INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. 2012; **25**:1178–1188
Published online 22 March 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2330

An integrated scheme based on service classification in pervasive mobile services

Yang Liu*,†, Zhikui Chen, Feng Xia, Xiaoning Lv and Fanyu Bu

Software School, Dalian University of Technology, Rd 8, Economy and Technology Development Area, Dalian, China

SUMMARY

Internet of Things and broadband communication are promoting the pervasive mobile services with their advanced features. However, security problems baffled the development. This paper proposes a trust model to protect the user's security. The billing or trust operator works as an agent to provide a trust authentication for all the service providers. The services are classified by sensitive value calculation. With the combined location-aware and identity-aware information and authentication history, the user's trustiness for corresponding service can be obtained. For decision, three trust regions are divided and referred to three ranks as follows: high, medium and low. The trust region tells the customer which authentication methods should be used for access. Penalty coefficient is also involved for forbidding force-crack. Copyright © 2012 John Wiley & Sons, Ltd.

Received 14 July 2011; Revised 28 January 2012; Accepted 28 January 2012

KEY WORDS: mobile service; trust; context-aware diary; service classification

1. INTRODUCTION

With the rapid promotion, the Internet of Things (IoT) and broadband communication system will offer us great convenience and huge opportunities of pervasive [1, 2] mobile service creation. But because of its wider application providing for billions of users, many security threats are also accompanied. Facing at identity theft, malicious or illegal service request, the loss or disclosure of personal data, privacy and related intellectual property, user identity authentication is an attractive issue that must be thoroughly addressed. However, some existing revolutions are so complex that bring bad influence on service quality and the consumers' convenience. Trust scheme seems to be a balanced way in this aspect.

In the human society, the social interactions are built around trust. The interaction histories or the evaluations from others are used to build the reputations of each other. The properties of trust are summarized as follows: subjectivity, non-transitivity, temporalness, contextualness and dynamicity, as well as non-monotonicity [3]. Numerous different kinds of trust satisfy different properties. In terms of computer science, there are many definitions and models for trust. As pointed in [4], on the basis of the trust values of transactions recently, a trust evaluation approach is proposed for e-commerce applications. The trust values are random samples. In this method, recent trust values are more important in the trust evaluation. The approach in [5] of the fuzzy logic is applied to trust evaluation, which divides sellers or service providers into multiple classes of reputation

*Correspondence to: Yang Liu, Software School, Dalian University of Technology, Rd 8, Economy and Technology Development Area, Dalian, China.

†E-mail: liuyang@dlut.edu.cn

ranks. A model for supporting trust in virtual communities is proposed in [6]. It is based on direct experiences and reputation. For agent system, trust management is also actively proposed, such as [7, 8]. Vaidya *et al.* [9] proposed a one-way hash functions and XOR operations to achieve lower computational and communication overheads to provide mutual authentication and user anonymity for user authentication protocols. Unfortunately, these methods do not concern that if the high-trust user's devices are stolen, the thief can cheerfully enjoy the high trustiness accumulated by the owner. In [10], smart card is used to solve this problem but is not convenient in facing at multiple applications. In [11], a location-aware scheme was proposed. The security of authentication can be improved by evaluating the amount of trust that can be reposed on the user standing in the area from where he tries to access a resource. But location-based sensing cannot be a stable measurement because the users are willing to enjoy their mobility. In Daidalos I and II, a virtual identity's (VID's) concept [12, 13] is designed to protect a user's privacy and secure communication data, which contemplate the multitude of identities and roles we take on each time we turn on our computer, mobile phone or personal digital assistant. The user has a contract with the trusted operator, who becomes a proxy for billing, which is a business in itself. Obviously, the proxy separates the user's real identity from the entity service provider without revealing much private information [14], which means that the middleman can centralized set different rules for different services, for example according to the sensitivities. Moreover, VID provides a correspondence between VID and applications that sometimes are constrained with certain locations or times. Therefore, time, location, identity and service could be restricted factors for user's access, which may be useful for the protection we discussed previously.

This paper proposes an integrated trust scheme based on the VID taking location-aware, identity-aware and services classification into concern. The location-aware and identity-aware systems are parts of context-aware engine [15]. The records of such information form dairies, and we call them 'context diary'. Then we bring trust rank in three levels: high, medium and low. For each rank, the authentication way is varied [16]. In high-rank case, no extra key is needed (already sign on the VID). For medium rank, users have to offer their PIN for login. Low rank means users need to provide the biometric information, such as face image, fingerprint and iris scan, which may be not convenient for its complexity, time consuming and hardware constraint. Then the authentication history will also affect the access. In addition, to fight against the force-crack by attackers, we induce a penalty coefficient; the trying times are extremely limited. To avoid that communication services burden users with increasingly complex authentication effort and to limit the number of operators a user may need, a trusted provider is utilized, usually also the identity provider and a billing provider, who ideally enables universal and ubiquitous access to everything via some kinds of 'single sign-on' [17], shown in Figure 1.

The remainder of this paper is organized as follows. A context-aware diary including location and identity is introduced in Section 2. Service classification method is proposed in Section 3. Section 4 gives an authentication mechanism with trust evaluation. In Section 5, the simulation is carried out to test the validity. Section 6 concludes at the end.

2. CONTEXT-AWARE DIARY

Context-aware information can upgrade the security in some cases. As mentioned earlier, traditional trust schemes are excessively relying on the trust values of users, which are accumulated via good history. However, for example, if a high-trust user's mobile phone is lost, the one who picks up the equipment will inherit the high priory completely because the trust scheme is not intelligent enough to know the master-change. Then the initial user's privacy and services will full expose to the picker. Therefore, extra factors should involve into the trust evaluation, which can constrain the scene mentioned previously. In another word, because the user's life mode is hard to copy, the tracks and habit of user could be exploited for warning some bizarre situation. The tracks are obtained for location-sensing technology, and the habits come from the usage of virtual identities in VID architecture.

DOI: 10.1002/dac

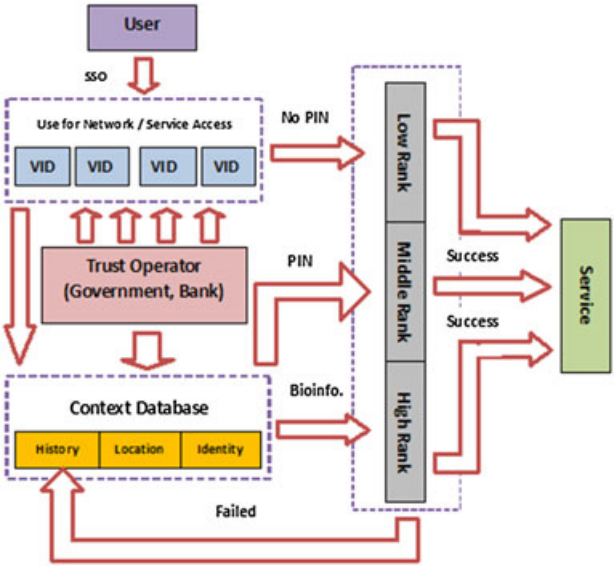


Figure 1. Authentication structure.

2.1. *Location-aware diary*

Location awareness is an essential characteristic of IoT networks. A location-aware architecture normally consists of location estimation and/or sensing, seamless positioning and interoperability, statistical learning and tracking, security and privacy, mobility management and location-based applications. The recent diffusion of handhold devices and smart phones equipped with localization capabilities is opening new scenarios in the development of context-aware services. We present the ideas of location-aware diary [18]: an application may be running on some localization methods, for example GPS, smart antenna and sensor networks, which record the list of relevant places visited by the user. The diary runs autonomously without requiring user's interaction and is able to classify semantically the places being visited in an unsupervised way. Semantic information can be added by exploiting the structure of people daily routine; see Table I as an example. We can realize a set of Bayesian networks to diagnose the kind of place given the temporal pattern of user visits. Further information can be extracted by geo-coding the place and mining the Web in search for relevant information [19].

2.2. *Identity-aware diary*

Virtual identities can be registered in the operator or trust provider according user's career, family, hobby and so on. For example, Tom is a teacher in a high school. He also buys stocks for investment. In his free time, he can browse website, download digital music, use MSN and so on. So he registered three VIDs in this operator.

Table I. Location-aware diary data.

Date	Duration	Name	Type	P_A (probability)
5/2/2011	00:00–09:00	xxx Flat.3	Home	0.98
5/2/2011	09:15–13:00	xxx School	Work place	0.94
5/2/2011	13:05–13:30	xxx Buffet	Restaurant	0.56
5/2/2011	13:50–17:00	xxx School	Work place	0.91
5/2/2011	17:10–17:30	xxx Toll	Shopping mall	0.68
5/2/2011	17:50–24:00	xxx Flat.3	Home	0.76

DOI: 10.1002/dac

1. Tom_Teacher = on/free
2. Tom_Investor = off/busy
3. Tom_Free time= off/busy

If Tom_Teacher is authenticated. Accounting and charging is in accordance to the specific VID. Also in the operator, similar as location aware, an identity-aware diary is generated and updated everyday (Table II). With the diary, the system can make statistic for the VID executing situation.

3. SERVICE CLASSIFICATION

Our system bases service classification on static information about the applications, such as the type of application, the cost of service and the host on which the application was executed. As a consequence, this split of multiple types of services is supported in the trust operator. The classification is basically related with the sensitivity or importance of the service provider. Here, we exploit the fuzzy mathematics to quantify the sensitivity [20].

3.1. Generate comparison matrix

Firstly, we make pairwise comparison of the importance of n targets $X_1, X_2, \ldots, X_n$ presenting the services. According to the combination principle, there are $1/2 \times n \times (n-1)$ times comparisons. The X_i and X_j are evaluated by the relative importance using relative importance value table (see Table III), which can be labelled as $a_{ij} = f(X_i, X_j)$. Hence, we have

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} = (a_{ij})_{n\times n}$$

where presenting the importance of X_i compared with X_j.

3.2. Confirm the weight coefficients

For comparison matrix $\boldsymbol{A} = (a_{ij})_{n\times n}$, the approximate eigenvalue and units eigenvector can be calculated by rooting; these targets of weighted vector $\bar{W}$:

Table II. Identity-aware diary data.

Data	Duration	Virtual identity	P_B (probability)
5/2/2011	00:00–9:15	Free time	1.00
5/2/2011	09:15–13:00	Teacher	0.94
5/2/2011	13:00–13:50	Free time	0.81
5/2/2011	13:50–17:00	Teacher	0.92
5/2/2011	17:00–19:00	Free time	0.77
5/2/2011	19:00–20:00	Investor	0.34
5/2/2011	20:00–24:00	Free time	0.95

Table III. Relative importance value table.

Comparison between service i and j	$f(X_i, X_j)$
i equal important to j	1
i slightly more important than j	3
i obviously more important than j	5
i great more important than j	7
i extremely more important than j	9
i and j in the intervals of two judgements	2,4,6,8

DOI: 10.1002/dac

(1) Calculate $a_i = \sqrt[n]{\prod_{j-1}^{n} a_{ij}}$, $i, j = 1, \ldots, n$, in row of $\boldsymbol{A}$.
(2) Normalize a_i as $W_i = a_i / \sum_{i-1}^{n} a_i$, $i, j = 1, \ldots, n$, $\bar{\boldsymbol{W}} = (W_1, W_2, \ldots, W_n)^T$ is approximate eigenvector of matrix **A**.
(3) Calculate $\lambda_{\max} = \frac{1}{n} \sum_{i-1}^{n} \frac{\boldsymbol{A_i} \times \bar{\boldsymbol{W}}}{W_i}$ as approximate largest eigenvalue of matrix **A**.

3.3. Self-consistency validation

Because $a_{ij} = f(X_i, X_j)$ is a kind of subjective evaluation, we have to make sure that our estimation of a_{ij} does not contradict one another. For example, value K is more important than L, and L is more important than M; then our evaluation function supports the conclusion that K is more important than M. If value K is equally important to M, we may well doubt whether the evaluation function is reasonable. Self-consistency validation is a way to solve this problem. Here, we calculate $CI = (\lambda_{\max} - n)/n - 1$, where n is the order of matrix **A**. Then consistency ratio $CR = CI/RI$, where RI presents average random consistency index; see Table IV. If $CR < 0.1$, we can accept the evaluation matrix **A** as well as the weight vector $\bar{W}$. However, if $CR \geqslant 0.1$, there may exist conflict in the evaluation function. So we have to adjust matrix **A** and do all the previous steps again.

3.4. Matrix calculation

The comparison matrix can be attached with some reasonable values. And as described in Section 3.2, we have Table V. Then $\lambda_{\max} = 9.2185899$, $CI = 0.0273237$ and $CR = 0.0187149 < 0.1$ to pass the check.

We can have the initial service classification estimation in Table VI. If a new service is emerging, of course, the table needs to be updated. The only task we should do is to make comparison between new service and original services and give a subjective value. For example, the new service is about online payment, and initial estimate is between level D and E. Then the matrix is expanded with subjective comparison value. Finally, the arrangement of levels and services is also renewed.

4. TRUST EVALUATION MODEL

4.1. Trust region

Three trust regions are divided representing three ranks. Each rank has its own entering way. In high-rank case, no extra key is needed (already sign on the VID). For medium rank, users have to offer their PIN for login. Low rank means users need to provide the biometric information, such as

Table IV. Average random consistency index [21].

Order	1	2	3	4	5	6	7	8
RI	0	0	0.52	0.89	1.12	1.26	1.36	1.41
Order	9	10	11	12	13	14	15	
RI	1.46	1.49	1.52	1.54	1.56	1.58	1.59	

Table V. Matrix calculation.

a_{ij}	A	B	C	D	E	F	G	H	I	a_i	W_i	$A_i \bar{W}$
A	1	2	3	4	5	6	7	8	9	4.14716627	0.30941616	2.91617
B	1/2	1	2	3	4	5	6	7	8	3.00799234	0.22442346	2.07087
C	1/3	1/2	1	2	3	4	5	6	7	2.11309937	0.15765635	1.44093
D	1/4	1/3	1/2	1	2	3	4	5	6	1.4592328	0.10887198	0.9904
E	1/5	1/4	1/3	1/2	1	2	3	4	5	1	0.07460905	0.6759
F	1/6	1/5	1/4	1/3	1/2	1	2	3	4	0.68529161	0.05112896	0.46075
G	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	0.47323851	0.03530788	0.31705
H	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	2	0.33244766	0.02480361	0.2245
I	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1	0.18473035	0.01378256	0.1375

DOI: 10.1002/dac

Table VI. Estimation table.

Level	Sensitive value	Service
A	$S_1 = 0.30941616$	Governmental military
B	$S_2 = 0.22442346$	Commercial
C	$S_3 = 0.15765635$	Academic
D	$S_4 = 0.10887198$	Banking Stork
E	$S_5 = 0.07460905$	e-Shopping
F	$S_6 = 0.05112896$	VoIP
G	$S_7 = 0.03530788$	Education
H	$S_8 = 0.02480361$	Entertainment
I	$S_9 = 0.01378256$	Public

face image, fingerprint and iris scan. To distinguish the rank of a specified field, an upper limitation Ω and a lower limitation ω are approximately defined for each certain field according to variable requirement, where $0 \leqslant \omega \leqslant 0.5 < \Omega \leqslant 1$. Therefore, three sets, $[0, \omega)$, $[\omega, \Omega)$ and $[\Omega, 1]$, are defined to calculate the thresholds of that field. The thresholds selection is related with the service classification. Initially, the two thresholds can be set by the customer via choosing the sensitive values of services. The operator provides the recommended value. For example, the customer considers the upper threshold and lower threshold 0.7 and 0.3, respectively. Therefore, the three regions are $[0, 0.3)$, $[0.3, 0.7)$ and $[0.7, 1]$. The trust region can be verified by the authentication history value. The details will be explained later.

4.2. Authentication history

The customer's authentication history is also an important factor for reference. On the basis of past experience in authenticating consumer, the trust provider will make statistic for the situation of authentication. A nice history will make the customer's senior trust region much easier to access. In contrary, bad history will bring stricter ways for validation. Because of the three ranks exploiting different validation methods, the statistic models are distinguished. The statistic results are labelled by T_1, T_2 and T_3 for high, medium and low ranks, respectively. Because high rank needs no extra key, this authentication can certainly succeed. Therefore, T_1 is the ratio of high-rank login to the totality. It says that if T_1 is high, the customer who has an extremely regular life usually succeed in access with no PIN. Naturally, the user certainly is treated as trustiness. If T_1 is not high, the user may not be easy to be recognized, perhaps not in regular. T_2 is the successful PIN login ratio. If T_2 is high, it is deduced that the user's life may be less regular and highly PIN controlled. But when T_2 is low, to some extent, the user often makes mistakes in PIN or lost PIN control and may be less trusted. Because the biometric information is the private feature that can be highly trusted, if the failure happens, the user cannot be trusted. Although biometric check is complex, no one can guarantee that the computers can recognize the features with only one chance or two and also the features have small possibility to loose. Thus, T_3 can be ignored here. In particular case, for T_2, if the history data of the customer with a good record in the past becomes bad currently, it can estimate that the identity is not safe this period, for example is stolen.

With authentication history involving, the trust thresholds have some adjustment. We have

$$\begin{aligned} \acute{\omega} &= \omega + a \\ \acute{\Omega} &= \Omega + b \end{aligned} \tag{1}$$

where a and b are functions of T_2 and T_1 and also related with two region $\Omega - \omega$ and $1 - \Omega$, respectively, which means that a and b cannot exceed the bounds (see Figure 2). We simply choose function of incremental curves here. In addition, because high rank is enough sensitive and constrained, it cannot be changed obviously as medium rank can so that the curve should be much

DOI: 10.1002/dac

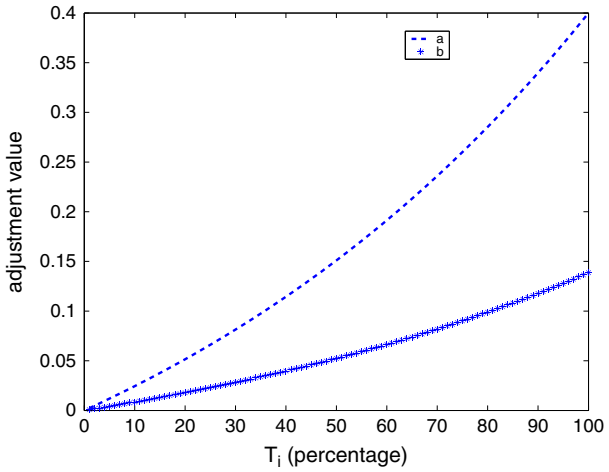


Figure 2. The forms of a and b.

more steady. Therefore, a and b are selected with experience and test in Equation (2), as illustrated as Figure 2.

$$\begin{aligned} a &= \frac{e^{1-T_2}-1}{e-1} \times (\Omega - \omega) \\ b &= \frac{e^{1-T_1}-1}{e+1} \times (1-\Omega) \end{aligned} \tag{2}$$

4.3. Trust evaluation

To evaluate the trustiness, $P_A \times P_B$ can tell system the matching degree between user's position and VID-based identity on his diary: the degree is positive with trustiness. S_i is also a crucial factor information: higher S_i needs more rigorous trust estimate. Additionally, S_i could independently impact as no contextual information initially. Hence, we map S_i to [0,1] region with logarithm function as curve fitting.

$$S_i^{\text{norm}} = \frac{lg\, S_i - lg\, \min(\boldsymbol{S})}{lg\, \max(\boldsymbol{S}) - lg\, \min(\boldsymbol{S})} \tag{3}$$

To counteract the improper setting of thresholds by the customers, a calibration factor $(1+\Omega+\omega)/2$ is involved. For instance, the upper and upper thresholds are 0.8 and 0.5, respectively, which seems that the set is a little high. The factor equal to 1.15 makes the trust value increase along and gently offsets the influence. Then the evaluation function is set to

$$Y = P_A \times P_B \times (1 - S_i^{\text{norm}}) \times \left(\frac{1+\Omega+\omega}{2}\right) \tag{4}$$

The system can judge which region can be matched via Y according to the thresholds and which authentication key should be provided by the customers. For example, without any loss of universality, we set $P_A = 0.9$ and $P_B = 0.9$ provided by the diary server. The application server provider is an online market, and the goods are not expensive, so the sensitivity weight is 0.075 for instance. The trust region according to user's choice and authentication history ($T_1 = 0.4$ usually not high and $T_2 = 0.9$ for simplicity, using Equations (1) and (2)) is [0,0.3245], [0.3245,0.7663] and [0.7663,1]. Thus, $Y = 0.4597$ is obtained by the parameters mentioned previously. Obviously, it is in the medium rank, and PIN is necessary for authentication. When a user wants to enter into military services, according to Equation (3), the trust value is zero in any case, so the bio-information is required definitely.

DOI: 10.1002/dac

4.4. Penalty coefficient

We do not hope that the theft try the PIN with no constraint. So the penalty coefficient is defined as follows:

$$Y' = YP^n \tag{5}$$

where n is the times of failure. If Y belongs to medium region, for example, the user can authenticate with PIN. But after several failures, P^n becomes small enough, the Y' may fall into low region and PIN is useless now. The penalty coefficient can be set by calculation. In the first transaction, for medium rank, as n times wrong in entering, the trust region falls into the low rank, which means that the upper threshold decreases to lower threshold. Hence,

$$\omega = \Omega P^n \tag{6}$$

While the customer choose the threshold and trying times, the penalty coefficient can be established. For instance, we have $P = 0.844$ according to Equation (6). Then for the first failure in the previous example, we have $Y' = 0.3880$ from Equation (5), which still locates in medium rank. For the second failure, $Y' = 0.3275$, also in medium rank. But for the third failure, $Y' = 0.2764$ and trust value falls to low rank.

5. SIMULATION

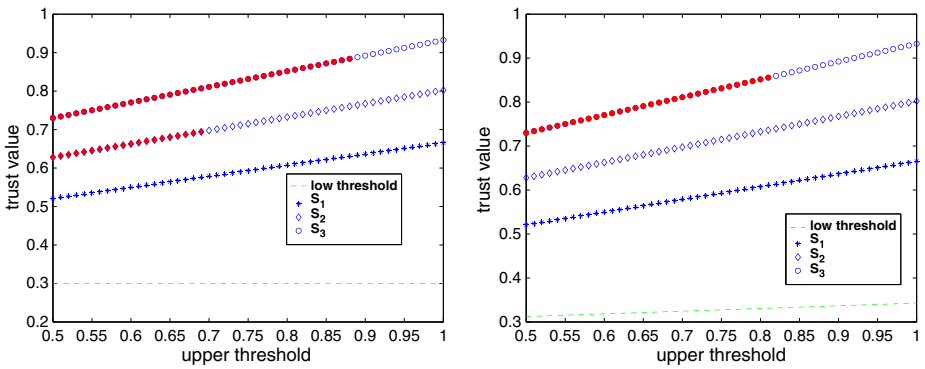
According to the function of evaluation, P_A and P_B are constant when diary data are given. We set $P_A = P_B = 1$ as an ideal case even without effecting simulation much.

5.1. Threshold test

Firstly, we test upper threshold's effect to the trust value.

5.1.1. Without the authentication history involved. The lower threshold ω is fixed at 0.3. We select $S_1 = 0.1577$, $S_2 = 0.0353$ and $S_3 = 0.0248$ as samples. All the three curves climb slightly when the upper thresholds increase, as seen from Figure 3(a). And for each upper threshold, the trust value follows $Y_3 > Y_2 > Y_1$. The red circle dots for S_3 and red diamond dots for S_2 present the trust values bigger than the upper thresholds, which means that at this time the customer is in the high rank. It implies that higher sensitivity of service needs stricter authentication in the high rank.

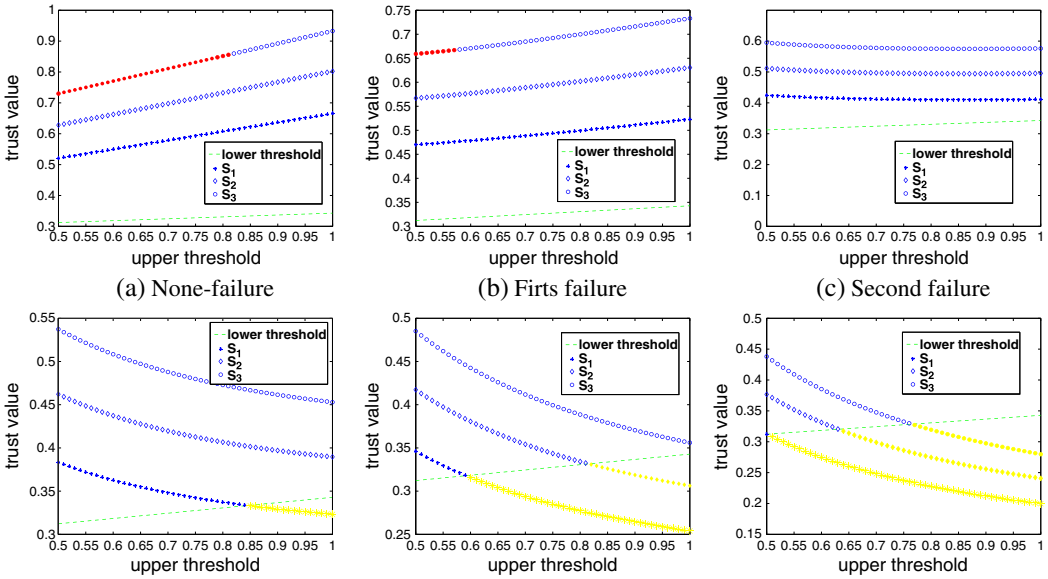
5.1.2. With consideration of authentication history. The other parameters unchanged as mentioned previously. $T_1 = 0.4$ and $T_2 = 0.9$ are assumed here. The rank situation is shown in Figure 3(b). Obviously, with the authentication history, comparing with Section 5.1.1, the high-trust region for S_3



(a) Without authentication history (b) With authentication history

Figure 3. Upper threshold's effect.

DOI: 10.1002/dac



(a) None-failure (b) Firts failure (c) Second failure

(d) Third failure (e) Fourth failure (f) Fifth failure

Figure 4. Situation of penalty coefficient involved.

is reduced and that for S_2 is even deleted. Additionally, the lower threshold is increasing with upper threshold, which makes the medium region also smaller. It demonstrates that the authentication history makes the scheme much stricter.

As Equation (4) shows, lower threshold also affects the trust value and appears similar with upper threshold.

5.2. *Penalty coefficient*

In this experiment, we discuss the penalty coefficient on the basis of Section 5.1.2. As the example in Section 4.4, we set that the times of trials PIN is up to 5. The penalty coefficient P is also related with Ω varying while the trust value and rank are changing, as shown in Figure 4. In Figure 4(a) and 4(b), only for S_3, the high rank exists. But after the first failure, the high rank is totally deleted. And from the third and fourth trials, the low rank for S_1 and S_2 emerged and extends with trials, respectively. Here, we can analyse the situation of S_1 as an example. From the none-failure to second failure cases, the customer can only use PIN to access S_1 service with any upper threshold selection ($\Omega > 0.5$). But from third to fifth failures, the upper threshold is decreased as 0.65, 0.6, 0.59 and 0.51 approximately, which implies that if the custom have five opportunities to stay in medium rank, the customer can only beg the host setting the upper threshold just a little above the smallest value 0.5. The force-crack is forbidden evidently.

6. CONCLUSION

This paper proposes a trust model to protect the user's security. Contextual information such as location and identity can give an inertial reference for the decision. The core is to build a service classification estimation table. A fuzzy mathematical method is exploited transferring subjective judgements quantized into weights. From the trust evaluation, all the factors are involved to evaluate the user's trustiness. In the experiment, threshold selection, which usually selected by users, is proved important. Also, the authentication history affects the thresholds of trust region, which makes the trust scheme stricter. The penalty coefficient is shown to be effective for forbidding force-crack. However, in this scheme, subjective selection from customer may effect the system significantly. For example, in the service classification, the relative important values are probably inconsistent if

DOI: 10.1002/dac

customer forgets his or her former setting. Therefore, a check and recommender system should be involved. Also, the algorithms of sensitivity computing should be 'fuzzy' enough to ignore some constraint wrong settings.

REFERENCES

1. Weiser M. The computer for the 21th century. *Scientific American* 1991; **3**:3–11.
2. Estrin D, Culler D, Pister K. Connecting the physical world with pervasive networks. *IEEE Pervasive Computing* 2002; **1**:59–69.
3. Boukerch A, Xu L, EL-Khatib K. Trust-based security for wireless ad hoc and sensor networks. *Computer Communications* 2007; **30**:2413–2427.
4. Zacharia G, Maes P. Trust management through reputation mechanisms. *Applied Artificial Intelligence Journal* 2000; **9**:881–908.
5. Song S, Hwang K, Zhou R, Kwok Y-K. Trusted P2P transactions with fuzzy reputation aggregation. *IEEE Internet Computing* 2005; **9**(6):24–34.
6. Abdul-Rahman A, Hailes S. Supporting trust in virtual communities. *HICSS '00 Proceedings of the 33rd Hawaii International Conference on System Sciences*, Maui, Hawaii; **6**: 2000; 6007.
7. Yu B, Singh MP. A social mechanism of reputation management in electronic communities. *Proceeding CIA '00 Proceedings of the 4th International Workshop on Cooperative Information Agents IV, The Future of Information Agents in Cyberspace*, Boston, USA, 2000; 154–165.
8. Zacharia G, Maes P. Trust management through reputation mechanisms. *Applied Artificial Intelligence* 2000; **14**(9):881–908.
9. Vaidya B, Rodrigues JJPC, Park JH. User authentication schemes with pseudonymity for ubiquitous sensor network in NGN. *International Journal of Communication Systems* 2010; **23**(9–10):1201–1222.
10. Tsai J-L, Wu T-C, Tsai K-Y. New dynamic ID authentication scheme using smart cards. *Int. J. Communication Systems* 2010; **23**(12):1449–1462.
11. Lenzini G, Bargh SM, Hulsebosch B. Trust-enhanced security in location-based adaptive authentication. *Electronic Notes in Theoretical Computer Science (ENTCS)* 2008; **197**(2):105–119.
12. Aguiar RL, Sarma A, Bijwaard D, Marchetti L, Pacyna P. Pervasiveness in a competitive multi-operator environment: the Daidalos project. *Communications Magazine* 2007; **45**(10):22–26.
13. Sarma A, Matos A, Girão J, Aguiar R, *et al*. Virtual identity framework for telecom infrastructures. *Wireless Personal Communications* 2008; **45**(4):521–543.
14. Zhong S, Chen T. An efficient identity-based protocol for private matching. *Int. J. Communication Systems* 2011; **24**(4):543–552.
15. Bellotti V, Edwards K. Intelligibility and accountability: human considerations in context-aware systems. *Human-Computer Interaction* 2001; **16**(2):193–212.
16. Fan C-I, Lin Y-H. Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. *IEEE Transactions on Information Forensics and Security* 2009; **4**(4):933–945.
17. O'Droma M, Ganchev I. The creation of a ubiquitous consumer wireless world through strategic ITU-T standardization. *IEEE Communications Magazine* 2010; **48**(10):158–165.
18. Castelli G, Mamei M, Rosi A. The Whereabouts Diary. In *International Symposium on Location- and Context-Awareness, LNCS*, Vol. 4718. Springer Berlin / Heidelberg: Germany, 2007; 175–192.
19. Bicocchi N, Castelli G. Supporting location-aware services for mobile users with the whereabouts diary. *MOBILWARE '08 Proceedings of the 1st international conference on MOBILE Wireless MiddleWARE, Operating Systems, and Applications,* Vol. 278, Brussels, Belgium, 2008.
20. Liu Y, Chen Z, Xia F, Lv X, Bu F, *et al*. A trust model based on service classification in mobile services. *Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom)*, Hangzhou, China, 2010.
21. Saaty TL, Vargas LG. *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process*. Kluwer Academic Publishers: Boston, 2001.

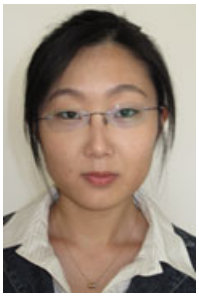
AUTHORS' BIOGRAPHIES

Yang Liu is a PhD candidate of Computer Science at Dalian University of Technology, China. His research interests are information security, cognitive network and Internet of Things. He received his MSc degree from the School of Electronics and Engineering at the University of Edinburgh, UK, in 2007 and his BSc degree from the School of Electronics and Information Engineering at Dalian University of Technology, China, in 2006.

DOI: 10.1002/dac

Zhikui Chen is a professor at Dalian University of Technology. He is also the director of the Institute of Network Communication and Database and the director of the joint research institute of Dalian University of Technology and Going.Com of Tokyo. From July 2001 to October 2007, he was a researcher at Stuttgart University of Germany on system communication for EU IST fifth and sixth framework projects in B3G or 4G. From November 1999 to June 2001, he was a postdoctoral researcher at IRISA of France for joint source and channel coding for picture and video. From October 1998 to April 1999, he was a postdoctoral researcher at the Computer Science Department of Hong Kong Baptist University for image processing. In June 1998, he received his PhD degree in Signal Processing from Chongqing University. In June 1993, he received his master's degree in Composite Material Mechanics from Chongqing University. In June 1990, he received his bachelor's degree in Mathematics from Chongqing Normal University.

Feng Xia is an associate professor and PhD supervisor in the School of Software, Dalian University of Technology, China. He has been an (guest) editor of several international journals. He serves as the general chair, PC chair, workshop chair, publicity chair, or PC member of a number of conferences. Dr. Xia has authored/co-authored one book and over 110 scientific papers in international journals and conferences. His research interests include mobile and social computing, intelligent systems and cyber-physical systems. He is a member of IEEE, IEEE Computer Society, IEEE SMC Society, ACM and ACM SIGMobile.



Xiaoning Lv is a PhD candidate in the School of Management at Dalian University of Technology, China. Her research interests are game theory, operations and finance engineering. She received her MSc degree from the School of Management at Dalian Jiaotong University, China, in 2009 and her BSc degree from Shanghai University of Finance and Economics, China.

Fanyu Bu currently, is a PhD candidate of Computer Science at Dalian University of Technology, China. His research interests are embedding system and Internet of Things. He received his MSc degree from the School of Computing Science and Technology at Inner Mongolia University, China, in 2009 and his BSc degree from the School of Computing Science and Technology at Inner Mongolia Agriculture University, China, in 2003.

DOI: 10.1002/dac