Hindawi
Security and Communication Networks
Volume 2023, Article ID 9763076, 1 page
https://doi.org/10.1155/2023/9763076

Retraction

Retracted: Influential Incremental Learning-Based Privacy Preservation for Social Network Information

Security and Communication Networks

Received 11 July 2023; Accepted 11 July 2023; Published 12 July 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. S. Alshudukhi, "Influential Incremental Learning-Based Privacy Preservation for Social Network Information," *Security and Communication Networks*, vol. 2022, Article ID 8150325, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8150325, 9 pages
https://doi.org/10.1155/2022/8150325

Research Article

Influential Incremental Learning-Based Privacy Preservation for Social Network Information

Jalawi Sulaiman Alshudukhi

College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia

Correspondence should be addressed to Jalawi Sulaiman Alshudukhi; j.alshudukhi@uoh.edu.sa

Received 9 February 2022; Revised 17 March 2022; Accepted 30 March 2022; Published 13 May 2022

Academic Editor: Bharat Bhushan

Social network influence dissemination focuses on employing a small number of seed sets to generate the most significant possible influence in social networks and considers forwarding to be the only technique of information transmission, ignoring all other ways. Users, for example, can post a message via this mode of distribution (called para), which is difficult to trace, posing a danger of privacy leakage. This research tries to address the aforementioned issues by developing a social network information transmission model that supports the paranormal relationship. It suggests a way of disseminating information called Local Greedy, which aids in the protection of user privacy. Its effect helps to reconcile the conflict between privacy protection and information distribution. Aiming at the enumeration problem of seed set selection, an incremental strategy that supports privacy protection is proposed to construct seed sets to reduce time overhead; a local influence subgraph method of computing nodes is given to estimate the influence of seed set propagation quickly; the group satisfies the constraints of privacy protection, and a plan is proposed to deduce the upper limit of the probability of node leakage state, avoiding the time cost of using the Monte Carlo method using the crawled Sina Weibo dataset. Experimental verification and example analysis are carried out, and the results show the effectiveness of the proposed method.

1. Introduction

Social networks, as an emerging network media, drastically enhance the speed of information dissemination and allow information to be distributed more efficiently and extensively. People use social networks extensively in recommendation systems, viral marketing, advertising, expert finding, and other disciplines, reaping the full benefits of information transmission. However, while quick transmission of information provides many benefits to users, it also presents hidden risks of privacy leakage.

In an existing social network, to protect their privacy, the information publisher can restrict the objects, which can see information by setting it to be visible only to specified friends. However, most social platforms provide a forwarding function, allowing those who know information to continue forward, thereby causing privacy leakage.

Some social platforms provide the function of setting invisible objects; even if information has been forwarded many times, it is still invisible to the specified things. For example, suppose A sends a message, B then forwards the message from A, C forwards the message from B, and D is a friend of B or C, but if A sets the object D to be invisible, then D cannot pass B or C's forwarding to see this message. However, such a feature does not entirely prevent privacy leaks from happening, as shown in Figure 1. For example, if B does not directly forward A, but sends it after describing information in the message sent by A in its language, assuming that D is a friend of B or someone who forwarded B's message, then D can see this. Information to obtain A's privacy is referred to in this article as reposting. It can be seen that both forwarding and reposting behaviors of users in social networks may cause privacy leakage, and privacy leakage caused by reposting behaviors is difficult to detect or prevent [1, 2].

The current research on social networks mainly focuses on influence maximization and privacy protection. However, the existing studies related to influence dissemination

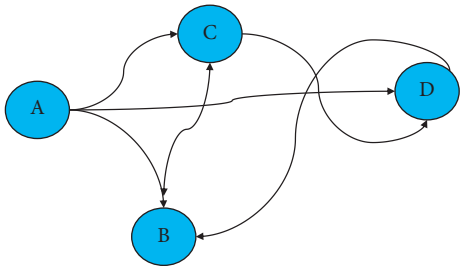

Figure 1: Information diffusion on social media.

do not consider the privacy protection needs of users, and the research related to privacy protection does not pay attention to the influence of users [3, 4]. Moreover, some information propagation models are difficult to effectively model the propagation process of privacy leakage in social networks. This brings three challenges to the research of social networks: (1) how to ensure the personalized privacy protection needs of users; (2) how to maximize the influence of information published by users; and (3) how to balance privacy protection and information dissemination the contradiction.

For example, when a user publishes information on a social network or a recommendation system pushes information, how to select relevant users (seed nodes) to make information so that information disseminated through social networks can be seen by more people (maximum influence) and will not be caught by blocked users [5–7]; similarly, when making brand recommendations through viral marketing, how to select interested users (seed nodes) in social networks to push information to maximize the number of people who spread (maximize influence), and avoid spread to nontarget user groups (blocked users).

To address the aforementioned issues, this paper first designs a social network information dissemination model that supports forwarding and rewetting behavior, in order to supplement and correct the source of privacy leakage; then, based on the social network information dissemination model, we proposed a method of constructing an information dissemination network that realizes the fusion modeling of forwarding behavior and retelling behavior. The maximizing technique chooses the seed set by calculating the upper limit of the probability of node leaking, in conjunction with privacy protection constraints and the heuristic impact maximization algorithm. As a result, it maximizes the influence of information dissemination while satisfying the privacy protection constraints. Through experimental verification and instance analysis on the crawled Sina Weibo dataset, the results show that the method in this paper can ensure maximum dissemination influence while protecting user privacy [8, 9].

The main contributions of this paper include the following:

(1) It is proposed that a social network information transmission model that supports the paranormal relationship be developed. The social network dissemination model that only activates new nodes in the forwarding method supports paraphrasing behavior and can effectively model paraphrasing behavior in social networks, providing mathematical model support for the tracking of privacy leakage caused by the propagation of paraphrasing behavior.

(2) This paper proposes constructing an information dissemination network that supports narration behavior. By solving the three-category problem of the forwarding edge, narrating edge, and no behavior of users paying attention to the Web, it can judge whether users in the network participate in the dissemination and predict the dissemination behavior of the message when it spreads to the user. The probability distribution complements the omission of information dissemination channels in traditional social networks.

(3) A privacy-preserving social network information dissemination influence maximization method Local Greedy is proposed. The seed set is constructed through an incremental strategy. The local influence subgraph of nodes is calculated, the influence of seed set propagation is quickly calculated, and the node leakage state is proposed. The probability upper limit calculation method ensures that the seed set meets the privacy protection constraints, reduces the time overhead, and balances the contradiction between influence and privacy protection.

2. Related Work

The current research on information dissemination and privacy protection in social networks is divided into four parts: information dissemination model, information dissemination prediction, influence dissemination, and social network access control.

2.1. Information Dissemination Model. Typical information dissemination models applied to social networks include independent cascade models [10], linear threshold models [11], and infectious disease models [12]. Based on the independent cascade model, the author [13] proposed a dissemination network model to describe the knowledge dissemination process of social question-answering websites. Furthermore, they gave a social question-answering website knowledge dissemination network inference method. Based on the linear threshold model and value cocreation theory, the author [14] proposed a social network communication and corporate value cocreation strategy model for the characteristics of negative word-of-mouth. They analyzed the impact of negative word-of-mouth on social media through simulation experiments the main influencing factors of outbreaks in the network. Based on the traditional SIR (susceptible infected recovered) infectious disease model, the author [15] proposed a new social network public opinion propagation dynamics model and used a particle swarm algorithm to consider the psychological characteristics and behavioral factors of users comprehensively. Taking the hot events that happened on Weibo in 2016 as an example, the optimal solution of the model

parameters is solved, and the experimental data are verified. The randomness of the linear threshold model only depends on the randomness of the threshold of the node being affected, and it is challenging to select the point; the infectious disease model is only suitable for the macro description of the propagation process but does not consider the specific propagation path, and the independent cascade model has better scalability by using the probability on edge to describe the strength or likelihood of information propagation. Therefore, the independent cascade model will serve as the basis for the information propagation model proposed in this paper. Researchers are also providing the security protocols [4–6] to maintain the integrity and confidentiality of the health care-related information over the wireless communication network.

2.2. Information Dissemination Prediction. Information dissemination prediction refers to learning the interests and behavior rules of users in social networks through a particular method to predict whether users will participate in disseminating certain information. According to the different basic assumptions, research on user information dissemination prediction can be divided into four categories: prediction based on historical user behavior, prediction based on user text interest, prediction based on user group influence, and prediction based on joint feature learning. The author [16] established a cooperative recommendation model by capturing the features related to the propagation in the user's historical behavior and combining the collaborative filtering and propagation process characteristics to predict the information propagation process based on the forwarding behavior. The author [17] proposed a propagation prediction method that combines user text, network structure, and time and used a nonparametric statistical model to infer forwarding behavior, and then predict the information propagation process. The author [18] defined interest-oriented influence, social-oriented influence, and epidemic-oriented influence. The comprehensive analysis of these three influences decided whether a user would perform a forwarding operation. Based on joint feature learning, the author [19] jointly considered factors such as forwarding history, user influence, time, and user interest and studied the impact of each element on forwarding behavior within a learning ranking framework. Information dissemination prediction methods are relatively abundant and essential for social network information dissemination analysis. However, existing studies often regard forwarding as the only way of information dissemination while ignoring other possible dissemination behaviors. Researchers are also providing data hiding techniques [20] for securing information on social media.

2.3. Influence Spread. Influence propagation describes the propagation mode of influence in a social network, that is, how the state of a node affects the shape of adjacent nodes on the Web and spreads the form on the network. Optimizing the spread of influence is the primary purpose of influence spread modeling, and the problem of maximizing power is the core content of this research. The current research methods are mainly divided into three categories: designing heuristic algorithms according to the specific characteristics of the spread model; Monte Carlo greedy algorithm for efficiency optimization; and using community discovery as an intermediate step, the influence problem is transformed from the user level to the community level. The heuristic algorithm is constructed based on intuition or experience and aims to give a feasible solution to the influence maximization problem under limited time and space loss. The author [21] improved the robustness and stability of the algorithm by synthesizing the influence ranking and influence estimation methods; the author [22] introduced multiple optimization strategies to ensure a shorter running time and lower memory usage. We maximize impact seed collection quality. Since the greedy approach cannot quickly process large-scale network inputs containing millions of orders in a relatively short time, the optimization of the Monte Carlo greedy algorithm is often solved by reducing the running time [23] or using a sketch-based method [24]. We influence maximization problem. The way to transform the influence problem to the community level is to maximize the influence from solving the performance guarantee that the heuristic algorithm cannot provide. The author [24] precalculated user community influence and selected seed sets from top to bottom to maximize impact; the author [25] proposed a seed selection algorithm based on community discovery, which realized the problem of maximization efficient selection of medium seed sets. The influence maximization problem does not consider the privacy protection needs of users. Still, the heuristic algorithms in related research usually have faster running time and better scalability than other methods, so this paper uses the influence maximization heuristic. A social network information dissemination method that supports privacy protection is proposed based on the algorithm.

3. Influence Maximization Approaches to Support Privacy Protection (Local Greedy)

3.1. Method Overview. According to the information dissemination model of Definition 4 and the constraints of privacy protection, the optimization objective of the algorithm is shown in thefollowing equation:

$$\max \mathrm{SIG}(\mathrm{S}), \text{s.t. } \mathrm{S} \subset \mathrm{F}, \quad \forall \mathrm{oj} \in \mathrm{O}, \mathrm{Q}(\mathrm{S}, \mathrm{oj}) \leq \mathrm{Tj}, \tag{1}$$

$$\max_R P_H(R), \text{s.t.} R \subset J \quad \forall o_j \in O, \mathrm{T}\left(\mathrm{R}, \mathrm{o_j}\right) \leq \tau_j. \tag{2}$$

In formula (1), $P_H(R)$ represents the influence of the seed set R on the social network H, J represents the optional set of seed nodes; that is, the seed set R must be a subset of J, and O means the network. The key node set of, which is the blacklist set by default, the user hopes that information will leak to the nodes in the set O with the lowest probability; $\mathrm{T}(\mathrm{R}, \mathrm{o_j}) \leq \tau j$ represents the privacy protection constraint, that is, the selected seed set R. It must be guaranteed that the probability of information leakage to node oj is less than τj,

and each element in set O corresponds to a privacy protection constraint.

There are three main difficulties in the problem of maximizing influence under the constraints of privacy protection constraints:

How to select the set of seed nodes, the number of subsets of the set J is $2|J|$, and enumerating all the subsets will cause a huge time overhead

How to estimate the size of the influence generated by the set of seed nodes and develop the strongest possible impact on the social network

How to ensure that the seed set generated by the algorithm can meet the requirements of privacy protection constraints

To deal with the three difficulties of the influence maximization problem under the constraints of privacy protection, this section proposes a privacy-preserving influence maximization method Local Greedy. Aiming at the issue of enumerating all subsets when selecting a seed set, the seed set is incrementally constructed based on a greedy strategy to avoid the time overhead caused by enumeration; a method for calculating the local influence subgraph of nodes is given to quickly estimate the influence caused by the propagation of the seed set. To ensure that the seed set satisfies the privacy protection constraints, a calculation method is proposed to derive the upper limit of the probability of node leakage state, to judge whether the seed set satisfies the privacy protection constraints, and to avoid the time overhead caused by using the Monte Carlo method. In this section, the algorithm is designed in three aspects according to the seed set selection strategy, the impact size estimation method, and the upper limit calculation of the node leakage probability.

3.2. Seed Set Selection Strategy. To deal with the difficulty (1) in Section 4.1, this paper uses an incremental method to generate the seed set R, initially making R an empty set and adding an element to the set R during each iteration at each iteration, the part with the most significant influence increment is selected among all the nodes that satisfy the privacy leakage condition constraint after adding. The definition $\Delta(R)$ represents the basis for each choice of the algorithm as follows:

$$\Delta(R) = \arg\max\{P_H(R \cup \{y\}) - P_H(R)\}, \tag{3}$$

$$y \in J/R, \quad \forall o_j \in O, \mathrm{T}\left(\mathrm{R}, \mathrm{o_j}\right) \le \tau_{\mathrm{j}}. \tag{4}$$

The selection of the seed set is based on the greedy strategy, which is mainly reflected in the following two aspects:

(1) There is monotonicity between the privacy protection constraint and the set R, when the set when R does not meet the restrictions of the privacy protection constraints, any superset of the set R does not meet the restrictions of the privacy protection constraints, so the incremental construction from the empty set can stop the algorithm in time to avoid redundant calculations

(2) $P_H(R)$ satisfies both monotonicity and submodularity, so each selection of the element addition that makes the most significant increment of $P_H(R)$ has a specific theoretical guarantee

3.3. Influence Calculation Method. The traditional Monte Carlo method is very inefficient in terms of time efficiency. This section proposes a non-Monte Carlo simulation method to quickly calculate the probability distribution of the state of each node after selecting a set of seed nodes. For a path of length $l-1$ and $M = <n_1, n_2, \ldots, n_l>$, we define the function $zp(M) = \prod_{i=1}^{l-1}(M_{n_0,n_{i+1}} + r_{n_i,n_{i+1}})$, which is called a path. The influence weight of M indicates the probability of the path appearing when the two attributes of each edge on the path are added together into one.

Definition 1 (maximum ideal path). For all paths $S(H, x, y)$ from node u to node v in the social network $H = (X, F, U, M)$, we define the maximum ideal path as node x to node y. The path $NIP(x, y)$ with the most significant influence weight between them is as shown in the following equation:

$$NIP(x, y) = \mathrm{ragmax}\{zp(M) | M \in S(\mathrm{H}, \mathrm{x}, \mathrm{y})\}. \tag{5}$$

Considering the probability of a single node y being affected, when $zp(NIP(x, y))$ is small, even if node x is involved, the probability of information reaching node y through it is usually tiny, that is, whether node y is affected. It is irrelevant whether node u is affected or not. So then, when estimating the probability of node y being affected, we can only consider the subgraph formed by the nodes and edges of its neighboring regions.

Definition 2 (local influence subgraph). For the information dissemination model $H = (X, F, U, M)$ including the subgraph of node y, we define the local influence subgraph of node y about θ as the following formula

$$\mathrm{MIA}(\theta, \mathrm{v}) = \cup \mathrm{u} \in \mathrm{V}, \mathrm{wp}(\mathrm{MIP}(\mathrm{u}, \mathrm{v})) > \theta, \tag{6}$$

$$\mathrm{MIP}(\mathrm{u}, \mathrm{v}) \tag{7}$$

$$NIA(\theta, x) = \bigcup_{y \epsilon x, \mathrm{zp}(\mathrm{NIP}(\mathrm{x},\mathrm{y})) > \theta} \mathrm{NIP}(\mathrm{x}, \mathrm{y}), \tag{8}$$

where θ is a parameter and $NIA(\theta, x)$ is obtained by taking the union of all paths $NIP(x, y)$ satisfying the constraint $\mathrm{zp}(\mathrm{NIP}(\mathrm{x}, \mathrm{y})) > \theta$. When θ is smaller, the local influence subgraph of node y represented by $NIA(\theta, x)$ contains more edges. And by definition, the local influence subgraph $NIA(\theta, x)$ is a tree structure, so the probability of influenced node y can be calculated in linear time complexity using dynamic programming. The influence calculation method proposed in this paper calculates the probability that node v is in each state, at last, considering only the nodes and edges in $NIA(\theta, x)$, and the probability of reaching the state is

expressed as $bp(R, x, NIA(\theta, x))$, and the probability of being in a leaking state is expressed as $bq(R, x, NIA(\theta, x))$. Where there is no confusion, $bp(R, x, NIA(\theta, x))$ is abbreviated as $bp(x)$ and $bq(R, x, NIA(\theta, x))$ is abbreviated as $bq(x)$. Further, by calculating the local influence subgraph of all nodes to obtain the $bp(R, x, NIA(\theta, x))$ and $bq(R, x, NIA(\theta, x))$ of each node, you can do it without using Monte Carlo. In the case of Luo's simulation, an estimate of the total influence size produced by the seed set R is obtained as follows:

$$P_H * (R) = \sum_{x \in X} bp(x) + bq(x). \tag{9}$$

(8) can efficiently estimate the influence of the seed node set without using the Monte Carlo method. The algorithm efficiency is only related to the number of nodes n and the average adjacent area size $B\theta$ of the nodes, and the time complexity is $O(n \times B_\theta)$. Adding in the complexity of computing the local influence subgraph for each node, the total complexity is $O(n \times B_\theta \times lb\ B_\theta)$.

3.4. Calculation of Upper Limit of Node Leakage Probability. Considering any node o in the node set O, to make $T(R, o) < \tau$, then for the in-neighbor set $N^{in}(o)$ of node o, the probability of the elements in the leak state should not be too large. Defining $vq(y)$ to represent the upper limit of $T(R, y)$, the range of $vq(y)$ can be inferred by the following rules so that each node can obtain an upper limit as small as possible. The calculation conditions are given below.

(1) If $o_j \in O$, then $vq(o_j) \le \tau j$;

(2) If $vq(v) \le x$, then $\forall u \in N^{in}(v)$, $uq(u) \le x/(m_{u,v} + r_{u,v})$. The smaller the value of $vq(y)$ is, the more the effect and efficiency of the algorithm can be improved by checking whether the conditions of equation (9) are satisfied.

$$J(R) = \begin{cases} 0\, if \exists o_j \in O, & T(\mathrm{R}, \mathrm{o_j}) \le \tau_j, \\ P_H(R), & \text{otherwise.} \end{cases} \tag{10}$$

Specifically, the calculation method for the upper limit of the node leakage probability proposed in this paper uses $uq(v)$ to determine whether the current seed set will violate the restrictions brought by the privacy protection constraints, that is, check $\forall u \in V$, $aq(v, \theta, MIA(\theta, u)) \le uq(v)$ condition is satisfied.

The essence of the calculation method for the upper limit of node leakage probability is an extension of the shortest path algorithm. By extending the original limitation of only key nodes to the whole graph after obtaining $uq(v)$, it can be compared with the influence mentioned in this paper. Moreover, by combining computing methods, it can estimate whether the result of the seed set is satisfying and whether the privacy protection constraint is satisfied.

4. Experimental Design

4.1. Evaluation Parameter. This paper uses the communication network constructed based on Weibo data as the experimental social network and uses three indicators for evaluation:

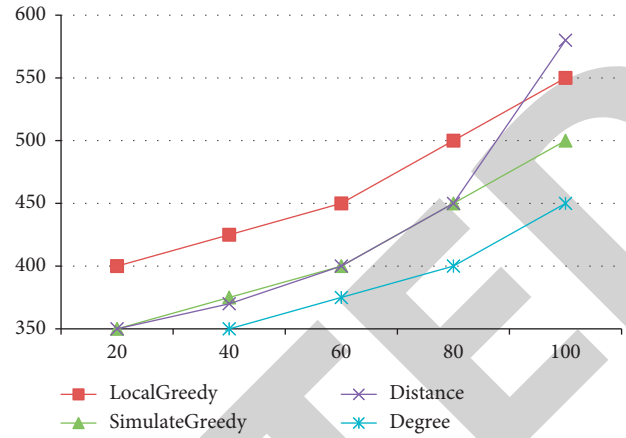

Figure 2: Comparisons of algorithms composite index.

(1) Influence index: for the seed set R generated by the algorithm, the mean value of the influence PH (R) when the seed set R satisfies the privacy protection constraints is used as the evaluation index, called the influence index. The larger the influence index is, the greater the influence of the seed set generated by the algorithm in the dissemination process, and the better the effect.

(2) Comprehensive indicators: considering that the algorithm has two goals, maximizing the influence of propagation, and satisfying the constraints of privacy protection, the function $J(H, R)$ is defined here as the evaluation index of the algorithm, and the following are abbreviated as $J(R)$, called the comprehensive index:

$$J(R) = \begin{cases} 0\, if \exists o_j \in O, & T(\mathrm{R}, \mathrm{o_j}) \le \tau_j, \\ P_H(R), & \text{otherwise.} \end{cases} \tag{11}$$

When the seed set R does not satisfy the privacy protection constraints, $J(R)$ is 0. In other cases, $J(R)$ equals the influence size $P_H(R)$ of the seed set R on the network. For the comprehensive index, when the probability that the seed set R generated by the algorithm satisfies the constraints of privacy protection is greater, the greater the index is, the better the effect of the algorithm is. In addition, when the influence of the seed set R generated by the algorithm is more significant, the indicator is also more excellent. Therefore, $J(R)$ is a comprehensive indicator of the algorithm's privacy protection effect and dissemination influence.

(3) Running time index: shorter running time means better efficiency for algorithms with similar effects. Therefore, the experiment counts the running time of each algorithm to evaluate its efficiency.

The experiments in this paper are all completed on a single machine platform, including Ubuntu 16.04.10 operating system, 1 Intel Xeon Silver 4110 CPU, 2 NVIDIA GeForce

Table 1: Composite index comparison.

Optional collection size	Local Greedy	Simulate Greedy	Distance	Degree
20	400	350	350	320
40	425	375	370	350
60	450	400	400	375
80	500	450	450	400
100	550	500	580	450

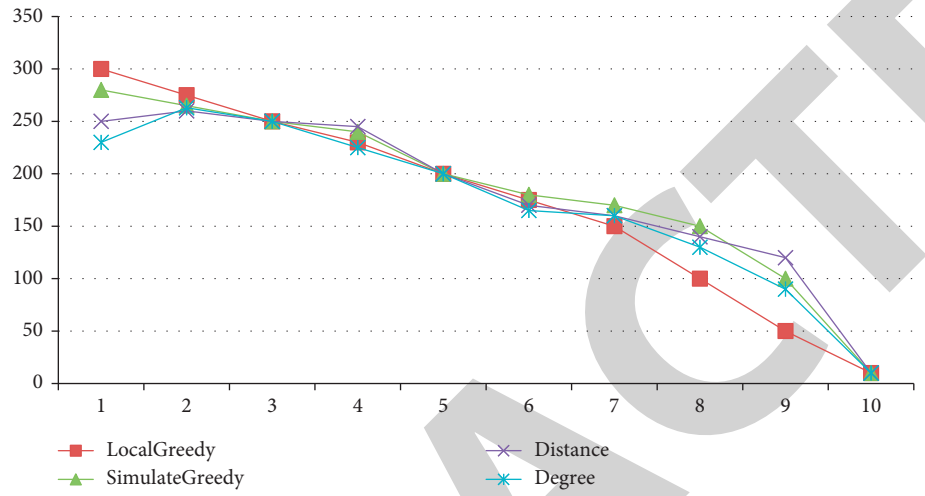

Figure 3: Influence of the number of privacy protection constraints on effect.

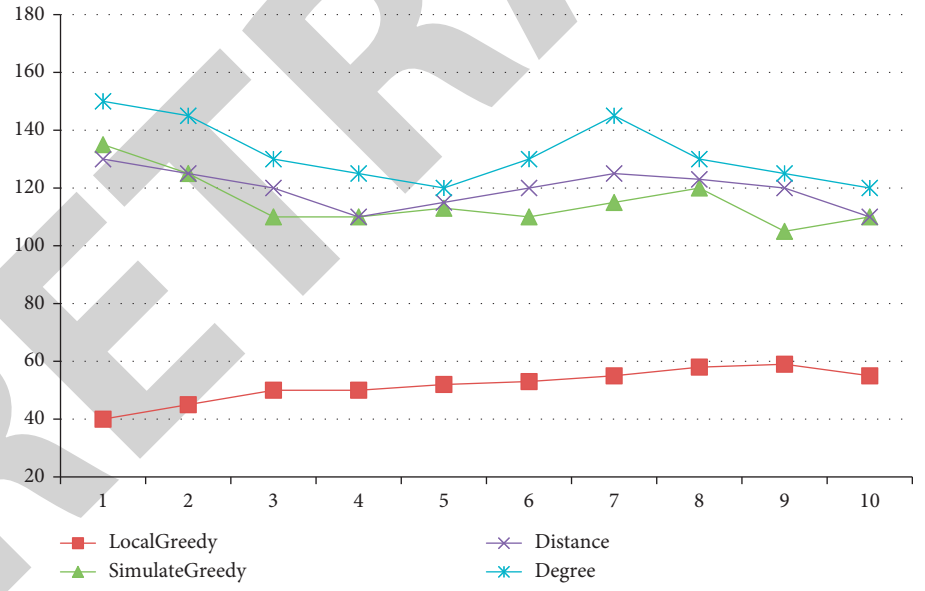

Figure 4: Influence of the number of privacy protection constraints on running time.

GTX 1080 Ti (11 GB) GPUs, and 32 GB memory. All algorithms are implemented using Python 3.6.

4.2. Results and Analysis. In addition to using $J(R)$ and $P_H(R)$ as the basis for judging the algorithm's effectiveness, the experiment also evaluates the algorithm's efficiency according to its running time.

4.2.1. Comparison of Each Index of the Algorithm. Figure 2 and Table 1 draw the line graphs of the algorithm's running time, influence index, and comprehensive index when the optional set size is taken as the abscissa.

It can be seen from Figure 2 that with the increase of the size of the optional set, the running time of the Simulate Greedy algorithm has the most significant growth trend, the Degree algorithm and the Distance algorithm are the same,

Table 2: Influence of the number of privacy protection constraints on effect.

Optional collection size	Local Greedy	Simulate Greedy	Distance	Degree
1	300	280	250	230
2	275	265	260	263
3	250	250	250	250
4	230	240	245	225
5	200	200	200	200
6	175	180	170	165
7	150	170	160	160
8	100	150	140	130
9	50	100	120	90
10	10	10	10	10

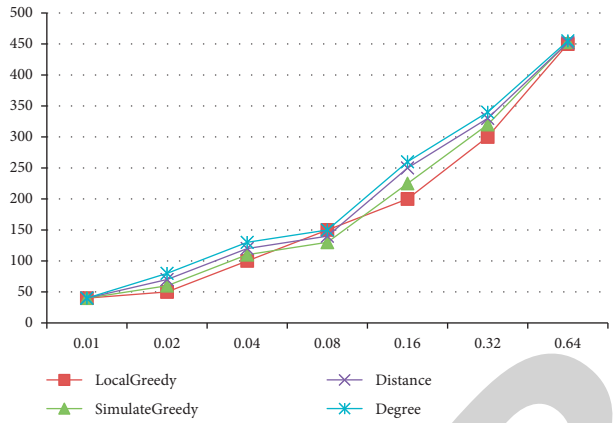

Figure 5: Influence of privacy protection parameter on composite index.

and the algorithm in this paper, that is, the Local Greedy algorithm, has the most miniature growth trend. In terms of absolute running time, the algorithm in this paper is also the best. The Degree algorithm is quite close to the Distance algorithm, and the Simulate Greedy algorithm takes the longest time. When the size of the optional set becomes more extensive because more nodes can be used as the seed set, the effect of the algorithm should be better and better, which has been verified in Figures 3 and 4. In addition, it can be seen from the figure that the longest running time of the Simulate Greedy algorithm is slightly better than the two heuristic algorithms, and the heuristic algorithm based on the node degree is better than the heuristic algorithm based on the average distance. Combining the above algorithm effect comparison, it can be concluded that the algorithm in this paper has a significant improvement in running time compared to the mainstream algorithm and has certain advantages in effect.

4.2.2. The Impact of Privacy Protection Constraints on Algorithms. When the critical node set O is more extensive (see Table 2), there are more constraints on privacy protection and more conditions in the algorithm solving process. Figure 5 draws the line graphs comparing the algorithm's influence index and running time with the number of privacy protection constraints as the abscissa.

Table 3: Influence of the number of privacy protection constraints on running time.

Optional collection size	Local Greedy	Simulate Greedy	Distance	Degree
1	40	135	130	150
2	45	125	125	145
3	50	110	120	130
4	50	110	110	125
5	52	113	115	120
6	53	110	120	130
7	55	115	125	145
8	58	120	123	130
9	59	105	120	125
10	55	110	110	120

Table 4: Influence of privacy protection parameter on composite index.

Optional collection size	Local Greedy	Simulate Greedy	Distance	Degree
0.01	40	40	40	40
0.02	50	60	70	80
0.04	100	110	120	130
0.08	150	130	140	150
0.16	200	225	250	260
0.32	300	320	330	340
0.64	450	453	452	455

When the number of privacy protection constraints increases, the algorithm's running time in this paper has a tiny growth trend, and the running time advantage is obvious. And in the case of various privacy protection constraints, the effect of this algorithm is still better than other algorithms.

Figure 5 with Tables 3 and 4 shows the change of the comprehensive index of the algorithm when the privacy protection parameter τ is changed. When the value of τ is more significant, the constraint of privacy protection is weaker. The seed set generated by the algorithm is easier to meet the conditions of privacy protection; thus, producing more substantial influence when $\tau \leq 0.04$, the effect of the algorithm in this paper is comparable to other algorithms. For larger τ values, the algorithm in this paper has certain advantages in development.

5. Conclusion

Aiming at the contradiction between maximizing influence dissemination and user privacy protection in the process of social network information dissemination, this paper proposes a social network information dissemination model and inference method that supports paraphrase relationship, as well as the seed set selection algorithm Incred Greedy, the local influence calculation algorithm Local Influence, and the node leakage probability algorithm Calculate Bound. On this basis, the Local Greedy algorithm is proposed. Experimental verification and instance analysis are carried out on the crawled Sina Weibo dataset. The results suggest that the Local Greedy algorithm can enhance dissemination influence while protecting user privacy. Future research will investigate the characteristics of social network information dissemination and the reasons for privacy leakage, take into account changes in the amount of information during the dissemination process, and introduce more features in the process of dissemination network construction based on the model and method proposed in this paper [26–29].

Data Availability

The data used to support the findings of this study are available from the author upon request (j.alshudukhi@uoh.edu.sa).

Conflicts of Interest

The author declares that he has no conflicts of interest.

References

[1] T. Puri, M. Soni, G. Dhiman, O. Ibrahim Khalaf, M. alazzam, and I. Raza Khan, "Detection of emotion of speech for RAVDESS audio using hybrid convolution neural network," *Journal of Healthcare Engineering*, vol. 2022, pp. 1–9, Article ID 8472947, 2022.

[2] W. Viriyasitavat, L. D. Xu, A. Sapsomboon, G. Dhiman, and D. Hoonsopon, "Building trust of Blockchain-based Internet-of-Thing services using public key infrastructure," *Enterprise Information Systems*, pp. 1–24, 2022, in Press.

[3] G. Dhiman, S. Juneja, H. Mohafez et al., "Federated learning approach to protect healthcare data over big data scenario," *Sustainability*, vol. 14, no. 5, p. 2500, 2022.

[4] N. Gupta, K. Gupta, D. Gupta, S. Juneja, and H. Turabieh, "Gaurav dhiman, sandeep kautish, and wattana viriyasitavat. "Enhanced virtualization-based dynamic bin-packing optimized energy management solution for heterogeneous clouds," *Mathematical Problems in Engineering*, vol. 2022, Article ID 8734198, 11 pages, 2022.

[5] S. Sharma, S. Gupta, D. Gupta et al., "Deep learning model for the automatic classification of white blood cells," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 7384131, 13 pages, 2022.

[6] R. Dinesh Kumar, E. Golden Julie, Y. Harold Robinson, S. Vimal, G. Dhiman, and M. Veerasamy, "Deep convolutional nets learning classification for artistic style transfer," *Scientific Programming*, vol. 2022, Article ID 2038740, 9 pages, 2022.

[7] G. Dhiman, J. Rashid, J. Kim, S. Juneja, W. Viriyasitavat, and K. Gulati, "Privacy for healthcare data using the byzantine consensus method," *IETE Journal of Research*, pp. 1–12, 2020, in Press.

[8] S. Kanwal, J. Rashid, J. Kim, S. Juneja, G. Dhiman, and A. Hussain, "Mitigating the coexistence technique in wireless body area networks by using superframe interleaving," *IETE Journal of Research*, pp. 1–15, 2022, in Press.

[9] V. Leiva and G. Dhiman, *Archery Algorithm: A Novel Stochastic Optimization Algorithm for Solving Optimization Problems*, in Press.

[10] C. Yuan and D. Ji, "Stochastic asymptotically stability of an information diffusion model with random perturbation in social network," in *Proceedings of the IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, pp. 1916–1920, Chongqing, China, May 2019.

[11] P. Shi, M. Fang, H. Lin, and L. Ding, "A method for information source locating with incomplete observation of online social network," in *Proceedings of the International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, pp. 98-99, Beijing, China, October 2015.

[12] H. Chang and H. Shen, "A modified community-level diffusion extraction in social network," in *Proceedings of the 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pp. 509–512, Gold Coast, QLD, Australia, December 2019.

[13] M. Eslami, H. R. Rabiee, and M. Salehi, "DNE: a method for extracting cascaded diffusion networks from social networks," in *Proceedings of the IEEE 3rd International Conference on Privacy, Security, Risk and Trust and 2011*, pp. 41–48, Boston, MA, USA, October 2011.

[14] C. Jiang, A. D'Arienzo, W. Li, S. Wu, and Q. Bai, "An operator-based approach for modeling influence diffusion in complex social networks," *Journal of Social Computing*, vol. 2, no. 2, pp. 166–182, 2021.

[15] A. Hajibagheri, H. Alvari, A. Hamzeh, and S. Hashemi, "Community detection in social networks using information diffusion," in *Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pp. 702-703, Istanbul, Turkey, August 2012.

[16] J. Wang, D. Zhang, and R. Xia, "An information diffusion model of micro public good based on social network," in *Proceedings of the 6th International Conference on Measuring Technology and Mechatronics Automation*, pp. 112–116, Zhangjiajie, China, January 2014.

[17] B. Klein and H. Hlavacs, "An effort based social diffusion approach for mobile encounter networks," in *Proceedings of the International Conference on Computational Aspects of Social Networks (CASoN)*, pp. 152–157, Salamanca, Spain, October 2011.

[18] G. Sarna, R. Walia, and M. Bhatia, "Analysis of information diffusion in dynamic information networks," in *Proceedings of the 2014 International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 1107–1111, Mysore, India, November 2014.

[19] C. Jiang, Y. Chen, and K. J. R. Liu, "Evolutionary dynamics of information diffusion over social networks," *IEEE Transactions on Signal Processing*, vol. 62, no. 17, pp. 4573–4586, 2014.

[20] A. Shobanadevi, G. Maragathm, M. P. G Syam et al., "Internet of Things-Based Data Hiding Scheme for Wireless Communication," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 6997190, 8 pages, 2022.

[21] Y. Chai, Y. Wang, and L. Zhu, "A stochastic information diffusion model in complex social networks," *IEEE Access*, vol. 7, Article ID 175897, 2019.

[22] S. Das and A. Biswas, "Deployment of information diffusion for community detection in online social networks: a comprehensive review," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 5, pp. 1083–1107, 2021.

[23] X. Yang, M. Dong, X. Chen, and K. Ota, "Recommender system-based diffusion inferring for open social networks," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 1, pp. 24–34, 2020.

[24] S.-A. Floria, F. Leon, and P. Cascaval, "Analyzing the effects of virality and topology for information diffusion in social networks," in *Proceedings of the 21st International Conference on System Theory, Control and Computing (ICSTCC)*, pp. 866–871, Sinaia, Romania, October 2017.

[25] M. Oono, "A method for extracting influential nodes while considering the development of social networks," in *Proceedings of the 2nd International Conference on Cloud and Green Computing*, pp. 456–459, Xiangtan, China, November 2012.

[26] P. Kumaran and S. Chitrakala, "Community formation based influence node selection for information diffusion in online social network," in *Proceedings of the 2016 International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE'16*, pp. 1–6, Kovilpatti, India, January 2016.

[27] L. He, W. Guo, Y. Chen, K. Guo, and Q. Zhuang, "Discovering overlapping communities in dynamic networks based on cascade information diffusion," *IEEE Transactions on Computational Social Systems*, pp. 1–13, 2021, in Press.

[28] S. Gao, H. Pang, P. Gallinari, J. Guo, and N. Kato, "A novel embedding method for information diffusion prediction in social network big data," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 2097–2105, Aug. 2017.

[29] M. E. Mehdiabadi, H. R. Rabiee, and M. Salehi, "Diffusion-aware sampling and estimation in information diffusion networks," in *Proceedings of the International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, pp. 176–183, Amsterdam, Netherlands, September 2012.