The Location Privacy Preserving of Social Network based on RCCAM Access Control

Xueqin Zhang and Qianru Zhou and Chunhua Gu. Liangxiu Han

Xueqin Zhang and Qianru Zhou is with the College of Information Science and Engineering, East China University of Science and Technology, Shanghai, China (e-mail: zxq@ecust.edu.cn).

Chunhua Gu was with University of Shanghai for Science and Technology, Shanghai, Shanghai,China (e-mail: guchunhua@usst.edu.cn).

Liangxiu Han is with the School of Computing, Mathematics and Digital Technology, Manchester Metropolitan University, Manchester, UK (e-mail: l.han@mmu.ac.uk).

ABSTRACT

Location-based services in social networks provide much convenience for people but bring much risk of location privacy disclosure. Aiming at this problem, a location privacy preservation algorithm based on RCCAM access control model is proposed to assign the accessing users of the access permission and the visibility level of location information through the combination of conflicts resolution strategy, permission allocation strategy and location generalization strategy. RCCAM is a relationship-based multi-users cooperation access control model, which takes the same shared contents that may involves the privacy profits of multi-users into consideration. The core of the algorithm is the value of open tendency which depends on the location sensitivity and the intimacy between users. Conflicts resolution strategy adopts the value of open tendency to vote for concessions. Permission allocation strategy and location generalization strategy to obtain the specific access permission and the location visibility level for accessing users according to the value of open tendency. The algorithm can achieve fine-grained control of location publishing of the shared content which involves stakeholder's privacy profit and maintain the sharing will of promulgator as possible.

Keywords:

Social Network, Privacy Preservation, Location Privacy, Access Control, Location Sensitivity, Location Publishing Strategy

1. INTRODUCTION

The rapid development of the internet has promoted the widespread use of social network. In recent years, the internet has provided users with rich and personalized services such as location-based services. All these services can be applied to share photos, videos and texts associated with location information which provide users with better experience and more convenience. The behavior of sharing actually is an active behavior of privacy disclosure. Thus, the leakage of user's privacy cannot be inevitable when user shares location information to others if the user has low privacy protection awareness. Naini F et al[1] considers that users can be identified by attracters through the exposure of location information which will result in incalculable losses[2]. Many users are concerned about the leakage of their location privacy. Therefore, the preservation of location privacy is important. This paper proposes an access control based method to protect location privacy.

2. RELATED WORK

The protection of location privacy in social network just started. [3] introduces the concept of location and reviews many methods which can be categorized into heuristic privacy measurement, probability deduction and private information retrieval based technologies. But all these methods are based on traditional protection methods of LBS-based services, not fully applicable in location privacy sharing by content. Access control is one of the most common methods in view of this situation. There are many types of access control models proposed to adapt to different needs. Chen T Z et al[4] reviews the current access control models for social network and show that it mainly includes relationship-based, attribute-based etc. Relationship is the core of social network so the relationship-based access control model which uses the relationship between users to resolve the problem of authorization is very suitable. However, Most of the prior research didn't pay attention to the fact that shared content may involves multiple users' privacy. Thus Hu and Ahn [5] proposes a multi-authorization framework based on a vote-based resilience mechanism. Pang J et al [6] proposes an access control mechanism based on user-to-user relationships and shared information. But they are not focus on the location privacy preservation. Chao L I et al [7] proposes a CS-LPPM model based on the combination of the above deficiencies to achieve a fine-grained location privacy protection based on access control method. Inspired by it, this paper proposes a relation-based multi-users corporative access control model (RCCAM) and combines conflicts resolution strategy, permission allocation strategy and location generalization strategy to achieve the RCCAM-based location publishing strategy. Finally provides users with fine-grained protection of location privacy and resolves the issue of the same shared

content involves multi-user's privacy to provide the location privacy protection of other users.

3. RCCAM ACCESS CONTROL MODEL

3.1 Description of Location Privacy Issue

Suppose there are four users in the social network, named Alice, Bob, Carol and David. The relationship between these four users is shown in Figure1. Alice, Bob and Carol are friends, Bob, Carol and David are friends, Alice and David are indirect friends.

Alice and Bob meet together then Alice uploads a content which including the information of location to the social network and "@" Bob. Carol forwards after commenting it. For this content, Alice is a promulgator, Bob is a stakeholder, Carol and David are accessing users. Assume that the location is a non-sensitive location for Alice, but sensitive to Bob. However, since Alice uploaded the location, Carol obtained the sensitive information of Bob and because of the forward of Carol, David could obtain the sensitive location of Bob. Thus, the location privacy of Bob was indirectly leaked. The process is shown in Figure1.

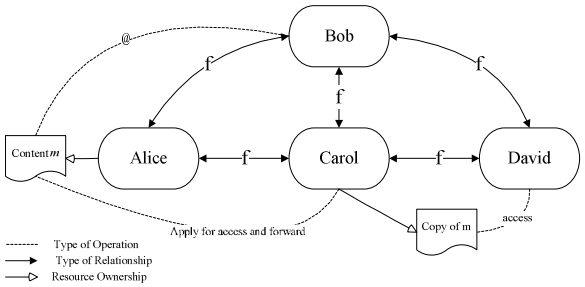

Figure 1. The diagram of the description of the location privacy issue

However, in the most current access control strategies for social networks, owner has absolute control over the content while other stakeholders have no control over it. Due to the interactivity of social networks, a content often indirectly leaks other users' privacy. Aiming at the above problem, this paper proposes a location publishing strategy based on multi-user corporation access control model(RCCAM) to solve the problem of how to protect the privacy of other users when the content influent multiple users' privacy.

3.2 Rccam Model Components

In RCCAM, subject is user, object is the content with location information, strategy determines whether the subject has the permission to the object and can be divided into system strategy and customized strategy. Elements are shown in Figure 2.

Content m The content can be texts, videos, or pictures. Each user has their own content set M_{u_i}. Unless otherwise specified, the content contains real location information.

Participant User U For a specific m, all related users are the participant users.

Promulgator u_{post} For a specific m, if $m \in M_{u_i}$, user u_i is the u_{post} of content m.

Stakeholder u_{rel} For a specific m, $find(m)$ is an abstract function that can identify the content-related users by the function of "@". All these content-related users are stakeholders. U_{rel} is the set of all stakeholders.

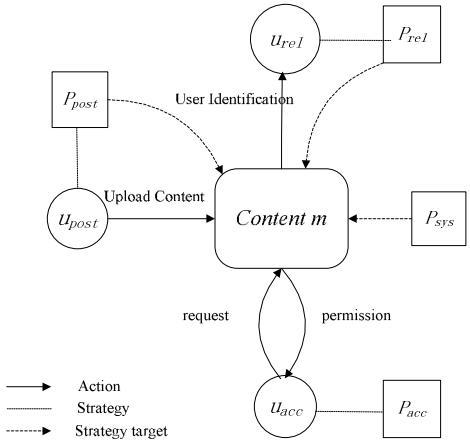

Figure 2. The components of RCCAM

Accessing user u_{acc} For a specific m, the user who send an access request is an accessing user of m.

System Strategy P_{sys} As a default strategy made by the network operator that applies to all users who are included in the social network.

Customized Strategy P_{def} In a social network, each user can set personalized privacy strategy according to their own privacy needs and privacy preferences. And the customized strategy can be further divided into promulgator's strategy P_{post} and stakeholder's strategy P_{rel} according to the relationship between user and content.

3.3 LOCATION SENSITIVITY

Location sensitivity(*Sen*) is an indicator that judges whether the location is user's privacy. The higher the *Sen* is, the stronger the user is unwilling to share it with other users.

3.3.1 The Definition of Location Sensitivity

Sen is different in different scenarios [8].

a. *Sen* of the same location is different for different users.

b. *Sen* of the same location is different for the same user at different time.

c. *Sen* of the same location is different for the same user when the accessing user is different.

Thus, location sensitivity depends on four elements: location l, user u, time t and the type of relationship r_u. Using function $Sen(l,u,t,r_u)$ to set the location sensitivity, $Sen \in [0,1]$.

E.g. $Sen(l_1, Alice, t_1, family) = 0.9$ means that location l_1 in the period of t_1, if the relationship between accessing user and Alice is family, the sensitivity is 0.9.

3.3.2 The Acquisition of Location Sensitivity

When the accessing user send an access request, the social network system will identify the related stakeholders then performs the sensitivity matching using the function

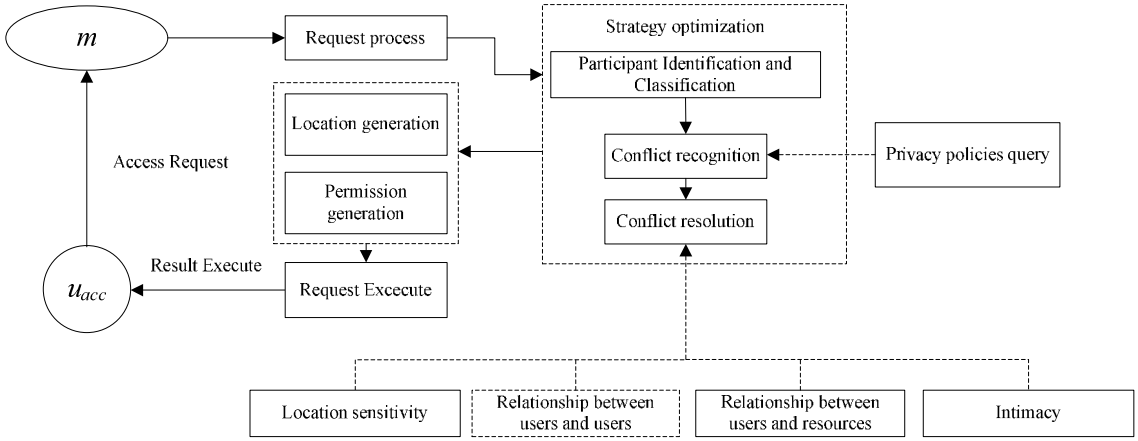

Figure 3. Location Publishing Strategy

$Sen = Matching(u, u_{acc})$, finally return the *Sen* of each related users. If the result is empty, the system will request the user to set a sensitivity as the format: $L_{sen} = (l_i, t_p, r_{u,} Sen)$.

E.g. $L_{sen} = (l_1, morning, family, 0.5)$ represents that when the relation of accessing user is 'family', location l_1 is 0.5-sensitivity during morning.

4. Location Publishing Strategy Based On RCCAM

This chapter proposes a location publishing strategy based on RCCAM model which combines conflict resolution strategy, permission allocation strategy and location generalization strategy.

4.1 Location Publishing Strategy Construction

Figure 3 shows the frame of location publishing strategy.

- U_{pr} The set of u_{post} and u_{rel} of the same content m. u_{rel} can be one or multiple.

- t_p Valid time of the sensitivity for a location information. It can be a specific time or can be represented by a fuzzy set, e.g. $t_p \in (morning, afternoon, evening)$.

- L The location information set of user.

- P_u A set of customized strategy set by user selves. Each user's customized strategy can be more than one. E.g. $P_{Alice} = \{p_1, p_2\}$ represents the customized strategy of Alice. $p_1 =< open, friend >$ is a customized grouping strategy means this *m* only open to friend. $p_2 =< L, [morning, friend : 0] >$ is a customized location sensitivity strategy means in the morning, the location information belongs L is 0-sensitivity to the user whose relationship is 'friend'.

- R_u A set of the relationship between user and user. $R_u \subseteq U \times U = \{r_1, r_2, ...r_n\}$ represents different type of user-to-user relationship, such as 'close friend', 'family' etc. [9].

- R_r A set of the relationship between user and the content. $R_r \subseteq U \times R = \{y_1, y_2, ...y_n\}$ represents the different type of user-to-resource relationship. This paper divides the relationship of user-to-resource into owner, sharer, creator and disseminator [8].

- P $P = \{P_{read-only}, P_{read-forward}\}$ is the permission of u_{acc} to access the content, $P_{read-only}$ represents read-only permission and $P_{read-forward}$ represents that the user can read and forward it. Specific permission can be classified as Table 1.

Table 1: The classification and the representation of permissions.

	$P_{read-only}$	$P_{read-forward}$
No-permission	0	0
Read-only	1	0
Read-forward	1	1

- *Decision* The final access control decision for specific u_{acc}. $Decision \leftarrow (l, u_{acc}, d, P)$ represents that the specific u_{acc} has the *P* permission to access the content and the location *l* will be shown at the *d* visible level.

4.2 Conflict Resolution Strategy

Due to the existence of stakeholders, each u_{rel} has independent access customized strategy which will result in strategy conflicting. E.g. Alice is u_{post} and Bob is the u_{rel}. As for the same location, Alice set the 0-sensitivity and Bob set the 1-sensitivity which means a non-sensitive location is extremely sensitive to Bob. Obviously, the strategies of Alice and Bob have conflicts.

- $U_{conflict}$ Set of u_{rel} who has conflict with u_{post}.

- $Identify(u_{acc}, P_i)$ The function to identify the conflict between u_{post} and u_{rel}. *Identify*=1 means there is a conflict.

Table 2: The different case of the sensitivity between promulgator and stakeholder.

Alice	u_{rel}	Description
0	0	L is both not sensitive to u_{post} and U_{rel}
1	0	L is sensitive to u_{post} but not sensitive to U_{rel}
0	1	L is not sensitive to u_{post} but $\exists u_{r_i} \in U_{rel}$ L is sensitive
1	1	L is sensitive to u_{post}, and $\exists u_{r_i} \in U_{rel}$, L is sensitive

According to the sensitivity of location, the situation is shown as Table 2. There, 0 indicates that the location is insensitive and 1 indicates that the location is sensitive. For the first two cases in Table 2, there is no conflict. The final decision follows the principle of the owner priority and executes as the strategy of u_{post} . As for the latter two cases in the table need to be solved by voting based on Open Tendency(OT).

OT represents the wiliness that how much the user is willing to share the location to a certain u_{acc} , depending on the sensitivity of location and the intimacy between users. The calculation of intimacy refers to [10]. Intimacy do not necessarily be the same even if the users are in the same group. For each u_{acc} , each u_{post} or u_{rel} has its own *OT*. There, the Intimacy is the intimacy between u_{acc} and u_{post} , the intimacy between u_{acc} and u_{rel} . *OT* is defined as follow:

$$OT_{u_i} = w_1 * (1 - Sen(u_i, u_{acc})) + w_2 * close(u_i, u_{acc}) \quad (1)$$

$u_i \in \{u_{post}, u_{rel}\}, w_1 + w_2 = 1, Sen(u_i, u_{acc})$ represents the location sensitivity set by u_i for u_{acc} , $close(u_i, u_{acc})$ represents the intimacy between u_i and u_{acc} .Then the definition of the voting function shown as follow.

$$V_{OT} = \sum_{i}^{n} w_{u_i} * OT_{u_i} \quad (2)$$

$V_{OT} \in [0,1]$ is the voting results of u_{acc} according to the OT. *n* is the total number of people who participant in the vote. Due to the relationship between each participant and the content, assign different weights w_{u_i} of different R_r . Therefore, the assignment of weights is based on the principle of the priority of u_{post} and the principle of the importance of relationship. The intimacy of u_{post} itself is 1. w_{u_i} is assigned as follow:

$$w_{u_i} = \begin{cases} a, & if\ u_i = u_{post} \\ \dfrac{close(u_i, u_{post})}{\sum_{u_i \in U_{rel}} close(u_i, u_{post})}(1-a), & if\ u_i \in U_{rel} \end{cases} \quad (3)$$

$a \in (0,1)$ is the weight of w_{u_i} when u_i is u_{post} . $close(u_i, u_{post})$ represents the intimacy between u_i and u_{post} . when u_i is the stakeholder, w_{u_i} represents the weight of u_{rel} . The degree of concessions is different while the different importance between u_{post} and different u_{rel} . The more $close(u_{rel}, u_{post})$ is, the higher intimacy between u_{rel} and u_{post} , u_{rel} is more important to u_{post} and the more the disclosure of the location will damage the privacy profit of the u_{rel} will be taken into account .Therefore, u_{post} is more willing to make concessions in terms of *OT*.

4.3 Permission Allocation Strategy

Permission allocation strategy is one of the system strategies and it is for the further allocation of the user's permission of read and forward, which is achieved through the permission allocation table. In social network, communication has multiple directions. In order to implement finer access control and minimize privacy leakage in the process of dissemination, the social network system should develop a permission allocation table shown as Table 3 to do some permission division according to the V_{OT} which has been calculated.

Table 3: The table of permission allocation.

V_{OT}	$[0, X_1)$	$[X_1, X_2)$	$[X_1, 1]$
P	$P = [0,0]$	$P = [1,0]$	$P = [1,1]$

Here, $P = [0,0]$ represents that the u_{acc} cannot see the content. $P = [1,0]$ represents that the u_{acc} can only see the content but cannot forward. $P = [1,1]$ represents that u_{acc} can see the content and forward.

4.4 Location Generalization Strategy

Location generalization strategy also belongs to the system strategy, which is used to classify the visible level of the location so as to strengthen the location privacy preserving of user under the premise of retain promulgator's willingness to share. It is achieved through the location generalization table shown as Table 4 by dividing the scope of visibility of location at all levels based on V_{OT} , which is uniformly formulated by the social network operator. E.g. $V_{OT} \in [0, X_1]$, the location will be generalized to the level L1. Location is not necessarily divided into only three levels, according to the different grained requirements of different social networks, more levels can be divided.

Table 4: The table of location generalization.

V_{OT}	$[0, X_1]$	$[X_1, X_2)$	$[X_2, 1]$
level	L1	L2	L3

4.5 Rccam-based Location Publishing Strategy

When u_{acc} sends an access request for the content *m* containing the real location information *l* to the server, the permission of u_{acc} will be controlled through the location publishing strategy, and finally the system returns the authority of u_{acc} ,and the u_{acc} 's visibility level of *l*. RCCAM-based location publishing strategy is shown as Table 5.

Table 5： The algorithm of location publish strategy based on RCCAM model.

RCCAM-based location publishing strategy algorithm

Input u_{acc} ,*m containing location l*

Output final *Decision*

1. $U_{rel}, u_{post} \leftarrow find(m)$ // identify participants and get the set of content stakeholders
2. $P_{post} \leftarrow get\_police(u_{post})$ //get the customized strategy P_{post} of u_{post}
3. $U'_{rel}, flag \leftarrow Identify(u_{acc}, P_i)$ //identify the strategy conflicts and set of stakeholders who get conflict.
4. $U_{pr} = \{u_{post} \cup U'_{rel}\}$
5. **If** $flag == 1$ and u_{acc} satisfies P_{post} **do**
6. **Foreach** $u_i \in U'_{rel}$ **do**

   $P_{u_i} \leftarrow get\_police(u_i)$ // get the customized strategy P_{rel} of u_{rel}

$Sen(u_i, u_{acc}) \leftarrow matching(u_i, u_{acc})$ //get the sensitive of location of each u_i

$close(u_i, u_{acc}) \leftarrow get\_close(u_i, u_{acc})$ //calculator the intimacy between u_i and u_{acc}

$close(u_i, u_{post}) \leftarrow get\_close(u_i, u_{post})$ //calculator the intimacy between u_i and u_{acc}

$OT_{u_i} \leftarrow OT(close(u_i, u_{acc}), Sen(u_i, u_{acc}))$ // calculator the OT of u_i

7. **End foreach**
8. **End If**
9. $d, P \leftarrow V_{OT}()$ //conflicts resolution through voting
10. $Decision \leftarrow (l, u_{acc}, d, P)$ //get the final decision

4.6 Forward Strategy

In social networks users can forward the content of their friends. However, the forwarder often adopts a weaker control strategy for the forwarded content. The forwarded content is sensitive to content creator and related stakeholders. Therefore, a simple strategy for secondary forwarding is needed. If Carol forward the content *m* up-loaded by Alice, the role of Alice transfers from u_{post} to u_{rel} , the relation with *m* changes from owner to creator. And the role of Carol transfers from u_{acc} to u_{post} , and the relation with *m* changes from disseminator to sub-owner. Thus, the permission assigned to the accessing user must satisfy Alice's privacy control strategy and Carol's strategy at the same time.

5. Application Case Analysis

5.1 Two-user Application Analysis

Assume that Alice uploads a content and "@" friend Bob as shown in Figure 4. a. The location information is 'Star-bucks, Shanghai South Railway Station'. Therefore, Alice is u_{post} , Bob is u_{rel} and friend Carol is u_{acc} .

Figure 4. Alice upload a content with location information and @ friends

a. The customized strategy of Alice:

$P_A = \{p_1, p_2\}, p_1 =< open, friend >$

$p_2 =< l, [morning, friend : 0] >$

b. The customized strategy of Bob:

$p_B =< l, [morning, friend : 1] >$ indicates that l is 1-sensitivity for u_{acc} whose relationship with Alice is 'friend' in the morning.

c. The relationship between Alice and Carol, Bob and Carol is 'friend'.

d. Establish the permission allocation Table. $X_1 = 0.3, X_2 = 0.4$.

e. The intimacy between accessing user and promulgator, between accessing user and stakeholder are both 0.5. $close(A, C) = close(B, C) = 0.5$

f. The intimacy between Alice and Bob respectively equals to 0.1 and 0.8 to verify the different concessions when there is low/high intimacy with Bob.

g. Establish the location generalization table shown as Table 6.

Table 6: The table of location generalization

OT	Level
[0.75,1]	L_real
[0.55,0.75)	L1(Street)
[0.4,0.55)	L2(District)
[0.2,0.4)	L3(City)
[0.1,0.2)	L4(Country)
[0,0.1]	L _no

The result of voting by conflicts resolution strategy is shown as Table 7. It's obvious that there is a conflict.

Table 7: The results of concession voting.

	OT	Vot_low	Vot_high
Alice	0.75	0.4625	0.3875
Bob	0.25		

If the intimacy between Alice and Bob is high, the final decision is:

$Decision \leftarrow (L, Carol, L3, [1,0] : read - only)$

Carol is only authorized the read-only accessing permission of the content and the location is visible in L3 level means Carol can see the location as 'Shanghai'. If intimacy between Alice and Bob is low, the final decision is:

$Decision \leftarrow (L, Carol, L2, [1,1] : read - forward)$

Carol is authorized the read-forward accessing permission of the content and the location is visible in L2 level that means Carol can see the location as 'Xuhui District'. If we consider Alice's strategy only, the location is 0-sensitivity to Carol and the OT of Alice is 0.75. That is Carol has read-forward permission of the content and the location is visible in L_real level that means Carol can see the location as 'Shanghai South Railway Station'. Obviously, Alice takes the privacy needs of Bob into account and made some concessions. And the closer the intimacy between Alice and Bob is, the more concession Alice willing to make to protect the privacy of Bob.

5.2 Multi-users Application Analysis

This section discusses the scenarios of multiusers based on the chapter 5.1 and as shown in Figure 4.b. Alice is u_{post} , friend Bob, Ella, David, Sophia, Ana, Susan and Zoe are u_{rel} , and Carol is u_{acc} .

a. $U_{conflict} = [Bob, Ella, Sophia]$

b. The customized strategy of Alice is the same as chapter 5.1.

c. The customized strategy of Bob, Ella and Sophia as follow:

$p_B =< L, [morning, friend : 1] >$

$p_E =< L, [morning, friend : 0.7] >$

$p_S =< L, [morning, friend : 0.4] >$

d. Establish the permission allocation Table 3.

$X_1 = 0.3, X_2 = 0.5$ 。

e. $close([A, E, S], C) = 0.5$.

f. The importance of u_{rel} and u_{post} may be different, which depending on the intimacy between u_{rel} and u_{post} . Two kinds of intimacy condition as shown in Table 8 to verify the concession of Alice in the case of different stakeholder's importance.

g. permission allocation table same as Table 6.

Table 8: Different importance of stakeholders to Alice

	The intimacy of Alice and stakeholders	Description
same	$close(A, [B, E, S]) = 0.5$	Same intimacy so the importance is the same
different	$close(A, B) = 1,$ $close(A, [E, S]) = 0.5$	Alice is closer to Bob so the importance is different.

Table 9: The result of concession voting

	Alice	Bob	Ella	Sophia
OT	0.75	0.25	0.4	0.55
same			0.575	
different			0.500	

The results of voting are shown in Table 9. When the importance of stakeholders are the same, the final decision as follow:

$Decision \leftarrow (L, Carol, L1, [1,1] : read - forward)$

Carol is authorized the read-forward accessing permission of the content and the location is visible in L1 level that means Carol can see the location as 'Lingyun Street'. And when the importance of u_{rel} are different (the importance of Bob is higher than others), final decision is:

$Decision \leftarrow (L, Carol, L2, [1,1] : read - forward)$

Carol is authorized the read-forward accessing permission of the content and the location is visible in L2 level that means Carol can see the location as 'Xuhui District'. From Table 9, taking the privacy needs of stakeholders into consideration, Alice makes some concessions in the visibility of location. But compared with the two case in which the stakeholder's importance is the same and different, because the importance of Bob is higher, Alice makes more concession for him.

6. CONCLUSIONS

This paper proposes a multi-users cooperative access control model in order to provide fine-grained privacy protection for social network users while they share the content with location information. Location sensitivity and intimacy are the core elements to get the value of OT and the value of *OT* is the core of the total strategy of location publishing, which includes the conflicts resolution strategy, the permission allocation strategy and the location generalization strategy. Through the case analysis find that we can greatly solve the problem, when a content involves multiple users' privacy, the location privacy of stakeholders can be greatly protected and maintain the sharing behavior of promulgator.

ACKNOWLEDGMENT

This paper is supported by National Natural Science Foundation of China 61472139.

REFERENCES

1. G. Marchesini, S. Karni, and N. Ahmed, "On obtaining transfer functions from gain-function derivatives*," IEEE Trans. Autom. Control AC*, Vol. 12, pp. 229-230, Apr. 1967.

2. Y. S. Lin and D. Sylvester, "Runtime leakage power estimation technique for combinational circuits," *in Proceedings of the Asia and South Pacific Design Automation Conference,* Yokohama, 2007, pp. 660-665.

3. S. K. Kumar, S. Kaundinya, S. Kundu, and S. Chattopadhyay, "Particle swarm optimization based pattern reordering for low power testing," *in Proceedings of the International Conference on Computing, Communication and Networking Technologies*, Tamil Nadu, 2010, pp. 1-5.

4. V. Sheshadri, V. D. Agrawal, and P. Agrawal, "Optimal power-constrained SOC test schedules with customizable clock rates," *in Proceedings of the IEEE International SOC Conference*, Niagara Falls, New York, 2012, pp. 271-276.

5. H. Zhiyun, P. Zebo, and P. Eles, "Multi-temperature testing for core-based system-on-chip," *in Proceedings of the Design, Automation & Test in Europe Conference & Exhibition*, Dresden, 2010, pp. 208-213.

6. M. R. Chidambara, "Two simple techniques for the simplification of large dynamic systems," *JACC*, Vol. 1, pp. 669-674, Dec. 1969.

7. Y. Shamash, "Stable reduced-order models using Pade type approximation," *IEEE Trans. Autom. Control*, Vol. 19, no. 5, pp. 615-616, Oct.1974.

8. M. Hutton, and B. Friedland, "Routh approximations for reducing order of linear, time-invariant systems," *IEEE Trans. Autom. Control*, Vol. 20, no. 3, pp. 329-337, Jun. 1975.

9. T. C. Chen, C. Y. Chang, and K. W. Han, "Reduction of transfer functions by the stability equation method," *J. Franklin Inst.*, Vol. 308, pp. 389-404, Oct. 1979.

10. Y. Bistritz, and G. Langholz, "Model reduction by Chebyshev polynomial techniques," *IEEE Trans. autom. Contr. AC* Vol. 24, pp. 741-747, Oct. 1979.

11. T. N. Lucas, "Factor division: A useful algorithm in model reduction," *IEE Proc*. Vol. 130, no. 6, pp. 362-364, November 1983.

12. R. Prasad, J. Pal, and A. K. Pant, "Multivariable system approximation using polynomial derivatives," *J. Inst. Eng., India IE(I),* Vol. 76, pp. 186-188, Nov. 1995.

13. D. A. Wilson, "Optimal solution of model reduction problem," *Proc. Inst. Electr. Eng.*, Vol. 117, no. 6, pp. 1161-1165, Jun. 1970.

Authors

Xueqin Zhang received the Ph.D. degree in Detection Technology and Automation Devices from East China University of Science and Technology (ECUST), Shanghai, China, in 2007. Since 1998, she has been in the Electrical and Communication Engineering Department, ECUST, where she is currently an ASSOCIATE PROFESSOR.

At 2006, she worked as a visiting scholar in University of Wisconsin Madison. Her research interests include pattern classification, information security and data mining etc.

Corresponding author. Email: zxq@ecust.edu.cn

Qianru Zhou received M.S. degree in Signal and information procession from East China University of Science and Technology (ECUST), Shanghai, in 2012. His research interests is privacy preservation of social network

Email：arrowz@gmail.cn

Chunhua Gu received the Ph.D. degree in Control Science and Engineering from East China University of Science and Technology (ECUST), Shanghai, China, in 2007. From 1992 to 2013, he was in the Computer Science and Engineering Department, School of Information Science and Engineering, ECUST, where he is currently a PROFESSOR. Now he is in University of Shanghai in Science and Technology.

At 2002, he worked as a visiting scholar in School of Computing and Information Sciences, Florida International University. His research interests include intelligent computing, software engineering and information security.

Email:

Email: guchunhua@usst.edu.cn

Liangxiu Han received the Ph.D. degree from Fudan University, Shanghai, China, in 2002. She is currently with School of Computing, Mathematics and Digital Technology, Manchester Metropolitan University Her research interests include pattern classification, information security and data mining etc. As a Principal Investigator (PI) or Co-PI, Han has been conducting research in relation to big data processing, data mining, parallel and distributed computing/cloud computing (funded by EPSRC, BBSRC, Royal Society, Innovate UK, Horizon 2020, Industry, Charity, Newton Fund, etc.).

Email: l.han@mmu.ac.uk