ubiquitous Computing,* vol. 15, no. 4, 2011, pp. 431-440.

[12] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, “Smart Objects as Building Blocks for the Internet of Things,” *IEEE Internet Computing,* vol. 14, no. 1, Jan.-Feb. 2010, pp. 44-51.

[13] M. Kranz, P. Holleis, and A. Schmidt, “Embedded Interaction: Interacting with the Internet of Things,” *IEEE Internet Computing,* vol. 14, no. 2, Mar. 2010, pp. 46-53.

[14] Q. Li, S. Zhu, and G. Cao, “Routing in Socially Selfish Delay Tolerant Networks,” *IEEE Conference on Computer Communications*, San Diego, CA, March 2010, pp. 1-9.

[15] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, “Smart Community: An Internet of Things Application,” *IEEE Communications Magazine,* vol. 49, no. 11, Nov. 2011, pp. 68-75.

[16] W. Ren, “QoS-aware and compromise-resilient key management scheme for heterogeneous wireless Internet of Things,” *Network Management,* vol. 21, no. 4, July 2011, pp. 284-299.

[17] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” *Computer,* vol. 44, no. 9, Sep. 2011, pp. 51-58.

[18] A. daSilva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, “Decentralized Intrusion Detection in Wireless Sensor Networks,” *ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks*, Montreal, Quebec, Canada, Oct. 2005, pp. 16-23.

[19] L. Zhou, and H.-C. Chao, “Multimedia Traffic Security Architecture for the Internet of Things,” *IEEE Network,* vol. 25, no. 3, May-June 2011, pp. 35-40.

[20] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, “From Today's INTRAnet of Things to a future INTERnet of Things: A Wireless- and Mobility-Related View,” *IEEE Wireless Communications,* vol. 17, no. 6, Dec. 2010, pp. 44-51.