Vulnerable friend identification: Who should you beware of most in online social networks?

Yunjuan Yang*, Ye Tian*, Edith Ngai†, Lanshan Zhang‡, Yining Teng§ and Wendong Wang*
*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China
†Department of Information Technology, Uppsala University, Sweden
‡School of Digital Media and Design Arts, Beijing University of Posts and Telecommunications, China
§International School, Beijing University of Posts and Telecommunications, China
Email: yangyunjuan51@126.com, humanty@163.com, edith.ngai@it.uu.se,
zls326@sina.com, ynteng.ac@gmail.com, wdwang@bupt.edu.cn

***Abstract*—Web users are immersed in their roles as information producers and propagation pushers. They are unaware of being potential threats to privacy-protection towards themselves and their friends. It is necessary to know who they should beware of most in their friend-networks once their privacy information is divulged inadvertently. In this paper, we aim to identify the vulnerable friend who maximizes the dissemination of privacy information. First we develop a Privacy Receiving-Disseminating (PRD) model to simulate the iterative course of privacy information dissemination within social graph. The subgraph constituted of those users who are involved in the dissemination, called Ultimate Circle of Disseminating (UCD), is then detected by an iterative algorithm. The contribution of each direct friend could be evaluated by comparing the disseminating intensities of detected UCDs before and after unfriending himself. The performance of our work has been validated empirically with the comparison of different unfriending strategies.**

***Index Terms*—Vulnerable Friend Identification, Privacy Information Dissemination, Unfriending Strategy**

I. INTRODUCTION

With the advent of Web 2.0, information communication over Online Social Networks (OSNs) has developed into an unprecedented scale. Users are immersed in its open atmosphere, where they can speak out freely with the desire to be concerned by as many friends, near or far, as possible. In face of the large-scale information source and the fast information propagation, unfortunately, privacy-protection extends far beyond the tedious preferences of privacy settings in OSNs [1]. Privacy information is divulged inadvertently every moment. Considered as information producers, users are unaware of where the posted privacy information travels to and who will abuse it maliciously. The forwarding behaviors of their direct friends, who act as the indispensable propagation pushers, are also likely to propel the dissemination of privacy information.

Based on the qualitative study about regretting the posting behaviors, most Facebook users once posted sensitive contents with the risk of privacy leakage. They do not foresee that these contents was broadly spread and led to unintended consequences with unexpected audiences [2]. Similar remorse occurred with Twitter users according to an online survey [3]. On Sina Weibo, for example, a young lady named Guo Meimei flaunted her wealth in her postings, which were massively forwarded by her followers and caused a big disturbance in the whole China [1]. Due to the vulnerability, each of users' direct friends offers varying degrees of assistance to privacy leakage. Users really need to know what role each of their direct friends plays once their privacy information is disseminated.

Privacy-protection in OSNs has became a research hotspot. While the discussion on identifying the vulnerable social tie just starts in recent years. In this paper, we study the problem of vulnerable friend identification through the dynamic process of privacy information dissemination. More specifically, a Privacy Receiving-Disseminating (PRD) model is proposed to simulate this process based on three accepted facts: (1) User's privacy-protection consciousness may not enough to protect himself, let alone the friend-network he belongs to; (2) User's forwarding tendency determines the possibility that he disseminates the received privacy information; (3) User's status within social graph results in distinct spread scope when he forwards the received privacy information. With an iterative algorithm, the Ultimate Circle of Disseminating (UCD) is detected as the subgraph involved in the dissemination. After that we analyze the variations of disseminating intensity within the detected UCDs, which is caused by unfriending each of one's direct friends respectively, and estimate their vulnerabilities. The one whose removal lowers the disseminating intensity the most is then identified as *vulnerable friend*. Multi-group experiments are conducted based on two real-world datasets with different unfriending strategies, and the performance of our approach is validated with a series of evaluation indexes.

The contribution of our work is two-folded: (1) As far as we know, this is the first work to identify the vulnerable social tie from the sight of privacy information dissemination process. It provides a novel perspective for users to see the straightforward impact of vulnerable social tie on real propagation course; (2) Considering the peculiarity of privacy information dissemination, an asynchronous PRD model is proposed based on the comprehensive factors of vulnerability. This model describes the dissemination process by dynamic

---

[1] http://www.smh.com.au/world/guo-meimei-chinas-most-brazen-professional-mistress-confesses-on-tv-20140804-100fp2.html

978-1-4799-5952-5/15/$31.00 ©2015 IEEE

updating each user's possibility of knowing and forwarding the privacy information within intricate social graph.

The rest of paper is structured as follows. Section II reviews the literature of related works and highlights the novelty of our work. The problem definition and model description are introduced in Section III. Section IV illustrates the experimental evaluation and Section V summarizes the conclusion.

II. RELATED WORK

Existing researches focus on the defense of accessing and inferring the privacy information of OSN. They intend to improve privacy setting mechanism to protect privacy [4] [5]. According to the empirical study in Facebook, unfortunately, Labitzke et al. [1] showed regardless of how privacy settings are adjusted, privacy information can be inferred easily from one's friends. Online friends are potential threats, as Adhikari and Bachpalle [6] discussed in their work, even one's privacy information is visible to his direct friends only, information sharing among friends of friends still leaks it widely.

Considering whether the privacy settings of users can protect themselves and their friend-networks or not, Gundecha et al. [7] firstly identified the vulnerable social tie. They suggested that unfriending the vulnerable friend can improve users' security [8]. Based on it, Alim et al. [9] extended an axiomatic approach to explore the effect of different computing operation on profiles. These works simply rely on the static attributes of users. They do not realize that the threatening interactive behaviors among users also raise the vulnerability. Thus our work attempts to identify the vulnerable friend based on the dynamic process of privacy information dissemination.

Some previous works proposed different models to simulate the information propagation. Pergament et al. [10] simulated the diffusing process based on reputation scores. Dinh et al. [11] developed a sharing-mentioning leakage model with two propagation mechanisms. Othmane et al. [12] designed a time series propagation model and proved that privacy information declines to saturation rather than vanishes. These works studied privacy diffusing with generic models but not considered the peculiarity of privacy information dissemination.

III. PROBLEM DEFINITION AND MODEL DESCRIPTION

The privacy information posted inadvertently by users can be accessed from multiple approaches. By forwarding behaviors, their direct friends, who have immediate links with them, offer most springboards of accessing approach for possible adversaries. This motivates us to specify who users should beware of most among their direct friends. In our approach, it is addressed by analyzing their dissemination behaviors of privacy information, which is stated below:

> **Vulnerable Friend Identification Problem:** *Given an object user and the friend-network centered with him, the privacy information posted by him is disseminated though disparate social ties between his direct friends and others. The vulnerable friend identification problem aims to identify the most destructive direct friend who results in the most widely spreading of this privacy information.*

The one who contributes the greatest power to expand the dissemination is identified as *vulnerable friend*. In this paper, we consider three factors which determine whether a user would participate in the dissemination or not and to what extent he would make the privacy information visible to others.

Privacy-Protection Consciousness. The accessibility of personal profiles, particularly those hidden by most users, incurs varying degrees of risk for privacy-protection. One who does not possess enough consciousness to protect himself is far less likely to safeguard the privacy of his friend-network. We quantify the privacy-protection consciousness I_v of user v with the relative accessibility of his personal profiles as [7] does.

Privacy Leaking Tendency. User's propensity towards a certain topic, to which the received privacy information belongs, determines the extent to which he disseminates it. Since one's behavior tendency is an inherent personality, it can be assessed from the abundant records of his online behaviors. We suppose one's propensity towards certain topics impose the same influence on both posting and forwarding behaviors. Thus, the privacy leaking tendency L_v of user v could be estimated by the average privacy leakage probability of which he ever posted himself or forwarded from others.

Media Capability. The media capability S_v of user v reflects how widely his forwarding behavior would make the privacy information visible to others. It is closely related to his topological status within social graph, which is generally quantified by betweenness centrality [13].

A. Privacy Receiving-Disseminating Model

For convenience, the notations in this paper are shown in Table 1. We abstract the friend-network centered with o as a directed graph $G_o = (U_o, E_o)$. Each node $v \in U_o$ presents a user with two attributes I_v and L_v, and each directed edge $e < v, u > \in E_o$ presents the social link from u to his follower v. In this case, v is defined as u's direct friend.

Inspired by the traditional Linear Threshold Model (LTM), Privacy Receiving-Disseminating (PRD) Model is proposed. The core idea of PRD model is that, once o posts m_o inadvertently, it would be spread across the social graph. User would know m_o from disparate sources at diverse probabilities, which is defined as receiving probability. The steady accumulation of receiving probabilities from multiple sources would be gradually translated into an impetus to drive the user himself to disseminate m_o to his followers. Dissemination probability is then defined to describe this likelihood. Actually, the two probabilities are continuing updated iteratively until the propagation process terminates.

Receiving Probability. v can be informed of m_o by whom he follows, $u \in \{u : v \in DF_u\}$. Besides the prerequisite that u has disseminated m_o before, the degree of concern v expresses towards u is also a considerable influence. It determines the possibility that v would catch a sight of m_o from u. We propose receiving probability to present to what extent that v may know m_o from u, which is given by

$$R_{uv}(t_k^{uv}) = 1 - (1 - D_u(t_{k-1}^u))^{\alpha_{uv}} \quad (1)$$

Table 1: Notations

Symbols	Descriptions
o	Object user whom we intend to protect
m_o	Privacy information posted by o
$DF_o = \{\eta_i\}$	The set of o's direct friends
G_o	Directed graph of o's friend-network
$G_{o\setminus\eta_i}$	Subgraph of G_o after unfriending η_i
A_o	Authority of o
I_v	Privacy-protection consciousness of v
L_v	Privacy leaking tendency of v
S_v	Media capability of v
d_{ov}	Diameter between o and v
α_{uv}	Concerns frequency that v expresses towards u
t_k^{uv}	Time that v knows m_o from u
t_k^v	The latest time that v knows m_o
$R_{uv}(t_k^{uv})$	Receiving probability of v from u at time t_k^{uv}
$\tilde{R}_v(t_k^v)$	Total receiving probability of v at time t_k^v
$D_v(t_k^v)$	Disseminating probability of v at time t_k^v
ε	Receiving threshold
θ_i	Terminal node with $\tilde{R}_{\theta_i}(t_{k_{\theta_i}}) < \varepsilon$
$\Gamma_o = \{\gamma_i\}$	The set of disseminating routes within G_o $\gamma_i = \{o, v_1, v_2, \ldots\}$, where $e < v_i, v_{i+1} >\in E_o$
$\Gamma'_o = \{\gamma'_i\}$	The subset of Γ_o with constraint $\forall v_j \in \gamma'_i,\ v_k \in \gamma'_i,\ j \neq k,\ s.t.\ v_j \neq v_k$
w_i	End node of γ'_i
G'_o or $G'_{o\setminus\eta_i}$	UCD after the disseminating within G_o or $G_{o\setminus\eta_i}$
ϕ_i	Involved node within G'_o
$\mathbb{I}_o$ or $\mathbb{I}_{o\setminus\eta_i}$	Disseminating intensity of G'_o or $G'_{o\setminus\eta_i}$
$\mathbb{C}_{\eta_i}$	Disseminating contribution of η_i
$\hat{\eta}_o$	Vulnerable friend of o

v may know m_o from more than one user, and the more users he follows, the more likely he is to know m_o. Thus the receiving probability of v is asynchronously updated during a certain period. The total receiving probability of v is given by

$$\tilde{R}_v(t_k^v) = \min\{1, \sum_{u\in\{u:v\in DF_u\}} R_{uv}(t_k^{uv})\} \tag{2}$$

the circumstance of silent attention with few interactive behaviors is ignored due to its little dedication to dissemination.

Disseminating Probability. Under the premise that v has known m_o, whether v forwards the received m_o or not depends on three factors: (1) I_v, which reflects his self-awareness to safeguard other's privacy; (2) L_v, which indicates his disseminating tendency towards this kind of information; (3) $A_o^{\frac{1}{d_{ov}}}$, which intuitively shows his attitude of worship towards o. We propose disseminating probability to forecast the possibility that v forwards m_o as soon as he knows it, which is given by

$$D_v(t_k^v) = 1 - (1 - (1 - I_v) \times L_v \times A_o^{\frac{1}{d_{ov}}})^{\tilde{R}_v(t_k^v)} \tag{3}$$

We now describe the process of privacy information dissemination within PRD model, which is illustrated in Figure 1. Time t_0 is the initial time when o posts m_o. $t_1, t_2, \ldots$ are a series of discrete time that represent the continuous rounds of dissemination from node to node. At time t_1, o's direct friend $\eta_i \in DF_o$ may know m_o from o's personal page with a receiving probability, and forwards it with corresponding disseminating probability to propel the propagation course of m_o. So does η_i's direct friend $v \in DF_{\eta_i}$ at time t_2, and so on. The receiving probability of each node is dependent on the disseminating probability of whom in previous round, and further determines the disseminating probability of himself. Thus the two correlative probabilities of each node are asynchronously updated with the approaching of m_o from disparate routes $\gamma_i \in \Gamma_o$ of G_o at different time. The dissemination process along intricate routes continues until that each terminal node θ_i of distinct route is scarcely possible to know m_o, let alone to forward it. A receiving threshold ε is set to demarcate the receiving probability of θ_i at time $t_k^{\theta_i}$ separately.

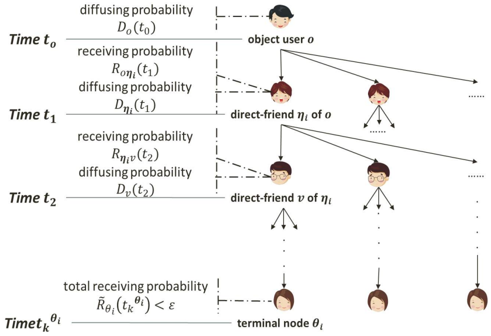


Figure 1: PRD Model

Due to the intricate structure of friend-network, there are two particular circumstances during the course of propagation.

First, there may be a loop among several users in dissemination process. In this case, a user may see m_o from others who forwarded m_o from him, direct or indirect, and would be less likely to forward it once again. The endless loop of propagation is avoided to accord with common sense.

Second, two users who have same diameter with o may follow each other. It means that they may be informed of m_o mutually from each other at same time. We consider both likelihoods and deny the round-tripping of propagation.

B. Ultimate Circle of Disseminating Discovery

The privacy information dissemination will gradually stop as it is far away from source [12]. The subgraph $G'_o \subseteq G_o$ involved in the dissemination is defined as Ultimate Circle of Disseminating (UCD). Considering the asynchronously updating with the progress of dissemination, an iterative algorithm is required to discover the UCD. Γ_o is pre-processed based on the two particular circumstances mentioned before. More specifically, we construct the subset $\Gamma'_o \in \Gamma_o$ with the constraint that each route $\gamma'_i \in \Gamma'_o$ contains a particular order of nodes without repetition.

The iterative algorithm is shown in Algorithm 1. At step 1, it abstracts the loop-free routes $\Gamma'_o = \{\gamma'_i\}$ from G_o. At step 2-19, an iterative computation is carried out with an inner iteration. In corresponding routes of each round, the two correlative probabilities of each node are successively updated at step 4-8. Then we find out the nodes with smaller receiving probabilities than the pre-set ε, and remove involved routes from Γ'_o. The outer iteration is re-executed until that all the nodes involved in the dissemination have steady receiving probabilities larger than ε. In the worst case that just one node is removed in each outer iteration and only o is left at last, the amount of iteration n reaches a maximum of $|U_o| - 1$. Because of the pre-filtering based on the constraint and the removing at the end of each outer iteration, each inner iteration diminishingly requires less than $O(|E_o|)$. Thus the algorithm is effectively executed with less than $O(n|E_o|)$ complexity.

```
Input  : $G_o = (U_o, E_o)$
Output : $G'_o$
 1 Obtain $\Gamma_o$ from $G_o$ and $\Gamma'_o \subseteq \Gamma_o$
 2 while
 3    Get the length $l$ of the longest route among $\Gamma'_o$
 4    foreach $j = 1$ to $(l - 1)$
 5       foreach $\gamma'_i \in \Gamma'_o$ whose length satisfies $|\gamma'_i| == j$
 6          Calculate $\tilde{R}_{w_i}(t_k^{w_i})$ and $D_{w_i}(t_k^{w_i})$
 7       end
 8    end
 9    Initialize $hasRemovedNode \leftarrow false$
10    foreach $\gamma'_i \in \Gamma'_o$
11       if $\exists v \in \gamma'_i \setminus \{w_i\},\ s.t.\ \tilde{R}_v(t_k^v) < \varepsilon$ then
12          Remove the route $\gamma'_i$, i.e. $\Gamma'_o \leftarrow \Gamma'_o \setminus \{\gamma'_i\}$
13          Set $hasRemovedNode \leftarrow truth$
14       end
15    end
16    if $hasRemovedNode == false$ then
17       Break out of the while loop
18    end
19 end while
20 Build the subgraph $G'_o$ with $\Gamma'_o$
21 return $G'_o$
```

Algorithm 1 : The Iterative Algorithm

C. Vulnerability Estimation

We research the variation characteristics of the detected UCDs before and after unfriending each of o's direct friends respectively, and consequently estimate their vulnerabilities. Before that, the formulated definitions of disseminating intensity and disseminating contribution are given as prerequisites.

Disseminating Intensity. Within the detected UCD G'_o, we consider both probability and impact scope in the dissemination process of each involved node ϕ_i. It can be reflected by his disseminating probability $D_{\phi_i}(t_k^{\phi_i})$ and media capability S_{ϕ_i}. We propose disseminating intensity of G'_o to measure how widely and how deeply m_o is disseminated, which is given by

$$\mathbb{I}_o = \sum_{\phi_i \in G'_o} D_{\phi_i}(t_k^{\phi_i}) \times (S_{\phi_i} + 1) \tag{4}$$

where $(S_{\phi_i} + 1)$ is given to avoid $\mathbb{I}_o = 0$ when involved nodes are all direct friends of o with zero value of media capabilities.

Disseminating Contribution. If o unfriends his direct friend η_i, the subgraph $G_{o\setminus\eta_i} \subseteq G_o$ is constructed by removing relevant routes. A new UCD $G'_{o\setminus\eta_i}$ is then detected with a reduced disseminating intensity $\mathbb{I}_{o\setminus\eta_i}$, more or less, after the dissemination of m_o. By measuring the magnitude of diminution, we propose disseminating contribution of η_i to estimate his vulnerability, which is given by

$$\mathbb{C}_{\eta_i} = \mathbb{I}_o - \mathbb{I}_{o\setminus\eta_i} \tag{5}$$

Corresponding to the definition of vulnerable friend mentioned before, o's vulnerable friend $\hat{\eta}_o$, who has the largest disseminating contribution, is identified as below:

$$\hat{\eta}_o = \arg \max_{\eta_i \in DF_o} \mathbb{C}_{\eta_i} \tag{6}$$

IV. EXPERIMENTAL EVALUATION

In this section, we conduct an empirical study to validate the new insight into identifying the vulnerable friend.

A. Experiment Setup

Table 2: Original Dataset VS. Selected Dataset

	Facebook		Twitter	
	Original	**Selected**	**Original**	**Selected**
Amount of nodes	4,039	781	81,306	884
Amount of edges	88,234	3,149	1,768,149	3.910
Maximum diameter	8	8	7	7
Average diameter	4.7	4.2	4.5	4.4
Average value of I_v	0.76	0.73	0.56	0.53
Average value of L_v	0.57	0.55	0.51	0.49
Average value of S_v	0.02	0.02	0.44	0.43

The experiments are constructed on two real-world datasets, Facebook and Twitter [14], including node profiles and directed ego-networks (the undirected social structure in Facebook dataset is processed as a bidirectional graph). Due to the lack of ground truth, we assign uniform random probabilities to L_v of each node and α_{uv} of each edge. We randomly select 30 object users and their friend-networks from each dataset respectively. As shown in Table 2, the comparison between original and selected datasets proves that the random selection does not affect the methodology. We study the process of privacy information dissemination in each friend-network with PRD model, and compare the results before unfriending with that after unfriending through three Calculated Strategies (CS) and three Intuitive Strategies (IS) as follows.

1) (CS1) *Largest disseminating contributor:* The vulnerable friend $\hat{\eta}_o$ proposed in our work is unfriended.
2) (CS2) *Minimizing the V-index:* The direct friend whose removal lowers o's V-index the most [7] is unfriended.
3) (CS3) *Largest absolute-V:* The direct friend who has the largest absolute vulnerability [9] is unfriended.
4) (IS1) *Weakest privacy-protection consciousness:* The direct friend who has the smallest I_v is unfriended.
5) (IS2) *Strongest privacy leaking tendency:* The direct friend who has the largest L_v is unfriended.

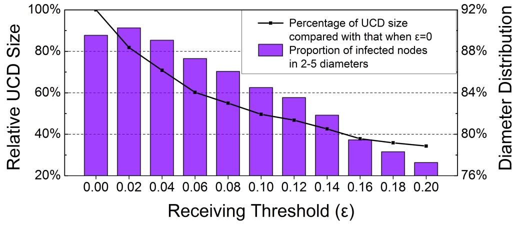
6) (IS3) *Highest media capability:* The direct friend who has the largest S_v is unfriended.

In order to comprehensively assess the performance of six strategies, we propose a series of evaluation indexes of the detected UCDs. All indexes are considered at an average level among 30 object users and their friend-networks.

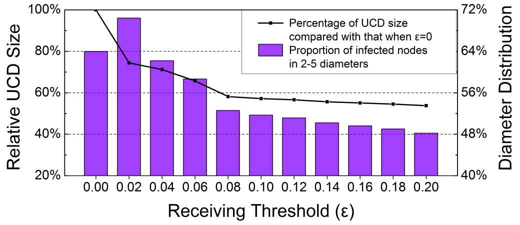
1) *Relative Disseminating Intensity (%):* The proportion of disseminating intensity compared with that before unfriending. It is defined as $\frac{\mathbb{I}_{o\setminus\eta_i}}{\mathbb{I}_o}$.
2) *Relative UCD size (%):* The proportion of the amount of nodes compared with that without receiving threshold or before unfriending. It is defined as $\frac{|U_{o,\varepsilon}|}{|U_{o,\varepsilon=0}|}$ or $\frac{|U_{o\setminus\eta_i}|}{|U_o|}$.
3) *Diameter distribution (%):* The proportion of the amount of nodes within different range of diameters compared with that before unfriending.
4) *Disseminating probability distribution (%):* The proportion of the amount of nodes within different range of L_v compared with that before unfriending.
5) *Media capability distribution (%):* The proportion of the amount of nodes within different range of S_v compared with that before unfriending.

B. Performance

The selection of ε is a challenge for a better simulation of true situation, in which information is propagated mostly within 2 to 5 hops [15]. It should block lesser nodes out of UCD and contain as much broader proportion of nodes between 2 to 5 diameters as possible. Figure 2 shows the relative UCD sizes and diameter distributions with different ε ranging from 0 to 0.2, and reveals that $\varepsilon = 0.02$ is adequate to the expectation. Multi-group experiments are then conducted under $\varepsilon = 0.02$ and the results are shown in Figure 3 and 4.



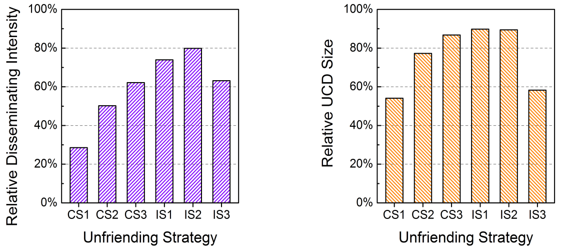
(a) Facebook



(b) Twitter

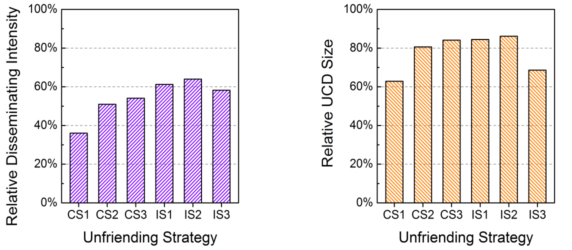
Figure 2: Selection of Receiving Threshold ε

Figure 3 shows the direct exhibition of vulnerability. All six unfriending strategies lead to varying degrees of reduction in disseminating intensity as expected. It decreases to 28% in Facebook dataset and 36% in Twitter dataset with CS1, which brings about an optimal protection against privacy leakage for object users. CS2 and CS3 do not perform as prominently as CS1, because they identify the vulnerable friend based on the impact of static attributes rather than that of dynamic behaviors. IS1 and IS2 perform bad based on the single factor of vulnerability, while the results of IS3 are slightly better with the consideration of topological structure.



(i) Relative Disseminating Intensity (ii) Relative UCD Size

(a) Facebook



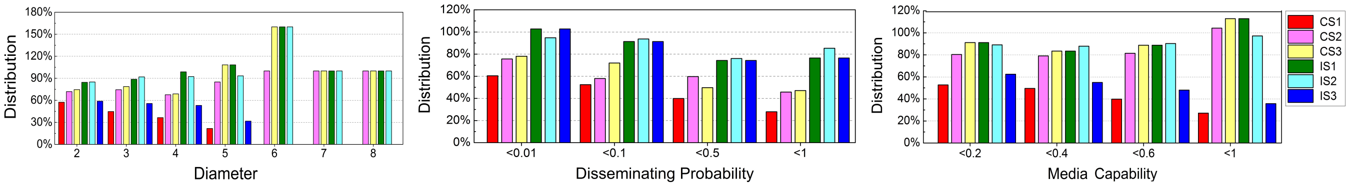
(i) Relative Disseminating Intensity (ii) Relative UCD Size

(b) Twitter

Figure 3: Performance Comparison when $\varepsilon = 0.02$

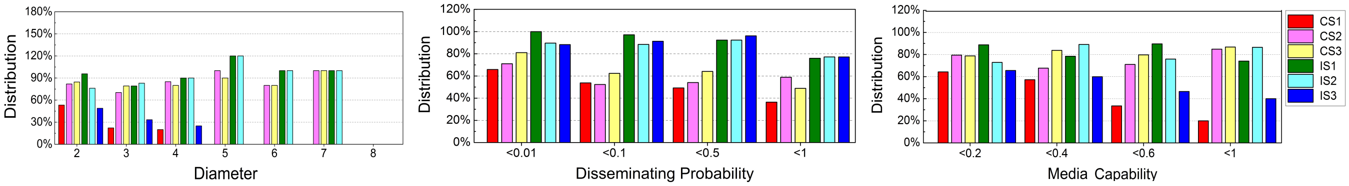
Next we take an in-depth study about how each strategy protects the object users. The relative UCD size in Figure 3 and diameter distribution in Figure 4 are considered firstly, which reflect the spread scope and depth respectively. Besides the maximum cutting of UCD size to 54% in Facebook dataset and 63% in Twitter dataset, CS1 successfully blocks those nodes with higher level of diameters. It means that the process of privacy information disseminating can be well controlled in terms of both scope and depth by CS1. The results of IS3 are almost as excellent as CS1, since it is directly correlated with topological structure. However, other strategies are of little effect towards the restriction of spread scope and depth due to the absence of consideration on topological structure.

Furthermore, we study the distributions of disseminating probability and media capability, which reflect the leakage strength and density within the disseminated range respectively. As shown in Figure 4, the two distributions of nodes are restricted to the maximum extent by CS1, and there is a tendency of more nodes being excluded with higher level of disseminating probability and media capability. It reveals that CS1 can adequately restrict the leakage strength and density of privacy information within the disseminated range. CS2 and CS3 perform weakly on leakage strength and much worse on leakage density. They even exhibit an increasing proportion of nodes with bigger media capabilities in Facebook dataset. The results of IS1 and IS2 are still bad since the single consideration of static attributes has much weak effect on



(i) Diameter Distribution (ii) Disseminating Probability Distribution (iii) Media Capability Distribution

(a) Facebook



(i) Diameter Distribution (ii) Disseminating Probability Distribution (iii) Media Capability Distribution

(b) Twitter

Figure 4: Distribution Performance when $\varepsilon = 0.02$

the dynamic process of dissemination. Based on topological structure, IS3 brings out a close-to-optimal result on the restriction of leakage density as CS1 does, but a feeble limiting effect on leakage strength similar to IS1 and IS2.

V. CONCLUSION

In this paper, we formulate the problem of vulnerable friend identification from a novel perspective with the dynamic process of privacy information dissemination. Based on an in-depth study about vulnerability, an asynchronous PRD model, which is specific to privacy information dissemination, is proposed to address this problem. Six unfriending strategies are validated empirically with a series of evaluation indexes. The observation of results provides a comprehensive externalization of their performance and proves that our work outperforms other strategies by a significant margin. Unfriending the vulnerable friend we suggested will offer an optimal protection for object users. In reality, whether one will be unfriended or not is further considered with his social utility [8]. Our work aims to identify the vulnerable friend through the assistance of unfriending and provides a significant proposal.

ACKNOWLEDGMENT

This work is supported by grants of the National Natural Science Foundation of China (61402045,61370197), the National High Technology Research and Development Program (2013AA013301), Specialized Research Fund for the Doctoral Program of Higher Education (20130005110011) and the Fundamental Research Funds for the Central Universities (2014RC1301).

REFERENCES

[1] S. Labitzke, F. Werling, J. Mittag, and H. Hartenstein, "Do online social network friends still threaten my privacy," in *Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy*, 2013, pp. 13–24.

[2] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor, "I regretted the minute I pressed share: a qualitative study of regrets on Facebook," in *Proceedings of the 7th ACM Symposium on Usable Privacy and Security*, 2011, p. 10.

[3] M. Sleeper, J. Cranshaw, P. G. Kelley, B. Ur, A. Acquisti, L. F. Cranor, and N. Sadeh, "I read my twitter the next morning and was astonished: a conversational perspective on twitter regrets," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2013, pp. 3277–3286.

[4] K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Addressing the privacy management crisis in online social networks." in *Proceedings of the 22th ACM International Conference on World Wide Web (Companion Volume)*, 2013, pp. 841–842.

[5] J. Chen, M. R. Brust, A. R. Kiremire, and V. V. Phoha, "Modeling privacy settings of an online social network from a game-theoretical perspective," in *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, 2013, pp. 213–220.

[6] A. Adhikari and S. D. Bachpalle, "Survey: evaluation study of privacy conflicts in osns," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3(11), 2013.

[7] P. Gundecha, G. Barbier, and H. Liu, "Exploiting vulnerability to secure user privacy on a social networking site," in *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2011, pp. 511–519.

[8] P. Gundecha, G. Barbier, J. Tang, and H. Liu, "User vulnerability and its reduction on a social networking site," *Transactions on Knowledge Discovery from Data (TKDD)*, vol. 9(2), p. 12, 2014.

[9] S. Alim, D. Neagu, and M. Ridley, "A vulnerability evaluation framework for online social network profiles: axioms and propositions," *International Journal of Internet Technology and Secured Transactions*, vol. 4(2), pp. 198–206, 2012.

[10] D. Pergament, A. Aghasaryan, and J.-G. Ganascia, "Reputation diffusion simulation for avoiding privacy violation," in *Proceedings of the 11st IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2012, pp. 401–408.

[11] T. N. Dinh, Y. Shen, and M. T. Thai, "The walls have ears: optimize sharing for visibility and privacy in online social networks," in *Proceedings of the 21st ACM International Conference on Information and Knowledge Management*, 2012, pp. 1452–1461.

[12] L. b. Othmane, H. Weffers, P. Angin, and B. Bhargava, "A time-evolution model for the privacy degree of information disseminated in online social networks," *International Journal of Communication Networks and Distributed Systems*, vol. 11(4), pp. 412–430, 2013.

[13] L. Ping and L. Zong, "Research on microblog information dissemination based on SNA centrality analysis: a case study with Sina microblog," *Intelligence, Information and Sharing*, vol. 8, pp. 71–72, 2010.

[14] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford large network dataset collection," http://snap.stanford.edu/data, Jun 2014.

[15] M. Cha, A. Mislove, and K. P. Gummadi, "A measurement-driven analysis of information propagation in the flickr social network," in *Proceedings of the 18th ACM International Conference on World Wide Web*, 2009, pp. 721–730.