Virtual Community IOT-oriented Recommended Trust Algorithm

Qiang Rong

[1]Eastern International Art College, Zhengzhou University of Light Industry, Zhengzhou, Henan, China

erongqiang163@163.com

Keywords: virtual community, internet of things, network security, trust recommendation algorithm, Lyapunov optimization.

Abstract. In available trust based recommendation schemes, users always tend to transact with the entity with highest trust value. That will result in the fact that the virtual community's resource cannot be fully utilized. The entity with the highest trust value will also delay the response because of its capacity constraint, so that its trust value will be bound to decline. To resolve this problem, we proposed a recommendation algorithm which takes the community benefit and the stability of the entities' trust value into account. The community's control center adopts the Lyapunov optimization method to make decision which can give it maximum benefit on the premise of satisfying the desired constraint of the interaction requester, meanwhile guaranteeing the stability of the community nodes' trust value. The theoretical analysis and the experiments show that our algorithm can stabilize the community nodes' trust value, also can enable the whole community and resource requester to get more benefit.

Introduction

The Internet of Things[1] integrates sensing technology, communication technology, computer network and control technology into a whole, making physical world connected with cyber space. Its application prospect is very vast, e.g. electric medical [2] etc. In the future, it is more likely to be combined with virtualization & cloud computing, SOA and other technologies to realize ubiquitous service of Internet of Things: TaaS[3]. The background of this paper is based on Internet of Things System of virtual community. Namely, virtual community is led in Internet of Things, and virtual technology is used to abstract, combine, allocate and manage resources on Internet of Things. Traditional virtual community is only limited to information & file sharing; however, in such a virtual community above, computing resources and file resources etc, all can be shared. Each virtual community has a control center to dispatch and manage resources in the community, to ensure efficient utilization of whole community resources and good operation of the community[4]. When entities in the network interact with each other, conversations between entities are full of uncertainty due to system instability, network interference, lack of acquaintance with interaction object, etc. Therefore a trust management model is needed to assess and manage trust relationship between entities so as to make an entity able to interact with another trust-worthy entity.

System Model

A virtual community contains several nodes. All the nodes are managed by community control center. In this section, the author describes virtual community system model, as shown in Figure 1. Thereinto, Node a, b, c, x, y and z express member nodes in community. Community control center manages whole virtual community. Duty of trust management center is to assess and store comprehensive trust rank of various nodes in virtual community. Other components have less relation with the problem to be solved by the paper, so hereby they are omitted due to length limit. When there is a need for Node x to interact with other nodes in virtual community, it needs to complete the following steps. Firstly, it sends a request to local community control center, corresponding to Step 1 in Figure 1. Secondly, community control center searches a virtual community able to respond to the request, and sends the request to the community, corresponding to

Step 2. Thirdly, control center of the community able to complete the request decides which node shall respond to the request by the algorithm proposed in the paper according to request content as well as load, trust rank and other information of various community nodes, corresponding to Step 3. Fourthly, request response node interacts with request initiation node, corresponding to Step 4, 5, 6. After the end of interaction, request initiator will make assessment on trust of the interaction node, and feed assessment result back to trust management center of local community of responder, corresponding to Step 7. Trust management center will make assessment on comprehensive trust rank of the node according to the feedback information so as to be convenient for community control center to make a decision.

Various variants used in the paper are described as follows (In the following formulas $i \in \{1,...,K\}$, K is quantity of community nodes):
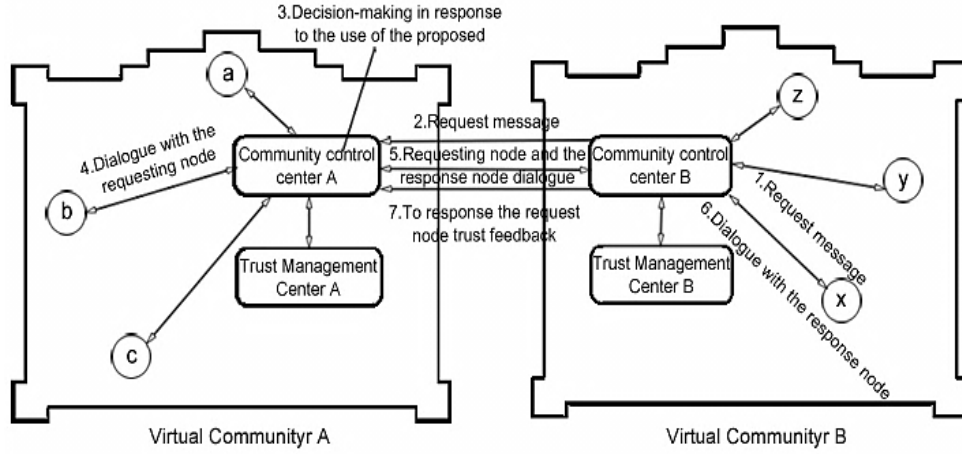

Figure 1   System Model

w(t) expresses interaction request handled by community control center at Time t. Thereinto, w(t)= < wtd, wQos, wcpl >, w expresses weight occupied by response delay in trust feedback. wtd expresses weight occupied by interaction result quality in trust feedback, and wQos expresses the complexity of the request, with $0 \le$ wtd, wQos, wcpl ≤ 100, wtd + wQos = 100. di expresses average time handling capacity of Node i, with $0 \le$ di ≤ 100. The bigger di is, the more requests it indicates that Node i can handle within unit time.

γ(t) expresses trust value of Node i at Time t. In the paper, node trust value is assumed to be an integer between 0 and 100. Trust value 0 indicates that the node is not reliable at all. Trust value 100 indicates that the node is fully reliable.

$$\alpha_i(t) = \begin{cases} 1 \text{ , Request } w_{(t)} \text{ is assigned to node } i \\ 0 \text{ , Node } i \text{ at time } t \text{ did not receive a request} \end{cases},$$

It expresses the decision made by community control center against its member Node i at Time t. Obviously, at Time t, a virtual community at most has only one node at t of 1.

Qi(t) expresses the load of Node i at Time t. And there exists Qi(0) = 0, Qi(t+1) = Qi(t) + yi(t),thereinto, yi(t) expresses the variation of load of Node i from Time t to Time t+1, namely difference between newly added load and handled load during the period. And there exists $y_i(t) = Y_i(\alpha_i(t), w_i(t)) = \alpha_i(t) \times e_i^w(t) - \min\{Q_i(t), d_i\}$, thereinto, $e_i^w(t) = \gamma_i(t) \times w_{cpl}(t)$ expresses if task w(t) is distributed to Node i, then the value of load likely to be added by Node i completing the task is in direct proportion to trust rank of node and task complexity.

Assuming that both interaction parties will acquire certain benefit after the end of each interaction, we use re(t) to express benefit acquired by local community of response node after the completion of w(t), and use $w_{el}^w(t)$ to express benefit acquired by task w(t) request node after the end of interaction:

$$r_e(t) = \sum_{i=1}^{K}\left\{\alpha_i(t) \times \gamma_i(t) \times cpl_{w(t)} \Big/ \max\{Q_i(t)/d_i, 1\}\right\}, w_{el}^w(t) = \sum_{i=1}^{K}\left\{\alpha_i(t) \times \left(w_{Qos} \times \gamma_i(t) - w_{td} \times (Q_i(t)/d_i)\right)\right\}$$

Lyapunov equation L is defined as: $L(t) = \dfrac{1}{2}\sum_{i=1}^{K} Q_i(t)^2$,

Then $\Delta(t) = L(t+1) - L(t)$ may be used to express community load variation. The author hopes to keep node load stable and simultaneously maximize the benefit of community and interaction requester. Therefore $\Delta(t) + V \times p(t)$ is drift − plus − penalty function, among which V is weight value and $p(t) = P(\alpha(t), w(t)) = -re(t)$ is penalty function. Then the problem needing to be solved is to minimize penalty function at the premise: load of various community nodes won't increase infinitely; benefit acquired by requester at the end of interaction is positive[5].

Recommended Trust Algorithm Based on the Optimization of Lyapunov

Qi(t+1) = Qi(t)+ yi(t) can be concluded from Section 1, and hence there is constant B such that:

$$\Delta t = L(t+1) - L(t) \le \frac{1}{2}\sum_{i=1}^{K} y_i(t)^2 + \sum_{i=1}^{K} Q_i(t)y_i(t) \le B + \sum_{i=1}^{K} Q_i(t)y_i(t) ,$$

$$\Delta t = L(t+1) - L(t) \le \frac{1}{2}\sum_{i=1}^{K} y_i(t)^2 + \sum_{i=1}^{K} Q_i(t)y_i(t) \le B + \sum_{i=1}^{K} Q_i(t)y_i(t) ,$$

Author hopes to the algorithm proposed not only can ensure the stability of community node load and trust, but also can acquire minimum penalty function, namely community acquires the most benefit. Therefore the sum of the two above must be minimized to achieve our purpose. Then community control center needs to make a decision to minimize $Vp(t) + \sum_{i=1}^{K} Q_i(t)y_i(t)$ at each Time t according to load state of various nodes and w(t). Algorithm 1 provides algorithm decided by community control center. Input of the algorithm is current time request w(t) as well as current load state and trust value of various community nodes, and output is decision result of control center.

Algorithm 1: recommended algorithm based on the optimization of Lyapunov

Enter: w(t) , Qi (t) , γ i (t), i $\in$ {1, ..., K}

The output: Decision results

1. int D = ∞;
2. for i = 1 → K
3. α j (t) = 0;   j $\in$ {1,..., K}
4. αi (t) = 1;
5. $T = V \times p(t) + \sum_{i=1}^{K}\left\{ Q_i(t) \times Y_i(\alpha^*(t), w(t)) \right\}$
6. if T < D and $w_{el}^{w}(t) > 0$
7. D = T ;
8. control _ action = i;
9. endif
10. endfor
11. return control _ action;

Experiment and Analysis

To verify the effectiveness of the algorithm proposed in the paper, the author carries out some numerical experiments. Relevant parameters of virtual community applied in the experiments are as shown in Table 1. In the experiments, users' assessment on community node trust applies trust value computing method proposed. Each cycle may randomly produce a service request event, and control center will make a decision according to the algorithm proposed in the paper.

Table 1　Node parameter settings

Node Type	d	Probability of providing quality services	Quantity
High Confidence nodes	40	0.85	40
Trusted nodes	40	0.70	20
Untrusted nodes	40	0.55	30
Malicious nodes	40	0.25	10

Stability Analysis of Node Trust Value. The author compares trust value variation of highly trust-worthy community node in execution of the algorithm proposed in the paper and greedy algorithm, with comparison results as shown in Figure 2.
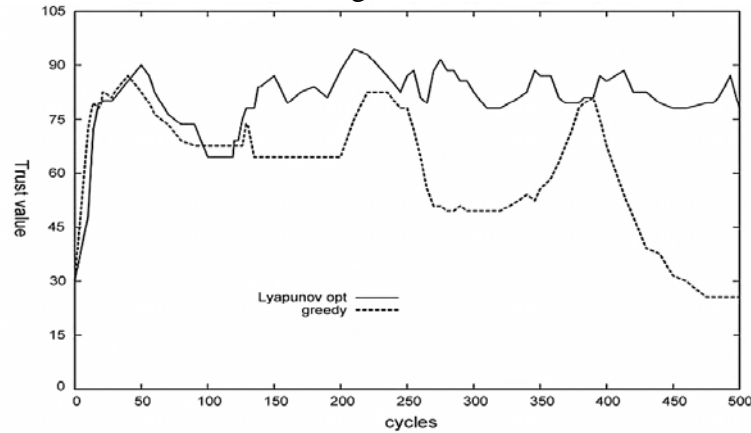

Figure 2 Trust Value Variation of Trust-worthy Node

From Figure 2, it can be seen that the algorithm proposed in the paper is to make a decision to maximize community benefit at the premise of ensuring stability of community load so that trust value of high credible node keeps good stability. But greedy algorithm will lead to great fluctuation of trust value of highly trust-worthy node because always selecting node with existing biggest trust value will make the node load increasing so that interaction request response delay is increasing, sequentially resulting in the decline of trust value. When trust value declines to certain extent, the request acquired will decrease, and the load will also gradually decrease; when it receives new interaction request again, it may timely make a response such that the trust value gradually increases again. Then trust value of the node will always keep such a cycle.

Conclusion

Aiming at the problem that it cannot make full use of virtual community resources in current trust management model, the author proposes a recommended algorithm with community member resource limit and current trust value into consideration. The algorithm is based on the optimization of Lyapunov such that it is able to make community control center make the recommended decision to maximize community benefit while ensuring trust rank stability of community member. Both theoretical analysis and simulation result indicate that control center makes community benefit by recommended algorithm proposed by the author much more than that by traditional greedy algorithm, and simultaneously trust rank of community member has better stability than that by greedy selection.

Acknowledgment

References

[1] Lee G M, Crespi N, Choi J K, et al. Internet of Things[M]. Evolution of Telecommunication Services. Heidelberg:Springer Berlin Heidelberg, 2013: 257-282.

[2] Jara A J, Zamora-Izquierdo M A, Skarmeta A F. Interconnection framework for mHealth and remote monitoring based on the Internet of Things[J]. Selected Areas in Communications, IEEE Journal on, 2013, 31(9): 47-65.

[3] Cho J H, Swami A, Chen I R. Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks[J]. Journal of Network and Computer Applications, 2012, 35(3): 1001-1012.

[4] Fan X, Li M, Ma J, et al. Behavior-based reputation management in P2P file-sharing networks[J]. Journal of Computer and System Sciences, 2012, 78(6): 1737-1750.

[5] Kuter U, Golbeck J. Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models[C]// Proceedings of the 22nd national conference on Artificial intelligence. Palo Alto:AAAI, 2007: 1377-1382.