Trust2Privacy: A Novel Fuzzy Trust-to-Privacy Mechanism for Mobile Social Networks

Guangquan Xu, Bingyan Liu, Litao Jiao, Xiaotong Li, Meiqi Feng, Kaitai Liang, Lei Ma, and Xi Zheng

Abstract

Mobile social applications have been widely used by Internet users. Users can efficiently acquire many kinds of information and share their statuses by various social platforms. However, when a user intends to share information through the user's social applications, the user can set the access permission only before the information is posted. Once the information is posted, it is completely beyond the user's control. Specifically, during the recommendation process (for friend or information) in social applications, a user cannot control who can get the recommendation and access his/her information. If one user is accessed by another malicious user, his/her privacy information can be disclosed, and even be further misused for malicious attacks. In this article, we propose *Trust2Privacy*, a trust-based access control mechanism to protect the personalized privacy of users after posting their information, which can effectively realize the transformation from *trust* to *privacy*. First, to represent the relations accurately among users, we define the *direction of trust* among users according to the user-follow status. Then we combine the similarity, correlation, and interaction among users to calculate the trust values. Considering the fuzzy relationship between the multi-dimensional features and trust levels, we propose a fuzzy comprehensive evaluation algorithm to compute the fuzzy trust. Moreover, for the sake of the high mobility of mobile social networks, we exploit so-called online-to-offline trust evidence to derive the trust value, including taking the location information (e.g., distance, semantics) into consideration. To meet the personalized privacy requirement, we design a filtering algorithm based on the trust relationships and the privacy policy of the target users or posted information, according to which the access requesters can get the list of accessible users or information. This enables achieving the goal of personalized privacy protection. The theoretical analysis and simulation experiment demonstrate that Trust2Privacy is able to achieve personalized privacy protection without bringing negative impact on the availability and usability of mobile social applications.

Introduction

According to Statista [1], there are 3.3 billion people with smartphones across the world, which takes up 42.8 percent of the world population. Among the most essential applications for smartphones, mobile social network applications have become an indispensable part of our daily lives. Nowadays, smartphone users heavily rely on mobile social platforms to get entertainment, news, and life services (e.g., Twitter, Facebook). They can expand their social circle by making new friends in the mobile social platforms. For example, users may be willing to make friends with someone having analogous hobbies. Therefore, there are many suitable recommendation approaches to make sure that smartphone users can get in touch with their target users.

For mobile social networks (MSNs), almost all users can be accessed or recommended, which increases the potential disclosure of their sensitive information. Although existing friend recommendation approaches often achieve high accuracy, they pay less attention to the privacy problem for users who will be recommended or accessed. When a user intends to post some information on the social platform, he can set the access permission only before the information is posted, after which it loses the user control completely. We propose a trust-based mechanism named *Trust2Privacy* to protect the privacy of users, enabling the privacy protection of the information even after it is posted.

Trust is an important concept in the human community, which facilitates the formation and development existence of human societies [2]. Up to the present, some trust measurement methods have been investigated for social networks. In 2010, Li *et al.* [3] calculated trust with the interactions and the number of messages. In 2016, Li *et al.* [4] put forward *Itrust* to evaluate trust by the interaction of users. In 2018, He *et al.* [5] utilized inference (e.g., Bayesian inference approach) to obtain the trust evaluation by integrating the rating of trust given by others. In 2019, Xu *et al.* [6] utilize the types of relationships (family, classmates, etc.) to initialize the trust between users, and calculate the indirect trust with the shortest path. However, these existing computation methods of trust are not applicable to the complex MSNs with high user mobility. In this article, we consider the mobility of users in MSNs into trust computation by combining the information online and offline. The online information contains basic attributes of users and the status of following and interactions among them, while the offline information is represented by the locations of users.

Guangquan Xu is with Qingdao Huanghai University and Tianjin University; Bingyan Liu (corresponding author), Xiaotong Li, and Meiqi Feng are with Tianjin University; Litao Jiao is with Qingdao Huanghai University; Kaitai Liang is with University of Surrey; Lei Ma is with Kyushu University; Xi Zheng is with the Macquarie University.

Digital Object Identifier:
10.1109/MWC.001.1900440

1536-1284/20/$25.00 © 2020 IEEE

In many cases, since the trust between two users is asymmetrical, in this article, we utilize the directed graph to depict such asymmetry according to the user-follow status (i.e., *one-way*, *two-way*, *none*). We assume there are two users in MSNs, *one-way* means that the one follows another; *two-way* represents that they follow each other; and *none* indicates that there is no direct relationship between them. In particular, we integrate the *similarity*, *correlation*, and *interaction* among users to obtain the trust results.

Similarity: Similarity primarily measures the basic attributes of users, which include but are not limited to *gender*, *age*, and *occupation*. Although we can get the similarity of the user's social background from their basic attributes, the basic attributes may be imperfect or even incorrect, causing the measurements of similarity to be inaccurate. Considering the characteristics of mobile sensors (MSNs), our key intuition is that the specific social circle of each user can be formed according to their offline habits. Accordingly, it is possible to obtain more accurate hobbies and habits of users by combining the measurements of both the social circle and basic attributes. In this article, the social circle can be obtained by analyzing the locations of users. Since such information belongs to personal information, we perform the computation through service providers (SPs) (i.e., trusted third parties).

Correlation: We cannot easily exclude there being two users who are completely dissimilar but with high correlation (e.g., doctors and patients, common friends). For the purpose of finding potential friends, the correlation among users should be considered in the trust computation. We take advantage of common friends, the basic attributes, and the offline social circle reflected by the locations to calculate the correlation among users.

Interaction: In this article, we also consider the frequency of interactions to update the trust among users. Interactions change with time, and we should set a suitable time threshold (e.g., half a year, a year) to count the frequency of interactions and update the interaction status between users. In this way, the trust will not change to a high or low level suddenly.

Often the trust level cannot be clearly classified by the numerical trust value. The contribution of each trust factor to the trust level is also fuzzy. For instance, if the similarity between two users is 0.7, we cannot intuitively determine that the similarity of 0.7 should be mapped to a higher or medium trust level. Therefore, we utilize fuzzy theory to evaluate the trust levels [7] comprehensively. After obtaining the levels of trust, we can protect the privacy of users by considering the trust levels. In this article, such trust level representation is called fuzzy trust.

When it comes to privacy preservation, the key problems are "what to protect" and "how to protect." Regarding privacy, different users can have different views. The same user might also change the view over time and location. In recent years, there have been many works on the measurements of privacy, such as information entropy [8]. So far, there has been no universal privacy metric model. In this article, we assume that users can determine the sensitivity of the information that they post according to their opinions. In terms of the different sensitivity, a user may set a corresponding threshold to filter users. In 2019, Xu *et al.* [4] formulated the selection of threshold as a multi-armed bandit problem, which belongs to game theory. At the same time, they made use of the feedback of users to obtain the optimal solution of the threshold [9]. Both game theory and feedback have not considered the different levels of privacy. In this article, the sensitivity may be represented with the numbers *1*, *2*, and *3*, and the corresponding trust can be *high*, *mid*, and *low*. High sensitivity requires high trust, while lower sensitivity needs lower trust. By this means, users themselves can control the degree of sensitive information protection.

In this article, we protect privacy according to different levels. In particular, we utilize the trust levels among users for their privacy preservation. We assume that trusted service providers may generate a series of keys that correspond to different users and their different levels of privacy. According to the privacy policy, the information of users is encrypted at first. Once a user is permitted to access the target users, the decryption keys will be sent to the user. However, considering the update of trust, the decryption keys cannot be stored locally in order to shield the users quickly when the trust value decreases.

Research Contributions

To satisfy the privacy and the regular requirements (e.g., making friends, entertainment) of users in MSNs, a trust-based privacy preservation mechanism named Trust2Privacy is proposed in this article. The main contributions of our work are summarized as follows.

We propose a Trust2Privacy mechanism, which can achieve personalized privacy protection without affecting the usability of mobile social applications.

During the computation of trust, we combine online and offline information along with fuzzy theory to calculate fuzzy trust, which avoids the chaotic phenomena of trust due to the fuzzy boundary.

According to the privacy policy of users, we build up the relationship between trust and privacy. Moreover, we use cryptographic tools to protect different levels of sensitive information. The hierarchical protection of privacy breaks the limitations of being either completely accessible or inaccessible.

According to the privacy policy of users, we build up the relationship between trust and privacy. Moreover, we use cryptographic tools to protect different levels of sensitive information. The hierarchical protection of privacy breaks the limitations of being either completely accessible or inaccessible.

MSNs Architecture

In this section, we first introduce the network model of MSNs, and then describe the design goals of our approach.

Network Model

As Fig. 1 illustrates, we introduce a network model for MSNs that is similar to [10]. In general, MSNs are virtual environments for smartphone users to communicate and get services at different locations and time slots, supported by a local service provider (LSP) and an Internet service provider (ISP).

The users can communicate with LSPs, ISPs, and other users via all sorts of communication technologies [10]. Mobile social applications enable users to share their daily lives, search for information, get location-based services, as well as enjoy entertainment services. For different applications, users can select different communication technologies to satisfy their needs, such as Bluetooth, NFC and the Internet.

Local Service Providers: A local LSP is often equipped with enhanced communication and storage devices that are placed on, or, nearby their

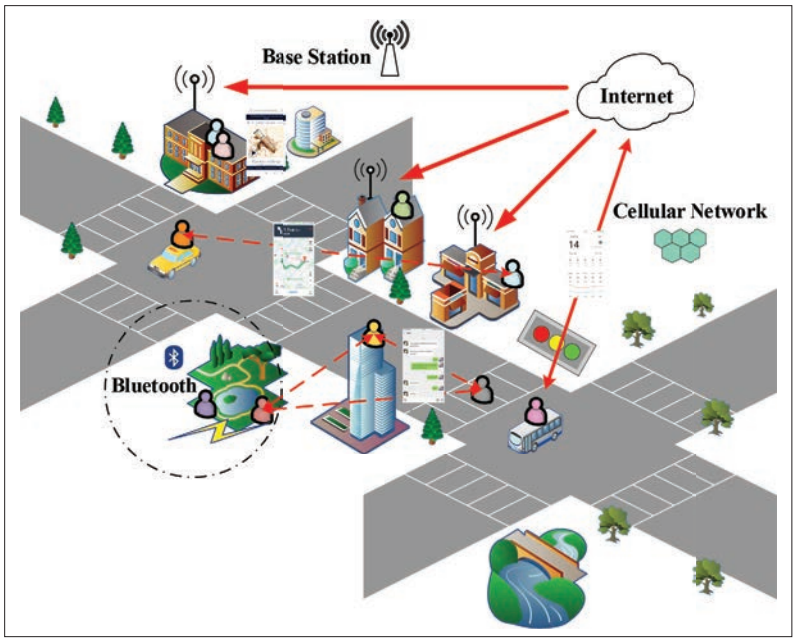

FIGURE 1. The network model of MSN.

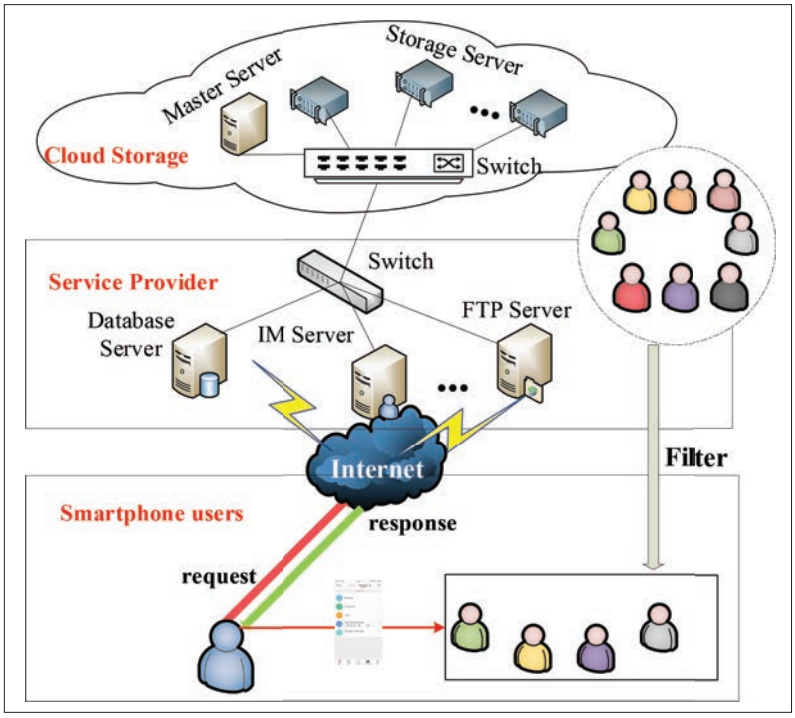

FIGURE 2. The architecture of the Trust2Privacy mechanism.

buildings [10]. It serves users in the vicinity, which can be exploited by the merchants to promote their products or services.

Internet Service Providers: Due to the pervasive development of cellular networks, mobile users can keep in touch with others almost at any time anywhere [11]. The users are allowed to surf the Internet via WiFi, which may appear in stores, hotels or residential buildings. The ISPs can provide service and entertainment information to users.

Design Goals

In order to protect the privacy of users, as well as to achieve personalized service in MSNs, our Trust2Privacy should satisfy the following goals.

The Accuracy of Trust Value: There are many kinds of factors that can affect the trust value [12], making the computation of trust value complex. We should consider the factors that influence trust values as comprehensively as possible.

The Diversity of Trust Value: The degree of sensitivity for personal information varies from one to another. We should design a flexible method for the computation of trust value according to the preference of users.

The Privacy-Preservation of Users: If a user posts some information in his mobile social applications, it is necessary for the user to control the access of his information.

The Normal Needs of MSNs: The users usually expect to make friends via MSNs, which conflicts with the privacy-preservation. Therefore, not only the privacy of users should be protected, but also the daily use of MSNs should be supported.

Trust2Privacy

In this section, we first describe the overview of our Trust2Privacy design. Then, we introduce the services of the Trust2Privacy, including the specific computation of trust values and the main access control process of users.

Trust2Privacy Overview

In order to protect the privacy of users in MSNs, we propose the Trust2Privacy mechanism to realize the dynamic privacy-preservation of users. In Fig. 2, it presents a brief process of access control, which is named as *Privacy-filter*. The main participants of the filter process and their tasks are defined as follows. We introduce them from three layers.

Cloud Storage (CS): It is composed of a large number of different types of storage devices (e.g., storage servers) in the network, which work together through application software to jointly provide data storage and service access functions [11]. In MSNs, the service provider may choose to store a huge amount of users' information into a private cloud, which makes the access to and utilization of this information convenient. In this article, users' information stored in CS can be utilized as the semantic training corpus.

Service Providers (SPs): It includes all kinds of servers to guarantee the normal needs of users. They deploy, manage, and maintain the applications on remote hosts and then provide the computing power for remote customers over a wide area network. In this article, the SPs are responsible for the analysis of semantics and distances to form the fuzzy trust among users.

Smartphone Users (SUs): A user may search or browse information in the MSNs at any time anywhere. In our Trust2Privacy mechanism, when a user searches or browses the recommended contents, the SPs can filter some users by calculating the fuzzy trust between a user and others. In such a way, the user can only access those users who have high trust in him/her.

Trust2Privacy Process

We here introduce the process of our Trust2Privacy mechanism, which includes the initialization of trust, the computation of multi-dimensional features, as well as the computation and transformation from trust to privacy. The details of each process are introduced in Fig. 3.

Initialization: The trust is directional based on the initial relationship of users, including *one-way*, *two-way*, and *none*. In addition, *one-way* can also be divided into two sub-types. They represent the strength of the relationship among users. The users can define different values regarding the different situation. For instance, the users who follow each other may be given super permission, while the users who are not followed with each other may have more restrictions. We can implement these functions by specific numerical value: 0.8, 0.6, and so on.

The Multi-Dimensional Features: We measure the trust among users from multi-dimensional features to make the trust more accurate. In Fig. 3, we construct a feature tree to achieve the stratification of features. We present the computation of each feature as follows:

- For similarity and correlation, we first divide these features into two types: *numerical* and *non-numerical*. Then we start our computation from the leaf nodes and aggregate to the parent nodes layer by layer. For the numerical attributes (e.g., age), we can compute their difference directly. For the non-numerical ones (e.g., profession), they are mapped to a vector space. We can use the skip-gram algorithm, which is one of the basic word embedding algorithms in natural language processing (NLP). The word embedding is a technology that maps a word to a vector [13], which could represent words. The skip-gram algorithm calculates the relationship between two words according to context. In the vector space, the relationship among these words can be computed via similarity or correlation algorithms. For example, it can calculate the similarity between *doctor* and *nurse*, and the correlation between *doctor* and *hospital*.
- The basic attributes of users can be measured directly, while the location information must be processed to construct a social circle of the user. In our approach, the utilization of location information is applicable to MSNs. The location logs of users may reflect their social circle. We can analyze the location logs and build a location chain by counting the number that they check in. The nodes in the chain are sorted by count of user stay, and we can get the latitude and longitude of the locations with the help of a digital map, in which a place can be described as {*place name*, *latitude*, *longitude*, *number of times*}. The semantics can be analyzed according to the place name. The actual geographical distance can be obtained by latitude and longitude. In Fig. 3, each node of U_1 should be compared to each in U_2 from these two aspects, where U_1 and U_2 denote two users. However, the weight of each two nodes may be different. The relationship between the first node of U_1 and U_2 is more important than the relationship between the first node of U_1 and the last node of U_2.
- For user interaction, the SPs can easily obtain the situation of interaction including the forward, the comments, and the thumb-up. In the period, the number of interactions may mirror the relationship among users. According to the interaction, we can get the trust update on time variables.

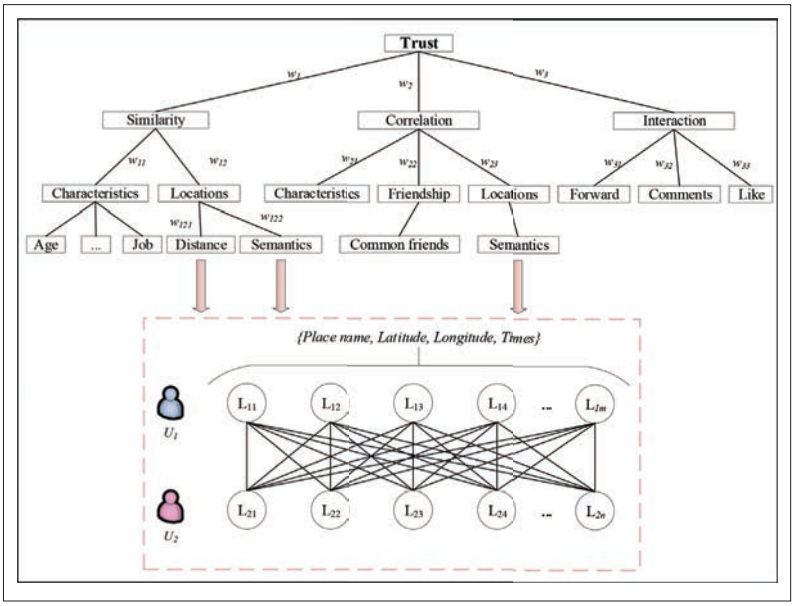

FIGURE 3. The multi-dimensional features for building fuzzy trust.

The Computation of Fuzzy Trust: In this stage, we utilize the fuzzy theory to realize the overall evaluation of trust. Figure 4 shows that the key steps of fuzzy trust are as follows:

- According to the feature tree, we construct a feature set *U* that affects the evaluation of trust levels. The form of the factors is represented as the similarity of job, the correlation of job, the semantic similarity of locations, and the ratio of common friends.
- We define a level set *V*, which contains the description about the trust level; for example, the set can be expressed as {*highest*, *higher*, *high*, *middle*, *low*, *lower*, *lowest*}.
- In terms of the multi-dimensional features, each node has a different influence on their parent node; therefore, the child nodes may be given different weights. Starting from the leaf nodes to the fist layer child of the root node, we put the weight of each node into a group as the weight vector *A*.
- The next step is to determine the fuzzy comprehensive evaluation matrix *R* that represents the degree of membership to trust level. In this article, we use a fuzzy statistical method to obtain the final matrix. The fuzzy statistic is to choose a huge number of testers randomly to give their opinions about the specific features and get the statistical results according to their opinions.
- The last step is to multiply the weight vector **A** and the evaluation matrix **R** to get a one-dimensional vector that corresponds to the possibility of the level in *V*. Here we utilize the biggest value as the degree of fuzzy trust.

The Transformation from Trust to Privacy: Our purpose is to achieve the privacy preservation of users by mapping fuzzy trust with privacy. As shown in Fig. 4, the main transformation process is as follows:

- Due to the different perspectives on privacy, we assume that the users may define the degree of privacy before they post their information. A user can divide his/her information into several levels according to different sensitivity, such as 0, 1, 2, and 3 in Fig. 4.

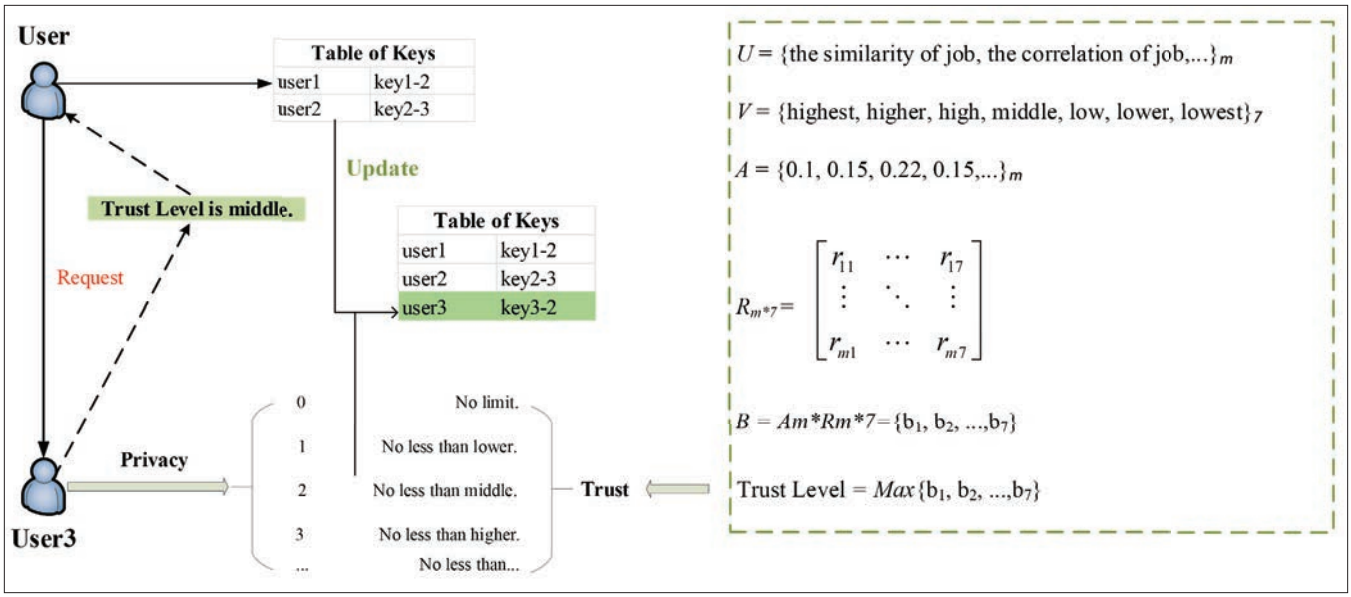

FIGURE 4. The transforming process of trust to privacy.

- Different degrees of privacy correspond to different degrees of trust, and high privacy naturally requires high trust. In Fig. 4, the user could determine the relationship between trust level and privacy level. Then the allowed list of users can be obtained according to the computing result of trust.
- The SPs can generate a series of keys to encrypt the different levels of the privacy information of users. When a user is in the allow list, the decryption keys will be sent to this user. To follow the update of the trust, the keys must not be stored locally. There can be a table of keys mapping to each user. When the trust or privacy levels are updated, only the table of keys needs to be updated.

Performance Evaluation

In this section, we first make a theoretical analysis for the computation of trust and the method of privacy preservation. In order to illustrate the necessity for the comparisons of the locations, we simulate the computation based on locations.

Theoretical Analysis

To demonstrate the advantages of our mechanism, we here compare ours and others on both trust computation and privacy preservation. The comparison results are shown in Table 1, we can see that our Trust2Privacy mechanism can achieve more flexible personalized privacy protection, while it does not have a negative influence on the availability of mobile social applications, which will be further analyzed in the follow-up sections.

The Direction of Trust: In MSNs, the trust among users is directional according to the user-follow status. For example, Alice follows Bob while Bob does not follow Alice, which means that "Alice knows Bob, while Bob does not necessarily know Alice." Therefore, if we initialize an undirected trust between Alice and Bob, it may be unfair for Bob. In [4], they initialize trust among users according to the types of relationships (e.g., family, friends, and colleagues), which needs a large number of definitions for these types. This may not be applicable to MSNs that contain many strangers.

Consideration of the Correlation: In the existing research, the similarity among users is usually measured to discover similar-minded friends. When two users are with high correlation but low similarity, they will be given a low trust value. However, if there is a correlation between two users, they will trust each other from either the indirect friendship or the correlation of interests.

Consideration of the Semantics: In the existing computation of trust, the semantics are mostly not considered. However, there is a lot of information in MSNs that cannot be transformed into numbers. It is necessary to think about the semantic relationships among them. For instance, there are *Japanese restaurants* and *sashimi*; they cannot be presented easily from the relationship via numbers, while they are highly correlated with each other in semantics.

The Combination of Online and Offline: The applications of MSNs are generally location-based, which can reflect the information about the real life of users. Since the online information of users is virtual, it is necessary to consider the offline information to enhance the truth of users in MSNs. We combine the online and offline to compute the trust, and achieve the integration of users and virtual networks.

The Update of Trust: In our Trust2Privacy approach, the trust can be updated according to the interactions to ensure the timeliness of trust.

The Trust to Privacy: Due to the individual preference in privacy, we assume that users can set the privacy level of information by their needs. Furthermore, they can set the correspondence between trust and privacy levels. In this way, the personalized privacy preservation for the applications of MSNs can be realized.

The Method of Privacy Preservation: After the computation of trust, we take measures toward privacy preservation. In this article, we classify the information of users for separate protection. It avoids the limitations of being either completely visible or invisible. At the same time, it also prevents the sensitive information of users from being

disclosed to some completely unrelated strangers. In this way, users may just access partial information of others, which ensures the normal use and access control of sensitive information.

Simulation Experiment

We perform the simulation experiments to evaluate the effectiveness of our consideration for locations.

Our simulation is performed on a personal computer (HP with an Intel I5-6500 3.20 GHz processor, 8 GB memory, and Windows 10) to compute the relationship among users according to their locations. We utilize the dataset sorted out by Liu [14], which is collected from *Weeplaces*, a website that aims to visualize users' check-in activities in location-based social networks (LBSNs). It includes a check-in location for each user for approximately one year. This dataset contains 7,658,368 check-ins generated by 15,799 users over 971,309 locations. The category information about the locations can be used to evaluate the semantic relationship of users.

We compute the partial trust with distance only, and distance and semantics, separately. The results are sorted from highest to lowest. We observe the changes in the results whether considering the semantics or not. We select users with the most changes in trust levels before and after to visualize their data to observe their characteristics. As shown in Fig. 5, we select two users with opposite changes to explain the problem. We generalize the places of *user0*, *user1*, and *user2* into several categories. As we can see from Fig. 5, the semantic relationship of the places between *user0* and *user1* is close, while their main places are at long distance. The *user2* is opposite to *user1*.

To verify the effectiveness of our design for locations, we use *Mapbox*, a live location platform [15], to describe the locations of users in our dataset. As illustrated in Fig. 5, we draw the places of the three users into dots in the map, which demonstrates the distance among the target user, user1, and user2, respectively.

The original intention for the utilization of MSNs is to get services and make friends. Compared to the geographical proximity, we find that the users are catering to make friends with the users who have a similar social circle. In our computation related to locations, we consider both the distance and semantics, which filter some of the users. In other words, we discover more potential friends with similar social circles, and get rid of users with only short distance.

Challenges and Future Directions

Here we capture the problems and challenges of privacy preservation in MSNs, and also introduce some future directions on the basis of this article.

Different Sensitivity in Privacy: For the same information, sensitivity varies from person to person and from location to location. Therefore, the measurements of privacy are not restricted to a unique bar. In this article, we assume that users can set the degree of privacy according to their opinions before posting their information, and the filter may work in light of their settings. In the future, we will pay more attention to the various measurements of privacy to provide more personalized applications for MSNs.

	[3]	[4]	[6]	[9]	[11]	Trust2Privacy
Directional	No	No	No	No	No	Yes
Correlation	No	No	No	No	No	Yes
Semantics	No	No	No	No	No	Yes
Offline	No	No	No	No	No	Yes
Update	Yes	Yes	No	No	Yes	Yes
Trust to privacy	No level	With level	No level	No level	No level	With level
Privacy preservation	Full control	Full control	Full control	Partial control	Partial control	Partial control

TABLE 1. The comparison of the existing research and the Trust2Privacy mechanism

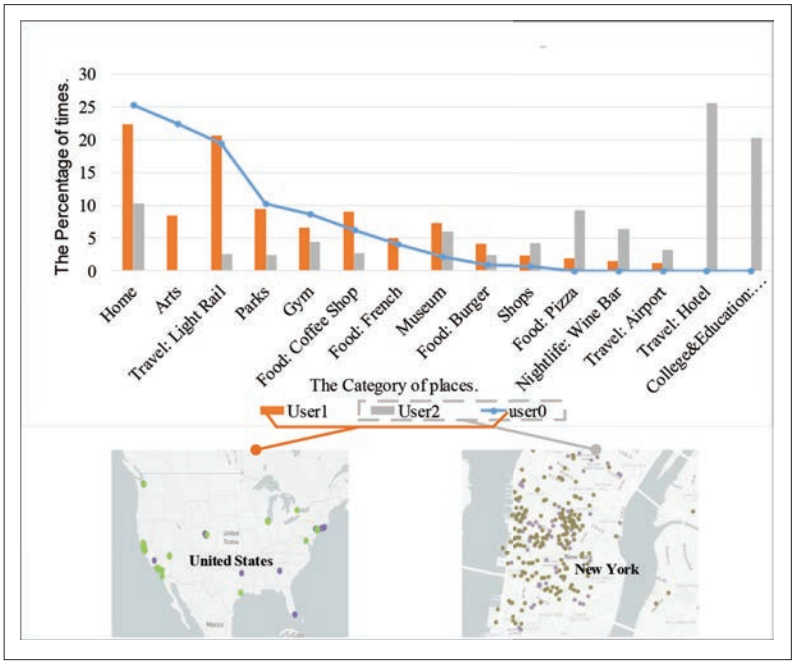

FIGURE 5. The necessity of semantic analysis.

Dependence on a Corpus: To present practical analysis, we usually use a corpus to train the model of semantics. However, the accuracy of this method heavily depends on the appropriateness of the corpus. In this article, we assume that trusted SPs can take advantage of the information of users to lay the foundation of semantics. In future work, we will plan to hunt for a more suitable corpus.

The Comments Are Emotional: In the interaction of users, the comments are generally emotional, leading to diametrically different results. For example, radical remarks may be counterproductive for trust among users, while friendly comments may facilitate trust. Therefore, emotion analysis needs to promote research on the relationship of users in the future.

The Subjectivity of the Membership Matrix: During the computation of fuzzy trust, the membership of each feature with different values is determined by statistics. The statistics should be large enough to be convincing. We will focus on discovering the relationship between membership and trust level, and fitting them to get the relationship curve.

Since the relationships among users are time-dependent and time-restricted, we will need a large number of users and long time period to verify the performance of our proposed mechanism. We plan to perform more in-depth evaluations in the large-scale applications in future.

The Degree of Privacy Preservation: In MSNs, the relationship among users is updated constantly, while trust and privacy preservation are time-sensitive. The degree of privacy preservation and the expansion of social circles should be measured in a fixed period according to the changes in the relationship among users.

Conclusions

Considering the needs and privacy of users in MSNs, a Trust2Privacy mechanism is proposed in this article. We use the multi-dimensional features of trust to ensure the accuracy of trust. Specifically, we consider offline information that could reflect the true social habits of users. In the simulation experiment, offline information could find out users with similar social circles and closer distance and rule out those only with close distance, demonstrating the effectiveness of our location measurements. We utilize fuzzy theory to map trust factors to trust level, which avoids the uncertain division of trust level with numerical trust. For privacy preservation, we propose to encrypt the information of users according to the level of privacy. In this way, we achieve partial protection for the information of users. Through theoretical analysis, our mechanism is proved to be effective for the privacy preservation and normal needs of users.

Since the relationships among users are time-dependent and time-restricted, we will need a large number of users and a long time period to verify the performance of our proposed mechanism. We plan to perform more in-depth evaluations of large-scale applications in the future.

Acknowledgments

This work has been partially sponsored by the State Key Development Program of China (no. 2018YFB0804402) and the National Science Foundation of China (no. 61572355, U1736115).

References

[1] Statistics, "Number of Smartphone Users Worldwide from 2016 to 2021"; https://www.statista.com/topics/840/smartphones/.
[2] H. Yu *et al.*, "A Survey of Trust and Reputation Management Systems in Wireless Communications," *Proc. IEEE*, vol. 98, no 10, Oct. 2010, pp.1755–72.
[3] Z. Yan, X. Y. Li, and R. Kantola, "Personal Data Access Based on Trust Assessment in Mobile Social Networking," *Proc. IEEE 13th Int'l. Conf. Trust Security Privacy Comp. Commun.*, Jan. 2014, pp. 989–94.
[4] X. M. Li *et al.*, "Itrust: Interpersonal Trust Measurements from Social Interactions," *IEEE Network*, vol. 30, no. 4, July/Aug. 2016, pp. 54–58.
[5] C. C. Liang *et al.*, " Enhancing Video Rate Adaptation With Mobile Edge Computing and Caching in Software-Defined Mobile Networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, Oct. 2018, pp. 7013–26.
[6] L. Xu *et al.*, "Trust-Based Collaborative Privacy Management in Online Social Networks," *IEEE Trans. Info. Forensics Security*, vol. 14, Jan. 2019, pp. 48–60.
[7] T. W. Um *et al.*, " Strengthening Trust in the Future Social-Cyber-Physical Infrastructure: An ITU-T Perspective," *IEEE Commun. Mag.*, vol. 54, Sept. 2016, pp.36–42.
[8] I. Wanger and D. Eckhoff, "Technical Privacy Metrics: A Systematic Survey," *ACM Computing Surveys*, vol. 51, no. 3, June 2018.
[9] L. Xu *et al.*, "Trust-Based Privacy-Preserving Photo Sharing in Online Social Networks," *IEEE Trans. Multimedia*, vol. 21, no. 3, Mar. 2019, pp. 591–602.
[10] X. H. Liang *et al.*, "Security and Privacy in Mobile Social Networks: Challenges and Solutions," *IEEE Wireless. Commun.*, vol. 21, no. 1, Feb. 2014, pp. 33–41.
[11] Q. Yang and H. G. Wang, "Toward Trustworthy Vehicular Social Networks," *IEEE Commun. Mag.*, vol. 53, no. 8, Aug. 2015, pp. 42–47.
[12] J. H. Cho, A. Swami, and I. R. Chen, " A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Commun. Surveys & Tutorials*, vol. 13, no. 4, 2011, pp. 562–83.
[13] L. Zheng, S. J. Wang, and Q. Tian, " Coupled Binary Embedding for Large-Scale Image Retrieval," *IEEE Trans. Image Processing*, Nov. 2014, pp. 739–48.
[14] Y. Liu *et al.*, "Exploiting Geographical Neighborhood Characteristics for Location Recommendation," *Proc. 23rd ACM Int'l. Conf. Info. and Knowledge Management*, Nov. 2014, pp. 739–48.
[15] Mapbox, "Mapbox is a Live Location Platform"; https://www.mapbox.com/.

Biographies

Guangquan Xu [M'18] (losin@tju.edu.cn) is a Ph.D. and full professor at the Tianjin Key Laboratory of Advanced Networking (TANK), College of Intelligence and Computing, Tianjin University, China. He received his Ph.D. degree from Tianjin University in March 2008. He is a member of the CCF. His research interests include cyber security and trust management.

Bingyan Liu (bingyan@tju.edu.cn) is a Master's student at the Department of Intelligence and Computing, Tianjin University. She received her B.S. degree from the School of Computer Science and Technology, Northeast Forestry University of China in 2018. Her current research interests include privacy preservation and trust in mobile social networks.

Litao Jiao (jiaolitao_11@163.com) received his M.B.A. degree in 2016 from Shandong University of Science and Technology. He is now an associate professor at Qingdao Huanghai University, China. He was awarded the prize for Provincial Educational Achievement in 2018, participated in five major provincial and municipal research projects, and posted more than 10 papers. His research interests include HR management and information security.

Xiaotong Li (lixiaotong@tju.edu.cn) is a Master's student at the College of Intelligence and Computing, Tianjin University. She received her B.S. degree from the School of Mechanical, Electrical & Information Engineering, Shandong University of China in 2018. Her current research interests include automated program repair and web application protection technique.

Meiqi Feng (fengmeiqi@tju.edu.cn) is studying for a Master's degree in intelligence and computing at Tianjin University. She graduated from Tianjin University with a Bachelor's degree in computer science and technology in 2019. Her main research direction is cyberspace security. She is interested in web security and the combination of artificial intelligence and security.

Kaitai Liang [M'15] (k.liang@surrey.ac.uk) is an assistant professor in Secure Systems at the University of Surrey, United Kingdom, and a member of the Surrey Centre for Cyber Security, a GCHQ recognized the U.K. Academic Centre of Excellence in Cyber Security Research. He received his Ph.D. degree in computer science (applied cryptography direction) from City University of Hong Kong in 2014. He has been involved (as CI and PI) in several European funded projects. His main research interests are data security, user privacy, cybersecurity, block chain security, and privacy-enhancing technology. He has posted a series of research works, applying secure tools to tackle real-world problems, in many high tier international journals. He has served on TPCs for many renowned international security/privacy conferences. He is also an official ISO member of the U.K. ISO Crypto Sub Committee IST/33/2, Associate Editor of the *Computer Journal*, and security consultant for SEMs.

Lei Ma [M'15] (malei@ait.kyushu-u.ac.jp) is currently an assistant professor with tenure at Kyushu University. He received his B.E. degree from Shanghai Jiaotong University in 2009, and his M.E. and Ph.D degrees from the University of Tokyo in 2011 and 2014, respectively. His major research interest focuses on quality assurance and reliability methodology for both traditional and machine learning systems. He has published more than 30 papers at top-tier international conferences. He has also served as PC/organizer for more than 20 international conferences/workshops. Over the past several years, his research has received two ACM SIGSOFT Distinguished Paper Awards (ASE '15, ASE '18), one IEEE Best Paper Award (HotWeb '15), one IEEE Best Testing Tool Award (SBST'15), one Best Candidate Paper Award (SANER '16), one IEEE Best Presentation Award (ICST '17), and one ACM FOSS Impact Paper Award (MSR '18).

Xi Zheng [M'16] (james.zheng@mq.edu.au) received his Ph.C in software engineering from the University of Texas Austin, with a Master's in computer and information science from the University of New South Wales and a Bachelor's in computer information systems from FuDan; now he is an assistant professor/lecturer in software engineering at Macquarie University.