A Dynamic Trust Model Based on Naive Bayes Classifier for Ubiquitous Environments

Weiwei Yuan, Donghai Guan, Sungyoung Lee*, and Youngkoo Lee

Department of Computer Engineering, Kyung Hee University, Korea
{weiwei, donghai, sylee}@oslab.khu.ac.kr, yklee@khu.ac.kr

Abstract. Computational models of trust have been proposed for use in ubiquitous computing environments to decide whether to provide services to requesters which are either unfamiliar with service providers or do not have enough access rights to certain services. Due to the highly dynamic and unpredictable characteristic of ubiquitous environments, the trust model should make trust decision dynamically. In this paper, we introduce a novel Naive Bayes classifier based trust model which can dynamically make trust decision in different situations. The trust evaluation is based on service provider's own prior knowledge in stead of assuming variable weights and pre-defined fixed thresholds. This model is also suitable to make decision when only limited information is available in ubiquitous environments. Finally we give the simulation results of our model and the comparison with the related works.

1 Introduction

Ubiquitous computing environment consists of a massively networked world supporting a population of diverse but cooperating mobile entities. The autonomous operation among the contributing units is necessary due to lack of central control [1]. Traditional authentication and access control are effective only in situations where the system knows in advance which users are going to access and what their access rights are. Later on, computational models of trust were proposed for ubiquitous computing environments which were capable of deciding on the runtime whether to provide services to service requesters which are either unfamiliar with service providers or do not have enough access rights to certain services. Access decision in ubiquitous computing environments has to rely on some kind of trust developed with past interactions.

Trust is the measure of willingness to believe in an entity based on its competence (e.g. goodness, strength, ability) and behavior within a specific context at a given time. Previous trust models used various time-consuming approaches to evaluate the trust value by considering different factors that may effect the trust decision. However, a common failing is that these models simply compared these painstaking gotten trust values with one or two fixed pre-defined thresholds to make the final trust deci-

* Corresponding author.

sion, which is not suitable for the highly dynamic ubiquitous environments. For example, in a ubiquitous supported smart office, the thresholds for different services providers to provide services may not be the same, e.g. the threshold for providing fax service may be higher than the threshold for enabling copy machine service. For the same service provider, its threshold to provide service may also change from time-to-time, e.g. the threshold for scanner may be raised since it has been frequently mis-operated by users recently. The change in threshold values is related to the changes in acceptance level of service providers to the whole ubiquitous environment. The raising of the scanner's threshold means that its acceptance level to the smart office has been decreased due to the previous unsuccessful interactions with the users. Hence we would dynamically make the decision due to the change in usage pattern.

The object of this paper is to propose a trust model in ubiquitous environments that can dynamically make trust decision based on different situations and different service providers. This paper sets the stage by introducing a novel Naive Bayes classifier based trust model, which makes decision based on each entity's own prior knowledge. The main advantage of our trust model is that it avoids using only one or two predefined fixed thresholds, and can dynamically update decisions according to each service provider's own judging standard. Moreover, our trust model can make use of limited information in decision making, which is usually the case in a real scenario.

The rest of the paper is organized as follows. We briefly introduce related work in Section 2. And we present the proposed trust model in detail in Section 3. Section 4 gives the simulation results. Finally, conclusions and future work are presented in Section 5.

2 Related Work

Since mid 90s the research on the key role of trust management models has been outlined in [2], [3], [4] to develop complex and dependable computer systems. In the field of ubiquitous computing, research has paid much more attention to build autonomous trust management as fundamental building block to design the future security framework, such as [6], [12], [13], [14], [15].

A general concept of dynamic trust model in ubiquitous computing environments had been given in [1]. In [5], the authors explained basic scenarios in ubiquitous computing and modeling requirements of trust. A solution to evaluate trust from the past experience was given in [7]. In [8], the authors proposed a role-based trust model in ubiquitous environment, where recommendations were used to make decision. Trust level, a measure of one's belief in the honesty, competence and dependability to a certain entity, was used to make decision in [9]. The trust was divided into 6 levels and operators such as time and distance were used to evaluate the trust level. In [10], the authors involved the concept of confidence, which reflects the communication frequency between two entities, in the trust evaluation. Trust value and confidence values were used to made the finally decision together. In [11], the authors proposed a novel Cloud-Based trust model to solve uncertain problem. These works involved great efforts to evaluate the trust values, however, when it comes to decision making

based on these trust values, they just simply compare with one or two thresholds, which can not dynamically change due to the altering of the environments.

Our trust model provides improvement in earlier works by proposing a probabilistic model which involves precise computation to update the decisions dynamically. And the evaluation of the trust is also based on each entity's own situation which can better suit the ubiquitous environments.

3 Naive Bayes Classifier Based Trust Model

In our trust model, trust decision for unfamiliar service requesters is based on the recommendations from other entities in ubiquitous environments. One of the example scenarios is ubiquitous supported smart office as showed in Fig.1.

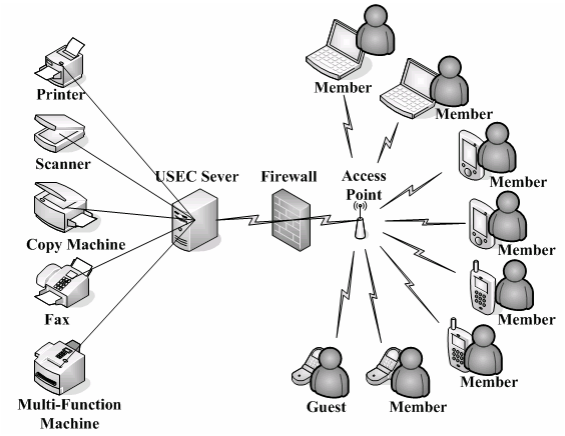


Fig. 1. Smart office supported by various ubiquitous units.

The working procedure for the trust model to make decision is as follows: (1) Service requester (Sr_i) sends a request to USEC server to apply certain service. USEC server serves as service provider agent. (2) If Sr_i is not an acquaintance to service provider (Sp_j) or it does not have enough priority to access the service, USEC server will ask other entities who are now in a certain range of this smart office to give recommendations for Sr_i . (3) If entities who are requested to give recommendations have past interaction history with Sr_i , they will act as recommender (R_k) and give back recommendations to USEC server, (4) USEC server makes trust decision according to Sp_j 's own judging standard based on the recommendations from the recommenders together with its own knowledge.

3.1 Factors Involved in Our Trust Model

There are totally five factors involved in our trust model.

Prior Probability. Prior probability reflects the acceptance level of certain service provider. It corresponds to the service provider's trusting beliefs for the whole ubiquitous environment. The lower the prior probability is, the more unbelieving the service provider is.

Definition 1: $P_{Sp_j}(y)$ and $P_{Sp_j}(n)$ are used to denote service provider Sp_j 's prior probability of acceptance and rejection respectively.

$$P_{Sp_j}(y) = \begin{cases} \frac{k}{m} & m \neq 0, \\ 0 & m = 0, \end{cases} \quad P_{Sp_j}(n) = 1 - P_{Sp_j}(y),$$

where $j, m, k \in N, k \leq m$ .Here m is the size of training sample; k is the size of acceptance sample. In case $P_{Sp_i}(y) \neq P_{Sp_j}(y)$, if $i = j$, it means we got one service provider in different situations. In this case, the same service provider has different acceptance levels for the environment due to the dynamic nature of service provider as well as the surroundings ubiquitous environment. Otherwise, if $i \neq j$, it means that they are different service providers. In case $P_{Sp_i}(y) > P_{Sp_j}(y)$ (i.e. Sp_i has a higher acceptance level when get same request), Sp_i is more likely to provide the service when requested. This situation is similar to our social society, Sp_i is easier to believe others comparing with Sp_j .

Trust Level. In our trust model, each entity is initially assigned a trust level according to its identity. If no information is available about the trustworthiness of an entity, it will be assigned as an unknown trust level. The trust level of an entity can be adjusted dynamically according to its behavior.

Definition 2: $Tl(S_k)$ is used to denote the trust level of entity S_k , where $k \in N$, $Tl(S_k) \in N$. Entity S_k may be a recommender or service requester.

If $Tl(S_k) > Tl(S_j)$ ($k, j \in N$), S_k is regarded as more reliable. However, in case $Tl(Sr_k)$ is unknown trust level, Sr_k may probably be provided services which are unavailable to the service requester who has a little bit higher trust level than him. This behavior also see parallels in our society, you may choose to trust an unfamiliar stranger that has never done harm to you instead of an acquaintance that had unpleasant interaction history with you.

Past Interaction History. Past interaction history is an entity's prior knowledge (this entity may be a recommender or service provider in our model) of acceptance to certain service requester.

Definition 3: $Pi(S_i, S_j)$ is used to denote the past interaction history between entities S_i and S_j. Entity S_i and S_j may be service requester, service provider or recommender.

$$Pi(S_i, S_j) = \begin{cases} \dfrac{n-(m-n)}{m} & m \neq 0, \\ 0 & m = 0, \end{cases} \text{ where } i, j, m, n \in N, i \neq j, n \leq m.$$

Here *m* and *n* denote the total communication times and successful communication times between S_i and S_j respectively. $Pi(S_i, S_j) \in [-1, 1]$.

We suppose that past interaction history has Gaussian distribution. If S_i never communicate with S_j before, then $Pi(S_i, S_j) = 0$. If S_i and S_j had unpleasant interaction history, in previous work, $Pi(S_i, S_j)$ was set a positive small value. However, it means that the past interaction history for unknown entity is always worse even than the very malicious entity, which is obviously not correct. Hence our model set $Pi(S_i, S_j) \in [-1, 0)$ for malicious entities, which is more convenient to differentiate unknown entities from malicious entities.

Time Based Evaluation. Intuitively, very old experiences of peers should have less effect in recommendation over new ones. Thus we take into account the time based evaluation.

Definition 4: $T(R_k, Sr_i)$ is used to denote the time based operator for recommender R_k to service requester Sr_i.

$$T(R_k, Sr_i) = \eta \frac{t_{R_k, Sr_i} - t_m}{\Delta\tau_0}, \text{ where } k, i \in N,$$

here t_{R_k, Sr_i} denotes the time when last communication between R_k and Sr_i happened. And η is time adapting operator. Suppose our measurement for time is based on a time window $[t_m, t_n]$, let $\Delta\tau_0 = t_m - t_n$.

Peer Recommendation. Peer recommendation is needed when service provider has no or not enough information to make decisions. Apparently if R_k had more interactions with Sr_i , the recommendation of R_k should be more importance for decision making, which introduces the notion of confidence.

Definition 5: $C(R_k, Sr_i)$ is used to denote the confidence for recommender R_k to service requester Sr_i .

$$C(R_k, Sr_i) = \frac{1}{std(M)\sqrt{2\pi}} \exp(-\frac{(m_k - mean(M))^2}{2std(M)^2}),\ i, k \in N ,$$

where M is an array of communication times. $M[k] = m_k$, $k = 1, 2, ..., n$. Here m_k is the communication times between R_k and S_i . We suppose that M has Gaussian distribution.

We are now ready to use the above definitions to express the notion of peer recommendation.

Definition 6: $\Pr(R_k, Sr_i)$ is used to denote the peer recommendation from recommender R_k to service requester Sr_i .

$$\Pr(R_k, Sr_i) = \frac{Tl(R_k)}{Tl_N} * C(R_k, Sr_i) * \frac{n_k}{m_k} * \frac{T(R_k, Sr_i)}{\Delta\tau_0}, \text{ where } k, i \in N ,$$

here m_k and n_k are the total communication times and successful communication times between R_k and Sr_i respectively. Tl_N is the total trust levels.

The final recommendation is the aggregate of all the peer recommendations.

Definition 7: $R(Sr_i)$ is used to denote the aggregate of recommendation for Sr_i from all the recommenders in the ubiquitous environment.

$$R(Sr_i) = \frac{\sum_{k=1}^{n} \Pr(R_k, Sr_i)}{n},$$

where $k, n, i \in N$, n is the number of the recommenders in the environment.

3.2 Trust Decision Making

Using the factors mentioned in section 3.1, our trust model uses Naive Bayes classifier twice to make the dynamic trust decision based on each service provider's acceptance level. Naive Bayes classifier is a technique for estimating probabilities of individual variable values, given a class, from training data and then to allow the use of these probabilities for classify new entities.

The decision is first made without recommendations, and it only depends on the service provider's own prior knowledge. Sometimes, the service provider may not be able to make the decision in the first decision, which means that the service requester

is unfamiliar with the service provider or it does not have enough priority to access this service. Then recommendations given by other recommenders will be used to make the final decision together with service provider's own prior knowledge.

First Decision: When Sr_i gives a request to Sp_j, $h(Sr_i, Sp_j)$ is used to denote Sp_j's trust decision. Accept=1; Reject=0.

$$h(Sr_i, Sp_j) = \begin{cases} 1 & V_{NB|y} \geq V_{NB|n} \\ 0 & V_{NB|y} < V_{NB|n} \end{cases}, \quad (1)$$

where $V_{NB|y}$ and $V_{NB|n}$ are the acceptance and rejection value respectively.

Using Naive Bayes classier:

$$V_{NB} = \arg\max_{v_m \in V} P_q(v_m) \prod_n P(a_n|v_m) = \arg\max_{v_m \in \{yes,no\}} P_q(v_m) \prod_n P(a_n|v_m). \quad (2)$$

Definition 8: If attribute A has Gaussian distribution, we use $f_y(A)$ and $f_n(A)$ to denote the probability of A when given acceptance and rejection respectively.

$$f_y(A) = \frac{1}{std_y(A)\sqrt{2\pi}} \exp(-\frac{(A-mean_y(A))^2}{2std_y(A)^2}),$$

$$f_n(A) = \frac{1}{std_n(A)\sqrt{2\pi}} \exp(-\frac{(A-mean_n(A))^2}{2std_n(A)^2}),$$

where $mean_y(A)$ and $mean_n(A)$ denote the mean of A when given acceptance and rejection respectively. And $std_y(A)$ and $std_n(A)$ denote the standard deviation of A when given acceptance and rejection respectively.

$$V_{NB|y} = P_{Sp_j}(y) P(Tl(Sr_i)|y) f_y(Pi(Sr_i, Sp_j)), \quad (3)$$

$$V_{NB|n} = P_{Sp_j}(n) P(Tl(Sr_i)|n) f_n(Pi(Sr_i, Sp_j)), \quad (4)$$

where $P(Tl(Sr_i)|y)$ and $P(Tl(Sr_i)|n)$ are the probability of $Tl(Sr_i)$ when given acceptance and rejection respectively.

Final Decision: If $h(Sr_i, Sp_j)$ =0 in the first step of decision, Sp_j will use (1) to make trust decision again based on its own prior knowledge together with recommendations gotten from recommenders, that is, to add the factor of recommendation in(2).

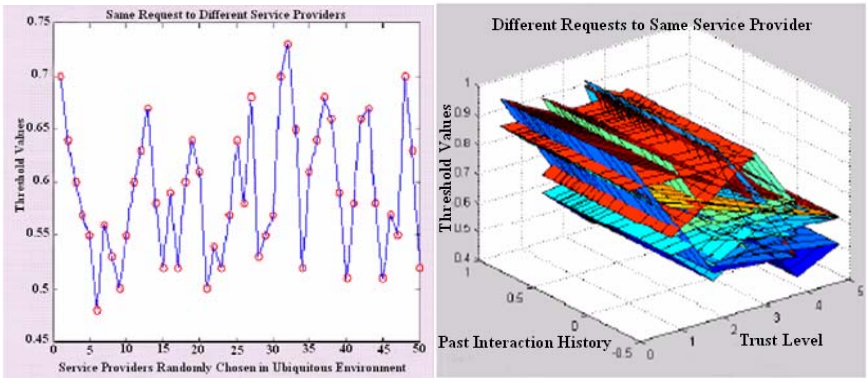
$$V_{NB|y} = P_{Sp_j}(y) f_y(R_{Sr_i}) P(Tl(Sr_i)|y) f_y(Pi(Sr_i, Sp_j)), \quad (5)$$

$$V_{NB|n} = P_{Sp_j}(n) f_n(R_{Sr_i}) P(Tl(Sr_i)|n) f_n(Pi(Sr_i, Sp_j)) . \quad (6)$$

As shown above, when making trust decision (both with and without recommendations), our trust model compares the value of $V_{NB|y}$ and $V_{NB|n}$. Since the calculation of $V_{NB|y}$ and $V_{NB|n}$ involves different factors as well as the prior probability, which reflects the current acceptance rate of Sp_j and varies from time-to-time, $V_{NB|y}$ and $V_{NB|n}$ will keep on changing according to different situations.

4 Simulation Result

Using the method mentioned in section 3, we got the simulation results as showed in Fig.2. For the brevity, we only give the simulation results of decision making for Sp_j with recommendations from recommenders. The result of decision making without recommendations is similar to this case.



(a) (b)

Fig. 2. Decision making with recommendations.

Fig.2(a) shows the result of thresholds when Sr_i gives request to different service providers who have same past interaction history with it, i.e. for different service provider Sp_m and Sp_n, $m, n \in N$, $Pi(Sr_i, Sp_m) = Pi(Sr_i, Sp_n)$. The thresholds here is the intersection of formulas (5) and (6), if the trust value is above threshold, our trust model will accept the request, otherwise, the request will be rejected. It is clear from the result of Fig.2(a) that when different service providers get the same request, even the past interaction histories between service provider and service requester are the same, the threshold is not a fixed value and it changes for different service providers. This is because the acceptance levels of different service providers are not the same.

Fig.2(b) gives the result of thresholds when different service requesters $Sr_1 \ldots Sr_k$, $k \in N$ give requests to same service provider Sp_j. Since all the requesters are given to the same service provider, Sp_j's acceptance level (i.e. prior probability) is same to all the service requesters. At the same time, our simulation set whole the recommendations given to different service requests to be the same, i.e., $R(Sp_m) = R(Sp_n)$ $1 \le m \ne n \le k$, $m, n \in N$ .However, Fig.2.(b) shows that the threshold keeps on changing. This is because of the variation in $Tl(Sr_m)$ and $Pi(Sr_m, Sp_j)$.

Our simulation results suggest that when requested by same service requester, different service providers or the same provider in different situations make different trust decisions. It is impossible to find a fixed threshold to make trust decision since the decision changed according to the entity's own prior knowledge. The results also give a look for the entity's dynamic trust decision with the variation of different factors. When one entity makes trust decision according to different service requesters, there is no fixed so-called threshold value for the service provider to make decision. However, in previous trust models, pre-defined fixed thresholds were always used to make decisions, it is obviously not suitable for the dynamic characteristic of ubiquitous environment. By considering every service provider's prior probability and its own knowledge, our trust model is able to dynamically evaluate the threshold values as shown in the simulation results. At the same time, since Naive Bayes classifier is a statistical method, it is also suitable to make decision when limited information is available, which is usually the case in ubiquitous environment.

5 Conclusion and Future Work

Our trust decision making avoids using simple thresholds, which were commonly used in previous works. This makes our Naive Bayes classifier based trust model more suitable to be used in ubiquitous computing environments since it can dynamically make decision due to different situation as shown in the simulation results. Meanwhile, compared with previous works, our trust evaluation is based on each entity's own prior knowledge in stead of using common evaluation and pre-defined weight values, which effectively reduce the subjectivity by human opinions compare with the other trust models. Our model also uses a reasonable way of evaluating recommendations by considering the surrounding environments of one certain entity.

We will add risk analysis in the coming work, since trust and risk always coupled tightly with each other. Other works like how to choose reliable recommenders to avoid unfair recommendations in ubiquitous trust model will also be involved in the coming work. We also propose to implement our trust model to be used in CAMUS, a middleware platform for a ubiquitous computing, in the future work.

Acknowledgment. This work is financially supported by the Ministry of Education and Human Resources Development (MOE), the Ministry of Commerce, Industry and

Energy (MOCIE) and the Ministry of Labor (MOLAB) through the fostering project of the Lab of Excellency.

Reference

1. Marsh, S. P.: Formalising Trust as a Computational Concept. Ph.D. Thesis, University of Stirling (1994)
2. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In Proc. of the 1996 IEEE Symposium on Security and Privacy, (1996) 164-173
3. Josang, A.: The right type of trust of distributed systems. In New security paradigms workshop, USA (1996) 119-131
4. English, C. and Nixon, P.: Dynamic Trust Models for Ubiquitous Computing Environments. In Proc. of the Fourth Annual Conference on Ubiquitous Computing, (2002)
5. Lamsal, P.: Requirements for modeling trust in ubiquitous computing and ad hoc networks. Ad Hoc Mobile Wireless Networks – Research Seminar on Telecommunications Software, (2002)
6. Ranganathan, K.: Trustworthy Pervasive Computing: The Hard Security Problems. In Proc. of IEEE Conference on Pervasive Computing and Communications, (2004)
7. Aime, M.D. and Lioy, A.: Incremental trust: building trust from past experience. In Proc. of IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, Italy (2005) 603-608
8. Shand, B., Dimmock, N., Bacon, J.: Trust for Ubiquitous, Transparent Collaboration. In Proc. of ACM: Special issue: Pervasive computing and communications, (2004) 711- 721
9. Liu, Z.Y., Jo, A.W., Thompson, R.A.:A Dynamic Trust Model for Mobile Ad Hoc NetWorks. In Proc. of 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, (FTDCS'04) (2004) 80-85
10. Theodorakopoulos, G. and Baras, J.S.: Trust Evaluation in Ad-Hoc Networks. In Proc. of the 2004 ACM workshop on Wireless security, USA (2004) 1-10
11. He, R., Niu, J.W., Yuan, M.: A Novel Cloud-Based Trust Model for Pervasive Computing. In Proc. of the Fourth International Conference on Computer and Information Technology, (2004) 693-670
12. Guha, R., Kumar, R., Raghavan, P.: Propagation of trust and distrust. In Proc. of International Conference on World Wide Wed, USA (2004) 403-412
13. Michiardi, P. and Molva, R.: A collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks. In Proc. of IFIP Communication and Multimedia Security Conference, Portoroz (2002) 107-121
14. Ganeriwal, S. and Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. In Proc. of ACM Workshop on Security of ad-hoc and sensor networks, USA (2004) 66-77
15. Castelfranchi, C., Falcone, R., Pezzulo, G.: Trust in Information Sources as a source for Trust: A Fuzzy Approach. In Proc. of the second international joint conference on Autonomous agents and multiagent systems, (2003) 89-96