Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems

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

Abstract— **An Internet of Things (IoT) system connects a large amount of tags, sensors, and mobile devices to facilitate information sharing, enabling a variety of attractive applications. It challenges the design and evaluation of IoT systems to meet the scalability, compatibility, extendibility, dynamic adaptability and resiliency requirements. In this paper, we design and evaluate a scalable, adaptive and survivable trust management protocol in dynamic IoT environments. Recognizing that entities in an IoT system are connected through social networks of entity owners, we consider a community of interest (CoI) based social IoT where nodes form into communities of interest. Given inter-CoI vs. intra-CoI social connections among entity owners as input, we identify best trust protocol settings for achieving convergence, accuracy, dynamic adaptability and resiliency properties in the presence of dynamically changing conditions and malicious nodes performing trust-related attacks. For scalability, we consider a design by which a node only keeps trust information of a subset of nodes meeting its interest and performs minimum computation to update trust. We validate our design by extensive simulation considering both limited and ideal (unlimited) storage space. The results demonstrate that our trust management protocol using limited storage space achieves a similar performance level compared with the one under ideal storage space, and a newly joining node can quickly build up trust towards other nodes with desirable accuracy and convergence behavior.**

Keywords – Trust management; Internet of things; social networks; scalability; adaptability; performance analysis.

I. INTRODUCTION

A future Internet of Things (IoT) system connects the physical world into cyberspace via radio frequency identification (RFID) tags, sensors, and mobile devices [2, 17]. The important application scenarios proposed for IoT include e-health (continuous care) [8, 18], smart product management, smart events for emergency management [24], etc. The IoT technology enables these applications by collecting and sharing information, which necessitates a trust management protocol for managing trust between IoT entities. Specifically, IoT systems challenge trust management in the following aspects. First, IoT systems are believed to have huge amount of entities. Existing trust management protocols do not scale well to accommodate this requirement because of the limited storage space and computation resources. Second, an IoT system evolves with new nodes joining and existing nodes leaving. A trust management protocol must address this issue to allow newly joining nodes to build up trust quickly with a reasonable degree of accuracy [22]. Third, the building blocks or entities of IoT systems are mostly human carried or human operated devices [3]. Trust management must take into account social relationships among entity owners in order to maximize protocol performance. Lastly and arguably most importantly, like other Internet systems, an IoT system is frequently the target of many cyber attackers [26] especially many IoT entities are accessible through wireless networks. A trust management protocol for IoT must be resilient to trustrelated attacks to survive in hostile environments. In this paper, we address these issues and design and validate a scalable, adaptive and survivable trust management protocol for IoT systems in the presence of dynamically changing conditions and malicious nodes preforming trust related attacks.

In the literature, Roman *et al.* [26] pointed out that traditional approaches for security, trust, and privacy management face difficulties when applying to IoT systems due to scalability and a high variety of relationship among IoT entities. Ren [25] proposed a key management scheme for heterogeneous wireless IoT systems. Zhou and Chao [30] proposed a media-aware traffic security architecture for IoT. The common drawback of their work is that they did not address the scalability issue. For trust management, Chen *et al.* [9] 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 such as packet forwarding/delivery ratio and energy consumption, and does not take into account the social relationship which is important in social IoT systems. Bao and Chen [4, 5] proposed a trust management protocol considering both social trust and QoS trust metrics and using both direct observations and indirect recommendations to update trust. Their proposed trust management protocol considers a social IoT environment where environment conditions are dynamically changing, e.g., increasing misbehaving node population/activity, changeable behavior, rapid membership changes, and interaction pattern changes. Again, the scalability issue was not addressed, which hinders its applicability to large-scale IoT systems.

In this paper, we design and evaluate a scalable, adaptive and survivable trust management protocol for a community of interest (CoI) based social IoT system where nodes can

dynamically join and leave, and form into communities of interest. The contributions of this paper are as follows:

1. We consider a CoI-based social IoT environment where intra-CoI nodes manifest substantially different social behaviors from inter-CoI nodes, such as the interaction frequency. We demonstrate that this heterogeneity dictates different trust parameter settings be used to maximize protocol performance (trust convergence vs. trust fluctuation).
2. The IoT system we consider could have new nodes joining and leaving dynamically. We demonstrate the dynamic adaptability property of our trust management protocol by showing that a newly joining node can quickly build its trust relationship towards other nodes with desirable accuracy and convergence behavior. On the other hand, other nodes can also establish the trust towards this new node.
3. For scalability, we design a storage management strategy for our trust protocol where each node only needs to keep the trust information towards a subset of nodes based on its interest and storage space. The storage management strategy can effectively utilize the limited storage space, making the trust management protocol applicable to large-scale IoT systems. Further, we show that under this storage management strategy using the limited storage space can achieve a similar performance obtainable using the ideal (unlimited) storage space for trust management.
4. We demonstrate the resiliency property (for survivability) by showing that a node's trust converges toward ground truth despite the presence of malicious nodes performing trust-related attacks.

The rest of this paper is organized as follows. Section II describes the system model. In Section III, we describe our trust management protocol and the proposed storage management strategy for scalable, adaptive and survivable trust management. Section IV gives numerical results of trust evaluation with physical interpretation given. Finally, Section V concludes the paper and discusses future work.

II. System Model

We consider a CoI-based social IoT [3] environment where nodes form into communities of interest (Figure 1). Each node has a unique address to identify. There is no centralized trusted authority. Two nodes belonging to the same CoI have specific social interests and strong social ties, which could be manifested by more frequent interactions. In addition, nodes from different communities may have different or controversial views of trust [21] towards the same trustee due to their different social interests. The multiple views of trust lead to different trust assessments even though the same behavior of the trustee is observed. This is the case especially in social IoT environments. We assume that nodes in the same CoI can achieve an agreement on trust since they share the same interests. The goal of our trust management is to make sure each node's trust evaluation converges to its community agreement (henceforward called *CoI ground truth*). Note that although we assume the existence of the communities, a node may or may not be aware of which CoI it belongs to. We consider a large IoT system in which each node has limited storage space and cannot accommodate the full set of trust values towards all other nodes. Each node can voluntarily join or leave the system. A node can be compromised and become malicious. A malicious node aims to break the basic functionality (e.g. service composition [4]) 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. Ballot stuffing 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.

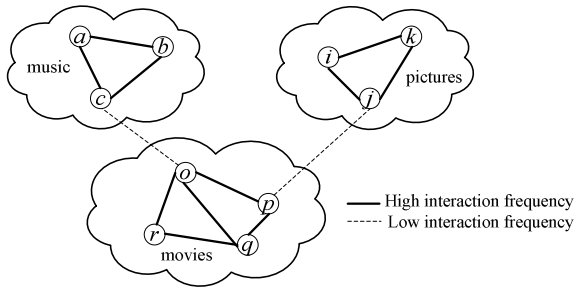


Figure 1: Communities of Interest in Social Internet of Things Systems.

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 just keeps its trust evaluation results towards a limited set of nodes sharing common interests. 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.

A. Trust Protocol Description

In our trust management protocol, a node could maintain multiple trust properties, e.g., *honesty*, *cooperativeness*, and *community-interest* [5]. 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 [20] with the trustor. The *community-interest* trust represents whether or not the trustor and trustee are in the same social communities of interest (e.g. co-location, co-work, or parental object relationship [3]). The specific analysis for each trust property is out of the scope of this paper. Since our trust protocol is generically applicable to these trust properties, we do not distinguish them here. We refer the readers to [5] for more details about these trust properties. The trust assessment

of node i towards node j at time t in a certain trust property is denoted by $T_{ij}(t)$. The trust value $T_{ij}(t)$ 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 $T_{ij}(t)$ as follows:

$$T_{ij}(t) = \begin{cases} (1-\alpha)T_{ij}(t-\Delta t) + \alpha D_{ij}(t) & if\ j = k \\ (1-\gamma)T_{ij}(t-\Delta t) + \gamma R_{kj}(t) & if\ j \neq k \end{cases} \quad (1)$$

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 ($D_{ij}(t)$) and its old trust toward node j based on past experiences to update $T_{ij}(t)$. 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 $D_{ij}(t)$ indicates node i's trust value toward node j based on direct observations accumulated over the time period $[0, t]$. When node i and node j interact or encountering each other within radio range, the detection mechanism for obtaining $D_{ij}(t)$ is specific to each trust property. In this paper, we assume that each detection mechanism is imperfect. That is to say, if the CoI ground truth trust status of node j at time t is $G_{ij}(t)$, then the $D_{ij}(t)$ value that node i obtained may deviate from $G_{ij}(t)$, e.g. $D_{ij}(t) \sim N(G_{ij}(t), \sigma_d)$ and bounded in the interval [0, 1]. Usually, the deviation σ_d would be higher if node i is untrustworthy.

On the other hand, in Equation 1, if node j is not node k, then node i will not have direct observation on node j and will use its past experience $T_{ij}(t-\Delta t)$ and recommendations from node k ($R_{kj}(t)$ where k is the recommender) to update $T_{ij}(t)$. The parameter γ is used here to weigh recommendations vs. past experiences and to consider trust decay over time as follows:

$$\gamma = \frac{\beta D_{ik}(t)}{1 + \beta D_{ik}(t)} \quad (2)$$

Here we introduce another parameter $\beta \geq 0$ to specify the impact of "indirect recommendations" on $T_{ij}(t)$ such that the weight assigned to indirect recommendations is normalized to $\beta T_{ij}(t)$ relative to 1 assigned to past experiences. Essentially, the contribution of recommended trust increases proportionally as either $D_{ik}(t)$ or β increases. Instead of having a fixed weight ratio $D_{ik}(t)$ 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 ballot stuffing and bad-mouthing attacks. Here, $D_{ik}(t)$ is node i's trust toward node k as a recommender (for node i to judge if node k provides correct information). The recommendation $R_{kj}(t)$ 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, $R_{kj}(t)$ is simply equal to $D_{kj}(t)$. If node k is a bad node, it can provide $R_{kj}(t) = 0$ when node j is a good node by means of bad-mouthing attacks, and can provide $R_{kj}(t) = 1$ when node j is a bad node by means of ballot stuffing attacks. In our analysis we assume this worst-case attack behavior to test resiliency (survivability to trust-related attacks).

The underlying idea of our trust protocol is Bayesian reputation system [16] where each node calculates the trust using Bayesian estimation over historical observations. Our protocol takes an iterative approach to aggregate new direct observations with past information considering trust decay and to aggregate new recommendations with past information considering trust discounting. When two nodes have interaction and obtain the direct interaction experience, they can update the trust towards each other with minimum computation (a single iteration).

B. *Storage Management Strategy*

Considering a large-scale IoT system in which each node has limited storage space to keep trust values of a small set of nodes with which it shares interests. A node has to decide which trust values to keep. In general, nodes are more interested in others with higher trust values. However, simply saving the trust values towards the most trustworthy nodes cannot make the trust evaluation process converge and is not adaptive to dynamic environments since there is little chance to accumulate trust towards newly joining nodes. Our storage management strategy considers nodes with the highest trust values and recent interacting nodes as these nodes are most likely to share common interests.

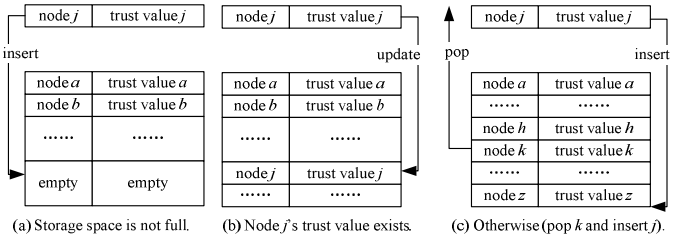


Figure 2: Storage Management Strategy.

Figure 2 illustrates how our approach works conceptualizing the storage size of each node as n (meaning that there is space to save trust values of up to n nodes). When a slot is needed, for a node's trust value to be kept it must be in the top Ω of the n trust values, or this node is one of the most recent interacting nodes. We consider Ω = 50% in this paper and leave the issue of the effect of Ω on trust evaluation performance as future work.

When node i obtains the trust value towards node j:

1. If the storage space is not full or node i does have the trust information of node j in its storage space, node i will simply save the trust value towards node j.
2. If the storage space is full and node i does not have the trust information of node j in its storage space, node i will put the trust value towards node j and pop out the trust value towards the earliest interacting node among those with trust values below the median (Ω = 50%).

The operations described above can be finished in $O(1)$ time on average by using the max-min-median heap. In addition, when two nodes interact with each other, they will only exchange the trust values kept as recommendations.

IV. SIMULATION RESULTS

In this section, we give simulation results obtained as a result of executing our proposed trust management protocol by IoT devices. Table 1 lists the default parameter values. We consider an IoT environment with N_T = 400 heterogeneous smart objects/devices. These devices are randomly distributed to N_C = 20 communities of interest. Given that trust is subjective (although it is controversial [21]) and nodes belonging to the same CoI have the same community interests, the CoI ground truth trust status toward a trustee node is the same for two trustors in the same CoI, but may be different for two trustors in different communities. We use a standard deviation parameter σ_c (set to 0.05 in simulation) to reflect the difference. When two nodes interact with each other, their direct trust assessment based on direct observation may deviate from the CoI ground truth trust status, and the deviation is higher for more untrustworthy nodes. We use a standard deviation parameter σ_d (set in the range of [0, 0.4]) to model the difference. We randomly select P_M = 20% 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 (ballot stuffing, bad-mouthing, and self-promoting attacks) to disrupt trust management. The initial trust value of all devices is set to ignorance (0.5). We assume the encounter or interaction pattern follows the power-law distribution (with or without exponential cutoff) which is supported by the analysis of many real traces [19, 23, 29]. For two nodes in the same CoI, we consider that the inter-contact time follows a bounded power law distribution ([10mins, 2 days]) with the slope equal to 1.4, resulting in the average interaction frequency about 6 times per day. For two nodes from two different communities, we consider that the inter-contact time follows a bounded power law distribution ([30mins, 7 days]) with the slope equal to 1.2, resulting in the average interaction frequency about 1 per day. The settings here are close to those obtained from the real traces [19, 23, 29].

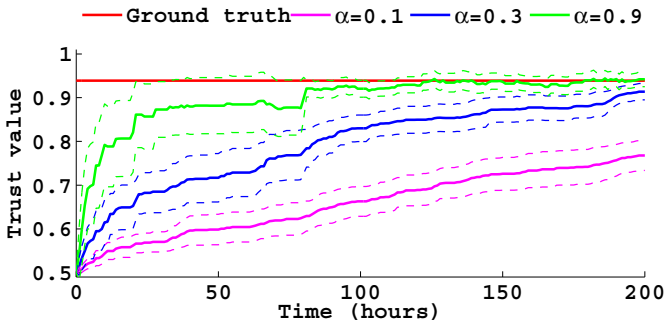
Table 1: Parameter List and Default Values Used.

Param	Value	Param	Value	Param	Value
N_T	400	N_C	20	T	200hrs
n	40	α	[0, 1]	λ_p	~6 /pair /day
Ω	50%	β	[0, 1]	λ_c	~1 /pair /day
m	20	σ_c	0.05	σ_d	[0, 0.4]

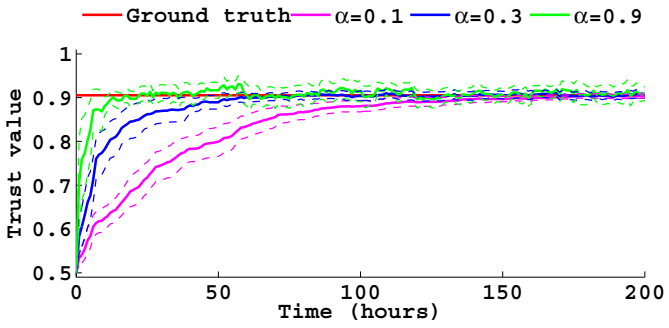
We first demonstrate the trust evaluation performance assuming there is sufficient storage space on each node to store the trust values towards all others. Then, we consider a more realistic case where each node can only accommodate the trust values towards 10% of the nodes (n = 40) for performance comparison in Section III.B.

A. Effect of Trust Parameters on Trust Evaluation

Figure 3 shows the effect of trust parameter α on trust evaluation results for a trustor node and a trustee node randomly picked. We vary the value of α by choosing three values 0.1, 0.3, and 0.9, and fix the value of β to 0 to isolate its effect. The horizontal straight line on each figure indicates the actual trust value derived from CoI *ground truth*. The dash lines show the confidence interval at 95% confidence level. We observe that when the value of α increases the trust convergence time becomes shorter, but the trust evolution fluctuates more. The reason is that using more direct observations (a higher α value) helps trust quickly converging to its CoI ground truth. However, each individual direct observation deviates from CoI ground truth status, which results in higher fluctuation. We also observe that the intra-CoI trust evaluation converges faster than the inter-CoI trust evaluation. This is expected because intra-CoI nodes interact more frequently and have more chances to directly observe each other.



(a) Inter-CoI Trust Evaluation

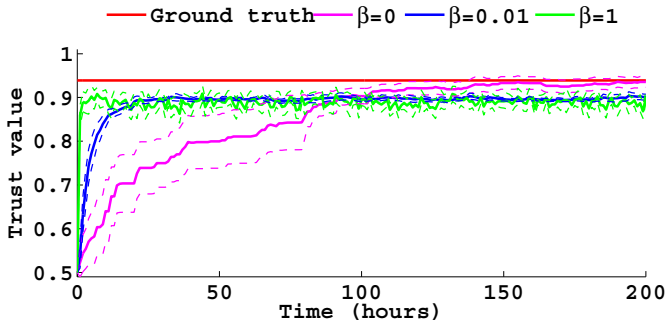


(b) Intra-CoI Trust Evaluation

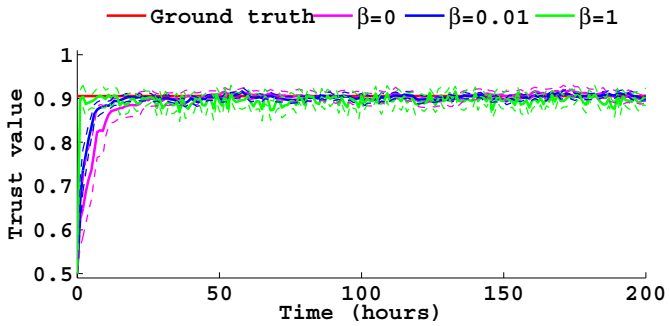
Figure 3: Effect of α on Subjective Trust.

Similarly, Figure 4 shows the effect of trust parameter β on trust evaluation results for a trustor node and a trustee node randomly picked. We vary the value of β by choosing three values 0, 0.01, and 1.0, and fix the value of α to 0.5 to isolate its effect. Again, we observe that intra-CoI trust converges faster than inter-CoI trust. In both cases, when using a higher β value, the convergence time becomes shorter, but trust fluctuation becomes higher because of the deviation of direct observation and false recommendations from attackers. Nevertheless, the mean absolute error (MAE) is less than 5% in the presence of 20% malicious nodes in the IoT system, demonstrating the resiliency of our protocol to survive from trust related attacks. Another important observation is that when using trust recommendations ($\beta > 0$), the MAE of inter-CoI trust is higher than the MAE of intra-CoI trust. The reason behind this is that trust is subjective and nodes from different communities of interest have different biased views toward CoI ground truth trust. Thus, using recommendations in trust evaluation may introduce bias if the recommender node is from

a different CoI. However, the effect of trust bias can be reduced and even eliminated if the trustor and trustee are from the same CoI and interact frequently.

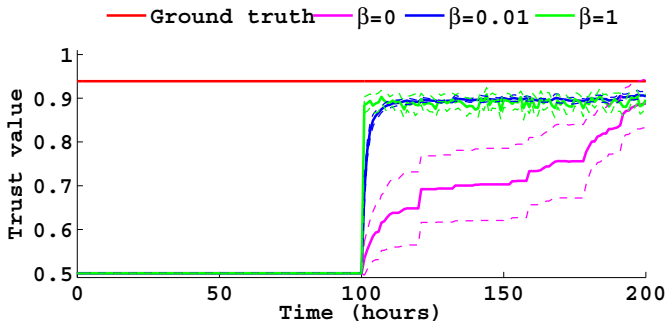


(a) Inter-CoI Trust Evaluation

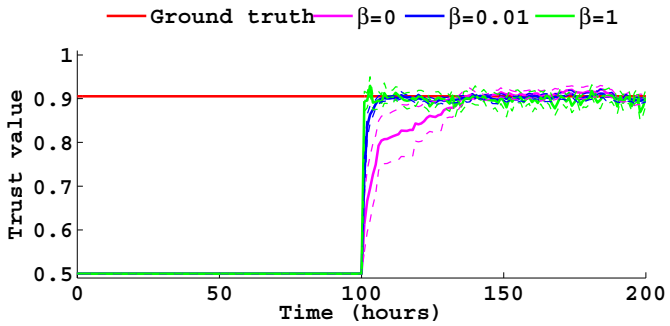


(b) Intra-CoI Trust Evaluation

Figure 4: Effect of β on Subjective Trust.



(a) Inter-CoI Trust Evaluation



(b) Intra-CoI Trust Evaluation

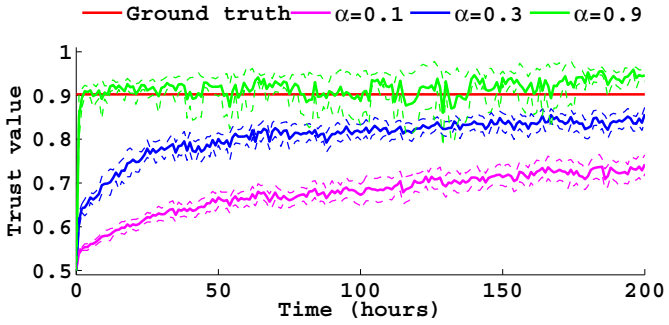
Figure 5: Effect of β on Trust of a Newly Joining Node.

B. Trust Evaluation of New Joining Nodes

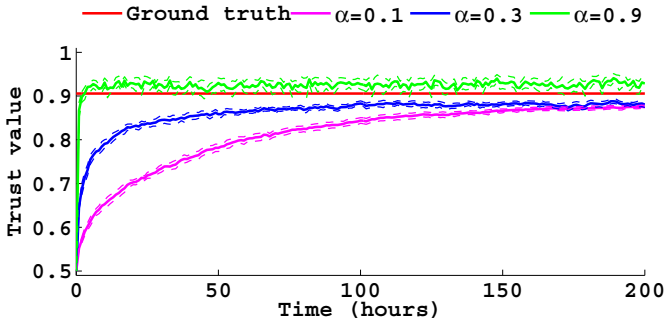
Next, we consider a dynamic environment where a new node joins the IoT system. Certainly, if we do not consider any recommendations in trust evaluation, the trust evaluation of this newly joining node towards others will behave the same as shown in Figure 3. Thus, it suffices to show the effect of β on the trust of the newly joining node towards others in Figure 5. We can see that this newly joining node very quickly builds up its trust towards both intra-CoI nodes and inter-CoI nodes in the IoT system. The reason is that the IoT system has already reached convergence, and this newly joining node can make use of such information through recommendations.

C. Trust Evaluation with Limited Storage Space

The simulation results we present above are based on the assumption that each node has sufficient storage size to save the trust values of all other nodes. In this section, we consider a more realistic scenario in which each node only has limited storage space to keep the trust values of up to 10% of the nodes in the system (with $n = 40$). We run our trust protocol using the storage management strategy (with $\Omega = 50\%$) described in Section III.B.



(a) Inter-CoI Trust Evaluation



(b) Intra-CoI Trust Evaluation

Figure 6: Effect of α on Trust (Limited Storage).

Figure 6 illustrates the effect of α on inter-CoI trust evaluation and intra-CoI trust evaluation for a trustee node randomly picked. We first observe a similar trend exhibited as the one in Figure 3 where unlimited storage is assumed, demonstrating the effectiveness of our storage management strategy. Trust fluctuation is higher especially for inter-CoI trust evaluation. The reason is that the trust value towards the trustee node may be dropped by some trustor nodes due to limited space and imperfect direct observation. We also observe that both inter-CoI trust evaluation and inter-CoI trust

evaluation overestimate when α is high (e.g. α = 0.9), as a result of our storage management strategy preferring to keep nodes with high trust values. However, this overestimation is system wide, meaning that the overestimation happens on every node towards all other nodes. Thus, it does not do much harm to the usage of trust. Another byproduct of this preference is fast trust convergence. Comparing Figure 6 with Figure 3, we can see significantly improvement on trust convergence for higher α value (e.g. α = 0.9). The reason behind this is that our trust management strategy works like a filter excluding highly deviated recommendations coming from untrustworthy nodes to shield the system from false recommendation attacks.

Lastly, we demonstrate the effectiveness of the storage management strategy using the hit ratio. The top-*m* hit ratio means the percentage of the top-*m* most trustworthy nodes (with highest CoI ground truth trust) having their trust values stored in the limited *n* slots. Figure 7 shows the top-20 hit ratio as a function of time for a randomly selected node. We can see that initially the hit ratio is zero because there is no trust information towards others. As the trust converges, the hit ratio quickly increases and approaches 80%. This demonstrates the effectiveness and high space utilization of our storage management strategy.

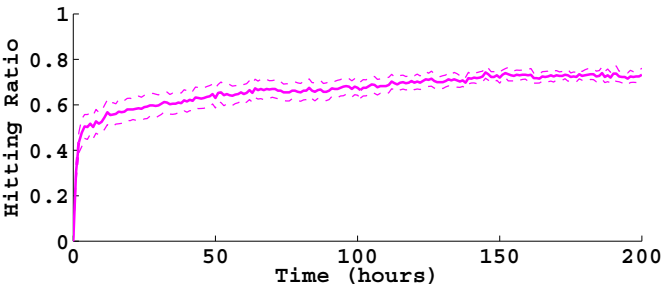


Figure 7: Hit Ratio.

V. CONCLUSION

In this paper, we designed and analyzed a scalable, adaptive and survivable trust management protocol for a community of interest based dynamic social IoT. The protocol is distributed and each node only updates trust towards others of its interest upon encounter or interaction events. We analyzed the effect of trust parameters (α and β) on intra-CoI and inter-CoI trust evaluation. The results demonstrate that the intra-CoI trust converges faster than inter-CoI under the same parameter setting. Dynamic adaptability is achieved by selecting the best trust parameter setting in response to changes to communities of interest. We also analyzed our trust protocol performance for a newly joining node to the network. Making use of existing trust information in the network, a newly joining node can quickly build up its trust relationship with desirable convergence and accuracy behavior. Finally, for scalability we proposed a storage management strategy to effectively utilize limited storage space in IoT devices. The results show that using the proposed method, our trust protocol with limited storage space achieves a similar performance level as that with ideal (unlimited) storage space and can perform better in the trust convergence time.

In the future, we plan to demonstrate the applicability of our scalable trust management protocol with IoT applications needing trust to mitigate risk such as secure routing and intrusion detection [6, 10] with fuzzy failure criteria [7] in communities of Robot as a Service (RaaS) [13] in a cloud computing environment, or in communities of associated smart phones. We also plan to investigate how to utilize community detection methods [1] to adaptively select best trust parameters in the presence of both malicious and selfish nodes. Another direction is to develop trust-based admission control [11, 12, 14, 15, 27, 28] for IoT systems. Lastly we plan to analyze the effect of Ω on the performance of the scalable trust management protocol design developed in this paper.

ACKNOWLEDGMENT

This material is based upon work supported in part by the U. S. Army Research Laboratory and the U. S. Army Research Office under contract number W911NF-12-1-0445.

REFERENCES

[1] R. Aldecoa, and I. Marín, "Closed Benchmarks for Network Community Structure Characterization," *Physical Review E,* vol. 85, no. 2, 2012, pp. 026109-1 - 026109-8.

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

[3] 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.

[4] F. Bao, and I. R. Chen, "Dynamic Trust Management for Internet of Things Applications," *2012 International Workshop on Self-Aware Internet of Things*, San Jose, California, USA, September 2012.

[5] F. Bao, and I. R. Chen, "Trust Management for the Internet of Things and Its Application to Service Composition," *IEEE WoWMoM 2012 Workshop on the Internet of Things: Smart Objects and Services*, San Francisco, CA, USA, June 2012.

[6] F. Bao, I. R. Chen, M. Chang, and J. H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-Based Routing and Intrusion Detection," *IEEE Transactions on Network and Service Management,* vol. 9, no. 2, 2012, pp. 161-183.

[7] F. B. Bastani, I. R. Chen, and T. Tsao, "Reliability of Systems with Fuzzy-Failure Criterion," *Annual Reliability and Maintainability Symposium*, 1994.

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

[9] 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.

[10] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Trust Management for Encounter-Based Routing in Delay Tolerant Networks," *IEEE Global Communications Conference*, Miami, Florida, USA, Dec. 2010, pp. 1-6.

[11] I. R. Chen, and T. H. Hsi, "Performance Analysis of Admission Control Algorithms Based on Reward Optimization for Real-Time Multimedia Servers," *Performance Evaluation,* vol. 33, no. 2, 1998, pp. 89-112.

[12] I. R. Chen, O. Yilmaz, and I. Yen, "Admission Control Algorithms for Revenue Optimization with QoS Guarantees in Mobile Wireless Networks," *Wireless Personal Communications,* vol. 38, no. 3, 2006, pp. 357-376.

[13] Y. Chen, Z. Du, and M. García-Acosta, "Robot as a Service in Cloud Computing," *IEEE 5th Symp. on Service Oriented System Engineering*, Nanjing, China, Jan. 2010, pp. 151-158.

[14] S. T. Cheng, C. M. Chen, and I. R. Chen, "Dynamic Quota-Based Admission Control with Sub-Rating in Multimedia Servers," *Multimedia Systems,* vol. 8, no. 2, 2000, pp. 83-91.

[15] S. T. Cheng, C. M. Chen, and I. R. Chen, "Performance Evaluation of an Admission Control Algorithm: Dynamic Threshold with Negotiation," *Performance Evaluation,* vol. 52, no. 1, 2003, pp. 1-13.

[16] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," *ACM Transactions on Sensor Networks,* vol. 4, no. 3, May 2008, pp. 1-37.

[17] 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.

[18] 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.

[19] T. Karagiannis, J.-Y. Le Boudec, and M. Vojnović, "Power Law and Exponential Decay of Intercontact Times between Mobile Devices," *IEEE Transactions on Mobile Computing,* vol. 8, no. 10, 2007, pp. 1377-1390.

[20] 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.

[21] P. Massa, and P. Avesani, "Controversial Users demand Local Trust Metrics: an Experimental Study on Epinions.com Community," *the 25th American Association for Artificial Intelligence Conference*, 2005.

[22] P. Massa, and P. Avesani, "Trust-aware Recommender Systems," *ACM Recommender Systems Conference*, Minneapolis, Minnesota, USA, Oct. 2007.

[23] A. Passarella, and M. Conti, "Characterising Aggregate Inter-Contact Times in Heterogeneous Opportunistic Networks," *the 10th International IFIP TC 6 Conference on Networking*, 2011, pp. 301-313.

[24] M. Presser, and S. Krco, *The Internet of Things Initiative D2.1: Initial report on IoT applications of strategic interest*, 2011.

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

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

[27] N. Verma, and I. R. Chen, "Admission Control Algorithms Integrated with Pricing for Revenue Optimization with QoS Guarantees in Mobile Wireless Networks," *IEEE 10th International Conference on Parallel and Distributed Systems*, Newport Beach, USA, July 2004, pp. 495-502.

[28] O. Yilmaz, and I. R. Chen, "Utilizing Call Admission Control for Pricing Optimization of Multiple Service Classes in Wireless Cellular Networks," *Computer Communications,* vol. 32, no. 2, 2009, pp. 317-323.

[29] J. Yoon, B. D. Noble, M. Liu, and M. Kim, "Building Realistic Mobility Models from Coarse-Grained Traces," *the 4th International Conference on Mobile Systems, Applications and Services*, 2006, pp. 177-190.

[30] 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.