Complex & Intelligent Systems
https://doi.org/10.1007/s40747-023-01052-0

ORIGINAL ARTICLE

HE-SNA: an efficient cross-platform network alignment scheme from privacy-aware perspective

Li Zhou[1,3] · Xiao-Jing Ma[2] · Dong-Hui Pan[2] · Dong-Mei Fan[1] · Hai-Feng Zhang[2] · Kai Zhong[3]

Received: 19 September 2022 / Accepted: 18 February 2023

Abstract
User alignment across online social network platforms (OSNPs) is a growing concern with the rapid development of internet technology. In reality, users tend to register different accounts on multiple OSNPs, and the network platforms are reluctant to share network structure and user's information due to business interest and privacy protection, which brings great obstacles to cross-platform user alignment. In view of this, we propose a homomorphic encryption-based social network alignment (HE-SNA) algorithm from the perspective of privacy leakage. Specifically, we first consider the OSNPs as a system containing multiple social networks, that each participant of OSNPs owns part of the network, i.e., a separate private sub-network. Then, encryption, fusion and decryption operations of the alignment information are performed by two third-party servers using HE scheme, which can protect the privacy information of sub-networks effectively. Finally, each sub-network uses the fused alignment information sent back from the third-party server for user alignment. Experimental results show that the HE-SNA method can provide a sum of locally trained models to third-party servers without leaking the privacy of any single sub-network. Moreover, the HE-SNA achieves a promising network alignment performance than only using the structural information and alignment data of single private sub-network while protecting its topology structure information.

Keywords Cross-platform network alignment · Private sub-network · Privacy-preserving · Homomorphic encryption

Introduction

With the rise of various online social network platforms (OSNPs), people tend to register different social accounts to log into these networks according to their personal preferences and needs [1]. However, user relationships on platforms are usually not publicly available because they may contain private information about the users, such as connections due to religious beliefs, specific identities and financial accounts. Once released without permission, it can violate the law and be harmful to business interests. Moreover, many shopping sites are reluctant to disclose the friendship of users from the profit perspective. In order to maximize the integration and perfection of users information to provide better services for users, network alignment strategy was raised to find out the same person behind different networks [2, 3]. Network alignment plays more and more important role in network analysis as it is conducive to facilitate many downstream applications, such as recommender systems [4, 5] and malicious entities detection [6], etc.

In many real-world scenarios, many complex systems may be recorded by multiple OSNPs due to privacy protection, commercial competition and other factors. For example, a person may be logged into WeChat, Facebook, Douban, Twitter at the same time. In this case, multiple OSNPs can be considered as a system of multiple private online social networks [7, 8], that each participant of OSNPs owns part of the network (i.e., a separate private sub-network) and part of the user alignment data. Existing alignment methods do not consider the issue of privacy protection, which may be inconsistent with the fact that the information of multiple private sub-networks may not be available due to trade secrets and privacy protection. A question arises: is it possible to build a secure protocol framework in which multiple private

✉ Kai Zhong
kaizhong0402@ahu.edu.cn

1 College of Science, Anhui Agricultural University, Hefei 230036, China

2 School of Mathematical Science, Anhui University, Hefei 230601, China

3 Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, Institutes of Physical Science and Information Technology, Anhui University, Hefei 230601, China

Published online: 18 April 2023

sub-networks can be used collaboratively without exposing the network structure and user privacy? thus the user alignment problem can be solved effectively. It is well known that the main economic sources of online platforms are advertising and product pushing, and user alignment helps the platform monetize more broadly and precisely. However, due to the relationships between users are partially recorded by different OSNPs that belong to different companies and they are unwilling to disclose their social relationships, it is necessary to design a secure protocol framework to realize user alignment and protect data privacy of each platform simultaneously. The illustration of using multiple private sub-networks to realize network alignment is shown in Fig. 1.

Cloud computing technology is becoming more mature as web technology evolves. The adoption of cloud computing shortens the product development cycle while saving the cost of purchasing and maintaining infrastructure [9, 10]. Despite those potential benefits of cloud computing, security remains a major obstacle to cloud computing development from the perspective consumers [11]. In recent years, ciphertext data computing supported by homomorphic encryption (HE) technology is widely used for privacy protection and large-scale computing scenarios [12]. Due to the good property of HE, the data holder sends the encrypted private data to a third-party (whether the third-party is trusted or not), which processes the data on the ciphertext and returns it to the data holder after finished. In this process, the data is confidential to the third-party, so the data privacy of users is well protected.

In light of this, a privacy protection-driven network alignment scheme (named HE-SNA) is proposed in this work. The algorithm “collaboratively" uses the topology structures of the multiple private sub-networks for alignment while protecting the user’s private information with the help of two third-party servers. Experimental results on different networks show that the HE-SNA method can achieves better network alignment performance, which is much better than using only the structural information and alignment data of single private sub-network. It is necessary to emphasize that we are not proposing a new algorithm for cross-platform alignment, but are more concerned with how to design a set of privacy protection protocols to better integrate information and leverage the capabilities of existing algorithms. The main contributions of this work are summarized as follows:

1. Considering the fact that online network topologic data is usually held by multiple platforms. A completely new problem is defined: how to collaboratively utilize the structure and the data owned by different networks to realize alignment across multiple networks in a confidential manner.
2. To the best of our knowledge, this work is the first time that considers the HE scheme for cross-platform network alignment applications. The proposed HE-SNA shows enhanced alignment performance than only using single private sub-network while protecting its topology structure information.
3. Experimental results on different networks show that HE-SNA achieves good results in terms of adaptability to new problem scenarios and robustness of model performance.

Related works

In this section, two classical categories of network alignment are reviewed, including the users attribute feature based methods and the network topology structure based methods. Besides, a brief history of homomorphic encryption (HE) and its applications are introduced, which plays an important role in understanding the proposed HE-SNA method.

Network alignment

As described in the introduction, network alignment method has recently emerged following the concept of OSNPs, privacy-preserving and so on. Recent advancements in network alignment can be broadly divided into the following two categories.

Attribute feature based methods

This method converts profile information such as user name, age, gender, occupation or address of users on different OSNPs into a multidimensional vector that is used to characterize user information in social networks. Consider the distribution discrepancy of user representations from different networks, Zheng et al. designed the mapping functions across the latent representation spaces, and the representation distribution discrepancy is addressed through the adversarial training between the mapping functions and the discriminators as well as the cycle-consistency training [13]. Nguyen et al. introduced NAWAL, a novel, end-to-end unsupervised embedding-based network alignment framework emphasizing on structural information, which demonstrates the robustness against adversarial conditions [14]. Li et al. proposed a user identification solution across social networks based on username and display name (UISN-UD), which enables the possibility of matching user accounts with high accessibility and small amount of online data [15]. Liu et al. predicted user anchors across the networks to facilitate the transfer of context information to achieve accurate user alignment on different OSNPs. Simulation results on large-scale social network datasets show the effectiveness of the new model [16]. With the development of social networks, people may register different usernames on different platforms and they are reluctant to expose the sensitive information

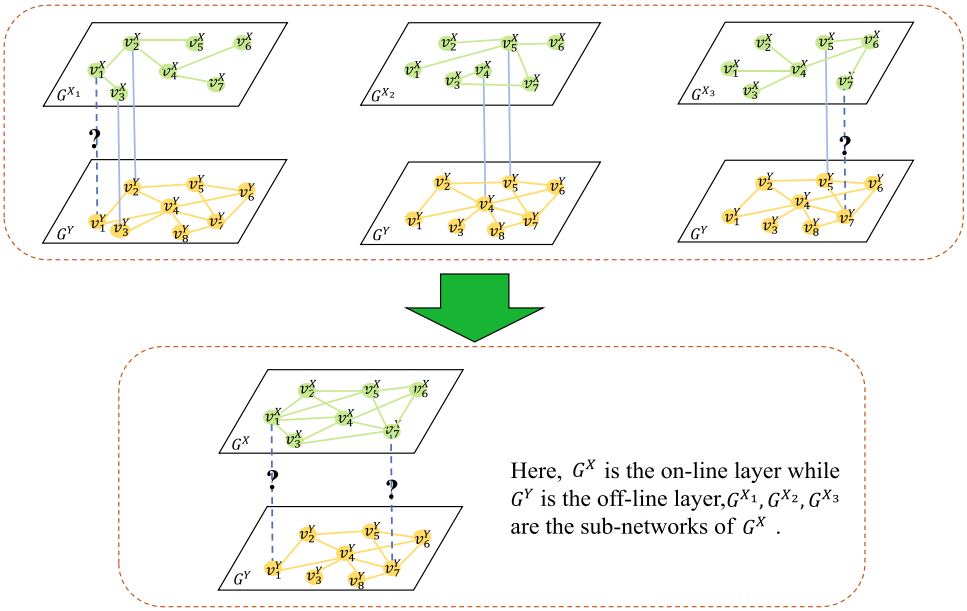

Fig. 1 Framework for solving network alignment problems using multiple private sub-networks. Solid lines between users of G^X and G^Y indicate the aligned users, and dashed lines indicate the users to be aligned

(age, gender, etc) on the network due to privacy protection reasons. Thus, the attribute features are usually unavailable, incomplete or unreliable in practice.

Network topology structure based methods

Since few people share the same circle of friends, it is more likely that the same person will share the same circle of friends on different social networks. Because the relationship between users can reflect the topological features of the network and is relatively easy to obtain, some scholars use the network topological structure to identify the matched users [17]. Alignment based on network topology is to transform the social relations between users into network topology equivalently, and then match the users according to the similarity between nodes. Depending on whether matching data is used, these methods are mainly divided into two categories: unsupervised and supervised. Narayanana et al. first proposed to identify users based on network topology, starting from a small number of known seed nodes and finding new matching nodes through continuous iterative updates, which can achieve user identification between two social networks [18]. Yan et al. proposed a meta-learning algorithm to guide the updating of the pseudo anchor embeddings during the network alignment process, which allows the learning framework to be applicable to a wide spectrum of network alignment methods with structural proximity preserving [19]. Tang et al. proposed a degree penalty principle to calculate the matching degree of all unmatched node pairs, and studied the importance of scale-free characteristic of SMNs for inter-layer link prediction in the real world [20]. The proposed method verifies that better user alignment can be achieved using the network topology. Chen et al. designed a novel semisupervised model, namely the multilevel attribute embedding for semisupervised user identity linkage (MAUIL) and the superiority of the MAUIL approach over other ones through extensive experiments on two real-world datasets [21]. Thanh et al. proposed an unsupervised alignment framework that emphasized structural information. The model embeds the network nodes into a low-dimensional space and then uses the generated adversarial deep neural network to extract structural features [14]. Since unsupervised method does not rely on labeled data, its performance is discounted when compared with the supervised ones. Due to the heterogeneity of social networks and the sparsity of some users, the network topology structure based methods leave much to be desired in terms of comprehensive performance of network alignment.

With the rapid development of machine learning technology, a large number of machine learning-based methods have been applied to the field of network alignment, and fruitful research results have been achieved [22, 23]. Among them, the representation learning approach uses graph embeddings to solve the network alignment problem. Specifically, the best user representation suitable for user alignment task is obtained from the model first, and then the mapping function is defined to match the users across different networks. The achievements, such as PALE [24], IONE [25], COSNET [26], LHNE [27], TransLink [28] are several classical representation learning methods.

Homomorphic encryption (HE) and its applications

In recent years, cloud computing has received a lot of attention, and one of the problems encountered in its imple-

mentation is how to ensure the privacy of data [29, 30]. Meanwhile, system security and cryptography provide a variety of security frameworks for the privacy protection of machine learning [31, 32]. In the field of cryptography, HE can solve this technical problem to a certain extent, which refers to the encryption function for the ciphertext that obtained from the encrypted plaintext. Note that the result of calculating and then decrypting the ciphertext is equivalent to that of calculating ciphertext after decryption. In this way, the third party only needs to calculate the ciphertext to protect the privacy of each participant from the third party. Due to this good nature, one can entrust a third-party to process the data without revealing information.

The concept of HE was first proposed by Rivest et al. in 1978 to construct an encryption mechanism that supported ciphertext retrieval [33]. Later, it was developed into the idea of computing before decrypting the ciphertext, which is equivalent to decrypting before computing [34]. Due to the advantages of HE in terms of computational cost, communication consumption and security, more and more theoretical and applied researches are conducted by scholars [35, 36]. For example, Paillier proposed a provably secure cryptosystem that allows additive operations on ciphertexts, and has been widely used in many applications [37]. In 2009, Gentry gave the first construction of a fully HE scheme that supports performing arbitrary multiplication operations on encrypted data, which is a milestone in homomorphic cryptography [38].

Since then, HE technology developed rapidly and has been widely used in various aspects. Dowlin et al. developed a cryptonets method based on HE that allows cloud servers to evaluate the security of cryptographic queries from trained neural networks [39]. Li et al. proposed a new framework for HE on nonlinear rings that could achieve one-way security based on the conjugate search problem [40]. Based on differential privacy and HE, Jia et al. presented the distributed clustering and distributed random forest methods for multiple data protection with data sharing and model sharing [41]. Lu et al. designed a privacy-preserving Cox regression protocol, which allows researchers to train models on horizontally or vertically segmented datasets while providing privacy protection for sensitive data and the trained models [42].

Preliminaries

In general, each participant is independent of each other and has only partial information about the structure of the original network. Our aim is to improve user alignment performance by using two third-party servers that can collaboratively use information from all sub-networks without exposing any sub-network information. Since no sensitive information will be exposed, which helps to protect the privacy of each participant, thus more and more users are willing to participate. At the same time, the more parties involved, the more network structure information is used, so the better network alignment performance can be guaranteed. In this section, two alignment matching metrics and the HE technology are introduced, respectively.

Matching degree metrics

The problem of network alignment has been thoroughly studied by many scholars with a number of matching degree metrics. In this paper, only two representative ones are selected to demonstrate the superiority of the proposed approach.

Given a matched inter-layer node pair (v_a^X, v_b^Y), for any two unmatched inter-layer nodes v_i^X and v_j^Y across the networks, the matched inter-layer node pair (v_a^X, v_b^Y) is called a common matching neighbor (CMN) [43] of the nodes v_i^X and v_j^Y, if there is an intra-layer link between the nodes v_a^X and v_i^X and an intra-layer link also exists between the node v_b^Y and v_j^Y, i.e., e_{ai}^X and e_{bj}^Y exist. It can be expressed as

$$\mathrm{CMN}(v_i^X, v_j^Y) = |\Gamma(v_i^X) \cap \Gamma(v_j^Y)|, \tag{1}$$

where $\Gamma(v_i^X)$ and $\Gamma(v_j^Y)$ denote the set of matched neighboring nodes of v_i^X and v_j^Y, respectively.

For a given matched inter-layer node pair (v_a^X, v_b^Y), if v_a^X has only one neighbor v_i^X at the network layer G^X and v_b^Y has only one neighbor v_j^Y at the network layer G^Y, then there is a high probability that the inter-layer nodes v_i^X and v_j^Y are the same user. Conversely, if the matched inter-layer nodes v_i^X and v_j^Y have many neighbors, which makes it difficult to determine the inter-layer matching relationship among their neighbor nodes. Therefore, a greater matching weight is given to matched inter-layer node pairs that have fewer neighbors [20], which can be expressed as:

$$\mathrm{IDP}(v_i^X, v_j^Y) = \sum_{\substack{\forall (v_a^X, v_b^Y) \in P \\ v_a^X \in \Gamma(v_i^X) \\ v_b^Y \in \Gamma(v_j^Y)}} [\log^{-1}(k_{v_a^X} + 1) + \log^{-1}(k_{v_b^Y} + 1)]. \tag{2}$$

where P denotes the set of pre-aligned users, $k_{v_a^X}$ and $k_{v_b^Y}$ denote the degree of nodes v_a^X and v_b^Y, respectively. It is worth noting that $\log^{-1}(k_{v_a^X})$ will be equal to 0 when $k_{v_a^X} = 1$. To overcome this problem, 1 is added to each logarithmic function.

Revisit of HE technology

HE is a cryptographic technique based on the complexity theory of mathematical computation, which has the advantage of performing computation without decrypting the encrypted data (ciphertext) in advance, i.e., the result of computation before decrypting the ciphertext is equivalent to decrypting the ciphertext before computing. HE methods can be divided into three categories according to the number of operations on the encrypted data: partially homomorphic encryption (PHE) allows only one type of operations for an unlimited times [37, 44], somewhat homomorphic encryption (SHE) allows some types of operations for a limited number of times [45, 46] and fully homomorphic encryption (FHE) allows an unlimited number of operations for an unlimited number of times [38, 47].

Paillier encryption system [37] in the HE scheme is used in our work, which is a novel probabilistic encryption scheme based on the composite residuosity problem [48]. It has four main operations: KeyGen, Encrypt, Evaluate, Decrypt. KeyGen operation generates public key k_p and private key k_s. First, two large prime numbers p and q are randomly selected, so that $\text{GCD}(pq, (p-1)(q-1)) = 1$, where $\text{GCD}(,)$ represents the greatest common divisor. Second, $n = pq$ and $\lambda = \text{LCM}(p-1, q-1)$ are calculated, where $\text{LCM}(,)$ represents the least common multiple. Finally, $g \in Z_{n^2}$ is randomly selected by checking whether $\text{GCD}(n, L(g^{\lambda \bmod n^2})) = 1$, where $L(u) = \frac{u-1}{n}$ for every u from the subgroup Z_{n^2} that is a multiplicative subgroup of integers modulo n^2 instead of n as in the Benaloh cryptosystem, then $k_p = \{n, g\}$ and $k_s = \{p, q\}$ are generated. $Encrypt$ operation encrypts plaintext m, where the number r is randomly chosen and the encryption works as follows: $c = E(m) = g^m r^n \ (mod\ n^2)$. Decrypt operation decrypts ciphertext c, where the decryption is done by $D(c) = \frac{L(c^\lambda \ (mod\ n^2))}{L(g^\lambda \ (mod\ n^2))} \ mod\ n$.

$Evaluate$ operation takes ciphertexts as input and outputs evaluated ciphertexts. Pailliler's encryption scheme is a PHE algorithm that supports the Evaluate operation for additive homomorphism:

$$E_{k_p}(m_1 * m_2) = E_{k_p}(m_1) * E_{k_p}(m_2), \forall m_1, m_2 \in M, \quad (3)$$

where E_{k_p} is the encryption algorithm and M is the set of plaintext messages.

The proposed HE-SNA method

In this section, we first give the motivations of this work, then present the key steps of HE-SNA methods, and finally provide the pseudo-code of the algorithm.

Motivations

Taking into account the users tend to register different accounts on multiple OSNPs, they are generally serialized. Thus, each private sub-network owns private data, which has the potential to contribute to network alignment. Intuitively, centralizing the data of the same/similar users across different social network platforms can train an excellent network alignment model. Despite of that, the private data is restricted in network alignment field due to privacy concerns and business competitions.

For the new problem scenario described above and inspired by the property that the HE scheme allows mathematical operations to be executed on ciphertexts, we design an HE-based network alignment method HE-SNA, which can fuse private sub-networks information for better alignment while protecting user's privacy. In addition, this work is the first time to link HE technology to network alignment across multiple social network platforms and show boosted model robustness.

Security assumptions

The framework is composed of multiple sub-networks and two cloud servers which will follow the protocol. Server 1 is responsible for fusing the matching degree information of the sub-networks. Server 2 is responsible for generating the public key and private key, and decrypting the ciphertext of the fused match information. Each sub-network intends to preserve its own private information against the cloud servers and other sub-networks, but they want to have access to the alignment information of other sub-networks for better user alignment.

The proposed HE-SNA method

As described earlier, network alignment is a process of integrating social accounts on different social network platforms. We consider two social networks G^X and G^Y, where G^X is online layer occupied by different participants and each private participant independently owns a sub-network and part of the alignment data respectively. In most cases, each participant is independent and has only partial topological information about the social networks G^X, while off-line layer G^Y is open and the structure information is known. Our goal is to leverage the topological information of the social networks G^X and the partial inter-layer alignment data

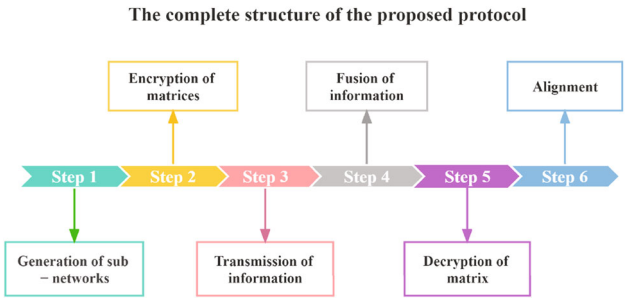

Fig. 2 The complete structure of the proposed protocol

that the participants have, then collaborate with third-party servers to better calibrate the network without exposing any information of participants.

The proposed protocol is composed of the following six steps: (1) generation of sub-networks, (2) encryption of matrices, (3) transmission of information, (4) fusion of information, (5) decryption of matrix, (6) alignment, as described in Fig. 2. The framework processes can be seen in Fig. 3, where the HE-SNA method is illustrated by the example of G^X divided into three sub-networks (G^{X_1}, G^{X_2}, G^{X_3}) and the details are introduced as follows:

Step 1: Generation of sub-networks

Social network is represented by $G(V, E)$, where V is the set of users, $N = |V|$ is the number of users and E is the set of relationships between users, respectively. Social network $G^X(V^X, E^X)$ is occupied by d private participants, denoted as $\{G^{X_1}, G^{X_2}, \ldots, G^{X_d}\}$, where G^{X_t} is the ith sub-network, $t \in \{1, 2, \ldots, d\}$. The structure of social network $G^Y(V^Y, E^Y)$ is completely known. The d sub-networks are aligned with the social network G^Y separately using the matching degree metric (i.e., CMN, IDP) to obtain the matching degree matrices, denoted as $\{S^1, S^2, \ldots, S^d\}$, where S^t represents the matching degree matrix obtained by aligning G^{X_t} with G^Y, and S^t_{ij} represents the matching degree value of the ith node in G^{X_t} with the j-th node in G^Y.

Step 2: Encryption of matrices

Server 2 (it has both public key k_p and private key k_s) distributes k_p to G^{X_t}, and G^{X_t} gets the result $E_{k_p}(S^t)$ obtained by encrypting all elements in S^t with k_p. For the matching degree matrix S^t, the ciphertext matrix element $E_{k_p}(S^t_{ij}) = (g^{S^t_{ij}} \times r^n) \, mod \, n^2$ is calculated using k_p, where $r \in Z_n$ is a random integer.

Step 3: Transmission of information

The d sub-networks $\{G^{X_1}, G^{X_2}, \ldots, G^{X_d}\}$ send the ciphertext matrices $\{E_{k_p}(S^1), E_{k_p}(S^2), \ldots, E_{k_p}(S^d)\}$ to server 1 (server 1 does not know k_p nor k_s).

Step 4: Fusion of information

Server 1 fuses all the ciphertext matrices $\{E_{k_p}(S^1), E_{k_p}(S^2), \ldots, E_{k_p}(S^d)\}$ from each sub-network to get matrix

$$V = \left(\sum_{t=1}^{d} E_{k_p}(S^t_{ij}) \right), (i, j = 1, 2, \ldots, N), \tag{4}$$

After that, the Server 1 sends V to Server 2. This is the most important step in HE-SNA, which fuses the alignment data of all sub-networks together.

Step 5: Decryption of matrix

Server 2 uses the private key k_s to decrypt V and obtains matrix U, the elements of which are calculated by the following:

$$D_{k_s}\left(\sum_{t=1}^{d} E_{k_p}(S^t_{ij}) \right) = \frac{L\left(\left(\sum_{t=1}^{d} E_{k_p}(S^t_{ij}) \right)^{\lambda} \bmod n^2 \right)}{L(g^{\lambda} \pmod{n^2})} \bmod n. \tag{5}$$

According to the additive homomorphism property, we have $U = D_{k_s}(V) = \sum_{t=1}^{d} S^t_{ij}$, where $D_{k_s}()$ denotes the decryption scheme. Finally, server 2 sends the matrix U to each sub-network.

Step 6: Alignment

Each sub-network receives the fused matching degree matrix U from Server 2, where U_{ij} represents the sum of matching degree value obtained by aligning the user i in G^{X_t} with the user j in G^Y using the matching degree metric (i.e., CMN, IDP). For the user i in G^{X_t}, the user j with the largest element U_{ij}, $(j = 1, 2, \ldots, N)$ in G^Y is taken as the user aligned with user i, i.e., user i in G^{X_t} and user j in G^Y are the same person. With the help of third-party servers, the alignment information can be aggregated efficiently without leaking the information of the sub-networks. Thus, the enhanced alignment performance can be achieved. Finally, the pseudo codes of HE-SNA algorithm are demonstrated in Algorithm 1.

Algorithm 1 HE-SNA algorithm

Require: Two social network G^X and G^Y, cloud servers 1 and 2, the inter-layer alignment data set T, encryption and decryption functions $E_{k_p}(\cdot)$ and $D_{k_s}(\cdot)$, parameters $\alpha_0, \alpha_s, \alpha_t$.
Ensure: The aligned users.
1: *Step* 1 : G^X generates d sub-networks $G^{X_1}, G^{X_2}, \ldots, G^{X_d}$.
2: Calculate the matching degree matrices $\{S^1, S^2, \ldots, S^d\}$.
3: *Step* 2 : Cloud server 2 generates a key pair k_p, k_s and sends k_p to $G^{X_1}, G^{X_2}, \ldots, G^{X_d}$.
4: Calculate the ciphertext matrices $E_{k_p}(S^1)$, $E_{k_p}(S^2)$,..., $E_{k_p}(S^d)$.
5: *Step* 3 : $G^{X_1}, G^{X_2}, \ldots, G^{X_d}$ send the ciphertext matrices $E_{k_p}(S^1)$, $E_{k_p}(S^2)$,..., $E_{k_p}(S^d)$ to server 1, respectively.
6: *Step* 4 : Server 1 fuses $E_{k_p}(S^1)$, $E_{k_p}(S^2)$,..., $E_{k_p}(S^d)$ and gets V.
7: Server 1 sends V to Server 2.
8: *Step* 5 : Server 2 decrypts V and obtains the matrix U.
9: Server 2 sends U to $G^{X_1}, G^{X_2}, \ldots, G^{X_d}$.
10: *Step* 6 : The aligned users are obtained.

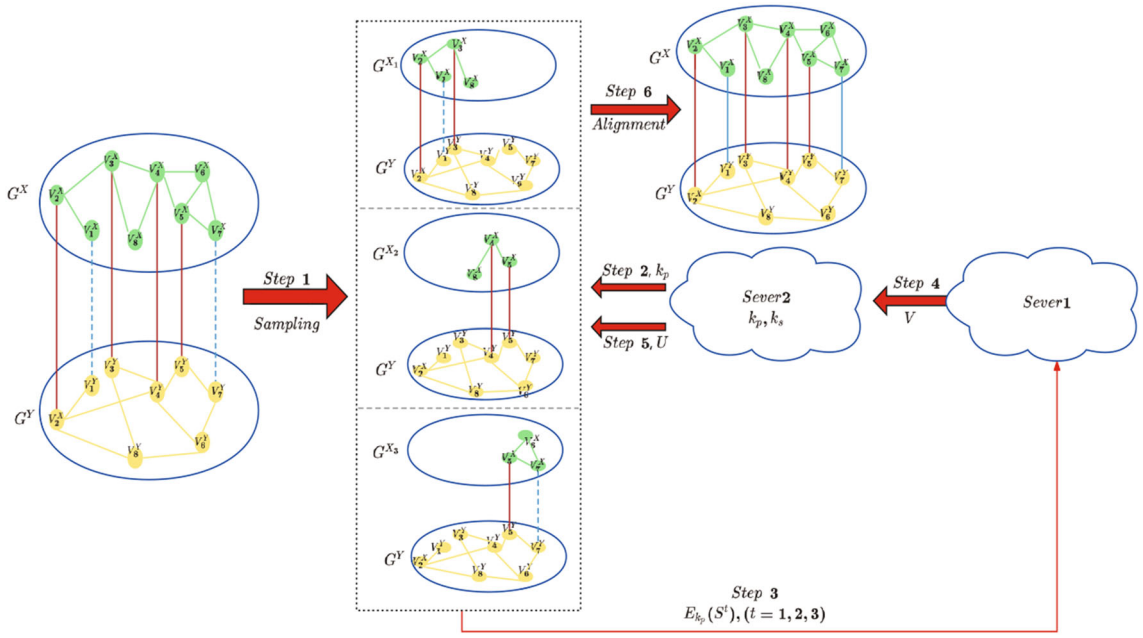

Fig. 3 Schematic diagram of the HE-SNA algorithm, where the G^X is divided into three sub-networks. Red solid lines between users of the G^X and G^Y indicate the aligned users, blue dashed lines indicate users to be aligned and blue solid lines indicate aligned users after using HE-SNA method

Security analysis

Since privacy is an important security requirement, the proposed HE-SNA approach should meet this requirement. Because sub-networks is reluctant to share information to others, the proposed method uses two third-party servers to achieve the purpose of fusing the information of sub-networks while protecting the information from leakage. The sub-networks encrypt the matching degree matrices with k_p and send them to Server 1 for fusion. Since Server 1 does not have k_s, it is unable to decrypt them to get the real matching information. Moreover, the encryption of information can prevent leakage by malicious attacks during transmission. Server 1 fuses the encrypted matching degree matrices and sends it to Server 2, which decrypts it using the k_s. In this case, the fused matching degree of all sub-networks can be obtained by Server 2, the real matching information of a single sub-network is not available.

Experimental results

Data sets introduction

In reality, it is difficult to obtain multiple private sub-networks of an online network, we consider a real online network as a system of "multiple private social networks" and generate several sub-networks using a special sampling strategy for the online network. Four real-world alignment datasets from different domains are used for simulation experiments: Douban online vs Douban offline [49], Twitter vs Foursquare [50], DBLP vs ACM [51], Youtube vs Twitter1 [52]. Douban online, Twitter, DBLP, Youtube are the online layers G^X while Douban Offline, Foursquare, ACM, and Twitter1 are the offline layers G^Y. The basic structural information of them is listed in Table 1, and the sub-networks of each original network are obtained by a specific sampling scheme [50].

Table 1 Basic structural information of social network datasets, including the number of users, edges and aligned user pairs of each dataset

Dataset	User	Edge	Aligned user
Douban online	3906	8164	1118
Douban offline	1118	1511	
Twitter	5120	130,575	1609
Foursquare	5313	54,233	
DBLP	9916	44,808	6325
ACM	9872	39,561	
Youtube	5702	21,068	4854
Twitter1	5540	15,941	

Without losing generality, this part takes $d = 2, 3$ as examples. Consider the case of dividing the online layer G^X into two sub-networks first: a random value $p \in [0, 1]$ is generated to determine whether an edge in the original network exists in one sub-network or in two sub-networks. If $p \leq 1 - 2\alpha_s + \alpha_s\alpha_0$, the edge is not retained in any sub-

Table 2 CMN: performance comparison between different methods for social network alignment on DBLP-ACM dataset. Here the " \ " means that the current overlapping level cannot be satisfied

Overlapping level	Methods	Proportion of training set of each subnetwork						
		1/9	2/9	3/9	4/9	5/9	6/9	7/9
0	Sub-network1	0.6677	0.7501	0.8111	0.8633	\	\	\
	Sub-network2	0.6536	0.7577	0.8275	0.8574	\	\	\
	HE-SNA	**0.7594**	**0.8625**	**0.9240**	**0.9556**	\	\	\
1/9	Sub-network1	0.6576	0.7386	0.8067	0.8561	0.8893	\	\
	Sub-network2	0.6589	0.7587	0.8298	0.8680	0.8944	\	\
	HE-SNA	**0.7120**	**0.8345**	**0.9124**	**0.9489**	**0.9676**	\	\
2/9	Sub-network1	\	0.7620	0.8168	0.8606	0.8998	\	\
	Sub-network2	\	0.7617	0.8265	0.8716	0.8938	\	\
	HE-SNA	\	**0.8218**	**0.8969**	**0.9389**	**0.9611**	\	\
3/9	Sub-network1	\	\	0.8131	0.8595	0.8966	0.9199	\
	Sub-network2	\	\	0.8077	0.8624	0.8935	0.9148	\
	HE-SNA	\	\	**0.8672**	**0.9256**	**0.9535**	**0.9703**	\
4/9	Sub-network1	\	\	\	0.8619	0.8936	0.9251	\
	Sub-network2	\	\	\	0.8646	0.9030	0.9192	\
	HE-SNA	\	\	\	**0.9132**	**0.9477**	**0.9671**	\
5/9	Sub-network1	\	\	\	\	0.8935	0.9202	0.9377
	Sub-network2	\	\	\	\	0.8994	0.9230	0.9399
	HE-SNA	\	\	\	\	**0.9407**	**0.9629**	**0.9775**

Bold values are the results obtained by HE-SNA method

network. If $1-2\alpha_s+\alpha_s\alpha_0 < p \leq 1-\alpha_s$, the edge is retained in the first sub-network. If $1-\alpha_s < p \leq 1-\alpha_s\alpha_0$, the edge is retained only in the second sub-network. Otherwise, the edge is retained in both sub-networks. In addition, parameter α_0 is used to measure the proportion of edges shared by two sub-networks, and parameter α_s is used to measure the sparsity level of the sub-networks.

For the three sub-networks case, we introduce an additional parameter α_t to control the overlapping level between the two sub-networks (where α_0 is used to control the overlapping level of all three sub-networks). Specifically, for each edge in the original network, a random value $p \in [0, 1]$ is generated. If $p \leq 1-3\alpha_s+3\alpha_s\alpha_t-\alpha_s\alpha_0$, the edge is not kept in any sub-network. If $1-3\alpha_s+3\alpha_s\alpha_t-\alpha_s\alpha_0 < p \leq 1+2\alpha_s\alpha_0-3\alpha_s\alpha_t$, the edge is kept in only one sub-network. If $1+2\alpha_s\alpha_0-3\alpha_s\alpha_t < p \leq 1-\alpha_s\alpha_0$, the edge is kept in two sub-networks. Otherwise, the edge is kept in all three sub-networks if $1-\alpha_s\alpha_0 < p \leq 1$.

Experimental settings and evaluation metrics

Experimental settings

When using traditional methods, such as CMN, IDP similarity, sub-networks can only be aligned using their own structure and partially aligned data. But the proposed method can "collaboratively" leverage the structure and alignment information of each sub-network for better alignment without revealing information of them. In this paper, the original cross-social networks G^X and G^Y are regarded as an on line layer and a common offline layer respectively (where the online layer is recorded by multiple OSNPs). 90% of the aligned user data (links between layers) are used as the training set and the rest are the test set. The training set is divided into 10 groups and the average results are taken. Each sub-network has a portion of the original user-aligned data training set. Without special description, we set the parameters $\alpha_s = 0.5$, $\alpha_0 = 0.5$ for generating the online layer containing two sub-networks and parameters $\alpha_s = 0.5$, $\alpha_0 = 0.2, \alpha_t = 0.4$ for generating the online layer containing three sub-networks.

Evaluation metrics

AUC (area under curve) measures the accuracy of inter-layer link prediction (user alignment) from an overall perspective [53]. Assuming that the process of comparing missing inter-layer links with nonexistent inter-layer links is implemented independently f times, if the case of missing inter-layer links with higher scores exists f_1 times and the case of both with the same score exists f_2 times, the AUC is described as:

$$\text{AUC} = \frac{f_1 + 0.5 f_2}{f}. \tag{6}$$

Table 3 IDP: performance comparison between different methods for social network alignment on DBLP-ACM dataset. Here the " \ " means that the current overlapping level cannot be satisfied

Overlapping level	Methods	Proportion of training set of each subnetwork						
		1/9	2/9	3/9	4/9	5/9	6/9	7/9
0	Sub-network1	0.6504	0.7354	0.7963	0.8404	\	\	\
	Sub-network2	0.6632	0.7507	0.8154	0.8625	\	\	\
	HE-SNA	**0.7524**	**0.8510**	**0.9129**	**0.9452**	\	\	\
1/9	Sub-network1	0.6404	0.7269	0.8073	0.8466	0.8766	\	\
	Sub-network2	0.6521	0.7393	0.8049	0.8614	0.8892	\	\
	HE-SNA	**0.7021**	**0.8214**	**0.9030**	**0.9442**	**0.9635**	\	\
2/9	Sub-network1	\	0.7359	0.7970	0.8445	0.8786	\	\
	Sub-network2	\	0.7620	0.8198	0.8604	0.8984	\	\
	HE-SNA	\	**0.8100**	**0.8856**	**0.9316**	**0.9594**	\	\
3/9	Sub-network1	\	\	0.7895	0.8488	0.8795	0.9012	\
	Sub-network2	\	\	0.8112	0.8606	0.8998	0.9233	\
	HE-SNA	\	\	**0.8630**	**0.9258**	**0.9553**	**0.9710**	\
4/9	Sub-network1	\	\	\	0.8500	0.8841	0.9078	\
	Sub-network2	\	\	\	0.8529	0.8860	0.9235	\
	HE-SNA	\	\	\	**0.9045**	**0.9407**	**0.9670**	\
5/9	Sub-network1	\	\	\	\	0.8912	0.9132	0.9296
	Sub-network2	\	\	\	\	0.8891	0.9223	0.9402
	HE-SNA	\	\	\	\	**0.9381**	**0.9659**	**0.9789**

Bold values are the results obtained by HE-SNA method

Experimental results analysis

Effects of overlapping level of training sets among sub-networks

The overlapping level of training sets between sub-networks is defined as the number of overlapping edges/total number of training set edges. Tables 2 and 3 represent the effects of the proportion of training sets of online layer owned by two sub-networks and the overlapping level of training sets between sub-networks on AUC using CMN and IDP metrics under DBLP-ACM network, respectively.

It is worth noting that when the overlapping level of training sets between two sub-networks is unchanged, the AUC increases as the proportion of training sets owned by the sub-networks increases. It can be seen that the HE-SNA approach does outperform the alignment using only a single network, regardless of the CMN or IDP metric, due to the fusion of information from sub-networks for alignment. It shows that the algorithm can indeed effectively fuse data from different private participants to achieve better alignment performance. Conversely, if the proportion of training sets owned by the two sub-networks is unchanged, the AUC gradually decreases as the overlapping level of training sets between sub-networks increases. This is not difficult to understand, because when the overlapping level of training sets between sub-networks keeps increasing, the fraction of having duplicate aligned data also increases, and HE-SNA is unable to obtain more different information from the aligned data of the two sub-networks, which leads to a decreasing trend of AUC. Here, only the DBLP-ACM network is used as an example, and similar results can be found for the other three sets of aligned networks.

Figure 4 compares the change in AUC with different training set overlapping level between sub-networks using only a single sub-network versus the fusion case (using HE-SNA method) when the proportion of training sets owned by each sub-network is 4/9 (the matching metric is CMN). It can be seen from the diagram that HE-SNA algorithm is much better than the model that only uses the information of a single subnetwork, regardless of the variation in training set overlapping level between the two sub-networks. The above results are reasonable and logical since the "fusion" trick can aggregate more alignment information than a single sub-network. To avoid tediousness, this paper only takes the case that the training set ratio of each sub-network is 4/9 as an example, and the similar results can also be obtained for other ratios.

Besides, we further discuss the effect of training set size on the alignment results. If train1 $\cup$ train2 = train, whether using CMN metric or IDP metric in Fig. 5, as the overlapping level of training sets between sub-networks increases, the AUC of both the single sub-network and fusion case in four sets of aligned networks increases due to the increasing number of edges of training sets owned by each sub-network, but the performance of using only a single sub-network is

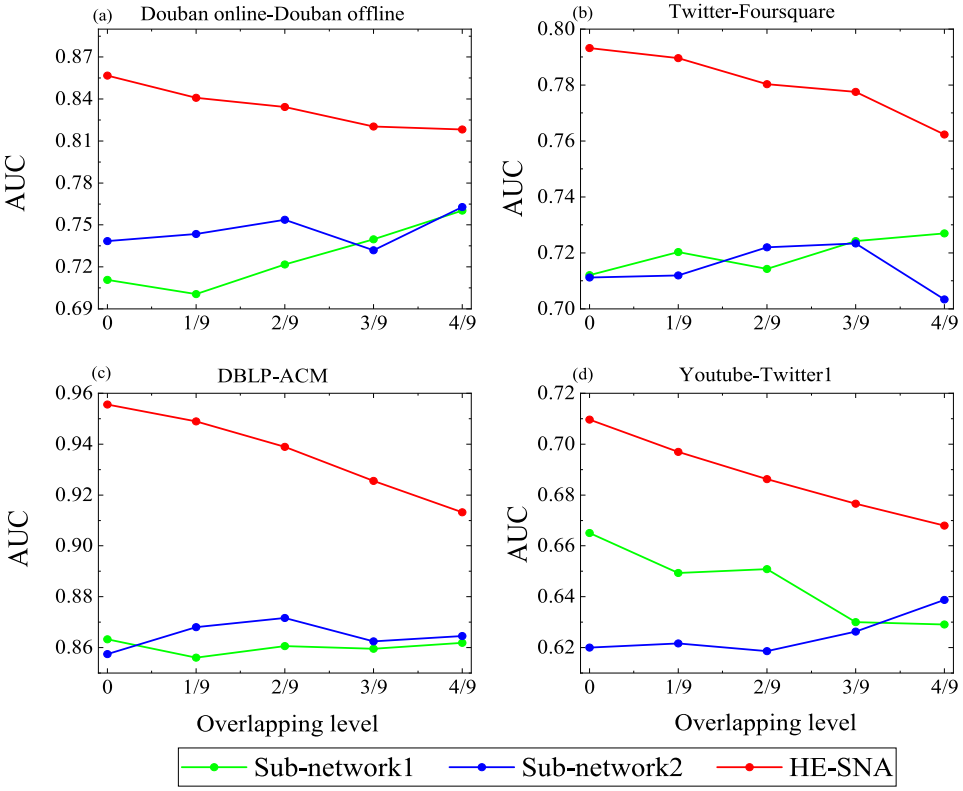

Fig. 4 The change in AUC with different training set overlapping level between sub-networks using only a single sub-network versus the fusion case when the proportion of training sets owned by each sub-network is 4/9 (CMN metric)

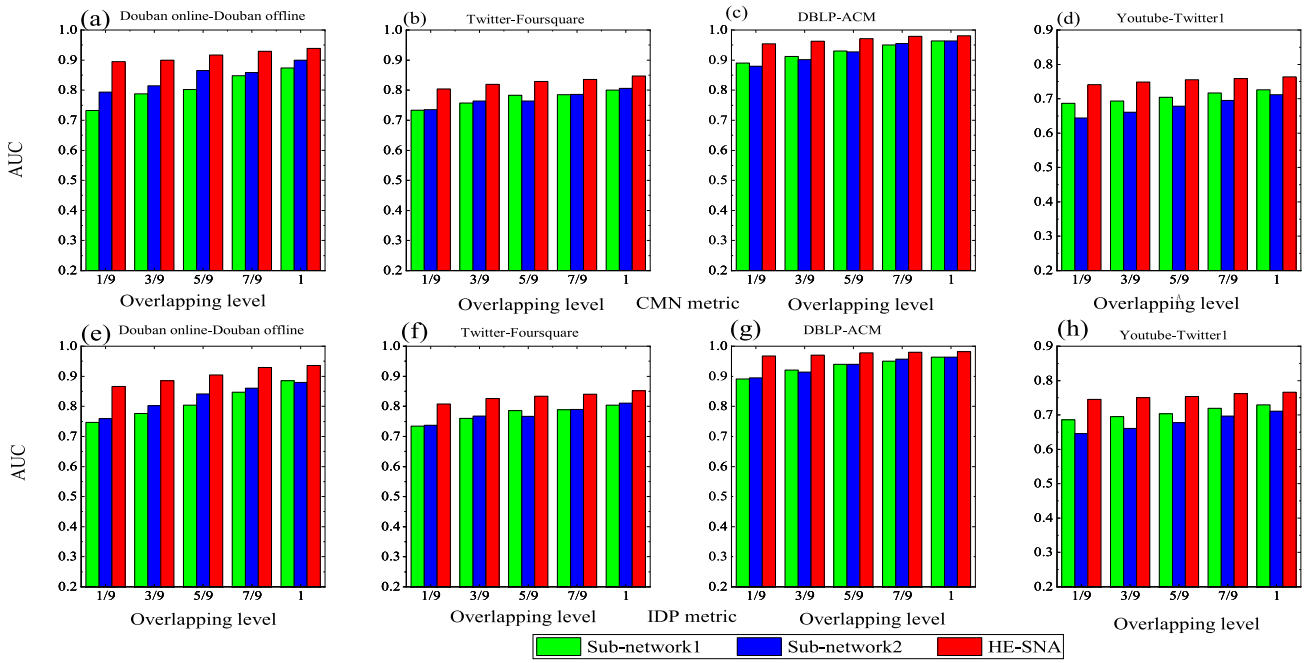

Fig. 5 The change in AUC with different overlapping levels of training sets between sub-networks using only a single sub-network versus the fusion case when training sets owned by two sub-networks satisfy train1 ∪ train2 = train (CMN metric above, IDP metric below)

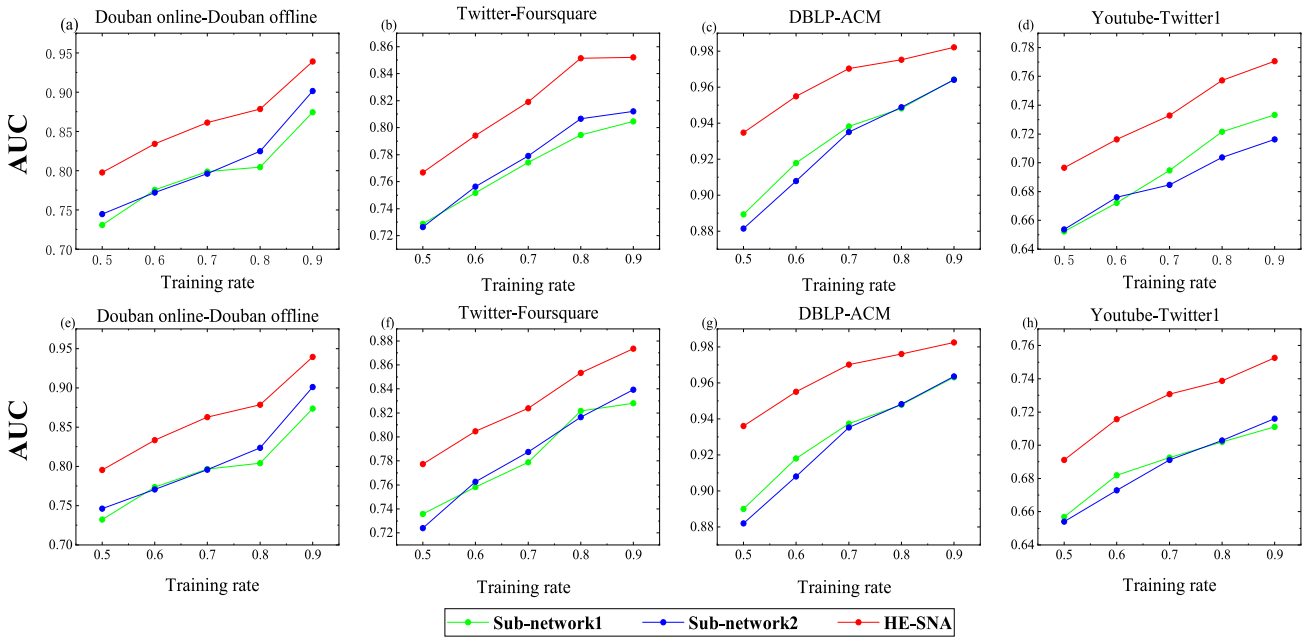

Fig. 6 The change in AUC of two sub-networks and fusion case when train1 = train2 = train with different proportions of divided training sets (CMN metric above, IDP metric below)

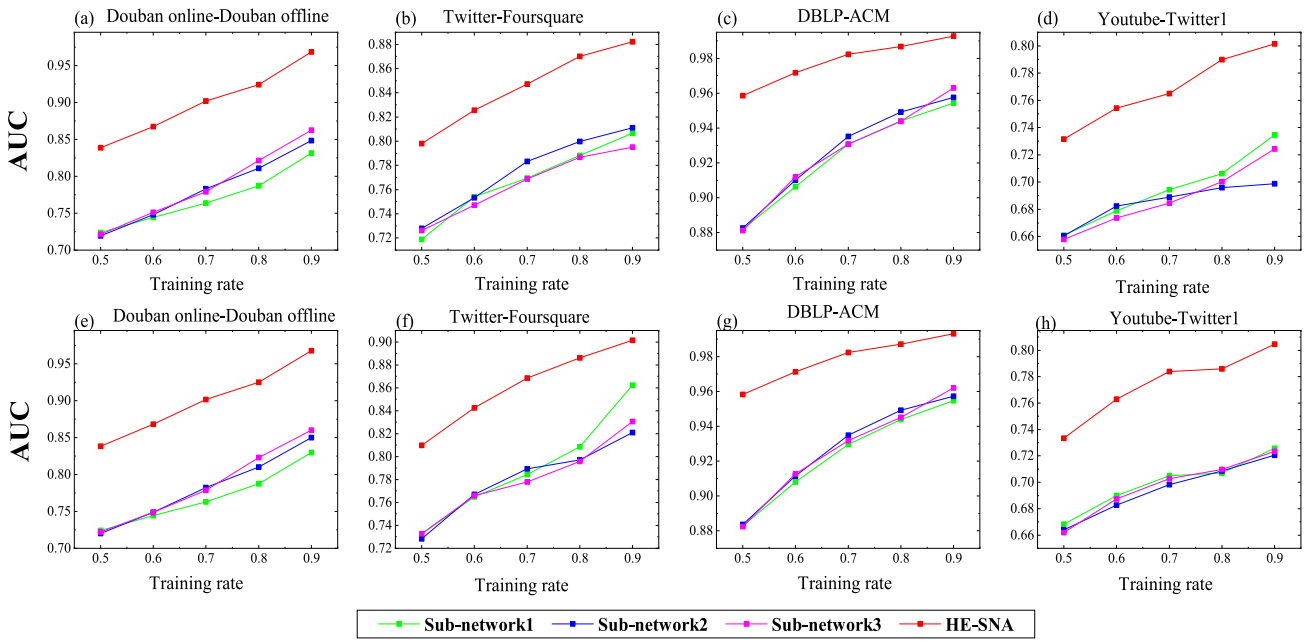

Fig. 7 The change in AUC of three sub-networks and fusion case when train1 = train2 = train3 = train with different proportions of divided training sets (CMN metric above, IDP metric below)

much less than that of HE-SNA since the fusion case has more alignment information. Here train1 and train2 denote the training sets of sub-network1 and sub-network2, respectively, and train denotes the training set of the original social network G^X.

From the above analysis, it is clear that when train1 ∪ train2 = train, the experimental alignment results are obviously more effective and privacy-protected than using only a single sub-network, since the HE-SNA method fuses the information from all sub-networks. Therefore, when the training sets of the sub-networks are the same as the original social network, is the HE-SNA method bad for alignment? This is not the case: when train1= train2 = train, train1 = train2 = train3 = train, Figs 6 and 7 show the change in AUC

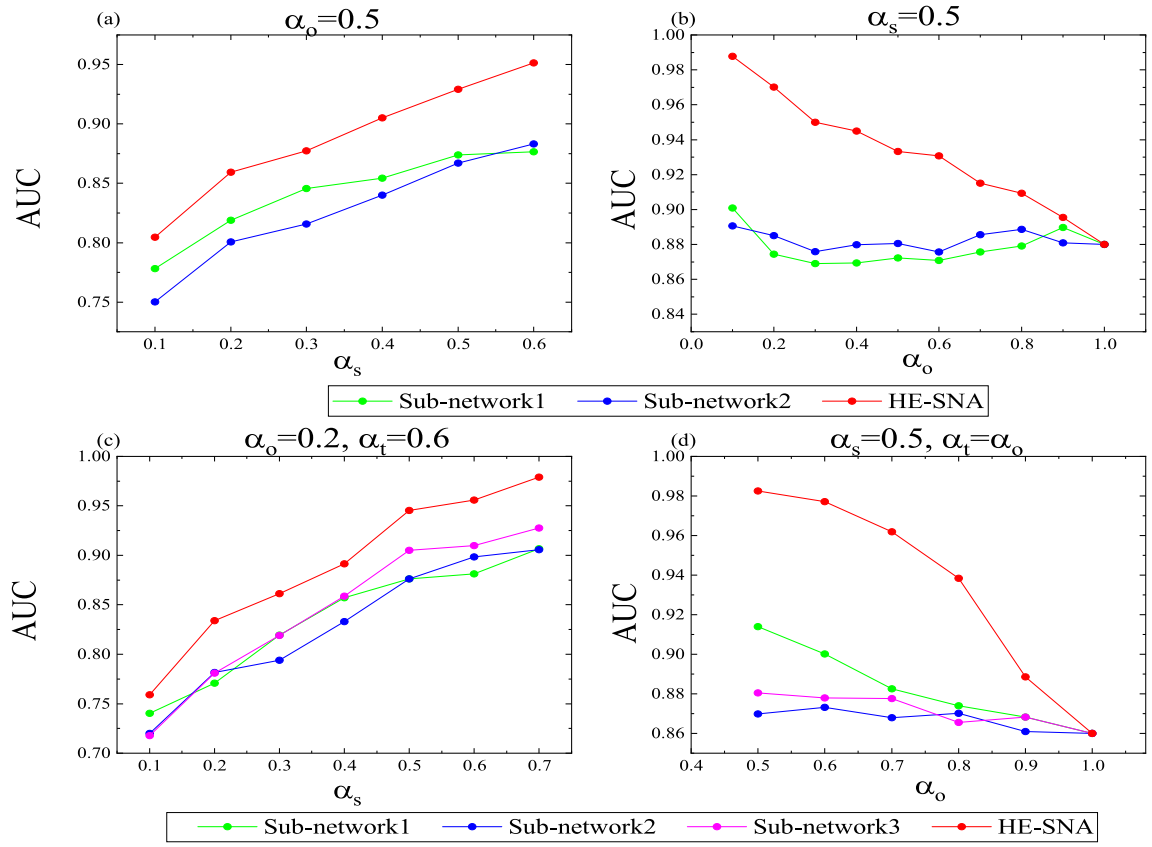

Fig. 8 Effect of sparsity α_s and overall overlapping level α_s on the performance of HE-SNA method in Douban online-Douban offline network

for two sub-networks and the fusion case, three sub-networks and fusion case with different proportions of training sets in four sets of aligned networks, respectively, where sub-figures (a), (b), (c) and (d) use the CMN metric while sub-figures (e), (f), (g) and (h) use the IDP metric. It can be seen that with the increasing proportion of training sets owned by sub-networks, the AUC of using only a single sub-network and fusion case are increasing, but the HE-SNA method in this paper achieves far better alignment in both the two and three sub-networks than the single sub-networks approach.

Parameter sensitivity analysis

To comprehensively evaluate the HE-SNA method, we investigate the effects of parameters α_s and α_0 on model performance. Taking the Douban online-Douban offline network as an example: set train:test = 9:1 and select the CMN metric, sub-figures (a) and (b) of Fig. 8 are the results of experiments containing two sub-networks when train1 = train2 = train, while sub-figures (c) and (d) of Fig. 8 are the results of experiments containing three sub-networks when train1 = train2 = train3 = train. The results in Fig. 8a, c indicate that whether it is two sub-networks or three sub-networks, the conclusion is similar, i.e., with increasing sparsity α_s, the AUC is increasing as each platform has a more complete sub-network structure. Therefore, it is more conducive to user matching regarding both individual sub-networks and the HE-SNA method.

As demonstrated in Fig. 8b, d, as the α_0 increases, the overlapping level between sub-networks is getting higher and higher, i.e., each sub-network becomes more and more similar, the advantage of HE-SNA method (i.e., fusing the structure of each sub-network) is weakening, so the AUC is decreasing. If $\alpha_0 = 1$, the structure of each sub-networks are the same, so the AUC of the HE-SNA method and the individual sub-network methods are identical. From the above analysis, we can draw the conclusion that the lower overlapping level between sub-networks, the greater the advantage of HE-SNA method.

Computation cost analysis

To compare the running times between the original model (i.e., HE mechanism is not considered) and the HE-SNA method, we consider the extra running time of the HE-SNA model to compare the computation cost difference between

Table 4 Extra running times of the HE-SNA

Dataset	Size of matching degree matrix	Extra running times (s)
Douban online vs Douban offline	3906 × 1118	821.22
Twitter vs Foursquare	5120 × 5313	5187.93
DBLP vs ACM	9916 × 9872	18636.04
Youtube vs Twitter	5702 × 5540	5969.15

the two methods. Suppose the number of sub-networks is 3, and the CMN metric is used to obtain the matching degree matrix of each sub-network. The following Table 4 presents the extra running times of our HE-SNA when HE mechanism is considered. It can be found that the extra running times increased by the HE-SNA method, which is proportional to the size of the matching degree matrix.

The operation of encrypting and fusing the matching degree matrix followed by the corresponding decryption is implemented on PyCharm 2019 with the phe open source library, and the running times of all networks are averaged over five runs obtained and run on a Windows 10 system with a 2.60 GHz Intel processor and running memory of 8.00 GB.

Conclusions

Due to the importance of privacy protection, different OSNPs are reluctant to share information about the structure of the network and the attributes of the users, which brings a significant obstacle to the alignment of users across the networks. Our work starts from privacy protection and designs an HE-SNA method based on HE to align the original cross-network users. Experimental results show that regardless of different matching metrics, our method can effectively protect the data privacy and perform cross-network user identity alignment more accurately than using information from a single network only. Therefore, the proposed method provides a new idea for collaborative identification of identical user entities in multiple private networks. In future work, how to better extract the structural features of the network and combine them with the attribute features of the nodes to improve the accuracy of the HE-SNA will be investigated, and the application of HE-SNA algorithm in other types of network data is also worth studying.

Acknowledgements This work is supported by the Anhui Provincial Natural Science Foundation under Grant 2108085MA02, the Key Projects of Natural Science Research of Universities in Anhui Province under Grant KJ2021A0071, the University Synergy Innovation Program of Anhui Province (GXXT-2021-032) and the MOE (Ministry of Education in China) Youth Foundation Project of Humanities and Social Sciences (Grant No. 20YJCZH025).

References

1. Fu S, Wang G, Xia S, Liu L (2020) Deep multi-granularity graph embedding for user identity linkage across social networks. Knowl-Based Syst 193:105301
2. Wen W, Ren W, Shi Y, Nie Y, Zhang J, Cao X (2022) Video super-resolution via a spatio-temporal alignment network. IEEE Trans Image Process 31:1761–1773
3. Djeddi WE, Yahia SB, Nguifo EM (2018) A novel computational approach for global alignment for multiple biological networks. IEEE/ACM Trans Comput Biol Bioinform 15(6):2060–2066
4. Fu C (2020) User intimacy model for question recommendation in community question answering. Knowl-Based Syst 188:104844
5. Pretet L, Richard G, Souchier C, Peeters G (2022) Video-to-music recommendation using temporal alignment of segments. IEEE Trans Multimed. https://doi.org/10.1109/TMM.2022.3152598
6. Mills R, Marnerides AK, Broadbent M, Race N (2021) Practical intrusion detection of emerging threats. IEEE Trans Netw Serv Manage 19(1):582–600
7. Luo W, Duan B, Ni L, Liu Y (2021) Collaborative detection of community structure in multiple private networks. IEEE Trans Comput Soc Syst 9(2):612–623
8. Zhang H-F, Ma X-J, Wang J, Zhang X, Pan D, Zhong K (2022) Privacy-preserving link prediction in multiple private networks. IEEE Trans Comput Soc Syst. https://doi.org/10.1109/TCSS.2022.3168010
9. Alam T (2020) Cloud computing and its role in the information technology. IAIC Trans Sustain Digit Innov (ITSDI) 1(2):108–115
10. Bello SA, Oyedele LO, Akinade OO, Bilal M, Delgado JMD, Akanbi LA, Ajayi AO, Owolabi HA (2021) Cloud computing in construction industry: use cases, benefits and challenges. Autom Constr 122:103441
11. Alouffi B, Hasnain M, Alharbi A, Alosaimi W, Alyami H, Ayaz M (2021) A systematic literature review on cloud computing security: threats and mitigation strategies. IEEE Access 9:57792–57807
12. Abbas A, Hidayet A, Selcuk UA, Mauro C (2017) A survey on homomorphic encryption schemes: theory and implementation. ACM Comput Surv 51(4):1–35
13. Zheng C, Pan L, Wu P (2021) Camu: cycle-consistent adversarial mapping model for user alignment across social networks. IEEE Trans Cybern 7(9):1–12

14. Nguyen TT, Pham MT, Nguyen TT, Huynh TT, Nguyen QVH, Quan TT et al (2021) Structural representation learning for network alignment with self-supervised anchor links. Expert Syst Appl 165:113857
15. Li Y, Peng Y, Zhang Z, Yin H, Xu Q (2019) Matching user accounts across social networks based on username and display name. World Wide Web 22(3):1075–1097
16. Liu L, Li X, Cheung WK, Liao L (2019) Structural representation learning for user alignment across social networks. IEEE Trans Knowl Data Eng 32(9):1824–1837
17. Ding X, Ma C, Zhang X, Chen H-S, Zhang H-F (2021) Soidp: predicting interlayer links in multiplex networks. IEEE Trans Comput Soc Syst. https://doi.org/10.1109/TCSS.2021.3068468
18. Narayanan A, Shmatikov V (2009) De-anonymizing social networks. In: 30th IEEE symposium on security and privacy. IEEE, pp 173–187
19. Yan Z, Liu L, Li X, Cheung W, Zhang Y, Liu Q, Wang G (2021) Towards improving embedding based models of social network alignment via pseudo anchors. IEEE Trans Knowl Data Eng
20. Tang R, Jiang S, Chen X, Wang H, Wang W, Wang W (2020) Interlayer link prediction in multiplex social networks: an iterative degree penalty algorithm. Knowl-Based Syst 194:105598
21. Chen B, Chen X (2022) Mauil: multilevel attribute embedding for semisupervised user identity linkage. Inf Sci 593:527–545
22. Trung HT, Toan NT, Van Vinh T, Dat HT, Thang DC, Hung NQV, Sattar A (2020) A comparative study on network alignment techniques. Expert Syst Appl 140:112883
23. Huynh TT, Duong CT, Nguyen TT, Van Tong V, Sattar A, Yin H, Nguyen QVH (2021) Network alignment with holistic embeddings. IEEE Trans Knowl Data Eng 1–12
24. Cui P, Wang X, Pei J, Zhu W (2018) A survey on network embedding. IEEE Trans Knowl Data Eng 31(5):833–852
25. Shen X, Dai Q, Mao S, Chung F-L, Choi K-S (2020) Network together: node classification via cross-network deep network embedding. IEEE Trans Neural Netw Learn Syst 32(5):1935–1948
26. Salamat A, Luo X, Jafari A (2021) Heterographrec: a heterogeneous graph-based neural networks for social recommendations. Knowl-Based Syst 217:106817
27. Chen X, Song X, Cui S, Gan T, Cheng Z, Nie L (2020) User identity linkage across social media via attentive time-aware user modeling. IEEE Trans Multimed 23:3957–3967
28. Li X, Cao Y, Li Q, Shang Y, Li Y, Liu Y, Xu G (2021) Rlink: deep reinforcement learning for user identity linkage. World Wide Web 24(1):85–103
29. Song F, Qin Z, Xue L, Zhang J, Lin X, Shen X (2021) Privacy-preserving keyword similarity search over encrypted spatial data in cloud computing. IEEE Internet Things J 9(8):6184–6198
30. Shen J, Yang H, Vijayakumar P, Kumar N (2021) A privacy-preserving and untraceable group data sharing scheme in cloud computing. IEEE Trans Dependable Secure Comput. https://doi.org/10.1109/TDSC.2021.3050517
31. Zhang X-J, Wang J, Ma X-J, Ma C, Kan J-Q, Zhang H-F (2022) Influence maximization in social networks with privacy protection. Phys A 607:128179
32. Xia X, Su Y, Lü L, Zhang X, Lai Y-C, Zhang H-F (2022) Machine learning prediction of network dynamics with privacy protection. Phys Rev Res 4(4):043076
33. Rivest RL, Adleman L, Dertouzos ML et al (1978) On data banks and privacy homomorphisms. Found Secure Comput 4(11):169–180
34. Gai K, Qiu M (2017) Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers. IEEE Trans Ind Inf 14(8):3590–3598
35. Meftah S, Tan BHM, Mun CF, Aung KMM, Veeravalli B, Chandrasekhar V (2021) Doren: toward efficient deep convolutional neural networks with fully homomorphic encryption. IEEE Trans Inf Forensics Secur 16:3740–3752
36. Munjal K, Bhatia R (2022) A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex Intell Syst 1–28
37. Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. In: International conference on the theory and applications of cryptographic techniques. Springer, pp 223–238
38. Gentry C (2009) Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st annual ACM symposium on theory of computing, pp 169–178
39. Gilad-Bachrach R, Dowlin N, Laine K, Lauter K, Naehrig M, Wernsing J (2016) Cryptonets: applying neural networks to encrypted data with high throughput and accuracy. In: International conference on machine learning, PMLR, pp 201–210
40. Li J, Kuang X, Lin S, Ma X, Tang Y (2020) Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. Inf Sci 526:166–179
41. Jia B, Zhang X, Liu J, Zhang Y, Huang K, Liang Y (2021) Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in iiot. IEEE Trans Ind Inf 18(6):4049–4058
42. Lu Y, Tian Y, Zhou T, Zhu S, Li J (2021) Multicenter privacy-preserving cox analysis based on homomorphic encryption. IEEE J Biomed Health Inform 25(9):3310–3320
43. Rexford J, Dovrolis C (2010) Future internet architecture: clean-slate versus evolutionary research. Commun ACM 53(9):36–40
44. Alexandru AB, Gatsis K, Shoukry Y, Seshia SA, Tabuada P, Pappas GJ (2020) Cloud-based quadratic optimization with partially homomorphic encryption. IEEE Trans Autom Control 66(5):2357–2364
45. Boneh D, Goh E-J, Nissim K (2005) Evaluating 2-dnf formulas on ciphertexts. In: Theory of cryptography conference. Springer, pp 325–341
46. Xiong L, Dong D (2019) Reversible data hiding in encrypted images with somewhat homomorphic encryption based on sorting block-level prediction-error expansion. J Inf Secur Appl 47:78–85
47. Viand A, Jattke P, Hithnawi A (2021) Sok: fully homomorphic encryption compilers. In: IEEE symposium on security and privacy (SP). IEEE, pp 1092–1108
48. Jager T (2012) The generic composite residuosity problem. In: Black-box models of computation in cryptology. Springer, pp 49–56
49. Zhang S, Tong H (2016) Final: fast attributed network alignment. In: Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining, pp 1345–1354
50. Man T, Shen H, Liu S, Jin X, Cheng X (2016) Predict anchor links across social networks via an embedding approach. In: Ijcai, vol 16, pp 1823–1829
51. Zhang S, Tong H (2018) Attributed network alignment: Problem definitions and fast solutions. IEEE Trans Knowl Data Eng 31(9):1680–1692
52. Dickison ME, Magnani M, Rossi L (2016) Multilayer social networks. Cambridge University Press, Cambridge
53. Amara A, Taieb MAH, Aouicha MB (2022) Cross-network representation learning for anchor users on multiplex heterogeneous social network. Appl Soft Comput 118:108461