Trust-based Privacy-Preserving Photo Sharing in Online Social Networks

Lei Xu¹, Ting Bao¹, Liehuang Zhu¹ and Yan Zhang²
¹School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, P. R. China
²Department of Informatics, University of Oslo, Oslo 0315, Norway
Email:¹xul04ster@gmail.com, tingbao@bit.edu.cn, liehuangz@bit.edu.cn ²yanzhang@ieee.org

Abstract—With the development of social media technologies, sharing photos in online social networks has now become a popular way for users to maintain social connections with others. However, the rich information contained in a photo makes it easier for a malicious viewer to infer sensitive information about those who appear in the photo. How to deal with the privacy disclosure problem incurred by photo sharing has attracted much attention in recent years. When sharing a photo that involves multiple users, the publisher of the photo should take into all related users’ privacy into account. In this paper, we propose a trust-based privacy preserving mechanism for sharing such co-owned photos. The basic idea is to anonymize the original photo so that users who may suffer a high privacy loss from the sharing of the photo cannot be identified from the anonymized photo. The privacy loss to a user depends on how much he trusts the receiver of the photo. And the user’s trust in the publisher is affected by the privacy loss. The anonymization result of a photo is controlled by a threshold specified by the publisher. We propose a greedy method for the publisher to tune the threshold, in the purpose of balancing between the privacy preserved by anonymization and the information shared with others. Simulation results demonstrate that the trust-based photo sharing mechanism is helpful to reduce the privacy loss, and the proposed threshold tuning method can bring a good payoff to the user.

Index Terms—social trust, anonymization, privacy preserving, photo sharing, online social networks.

I. INTRODUCTION

Social media [1], which enable people to interact with each other by creating and sharing information, has now become an imporation part of our daily life. Users of social media services create a huge amount of information in forms of text posts, digital photos or videos. Such user-generated content is the lifeblood of social media [2], [3]. However, user-generated content usually involves the creator’s sensitive information, which means the sharing of such content may compromise the creator’s privacy. How to deal with the privacy issues caused by information sharing is a long active topic in the study of social media [4], [5].

A major form of the content sharing activities in social media websites is the sharing of digital photos. Some popular online social networking services, such as Instagram¹, Flickr², and Pinterest³, are mainly designed for photo sharing. Compared to textual data, photos can deliver more detailed information to the viewer, which is detrimental to individual’s privacy. Moreover, the background information contains in a photo may be utilized by a malicious viewer to infer one’s sensitive information. On the good side, it is more convenient for a user to hide his sensitive information, without too much damage to insensitive information, by image processing (e.g. blurring) than by text editing.

In this paper we study the privacy issue raised by photo sharing in online social networks (OSNs). Privacy policies in current OSNs are mainly about how a user’s information will be explored by the service provider, and through which methods a user can control the scope of information sharing. Most OSNs offer a privacy setting function to their users [6]. A user can specify, usually based on his relationships with others, which users are allowed to access the photo he shares. It should be noted that the photo shared by a user may relate to other users. If the sharing of such photos is fully controlled by one user, then the privacy of other related users may be compromised. This privacy issue can be further explained via the following example. Suppose that Alice takes a photo of herself and her friend Bob, and then shares the photo to her colleague Charlie without telling Bob. If Bob does not know Charlie well, then the sharing of the photo will becomes a privacy invasion to Bob.

In the above example, the photo is actually co-owned by Alice and Bob. When Alice wants to share the photo with others, she should solicit Bob’s opinion, or at least, she should take some measures to reduce the possible privacy loss to Bob. For example, Alice can use a photo editing tool to make Bob’s face blurred, so that Bob can hardly be identified by Charlie. Given a photo, or more generally, a data item, related users usually have different opinions on whether a user is allowed to access it. Researchers have proposed different approaches to resolve the conflicts among users’ access control policies [7], [8], [9]. In most studies, an aggregated policy, which is essentially a set of users who are authorized to access the data item, will be generated by a mediator (e.g. the service provider). In our previous work [10], a trust-based mechanism is proposed for collaborative privacy management in OSNs. The proposed mechanism requires a user to solicit related users’ opinions before sharing a data item with others. The trust values between users are utilized to generate an aggregated option. By comparing the aggregated option with a threshold, the user decides whether to share the data item.

Lei Xu is the corresponding author.

1https://www.instagram.com/
2https://www.flickr.com/
3https://www.pinterest.com/
Previous studies usually consider the data item to be shared as a whole. That is to say, a user can either obtain all the information contained in the data item or get nothing. However, the aggregated access control policy cannot always make every related user satisfied. In the above example, suppose there is another user David in the photo taken by Alice. If both Alice and David want Charlie to have this photo and Bob does not, then the aggregated policy generated by a majority voting scheme will authorize Charlie to view this photo. As a result, Bob’s privacy is still compromised. While in fact, in the case of photo sharing, it is possible to completely resolve the conflicts among users’ privacy requirements, though it is hard to realize in the case of textual data sharing. The rationale is that a photo can be divided into multiple disjoint areas. Each area can be correlated to a specific user. If we delete this area or make the area blurred, then the corresponding user’s privacy can be preserved when the photo is accessible to an undesired user.

In this paper, we consider a photo-sharing scenario where the user who publishes the photo, referred to as publisher, decides how to process the photo so as to protect privacy of related users. A trust-based mechanism is proposed to help the publisher make a proper decision. Different from our previous work [10], the publisher does not communicate with other related users before he posts the photo. Instead, the publisher predicts the privacy loss to each related user in case that the photo is shared with a certain user. We explore the trust between users to measure the privacy loss. The basic idea is that whether a user allows another user to learn his sensitive information depends on how much the former trusts the latter. Also, whether a user is willing to protect another user’s privacy depends on how much the former trusts the latter. Basically, if the publisher predicts a high privacy loss to a related user who is also highly trusted by the publisher, then the publisher will “delete” the user from the photo by processing the corresponding area of the photo.

Those related users are not directly involved in the decision-making process of the publisher. After the photo is processed and sent to the user designated by the publisher, each related user can evaluate whether his privacy is disclosed. If the user suffers a privacy loss, he will lose trust in the publisher. And if the user finds that his privacy is protected by the publisher, he may have more trust in the publisher. Due to the correlation between privacy and trust, the publisher will not ignore other users’ privacy when sharing photos. Intuitively, if the publisher deletes all users from the photo, then no one will suffer a privacy loss, and the publisher will gain more trust from others. As a result, the publisher’s privacy will be more valued by other users. However, with all user-related information being deleted, the sharing of the photo becomes meaningless. In the proposed mechanism, a threshold is introduced to control the number of users deleted from a photo. To find a balance between privacy preserving and photo sharing, we propose a method to make the threshold adaptive to the trust relationship between users. The main contributions of this paper are summarized as follows:

- A trust-based mechanism is proposed for photo sharing in OSNs. The trust values between users are utilized to determine whether a user’s privacy will be protected. The trust values are updated according to the privacy loss, and the proposed mechanism can prevent the user from ignoring other users’ privacy.
- To balance between photo sharing and privacy preserving, we propose a method to tune the threshold that determines the number of users deleted from a photo.
- We have conducted a series of simulations to demonstrate the effectiveness of the proposed methods.

The rest of the paper is organized as follows. Section II introduces some studies on the privacy issues of photo sharing. Section III describes the basic model of photo sharing in OSNs and the trust evaluation model. The trust-based photo anonymization approach is presented in Section IV. And the method proposed for threshold tuning is described in Section V. Simulation results are presented in Section VI. Finally, conclusions are drawn in Section VII.

II. RELATED WORK

A. Privacy Management of Photo Sharing

The sharing of multimedia content has now become quite popular in online social networks. Compared to textual content, multimedia content are more appealing to users [11]. The large-scale and rapid spread of multimedia content may cause a great loss to individual’s privacy if the content contains sensitive information about the individual. Specifically, when a user shares a photo with others, all users related to this photo face a risk of privacy disclosure. Researchers have begun to investigate such privacy issues. It is generally believed that the sharing of the photo should be controlled by all the related users. In [12], Yuan et al. proposed a privacy-preserving photo sharing framework which uses visual obfuscation technique to protect users’ privacy. When processing a photo, the proposed framework considers both the content and the context of a photo. In [13], Xu et al. designed a mechanism that enables all the related users of a photo participate in the decision-making process of photo sharing. With the help of a facial recognition technique, they developed a distributed consensus-based method to generate the final decision. Based on the encryption algorithm proposed in [14], Ma et al. proposed a key management scheme to authorize and repeal a user’s privilege of accessing multimedia data [15].

With the help of image processing techniques, we can realize a fine-grained privacy management of photo sharing. In [16], Iliya et al. proposed an access control model for photo sharing, where a photo is transformed into a set of layers each of which contains a single blurred face. Based on each user’s privacy policy, the final photo presented to a viewer is generated by superimposing certain layers. In [17], Lee et al. proposed a multiparty access model for photo sharing in OSNs, where the granularity of access control can be gradually tuned from photo level to face level. In [18], Vishwamitra et al. proposed a collaborative privacy management approach for photo sharing in OSNs. The proposed approach considers the personally identifiable information (PII) items in a photo, and designs a conflict resolution method for PII-level access control policies. The photo sharing mechanism proposed in...
this paper also aims at a fine-grained privacy protection for users. Different from previous studies, the mechanism proposed in this paper does not utilize the access control policies of related users to make the decision on photo sharing. Instead, the service provider estimates the privacy loss to each related user, and then decides which users’ privacy should be preserved.

B. Trust-based Privacy-Preserving Approaches

Trust plays an important role in online social networks [19]. The trust relationship between users has been explored to deal with the access control problem. In the decentralized online social network proposed by Datta et al. [20], a user can tell another user with whom he trusts most to store his profile. Based on the access control policies provide by other users, a user can decide with whom to share the sensitive information. In [21], Rathore et al. proposed a trust-based access control model for resource sharing. The model considers the authorization requirements of all related users. And the trust between users is utilized to resolve the conflict among different users’ access control policies. In [22], Gay et al. proposed a relationship-based access control mechanism with which users can control how their data are reshared. And they built a trust model to quantify user relationships. In [23], Yu et al. applied deep learning algorithm to determine the privacy settings for photo sharing. During the training of learning models, both the content sensitiveness of the photo and the trustworthiness of the users with whom the photo is shared are considered. In this paper, we also utilize the trust values to determine with whom a photo can be shared. While different from previous studies, the trust values in the proposed mechanism are associated with users’ privacy loss: the privacy loss to a user is dependent on his trust in others, and a user will lose trust of other users if he causes privacy loss to them.

III. SYSTEM MODEL

A. Graph Representation of an Online Social Network

Consider an online social network (OSN) which consists of \( N \) users. The network can be represented by a directed graph \( G \equiv (V, E) \) with \( V \) being the set of vertices and \( E \) being the set of edges. Each vertex \( v_i \in V \) (\( i = 1, 2, \cdots, N \)) represents a user. Throughout this paper, unless otherwise stated, we use the two terms vertex and user interchangeably to refer to a real entity in an OSN. Given two users \( v_i, v_j \in V \) (\( i \neq j \)), the edge from user \( v_i \) to user \( v_j \) (if exists) is denoted as \( e_{ij} \). The edge indicates a certain relationship between the two users, e.g., user \( v_i \) is the employer of user \( v_j \). Here in this paper we define that as long as user \( v_i \) knows user \( v_j \), there is an edge \( e_{ij} \) between them. And we refer to \( v_j \) as a friend of \( v_i \).

B. Sharing Co-owned Photos

Suppose that user \( v_i \) wants to share a sensitive photo \( d \) with user \( v_j \). We refer to \( v_i \) as the publisher and \( v_j \) as the recipient. By sensitive we mean that one or more users can be identified in the photo. We refer to such users as stakeholders, and denote the set of stakeholders related to a photo \( d \) as \( S_d \).

When there are more than one users in \( S_d \), we say the photo \( d \) is co-owned by the stakeholders. It should be noted that user \( v_i \) is not necessarily included in \( S_d \). If \( v_i \notin S_d \), it is very likely that the photo is originally created by some other user, and \( v_i \) wants to share it with a third user \( v_j \).

The sharing of \( d \) may disclose privacy of the stakeholders. If the recipient \( v_j \) himself is a stakeholder of \( d \), which means \( v_j \) has the right to access \( d \), then \( v_i \) can share \( d \) with \( v_j \) directly. Otherwise, user \( v_i \) should, in principle, ask all the stakeholders for permission beforehand. However, different stakeholders generally have different opinions on whether the photo \( d \) can be shared to user \( v_j \), and it is difficult for the publisher \( v_i \) to make a decision. An intuitive way to deal with this problem is to treat the photo as a collection of personally identifiable data items \( \{d_k \}_{v_k \in S_d} \). If a stakeholder \( v_k \in S_d \) does not want to the photo to be shared with user \( v_j \), then the publisher \( v_i \) can just “delete” the corresponding data item \( d_k \) from \( d \) (e.g. by blurring user \( v_k \)’s face). After this photo anonymization process, the anonymized photo \( d' \) can be sent to the recipient \( v_j \).

To ease the burden of the publisher and stakeholders, in this paper we require the service provider (SP) of the OSN to do the anonymization work. The basic idea is that the publisher \( v_i \) first uploads the photo \( d \) to the SP. Then, the SP estimates the privacy loss to each stakeholder and determines which stakeholders should be deleted. The recipient will get the anonymized photo \( d' \) from the SP. In Section IV, we will discuss how the trust between users can be utilized in the above process.

C. Trust Evaluation

Trust is generally understood as a subjective concept. To conduct a formal analysis of the impact of trust on users’ photo sharing behaviors, we use a scalar to quantify the degree of trust. Given two users \( v_i, v_j \in V \) (\( i \neq j \)), we denote user \( v_i \)’s trust in user \( v_j \) as \( t_{ij} \). And we define \( 0 \leq t_{ij} \leq 1 \). A high value of \( t_{ij} \) indicates user \( v_j \) is highly trusted by user \( v_i \). It should be noted that user \( v_j \)’s trust in user \( v_i \), denoted as \( t_{ji} \), is generally different from \( t_{ij} \). One user’s trust in another is closely related to the type of the relationship between the two users. For example, a user usually trusts his family members more than his colleagues. Moreover, the value of trust constantly changes as the interactions between the two users become more. Specially, one will lose the trust of others if he causes a damage to others in some way. Given the network represented by \( G \), we first utilize the edge information to determine the initial trust values between users. That is, before user \( v_i \) and user \( v_j \) interact with each other, \( t_{ij} \) is set to a positive number if the edge \( e_{ij} \) exist, otherwise \( t_{ij} \) is set to 0. Then, \( t_{ij} \) is updated based on the interactions between the two users. Details of the update rule will be discussed in the following section.

IV. TRUST-BASED PHOTO ANONYMIZATION

Current OSNs impose no restriction on the sharing of co-owned photos. When a publisher shares a co-owned photo with others, some stakeholders’ privacy may be disclosed. To
reduce the privacy loss caused by photo sharing, in this section we propose an anonymization mechanism which preserves a stakeholder’s privacy by deleting his personally identifiable items from the photo. The key of the proposed mechanism is to associate trust with privacy loss. Next we first describe the trust-based mechanism, and then analyze how this mechanism can motivate a user to protect others’ privacy.

A. Associate Trust with Privacy Loss

When user \( v_i \) wants to share a sensitive photo \( d \) with user \( v_j \), he first uploads the photo to the SP. It is assumed that all the users appearing in the photo have been tagged by the publisher, or they can be identified by the SP via some face recognition technique. Either way, the SP can determine the stakeholders of the photo. After that, the SP estimates the privacy loss to each stakeholder. For any \( v_k \in S_d \), if the recipient \( v_j \) is able to identify \( v_k \) in the photo sent from the SP, user \( v_k \) may suffer a privacy loss. We use \( l_{jk}^{(d)} \) to denote the loss. Intuitively, the more user \( v_k \) trusts user \( v_j \), the less privacy loss user \( v_k \) will perceive. The value of \( l_{jk}^{(d)} \) also depends on how sensitive, from the perspective of user \( v_k \), the photo is. The more sensitive the photo is, the more privacy loss user \( v_k \) will perceive. Therefore, we define \( l_{jk}^{(d)} \) as

\[
l_{jk}^{(d)} = f_{loss} \left( t_{kj}, \delta_k^{(d)} \right),
\]

where \( t_{kj} \) denotes user \( v_k \)’s trust in user \( v_j \), \( \delta_k^{(d)} \) denotes the user-specific sensitivity of \( d \). The function \( f_{loss} \) is a decreasing function of \( t_{kj} \) and an increasing function of \( \delta_k^{(d)} \). For example, we can define \( f_{loss} \) as

\[
f_{loss} \left( t_{kj}, \delta_k^{(d)} \right) = (1 - t_{kj}) \delta_k^{(d)}.
\]

It is assumed that the SP knows the trust values between users. While the sensitivity \( \delta_k^{(d)} \) is only known to user \( v_k \) himself for now. Hence, the SP can only make an estimate of the privacy loss. The estimated privacy loss \( \tilde{l}_{jk}^{(d)} \) is defined as

\[
\tilde{l}_{jk}^{(d)} = f_{loss} \left( t_{kj}, \hat{\delta}_k \right),
\]

where \( \hat{\delta}_k \in [0, 1] \) is a constant specified by the SP.

Given the estimated privacy loss to each stakeholder, the SP can decide how to anonymize the photo. We use a binary variable \( p_k \) to indicate whether the stakeholder \( v_k \) can be identified in the anonymized photo \( d' \). Intuitively, if \( \tilde{l}_{jk}^{(d)} \) is high, then the SP should delete the identifiable data items of \( v_k \) from the photo, and there is \( p_k = 0 \). Considering that it is the publisher \( v_i \) who wants to share the photo, the SP should also take the publisher’s opinion into account when making the decision. To this end, we introduce a parameter \( \theta_i \) and define the anonymization rule as

\[
p_k = \begin{cases} 0, & \text{if } t_{ik} \tilde{l}_{jk}^{(d)} \geq \theta_i, \\ 1, & \text{otherwise}, \end{cases}
\]

According to above rule, the estimated privacy loss \( \tilde{l}_{jk}^{(d)} \) is weighted by the trust value \( t_{ik} \). The idea is that the more the publisher \( v_i \) trusts the stakeholder \( v_k \), the more the publisher values his relationship with the stakeholder, and the more the publisher is willing to protect the stakeholder’s privacy. The threshold \( \theta_i \in [0, 1] \) indicates how much the publisher \( v_i \) values other users’ privacy. A low value of \( \theta_i \) implies that the stakeholders’ privacy will be well preserved. In an extreme case where \( \theta_i = 0 \), every stakeholder will be deleted from the photo, which means the publisher \( v_i \) shares no information with the recipient \( v_j \). Contrarily, when \( \theta_i = 1 \), namely the publisher does not care about others’ privacy, the SP will not make any change to the photo.

The SP processes the photo \( d \) according to \( \{ p_k \}_{v_k \in S_d} \). Then the SP sends the anonymized photo \( d' \) to the recipient \( v_j \). It is assumed that the SP will inform every stakeholder that the photo \( d' \) is accessible to \( v_j \). Each stakeholder \( v_k \) can then evaluate his privacy loss and report the actual loss to the SP. Depending on how much the privacy loss is, the trust of stakeholder \( v_k \) in the publisher \( v_i \), denoted as \( t_{ki} \), may increase or decline. The whole process of photo sharing is illustrated in Fig. 1.

The SP updates the trust value via the following rule

\[
t_{ki}' = \begin{cases} f_{trust} (t_{ki}, l_{jk}^{(d)}) & \text{if } p_k = 0, \\ f_{trust} (t_{ki}, -l_{jk}^{(d)}) & \text{otherwise}, \end{cases}
\]

where \( t_{ki}' \) denotes the updated trust value. The function \( f_{trust} (x, y) \) satisfies:

- \( \forall x \in [0, 1], \forall y \in (-\infty, \infty) \), there is \( 0 \leq f_{trust} (x, y) \leq 1 \);
- Given \( x \in [0, 1] \), \( f_{trust} (x, y) \) is a decreasing function of \( y \);
- \( \forall x \in [0, 1], \) if \( y \geq 0 \), then there is \( f_{trust} (x, y) \leq x \);
- \( \forall x \in [0, 1], \) if \( y \leq 0 \), then there is \( f_{trust} (x, y) \geq x \).

According to the update rule defined above, if the stakeholder \( v_k \) can be identified in the anonymized photo, then he will suffer a privacy loss \( l_{jk}^{(d)} \) and lose trust in the publisher \( v_i \) (i.e. \( t_{ki}' \leq t_{ki} \)). The higher the privacy loss is, the lower the trust value will be. On the contrary, if the stakeholder \( v_k \) is deleted from the photo, then he will have more trust in the publisher \( v_i \) (i.e. \( t_{ki}' \geq t_{ki} \)), since his privacy is preserved. In such a case, \( l_{jk}^{(d)} \) denotes the privacy loss that the stakeholder could have suffered from the sharing of the photo. The more privacy loss the publisher prevents, the more the trust value will increase. To make the update rule works, each stakeholder shall provide a feedback \( l_{jk}^{(d)} \) to the SP after the photo is shared, whether he suffers a privacy loss or not. If the stakeholder provides no feedback to the SP, then the SP just presumes that the stakeholder has no privacy loss. An instantiation of \( f_{trust} \) is given by

\[
f_{trust} (x, y) = \min \left( \frac{2x}{1 + ey}, x \right), \forall x \in [0, 1], y \in (-\infty, \infty),
\]

where the function \( \frac{2x}{1 + ey} \) has the property that the decrease of the trust value caused by a privacy loss is equal to the increase of the trust value if the same amount of privacy loss is prevented. And we use the \( \min \) function to make sure that the updated trust value is no larger than 1.

As mentioned earlier, before the photo is sent to the recipient, the SP can only estimate the privacy loss of a stakeholder
B. The Motivation of Privacy Protection

The trust relationship between users is thoroughly explored in the photo sharing mechanism described above. On one hand, the trust of a stakeholder in the recipient is utilized to measure the privacy loss of the stakeholder. On the other hand, the trust of the publisher in the stakeholder is utilized to measure how much the publisher cares about the privacy loss to the stakeholder. Moreover, the trust of a stakeholder in the publisher is updated according to privacy loss of the stakeholder. By incorporating trust into the photo anonymization rule (see (4)) and incorporating privacy loss into the trust update rule (see (5)), we can prevent the users from ignoring the privacy issue when sharing photos with others. As a result, everyone’s privacy can be better preserved.

In the proposed mechanism, we introduce a threshold $\theta_i$ to quantify how much user $v_i$ cares about other users’ privacy. If user $v_i$ does not care about others’ privacy, i.e. $\theta_i = 1$, then whenever user $v_i$ wants to share a photo $d$ related to user $v_k$ with a third user, he will cause a privacy loss to $v_k$ as long as $v_k$ is sensitive to the photo (i.e. $\delta_k^d > 0$). As a result, user $v_i$ loses user $v_k$’s trust gradually. Suppose that at some point, user $v_k$ wants to share a photo $\tilde{d}$ related to user $v_i$ with a third user $v_j$. Since user $v_k$ has a low trust in user $v_i$, user $v_k$ does not care whether he will cause a privacy loss to user $v_i$, even if user $v_i$ is very sensitive to the photo $\tilde{d}$ and extremely reluctant to show the photo to user $v_j$. As a result, user $v_i$ suffers a privacy loss because of the sharing of $\tilde{d}$, and his trust in user $v_k$ declines. Next time when user $v_i$ wants to share a photo related to user $v_k$, if user $v_k$’s privacy loss is still ignored by $v_i$, user $v_k$’s trust in user $v_i$ becomes even lower.

From the above discussion we can see that, if a user pays no attention to other users’ privacy, then the relation between users will be deteriorating, in the sense that the trust values decline over time. The consequence is that everyone suffers a great privacy loss from the photo sharing activities. Given the proposed photo anonymization rule and the trust update rule, a user who wants to protect his own privacy should also protect other users’ privacy by specifying a positive threshold. If user $v_i$ sets the threshold $\theta_i$ to a low value, then when he shares a photo, most stakeholders’ privacy will be protected. As a result, user $v_i$ gains more trust of the stakeholders. Next time when these stakeholders share photos related to user $v_i$, it is less likely that user $v_i$ will suffer a privacy loss. In Section VI, we have conduct a series of simulations to demonstrate the influence of the threshold on user’s privacy loss.

When $\theta_i$ is set to 0, user $v_i$ will never compromise other users’ privacy, which means he will be highly trusted by others and his privacy will be well protected by others. However, in such a case, user $v_i$ shares no information with others. This contradicts to the user’s intention to join a social network. In the following section we will discuss how to tune the threshold so as to achieve a balance between privacy preserving and photo sharing.
V. TRADE-OFF BETWEEN PHOTO SHARING AND PRIVACY PRESERVING

The trust-based photo sharing mechanism proposed in the above section encourages users to protect other users’ privacy. However, a high degree of photo anonymization causes too much information loss, which has a negative effect on photo sharing. How to make a trade-off between data sharing and privacy preserving has always been an important issue in the study of data privacy [24], [25], [26], [27], [28]. In this section, we first describe how to formulate the publisher’s payoff by considering both the privacy loss and the benefit brought by photo sharing. Then we discuss how the publisher should set the threshold \( \theta \) so as to get a good payoff.

A. Payoff to the Publisher

Consider a user \( v_i \in V \) who continually shares photo with others. Suppose that at time point \( t \in \{1, 2, \cdots \} \), the user wants to share a photo \( d \) with user \( v_j \). As described in Section IV-A, user \( v_i \) first uploads the photo to the SP. Then according to the threshold \( \theta_i \) set by user \( v_i \), the SP can decide how to anonymize the photo. After that, the anonymized photo \( d' \) is published to user \( v_j \). The anonymization operation is beneficial to the stakeholders in the sense that the stakeholders’ privacy can be preserved. However, anonymization causes information loss, which is not preferred by the publisher \( v_i \), since he cannot share the information as he wants to. The more stakeholders the SP deletes from the photo, the less information user \( v_i \) can share with user \( v_j \), and the less satisfaction user \( v_i \) will feel. The benefit that user \( v_i \) gets from the sharing of \( d \) is defined as

\[
e_{\tau} = \frac{|S_d|}{|S_d'|}. \tag{7}
\]

where \( S_d \) denotes the set of users appearing in the original photo \( d \), \( S_d' \) denotes the set of users appearing in the anonymized photo \( d' \), and \( |A| \) denote the cardinality of set \( A \).

The benefit ranges from 0 to 1. If there is no stakeholder deleted by the SP (e.g. in the case of \( \theta_i = 1 \)), user \( v_i \) can get the maximal benefit. If all the stakeholders are deleted (e.g. in the case of \( \theta_i = 0 \)), user \( v_i \) gets zero benefit. Given the photo \( d \), according to the anonymization rule defined in (4), the size of \( S_d' \) is dependent on the threshold \( \theta_i \), user \( v_i \)'s trust in each stakeholder, each stakeholder’s trust in user \( v_j \), and the sensitivity \( \delta_{ki}(d) \) specified by each stakeholder. That is to say, given a photo \( d \) and current trust values between users, the benefit \( e_{\tau} \) changes with the threshold \( \theta_i \).

The sharing of the photo will cause privacy loss to some of the stakeholders. For each stakeholder \( v_k \in S_d \), his trust in user \( v_i \) changes after the anonymized photo \( d' \) is published to user \( v_j \). We consider the total change of the trust values and define the cost of photo sharing as

\[
c_{\tau} = \frac{\sum_{v_k \in S_d} t'_{ki}}{\sum_{v_k \in S_d} t_{ki}}. \tag{8}
\]

We refer to the sum of the trust values as user \( v_i \)'s reputation among the stakeholders.

According to the update rule defined in (5), a stakeholder’s trust in the publisher will decrease if he suffers a privacy loss. Otherwise, the stakeholders will have more trust in the publisher. That is to say, the cost \( c_{\tau} \) can either larger than or smaller than 1. The variation of \( t_{ki} \) depends on the privacy loss \( t'_{ki} \) perceived by the stakeholder \( v_k \), where the privacy loss is determined by the threshold \( \theta_i \), the trust value \( t_{kj} \), and the sensitivity \( \delta_{ki}(d) \). Therefore, given the photo \( d \) and current trust values between users, the value of \( c_{\tau} \) is determined by the threshold \( \theta_i \).

The payoff that user \( v_i \) gets from the sharing of the photo is defined as

\[
u_{\tau} = f_{\text{payoff}}(e_{\tau}, c_{\tau}), \tag{9}
\]

where the function \( f_{\text{payoff}} \) should satisfy the following two conditions. First, given \( e_{\tau} \), the payoff increases with \( c_{\tau} \). Second, given \( c_{\tau} \), the payoff increases with \( e_{\tau} \). An instantiation of the payoff function is given by

\[
f_{\text{payoff}}(e_{\tau}, c_{\tau}) = \begin{cases} e_{\tau}^c, & \text{if } c_{\tau} \geq 1, \\ e_{\tau}^{1-c_{\tau}}, & \text{if } 0 \leq c_{\tau} < 1. \end{cases} \tag{10}
\]

B. Tune the Threshold

From above discussion we know that given the photo \( d \) and the trust values between users, the payoff \( u_{\tau} \) can be seen as a function of the threshold \( \theta_i \). The objective of the user is to find the optimal threshold \( \theta^* \) that maximizes the payoff. However, the user cannot solve the optimization problem by himself. For user \( v_i \), some of the parameters required to compute the payoff, including the trust values \( \{t_{ki}, t_{kj}\}_{v_k \in S_d} \) and the sensitivities \( \{\delta_{ki}(d)\}_{v_k \in S_d} \), cannot be directly observed. Suppose that the SP will tell user \( v_i \) his current reputation among the stakeholders. Then only after the photo is anonymized and published to user \( v_j \), user \( v_i \) can compute the payoff corresponding to the threshold he has chosen. Considering that the trust values between users are actually evaluated by the SP, we propose the following solution.

Considering that the relationship between the threshold and the payoff is complicated and indeterminate, we restrict the value of the threshold \( \theta_i \) to be a finite set \( \Theta = \{0, \frac{1}{K}, \frac{2}{K}, \cdots, 1\} \), where \( K \) is a positive integer. As mentioned before, the payoff to user \( v_i \) is dependent on the sensitivity \( \delta_{ki}(d) \) specified by each stakeholder, and \( \delta_{ki}(d) \) is unknown to the SP, unless the SP has received a privacy loss report from the stakeholder \( v_k \). Therefore, as long as there is a stakeholder who has never reported privacy loss to the SP before, the SP cannot determine the analytical form of the payoff function, not to mention deriving the optimal threshold.

In addition to discretizing the threshold, we make another simplification. Given a photo \( d \), the sensitivity \( \delta_{ki}(d) \) indicates how much the stakeholder \( v_k \) is sensitive to the photo. The sensitivity is not only user-specific, but also data-specific. If user \( v_i \) wants to share another photo \( d' \) related to \( v_k \) at time \( \hat{\tau} \), the SP cannot use the sensitivity \( \delta_{ki}(d) \) inferred from user \( v_k \)'s privacy loss reported at time \( \tau \) to compute the privacy loss of \( v_k \) at time \( \hat{\tau} \), since generally \( \delta_{ki}(d') \) is different from \( \delta_{ki}(d) \). Due to the data-specific property, the information that
the SP learns from the past is of little help to the choice of the threshold for new photos. Nevertheless, we can explore the user-specific property to make past experience useful. We assume that given a user $v_k$, the sensitivity $\theta_k^{(d)}$ corresponding to any photo $d$ follows the same probability distribution. The expected value of $\theta_k^{(d)}$, denoted as $\tilde{\theta}_k$, indicates how much user $v_k$ cares about his own privacy. We refer to $\tilde{\theta}_k$ as the user’s sensitivity.

When searching the optimal threshold, we replace the data-specific $\theta_k^{(d)}$ in (2) with the data-independent $\tilde{\theta}_k$. With this approximation, the SP can use the information learnt from past to compute the privacy loss of stakeholders and the payoff to the publisher. When a user, say $v_k$, reports a privacy loss to the SP for the first time, the SP computes the sensitivity $\theta_k$ by using the reported loss and $v_k$’s trust in the recipient. Next time when user $v_k$ becomes a stakeholder of some photo, the SP can determine user $v_k$’s privacy loss before the photo is published to the designated recipient.

With above simplifications, the SP can find a proper threshold $\tau_i$ for user $v_i$ whenever $v_i$ wants to share a photo. The SP maintains a hash table which consists of users who have reported privacy loss and their sensitivity values. Given a photo $d$ to be shared at time $\tau$ and the corresponding stakeholders $S_d$, the SP first computes a payoff $\bar{u}_\tau(\theta)$ for each $\theta \in \Theta$, and then chooses the optimal one $\theta^* \triangleq \arg \max_{\theta} \bar{u}_\tau(\theta)$. To compute the payoff, the SP needs to predict the privacy loss to each stakeholder. Given $v_k \in S_d$, the SP checks if $v_k$ exists in the hash table. If exists, the SP uses the corresponding sensitivity $\theta_k$ to computes the privacy loss to $v_k$. Otherwise, the SP uses a pre-specified constant $\delta$ to estimate the privacy loss.

It should be noted that the privacy loss computed by the SP is not necessarily equal to the actual loss perceived by the stakeholder, since the stakeholder’s sensitivity may not be known by the SP. Hence, the payoff $\bar{u}_\tau(\theta)$ computed by the SP is different from the actual payoff obtained by the publisher $v_i$, unless all the stakeholders in $S_d$ have been recorded in the hash table. And the optimal threshold $\theta^*$ may be different from the actual one $\theta^* \triangleq \arg \max_{\theta} u_\tau(\theta)$. The threshold $\theta^*$ chosen by the SP is provided to user $v_i$ as a reference. User $v_i$ determines $\theta_i$ in a stochastic way: set $\theta_i$ to a value randomly chosen from $\Theta$ with a certain probability $\epsilon \in [0, 1]$; and set $\theta_i = \theta^*$ with probability $1 - \epsilon$. Based on the user’s final decision $\theta_i$, the SP conducts photo anonymization and sends the anonymized photo to the designated recipient. After receiving privacy loss reports from stakeholders, the SP updates the hash table by adding a new pair $(v_k, \delta_k)$ where $\delta_k$ is the inferred sensitivity of user $v_k$.

VI. SIMULATION

To deal with the privacy issue caused by the sharing of co-owned photos in online social networks, we propose a trust-based photo sharing mechanism in Section IV. And to make a better trade-off between photo sharing and privacy preserving, we propose a service provider-assisted method to adaptively tune the threshold that determines how the photo will be anonymized. In order to evaluate the feasibility and effectiveness of the proposed approaches, we conduct a series of simulations on both synthetic and real-world social networks. In this section, we first describe how the networks are constructed and how the simulation environment is set. Then we present the simulation results of the photo sharing mechanism. After that, we describe how to simulate the tuning process of the threshold and present the simulation results.

A. Experiment Setting

1) Dataset: Simulations are conducted on both synthetic data and real-world data. As we’ve done in [29], we generate a scale-free network and a small-world network with the help of the matlab package developed by Muchnik [30]. Both of the two networks consist of 1000 nodes. The average node degree of each network is 20. There are 20021 undirected edges in the scale-free network and 20000 undirected edges in the small-world network. The real-world data come from Stanford large network dataset collection [31]. The facebook dataset is chosen for simulation. The network consists of 1133 nodes and 10902 undirected edges. The average node degree is about 19.

2) Trust Initialization: Given a network, we initialize the trust values between users via two different approaches. The first approach utilizes the transitivity property of trust [32] to determine the initial trust value. Specifically, for any two users $v_i$ and $v_j$, the initial value of $t_{ij}$ is set to $0.8^{d_{ij}}$, where $d_{ij}$ denotes the length of the shortest path between the two users. If there is no path between them, namely the two users are disconnected, the initial value of $t_{ij}$ is set to 0. Though this distance-based approach sets $t_{ij}$ and $t_{ji}$ to the same initial value, as time goes by, the two trust values will become different, since $t_{ij}$ is affected by user $v_j$’s behavior and $t_{ji}$ is affected by user $v_i$’s behavior. The second initialization approach is to set $t_{ij}$ to a value chosen from $[0, 1]$ uniformly at random, for any pair of $v_i$ and $v_j$. In such a case, $t_{ij}$ and $t_{ij}$ generally have different initial values.

3) Experiment Setup: To simulate the trust-based mechanism proposed in IV, first we need to setup the photo sharing scenario for a given network. We consider a discrete time model. At each time point $\tau \in \{1, 2, ..., T\}$, we randomly select a group users as the publishers. The number of the publishers is given by $\rho N$, where $N$ denotes the total number of users in the network, and $\rho \in [0, 1]$ is a tunable parameter. For each publisher $p$, the photo that he wants to share is represented by the stakeholders and corresponding sensitivities. The stakeholders are randomly selected from all users. And we define that the number of stakeholders is at most 20, since the average node degree of the network is 20 or so. Each stakeholder’s sensitivity with respect to the photo is chosen from $[0, 1]$ uniformly at random. The recipient of the photo is randomly selected from the set of the publisher’s friends. Considering that the recipient may reshare the photo with other users, we construct a forward chain for the photo published by $p$. The publisher $p$, which is the head of the forward chain, is followed by the recipient $r_1$. And the recipient $r_1$ is followed by a user $r_2$ randomly chosen from the set $F_{r_1} \setminus \{p\}$, where $F_{r_1}$ denotes the set of $r_1$’s friends. This means that user $r_1$
will forward the photo to $r_2$. User $r_2$ is followed by a user $r_3$ randomly chosen from the set $F_{r_2} \setminus \{p, r_1\}$, and so on. The length of the forward chain, denoted as $L_f$, is pre-specified.

### B. Trust-based Photo Anonymization

We simulate the trust-based mechanism proposed in Section IV via the following way. Given a network, we first use the method described above to determine the initial trust values and setup the photo sharing scenario. The threshold used in the proposed mechanism is chosen from the set $\Theta \triangleq \{0, 0.05, 0.1, \cdots , 0.45, 0.5\}$. Given any $\theta \in \Theta$, we set the threshold of every user to $\theta$, and then simulate the photo sharing activities of users. At each time point $\tau \in \{1, 2, \ldots , T\}$, given a publisher and the corresponding recipient, we first estimate the privacy loss to each stakeholder by using a constant sensitivity $\delta$. Then by comparing the privacy loss to $\theta$, we determine whether a stakeholder should appear in the anonymized photo. After that, we compute the actual privacy loss to each stakeholder by using the random sensitivity chosen in the setup phase. The trust values are updated accordingly. For every user in the network we compute his privacy loss caused by the sharing behaviors of others. Each user’s privacy loss is accumulated over time. After the simulation process finishes, we record the average of accumulated privacy loss as the simulation result.

To further demonstrate the effectiveness of the proposed trust-based mechanism, we design a photo sharing mechanism which is slightly different from the one proposed in Section IV. This mechanism does not utilize the trust values to make the photo anonymization decisions. Instead, given a photo, we randomly select a number of stakeholders and delete them from the photo. The number of deleted stakeholders is equal to that determined by the trust-based mechanism for the same publisher and the same photo. We refer to this mechanism as Random Choose. By comparing the simulation results of the two mechanisms, we can find out whether it is necessary to utilize trust values.

Fig. 2 and Fig. 3 show the simulation results obtained under the following setting: $T = 100$, $L_f = 10$, $\rho = 0.5$, and $\delta = 0.5$. As we can see, the average privacy loss always increases with $\theta$, which implies that users who care more about others’ privacy will suffer less privacy loss than those who care less. And compared to the Random Choose mechanism, the trust-based mechanism generally leads to a lower privacy loss. This result demonstrates that the trust-based mechanism can encourage a user to protect other users’ privacy, so that everyone’s privacy can be better preserved. And from Fig. 2 and Fig. 3 we can see that, when the threshold $\theta$ approaches to 0 or 0.5, the advantage of the trust-based method becomes less significant. According to (2), (3) and (4), the expected value of the trust weighted privacy loss is 0.125 when we set the sensitivity $\delta$ to 0.5. When $\theta$ is high, say 0.5, almost every stakeholder will still appear in the published photo. That is, for every stakeholder $v_h$, it is very likely that $p_h = 1$. Contrarily, when $\theta$ is set to a very low value, say 0, every stakeholder will be deleted from the photo. That is, there is $p_h = 0$ for every stakeholder $v_h$. In both of the above cases, the trust values between users have little influence on the decisions made by the publisher. Therefore, the trust-based method has no significant advantage over the Random Choose method.

In the Random Choose mechanism described above, we require the number of stakeholders deleted from a photo to be equal to that in the trust-based mechanism. Here we propose a third mechanism, referred to as All Random, to further demonstrate the effectiveness of the trust-based mechanism. Given a photo and the corresponding stakeholders, the All Random mechanism randomly deletes some stakeholders from the photo. The number of deleted stakeholders is also random. To compare the trust-based mechanism and the All Random mechanism, we fix the threshold used in the trust-based mechanism to 0.125 which is the expected value of the trust-weighted privacy loss (see (4)). The simulation process is similar as before. To better observe the difference between the two mechanisms, we randomly select 3 users. For each user we compute the average privacy loss to the user. Fig. 4 shows the simulation results under the following setting: $T = 100$, $L_f = 10$, $\rho = 0.5$, $\theta = 0.125$, and $\delta = 0.5$. As we can see, compared to the All Random mechanism, the trust-based mechanism leads to a lower privacy loss. This result again demonstrates the advantage of the use of trust.

In above simulations, the sensitivity of each stakeholder with respect to a photo is set to a value randomly chosen from $[0, 1]$. Given a photo, the sensitivity varies from one stakeholder to another. To observe how the sensitivities affect the sharing of photos, we conduct the following simulation. Given a network, we fist initialize the trust to a random value chosen from $[0, 1]$. When setting up the photo sharing scenario, we fix the sensitivity of a stakeholder with respect to a photo to 0.5. The simulation process is similar as before. Fig. 5 shows the simulation results under the setting $T = 100$, $L_f = 10$, and $\rho = 0.5$. As we can see, compared to the case where sensitivity is set to a fixed value, the proposed trust-based mechanism can even lead to a lower privacy loss when the sensitivity varies from one user to another. In fact, the random setting is more realistic than the fixed setting. Hence the simulation result implies that the proposed mechanism can be well applied in practice.

### C. Tuning the Threshold

In above simulations, the threshold of each user is set to the same value in all time points. And the simulation results show that a high value of threshold is beneficial to the user in terms of privacy, while it impedes the information sharing between users. In Section V we have proposed a method for the user to set the threshold adaptively so as to keep a balance between privacy preserving and information sharing. To verify the effectiveness of the proposed approach, we conduct the following simulation.

Given a network, the parameters $\{K, T, \delta, \epsilon\}$, and a user $v_i$ selected from the network, we first create an “ego” network for the user by selecting the user’s friends and friends of friends from the network. For any two users $v_i$ and $v_j$ in this ego network, the trust $t_{ij}$ is initialized to a value chosen from $[0, 1]$ uniformly at random. The sensitivity of each user

---

1520-9210 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
And to simulate the learning ability of the SP, we replace half $v_i$ uniformly at random. At time point $\tau$ in the ego network is set to a value chosen from $[0, 1]$. The initial trust between two users is set to a random value chosen from $[0, 1]$. The blue stars denote the results obtained by the trust-based mechanism. The red circles denote the results obtained by the Random Choose mechanism. (a) Scale-Free. (b) Small-World. (c) Facebook.

Fig. 2. Simulation results of photo sharing mechanisms. The initial trust between two users is set based on the length of the shortest path between them. The sensitivity of a stakeholder with respect to a photo is set to a random value chosen from $[0, 1]$. The blue stars denote the results obtained by the trust-based mechanism. The red circles denote the results obtained by the Random Choose mechanism. (a) Scale-Free. (b) Small-World. (c) Facebook.

As described above. After the recipient and the stakeholders of a photo are determined, we use the three methods mentioned above. During the simulation, we first create the ego network is set to a value chosen from $[0, 1]$ uniformly at random. At time point $\tau \in \{1, 2, \cdots, T\}$, user $v_i$ randomly selects a friend $v_j$ as the recipient of a photo $d$. The stakeholders are randomly selected from the ego network.

The sensitivity of a stakeholder with respect to a photo is set to a random value chosen from $[0, 1]$. The blue stars denote the results obtained by the trust-based mechanism. The red circles denote the results obtained by the Random Choose mechanism. (a) Scale-Free. (b) Small-World. (c) Facebook.

Fig. 3. Simulation results of photo sharing mechanisms. The initial trust between two users is set to a random value chosen from $[0, 1]$. The sensitivity of a stakeholder with respect to a photo is set to a random value chosen from $[0, 1]$. The blue stars denote the results obtained by the trust-based mechanism. The red circles denote the results obtained by the Random Choose mechanism. (a) Scale-Free. (b) Small-World. (c) Facebook.

The first method is to set the threshold to a fixed value $\theta$. During the simulation, we first create the ego network, and set the initial trust values and users’ sensitivities as described above. After the recipient and the stakeholders of a photo are determined, we use the three methods mentioned above. After the recipient and the stakeholders of a photo are determined, we use the three methods mentioned above. After the recipient and the stakeholders of a photo are determined, we use the three methods mentioned above. After the recipient and the stakeholders of a photo are determined, we use the three methods mentioned above.
above to set the threshold respectively. The payoff produced by each method is recorded for comparison. Specifically, for the Fixed method, we test all possible values of the threshold and use the best result (i.e., the maximal accumulated payoff) for comparison. Similarly, for the $\epsilon$-Greedy method, we test different values of $\epsilon$: from 0 to 1 in steps of 0.1. And the best result is used for comparison. The above simulation process is repeated for 10 times so as to reduce the effect of randomness.

Given a network, we choose 5 users and run the above simulation for each of them. Fig. 6 shows the simulation results under the setting $T = 300$, $K = 10$, $\delta = 0.5$. Fig. 7 shows the results under the same setting except that the sensitivity is set to a random value. As we can see, the $\epsilon$-Greedy method always show better performance than the other two methods. This result demonstrates that the information that the SP learns from past interactions with users can help the publisher to choose a better threshold. The Fixed method performs worst among the three methods, which indicates that it is necessary for the publisher to adjust the threshold when sharing a new photo. This result also suggests that when the publisher wants to share the same photo to different recipients, the publisher should set different thresholds for different recipients.

During the simulation of the Fixed method, we have tried all possible values of the threshold. In each run, we record the best threshold that produces the maximal accumulated payoff. After 10 runs, we find the threshold that is most frequently selected as the best. According to the results shown in Table I, if the user does not want to reset the threshold every time he shares a photo, he may set the threshold to 0.6 or 0.7, which can bring him a fair payoff. During the simulation of the $\epsilon$-Greedy method, we have tried 11 values of $\epsilon$ in each run, we record the best $\epsilon$ that produces the maximal accumulated payoff. After 10 runs, we find the one that is most frequently selected as the best. According to the results shown in Table II, the user should not always be greedy, namely following the suggestion made by the SP. Since the privacy loss estimated by the SP is not always correct, a certain randomness is necessary for the user to get a good payoff.

### VII. Conclusion

Sharing one co-owned photo in an OSN may compromise multiple users’ privacy. To deal with such a privacy issue, in this paper we propose a privacy-preserving photo sharing mechanism which utilizes trust values to decide how a photo should be anonymized. The photo that a user wants to share is temporarily hidden by the service provider. Based on the trust relationship between users, the service provider estimates how much privacy loss the sharing of the photo can bring to a stakeholder. Then by comparing the privacy loss with a threshold specified by the publisher, the service provider decides if a stakeholder should be deleted from the photo. After the photo is shared, each stakeholder evaluates the privacy loss he has really suffered, and his trust in the publisher changes accordingly. This trust-based mechanism motivates the publisher to protect the stakeholders’ privacy. However, the anonymization operation leads a loss in the shared information. Considering that the threshold specified by the publisher controls the trade-off between privacy preserv-
and information sharing, we propose a service provider-assisted method to help the publisher to tune the threshold. By using synthetic network data and real-world network data, we conduct a series of simulations to verify the proposed photo sharing mechanism and the threshold tuning method. Simulation results demonstrate that incorporating trust values into the photo anonymization process can help to reduce user’s privacy loss, and adaptively setting the threshold is necessary for the publisher to balance between privacy preserving and photo sharing.

In current study, we mainly focus on the sharing between one publisher and one receiver. Considering that in practice, a user generally shares a photo with multiple users simultaneously, we’d like to investigate such a one-to-many case in future work. The proposed threshold tuning method can be seen as a greedy method, in the sense that the publisher prefers to choose the threshold that brings him the maximal instant payoff. Due to the correlation between privacy loss and trust values, current choice of the threshold is necessary for the publisher’s future payoffs. In future work, we’d like to investigate how to modify the tuning method so as to achieve a better result.

ACKNOWLEDGMENT

This work was supported by Natural Science Foundation of China (Grant No. 61871037 and No. 61571300). This work was supported by Beijing Institute of Technology Research Fund Program for Young Scholars.

REFERENCES


Fig. 6. Simulation results of different threshold tuning methods. The sensitivity of photo is set to a fixed value. (a) Scale-Free. (b) Small-World. (c) Facebook.

Fig. 7. Simulation results of different threshold tuning methods. The sensitivity of photo is set to a value chosen from [0, 1] uniformly at random. (a) Scale-Free. (b) Small-World. (c) Facebook.


Lei Xu received her Ph.D. degree in electronic engineering from Tsinghua University (THU), Beijing in 2015. She worked as a post-doctor in Department of Computer Science and Technology of THU from July, 2015 to July, 2017. She is now an assistant professor at School of Computer Science and Technology, Beijing Institute of Technology. Her research interests include privacy issues in social networks, data mining, and application of game theory, etc.

Ting Bao received her M.E. degree in Computer Science in 2017 from Beijing University of Technology, Beijing, China. She is currently pursuing the Ph.D. degree in Beijing Institute of Technology. Her research areas include privacy protection in social networks, cloud computing and large-scale multimedia systems.

Liehuang Zhu received his Ph.D. degree in computer science from Beijing Institute of Technology, Beijing, China, in 2004. He is currently a professor at School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China. He has published more than 100 peer-reviewed journal or conference papers, including a dozen of IEEE/ACM Transactions papers (IEEE TIFS, IEEE TII, IEEE TVT, IEEE TSG, Information Sciences, IEEE Network, Computer and Security, etc.). He has been granted a number of IEEE Best Paper Awards, including IWQoS’17, TrustCom’18. His research interests include security protocol analysis and design, wireless sensor networks, and cloud computing.

Yan Zhang is a Full Professor at the Department of Informatics, University of Oslo, Norway. He received a PhD degree in School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. He is an Associate Technical Editor of IEEE Communications Magazine, an Editor of IEEE Network Magazine, an Editor of IEEE Journal on Selected Areas in Communications, an Editor of IEEE Internet of Things Journal, an Editor of Vehicular Technology Magazine, and an Associate Editor of IEEE Access. He serves as chair positions in a number of conferences, including IEEE GLOBECOM 2017, IEEE VTC-Spring 2017, IEEE PIMRC 2016, IEEE CloudCom 2016, IEEE ICC 2016, IEEE CCNC 2016, IEEE SmartGridComm 2015, and IEEE CloudCom 2015. He serves as TPC member for numerous international conference including IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, and IEEE WCNC. His current research interests include: next-generation wireless networks leading to 5G Beyond, green and secure cyber-physical systems (e.g., smart grid, healthcare, and transport). He is IEEE VTS (Vehicular Technology Society) Distinguished Lecturer. He is also a senior member of IEEE, IEEE ComSoc, IEEE CS, IEEE PES, and IEEE VT society. He is a Fellow of IET. He received the award “Highly Cited Researcher” (Web of Science top 1% most cited) according to Clarivate Analytics. .