Computers & Security 119 (2022) 102778

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

# Everything you control is not everything: Achieving intention-concealed visit on social networks

Helin Li[a], Hui Zhu[a,*], Xiaodong Lin[b], Rongxing Lu[c], Zhipeng Yu[a], Wei Lan[a]

[a] National Key Laboratory of Integrated Networks Services, Xidian University, Xi'an, China
[b] School of Computer Science, University of Guelph, Ontario, Canada
[c] Faculty of Computer Science, University of New Brunswick, New Brunswick, Canada

ARTICLE INFO

*Article history:*
Received 20 August 2021
Revised 17 April 2022
Accepted 26 May 2022
Available online 28 May 2022

*Keywords:*
Intention-concealed
Privacy preserving
Browsing trajectories
Online social networks
Interest profile

ABSTRACT

With the flourishment of Artificial Intelligence (AI), the quality of services on online social networks (OSNs) has improved tremendously. Through the introduction of AI into OSNs, providers enhance the users experience. However, the risk of data misuse has also been magnified. And there has been a trend towards users' mistrust when it comes to sharing their true intention on OSN platforms, primarily because of privacy concerns. In this paper, we propose an effective intention-concealing visitation framework named Aviv, which acts as a credible and private third-party where it generates artificial intention-concealed browsing (AICB trajectories) for users to conceal their true intentions. The browsing trajectory is a sequence composed of blogs, bloggers, news, or a mixture containing visitable content. Specifically, Aviv first extracts accessible graphs composed of visitable contents from applied OSN platforms. Then an elaborate and personalized divert scoring process is conducted to measure optional decoy visits' effectiveness. Finally, using the divert scoring values, elaborate and personalized decoy visits are picked out, Aviv composes AICB trajectories with true intentions and picked decoy visits. Aviv is implemented as a credible private third-party and tested on a real OSN, the performance evaluation results show that Aviv is effective and efficient.



## 1. Introduction

With the rise of prominent social platforms such as Facebook, Twitter, and Weibo, there have been a large number of implementations to provide personalized services by these Online Social Networks (OSNs). These implementations of personalized services have thus cultivated an improved User experience (Shen et al., 2020; Wang et al., 2016), and at the same time, the daily lives of these individuals have been significantly enriched (Zhou and Fan, 2019).

However, to achieve these personalized services that improve the entire experience, users must provide their private browsing intention to these OSN platforms, where the intention is defined as "a distinctive attitude, not to be conflated with or reduced to ordinary desires and beliefs", and this distinctive attitude is involved both in intending to do something and in doing something intentionally (Bratman, 1987). Thus, a user faces serious privacy risks (Bashir et al., 2019). A good example is the Facebook and Cambridge Analytica scandal, in which tens of millions of Facebook users data was unlawfully harvested and analyzed for political advertising. As shown in Fig. 1, malicious online servers collect and analyze users browsing traces to determine their private intentions (Barford et al., 2014; Liu et al., 2013; Wang et al., 2020; Wills and Tatar, 2012; Xu et al., 2021).

These widely reported privacy issues concerning major social network platforms (e.g., Facebook) have led to heightened concerns among users regarding the data collected from them (Bashir et al., 2019). Furthermore, a previous study has shown that a users intention and cultural background can be accurately predicted (Atouati et al., 2020; Song et al., 2018). Moreover, the user and the platforms motives are not aligned: the OSN platforms occupy most of their abundant computing resources and plentiful data for their purposes, while the user could only achieve limited computing power and few public datasets. Users almost have no chance to escape these platforms supervision unless they go towards the end and abandon all these platforms' services.

To solve the problem mentioned above, some relevant approaches have been proposed. PrivSR is a privacy-preserving framework that conducts itself in the area of social recommendation. The way it works is to allow users to model ratings and social relationships privately (Meng et al., 2018). A novel access control

* Corresponding author.
*E-mail address:* zhuhui@xidian.edu.cn (H. Zhu).

https://doi.org/10.1016/j.cose.2022.102778
0167-4048/

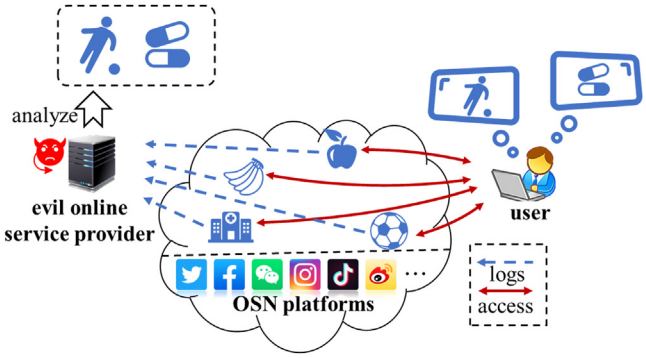



**Fig. 1.** OSN servers analyze user's intentions.

framework is proposed in Cheng et al. (2013), which splits third-party applications into internal and external components, allowing the internal members to access private information but keeping it away from the external ones. Veil (Wang et al., 2018) is a privacy-preserving deployment framework that provides a particular veil compiler that helps rewrite pages to further blind servers collecting the users data by manipulating the page contents so that the private information regarding the user is protected from leaking. A novel adversarial attack algorithm is proposed in Kumar et al. (2020), which produces both contradictory features and graphs under a given shopping budget to escape the identification of private information, such as family information. However, the continuity of the users visiting contents is ignored in the approaches mentioned above, which is a typical character of the users online behaviors; these approaches only focus on hiding intentions but neglect the covertness of the approaches themselves; moreover, users need the association from other users even in OSN platforms (Biega et al., 2017; Reiter and Rubin, 1998; Zhu et al., 2010). To our knowledge, we are the first to conceal users intentions by constructing browsing trajectories.

**Purpose.** Provide a scheme to hide users' intentions during online access while minimizing the involvement of other users to ensure the effectiveness and availability of intention hiding. When a user performs a visit action, the action itself is given an attached purpose, and that purpose itself is called an intention, such as a desired visit to a blog, a blogger, or a website. An OSNs server can mine a users intentions to make accurate portraits of the particular user, and this act itself leads to the opportunity of an enormous privacy risk (Tanjim et al., 2020). We divide user visits into two primary categories. The first is the users intention, which may be a blogger that the user wants visit, a blogger that the user wants to follow or a website that the user wants to browse. The second category contains the visits that are classified as casual visits or process visits that are irrelevant to the user's purpose. Moreover, we only care about the content that can be described with text, not the form of a visit. In this paper, we do not hide the intention directly. But instead, our process is to make it look as if the users targeted intentions (desired visit a blog, author, etc.) are casual visits. By doing so, we prevent the OSNs from intervening and analyzing the users private and sensitive intentions, thus providing users with the ability to counter an OSNs invasive and accurate profiling.

**Motivations.** Our work is motivated by a set of observations in our daily life:

*Observation I*: While constructing users browsing trajectories, we could only concern users profiles, accessible graphs composed of visitable contents, and respective concomitant multimedia information along with different visitable content.

*Observation II*: We could disguise the users intention as a casual visit to reduce the risk of an intention leak. For example, say a user has an intention where it is a visit of the personal homepage belonging to a famous football player Alice. If we directly visit her/his homepage, then the intention is evident and undeniable. The OSN platform could realize that you are paying attention to Alice for whatever reason. Still, if some similar homepages are successively visited before and after player Alices, the visit action looks casual, and thus the intention is obfuscated and cloaked.

*Observation III*: We can conceal the intention when it comes to the process of implementing an artificial decoy visits system by improving the smoothness of topic changes in browsing trajectories. Commonly, topics in a casual browsing trajectory change smoothly. Still, in intentional browsing trajectories with apparent intentions, topics change abruptly (Wang et al., 2017), which is a typical character in the overall browsing characteristics, to distinguish between casual browsing trajectories and intentional browsing trajectories.

**Contributions.** In this paper, we propose an effective and efficient intention-concealed visit framework named Aviv, which can generate AICB trajectories and make the intentions look like casual visits with the help of some artificial decoy visits. With Aviv, users can browse online content on OSN platforms without leaking the true intentions to curious and malicious OSN platform servers. Specifically, the main contributions of this paper are fourfold:

- First, Aviv provides adaptive representation for user profile and visitable contents to adapt to complex application scenarios. Concretely, we use semantic based embedding schemes such as Skip-Gram model with Negative Sampling(SGNS) and Item2vec. User's profile and accessible visit contents are embedded into vectors, where text information processing tools such as TF-IDF/ Textrank /LDA are added adaptively.
- Second, Aviv achieves visit actions picking method based on user's profile and interests. We propose a divert scoring process according to users interests, topics of visitable contents in accessible graphs, and connectivity among visitable contents. A high score one visitable content gains means its suitable for the visitable content to be picked up as a decoy visit. Concretely, the proposed DecoyRank algorithm creates scores on the visitable contents according to the connectivity, adjacent similarity, and the similarity between a users interests and the topics of the visitable contents. Moreover, considering that the real users browsing attention could be impacted by their visited contents, during their browsing sessions. We add an Attention drift imitation (ADI) scheme to make the generated browsing trajectories more verisimilar.
- Third, Aviv guarantees effective and efficient AICB trajectories construction algorithms. We introduce two browsing trajectories construction algorithms which are individually based on local optimum and global optimum. The algorithm focusing on local optimum is more efficient and the other one focusing on global optimum is more effective. Concretely, BGTC is a locally optimal greedy algorithm to get effective AICB trajectory rapidly, and BDPTC could get the most suitable AICB trajectory by iterating over all visitable content.
- Finally, Aviv realizes an intention-concealed visit framework without cooperation with other users. We conduct the design, performance evaluation, and security discussion of Aviv, which generates AICB trajectories and allows users to achieve intention-concealed visits over OSN platforms.

The remainder of this paper is organized as follows. In Section 2, we formalize the system model and design goals. Then, we introduce the security metrics in Section 3 and propose intention-concealed framework named Aviv in Section 4. Section 5 shows the performance evaluation of Aviv. Section 6 shows the security discussion about Aviv and proves that Aviv satisfies security when facing abnormal detection and


**Fig. 2.** System model under consideration.

sudden-intention mining. We also review some related works in Section 7. Finally, we draw our conclusions in Section 8.

## 2. System model and design goals

In this section, we formalize the system model and identify our design goals.

### 2.1. System model

As shown in Fig. 2, the system model consists of three main components: (i) User, (ii) Privacy-preserving Advice Provider (PAP), and (iii) Evil online Service Provider (ESP). We now provide details of each component.

**User**: The user who accepts online services and accesses online content has the ability to call upon their intention when using a service (i.e. OSN) that is hosted by an ESP. The user also possesses limited computational abilities, but desires secure, and personalized OSN services.

**PAP**: The third-party who provides privacy-preserving advice for users. When receiving user's queries, PAP generates customized privacy-preserving advice and sends it to the user. PAP could be a credible third-party or a computing device owned by the user. PAP possesses adequate computational abilities and adequate public datasets.

**ESP**: The evil service provider who is curious about the user's private information, such as intentions. For achieving personalized services, users must deliver their online intentions to ESP. Commonly, ESP possesses adequate computational abilities and analytical abilities, thus they have the ability to endanger the users private intentions.

In this system model, a user first delivers their queries to PAP system; then, PAP generates privacy-preserving advice, and in return, sends that advice to the respective user; finally, the user is now able to obtain the liberty of having privatized online visits by taking advantage of the PAPs advice. The system model and processes are presented in Fig. 2.

### 2.2. Design goals

According to the **Motivations**, we prepared three design goals following our proposal. The detailed introductions are given as follows:

**Normal browsing trajectories imitation**: The proposed framework should have the ability to generate verisimilar browsing trajectories to reduce ESP's alertness and escape the abnormal detection such as bot detection, which could conceal not only intentions but also approaches themselves.

**Intention-concealed guarantee**: The proposed framework should guarantee that when it comes to the ESPs, they cannot distinguish the users true intention. The true intention (intentional visitable contents) should be concealed with several privacy-preserving measures.

**Effective and efficient**: Proposed framework must provide not only effective but also efficient privacy-preserving services. Time delay is influential in user experience. The low-level time cost is another vital demand.

## 3. Security metrics

### 3.1. Potential threats

There are three primary challenges that Aviv is facing. The first challenge is to prevent Aviv's users from being recognized as bots. This is because Aviv's primary solution is its ability to have constructed browsing trajectories similar to the real-life browsing trajectories to a certain extent. This challenge is called the OSN servers abnormality detection. The second challenge is the ability to maneuver around the detection systems of OSNs, where they may be able to detect the user's intentions, especially sudden intentions. This challenge is organized as sudden-intention mining. The third challenge is the collusion attack, which means users and users or users and service providers collude to threaten other users' privacy security.

#### 3.1.1. Abnormal detection

We have designed a GRU-based RNN model trained from the collected real access trajectory data to perform anomaly detection on the AICB trajectory. The evaluation results in section IV show that the values of these indicators when detecting AICB trajectories are an approximation when it comes to the values of detecting real browsing trajectories. Moreover, the evaluation results indicate that AICB trajectories could not cause OSN service providers to be vigilant against concealed intention.

#### 3.1.2. Sudden-intention mining

Unlike the traditional obfuscation scheme based on k-anonymity (Sweeney, 2002), we cannot directly use entropy as a security metric. Entropy can only consider the probabilistic closeness of the visitable content appearing in one trajectory. When the probability of all content appearing is equal, entropy is maximized. However, the visitable content in one AICB trajectory should be close in semantics rather than close in probability. As a result, we adopt an *adjacent similarity* in the aspect of semantics based on cosine similarity as a security metric. Users tend to visit visitable content semantically close to the current visiting content. The subsequent visits are generally considered casual visits without distinct intention. Based on this premise, we consider the similarity of adjacent visitable content on one trajectory as a security metric called **adjacent similarity**. The higher the similarity of adjacent visitable content, the more it can be considered that the visit is casual. Moreover, the computational formula is shown as follows, just as same as cosine similarity:

$$similarity(X,Y) = \frac{\sum_{i=1}^{n}(X_i \times Y_i)}{\sqrt{\sum_{i=1}^{n}(X_i)^2} \times \sqrt{\sum_{i=1}^{n}(Y_i)^2}},$$

where, $X$, $Y$ are objects of comparison in the form of vector, and $n$ is the length of vectors.

The adjacent similarity can then be used for measuring the semantic similarity between two adjacent visitable content in one trajectory. High values of the measured adjacent similarity in one trajectory mean that the visit looks casual. It is not easy to mine true intention in one trajectory consisting of visits with high values. Moreover, adjacent similarity can also measure the semantic similarities between a users profile and adjacent visitable content. In this situation, a high value of the measured adjacent similarity means that the user is more inclined to visit this visitable content.

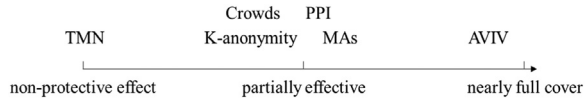



**Fig. 3.** Degree of privacy, Aviv performed best compared to baselines.

#### 3.1.3. Collusion attack

In conventional solutions, rivacy protection is usually done through cooperative request forwarding or identity replacement between users. However, collusion between malicious users or between users and service providers can steal other users' private information.

### 3.2. Degree of privacy

To formally analyze a privacy-preserving scheme, we need to characterize the degree of privacy. The ability of privacy protection depends on the effectiveness of the schemes against attacks.

#### 3.2.1. Non-protective effect

This is the lowest level of privacy preservation. The scheme may provide a functional auxiliary role or safety protection from other aspects, but it does not have an effective defense effect on abnormal detection, sudden-intention concealing or collusion attack.

#### 3.2.2. Partially effective

The protocol can partially complete the privacy protection work, but there are still obvious loopholes in the face of certain attacks. For example, schemes that rely on constructing irrelevant obfuscation requests, such as K-anonymity, can significantly expose the characteristics of privacy protection schemes, which not only arouses the alertness of attackers, but also motivates the emergence of adversarial attack methods.

#### 3.2.3. Nearly full cover

This level means the protocol can roughly deal with all above attack methods, including exposing privacy protection features as little as possible during the execution of the privacy protection scheme to avoid attackers' detection; hiding the user's real access intention as much as possible; resisting collusion attacks.

Aviv gets excellent performance when compared with conventional work as shown in Fig. 3. The mentioned conventional researches are TrackMeNot (TMN) (Toubiana et al., 2011), Crowds (Reiter and Rubin, 1998), Mediator Accounts Proxy (MAs) (Biega et al., 2017), K-anonymity (Sweeney, 2002) and Privacy-preserving indexing (PPI) (Bawa et al., 2009).

## 4. Proposed intention-concealed framework

This section presents our proposed framework, Aviv, which mainly consists of three phases: 1) Decoy representation for the users profile and visitable content; 2) Divert scoring; 3)Trajectories constructing. Concretely, in the decoy representing phase, a users profile and accessible visit contents are embedded into vectors based on accompanying text. In the second phase, a DecoyRank algorithm and attention drift imitation (ADI) process is proposed to score suitable optional decoy visit contents. From there, it also makes sure that its able to have the ability to select a decoy visit when an accessible visit content has a high divert score. Finally, in the third phase, two trajectories construction algorithms are prepared individually according to the local optimum and global optimum. Detailed introductions of phases are given as follows, and the overview of Aviv is given as shown in Fig. 4.

### 4.1. Decoy representing

Two embedding schemes are prepared in this phase, which embeds the users profile and accessible visit contents into vectors for representation based on accompanying text. These embedding schemes are made sure to be adaptively selected. Detailed embedding is also applied to achieve accurate representations for scenarios with the abundant corpus (such as numerous tweets, blogs, self-introductions, and so on). Simplified embedding is more suitable for barren information scenarios (e.g., only simple aggregation and aggregation relationships in accessible graphs composed of visitable contents).

#### 4.1.1. Precondition

Specifically, we use Skip-gram model (Mikolov et al., 2013) with negative sampling (SGNS) and item2vec (Barkan and Koenigstein, 2016) model for basal embedding. SGNS learns high-quality distributed vector representations that capture a large number of precise syntactic and semantic word representations, and item2vec produces embedding for items in a latent space and captures the relations among different items in collaborative filtering datasets. The similarity between representations could be measured with cosine similarity. Before embedding processes, the SGNS model and Item2Vec model need to be well pre-trained. Training data for SGNS must be sentences, and training data for Item2Vec must be aggregation sets (or sequences). Then with the help of these two well-prepared models, the embedding process of words or items could be a simple query procedure. Only one embedding process could be used at one time.

#### 4.1.2. Detailed embedding

Applied datasets must contain visitable contents and abundant text corpus (such as tweets, blogs, self introductions and so on) along with embedding results which mainly depend on the concomitant text corpus. In the overall process of a user's profile is shown in Fig. 5(a): firstly, the user's text corpus (such as user's daily visit content or user's history blogs) is gathered, spliced,

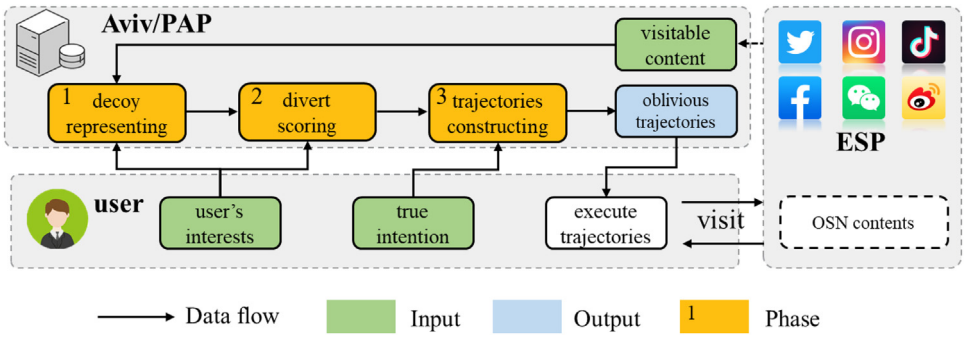
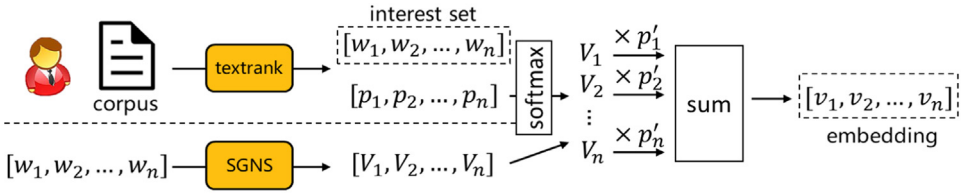
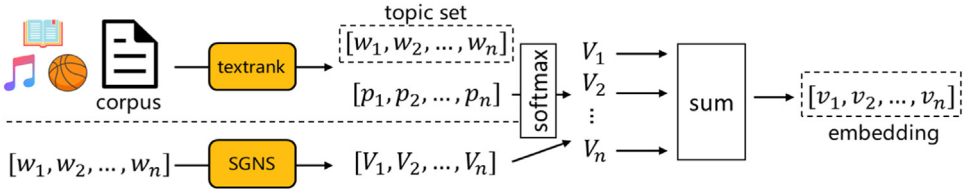


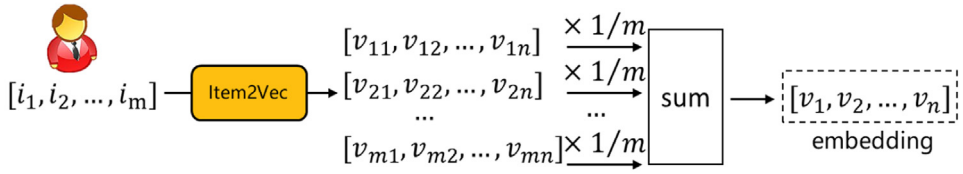

**Fig. 4.** Overview of Aviv.



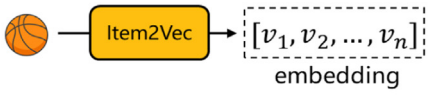

(a) Detailed embedding for users.




(b) Detailed embedding for visitable content.




(c) Simplified embedding for users.




(d) Simplified embedding for visitable content.

**Fig. 5.** Decoy representing.

and segmented. Secondly, text segments are inputted into a topics/keywords extract procedure (such as TF-IDF/textrank/LDA (Blei et al., 2003; Mihalcea and Tarau, 2004; Roelleke and Wang, 2008), and in the case we set textrank as an example),

$n$ keywords $[w_1, w_2, ..., w_n]$ as well as their respective textrank values $[p_1, p_2, ..., p_n]$ are extracted out, and these keywords are regarded as a user's *interest set*; then textrank values $[p_1, p_2, ..., p_n]$ are set as the input of a softmax for normalization, and the output $[p'_1, p'_2, ..., p'_n]$ are regarded as a probability distribution of the user's interests. After that, $[w_1, w_2, ..., w_n]$ are embedded into vectors $[V_1, V_2, ..., V_n]$ by querying each word in a SGNS model; finally, the user's embedding/representation $[v_1, v_2, ..., v_n]$ is figured out by calculating $\sum_i^n p'_i V_i$. For **visitable contents** embedding, as shown in Fig. 5(b) the processes are as the same as user embedding process, but in this case we replace the appellation of $[w_1, w_2, ..., w_n]$- "*interest set*" with "*topic set*".

#### 4.1.3. Simplified embedding

Applied dataset must contain visitable contents and aggregation information (such as categories, classifications, shopping baskets, etc.) among these visitable contents, embedding results of user's profile and visitable contents mainly depend on aggregation information. The process of a **user's profile** embedding is given as shown in Fig. 5(c): firstly, the user's associated visitable contents are gathered as a set $[i_1, i_2, ..., i_m]$; then $[i_1, i_2, ..., i_m]$ is embedded into a vector set $[V_1, V_2, ..., V_n]$ by querying each item in a Item2Vec model; finally, the user's profile embedding/representation $[v_1, v_2, ..., v_n]$ is figured out by calculating $\sum_i^n \frac{1}{m} V_i$. For **visitable contents** embedding, as shown in Fig. 5(d) we regard the output of Item2Vec $[v_1, v_2, ..., v_n]$ as the embedding/representation of one visitable content directly.

### 4.2. Divert scoring

The candidate obfuscated accessible content is graded, and the candidate accessible content with higher score is selected to construct user browsing trajectories which help to conceal users' true intentions. The divert scoring process consists of the Attention drift imitation (ADI) and the DecoyRank algorithm. In this process, the proposed DecoyRank algorithm creates scores on the visitable contents according to the connectivity, adjacent similarity, and the similarity between a users interests and the topics of the visitable contents. It then becomes difficult for an ESP to use its analysis systems to detect whether a single decoy visit was the users true intention, especially if the direct score (*DS*) itself was relatively high. Moreover, considering that the real users attention, or the general topic, during their browsing session could be impacted by

their visited contents, and thus it changes frequently. We add an ADI to make the generated browsing trajectories more verisimilar.

#### 4.2.1. Precondition

Before DecoyRank calculating, user's interest set $\vec{w}$, user's embedding $\vec{v_u}$, representations of visitable contents, and hyper-parameters (such as $\vec{W}$, $\alpha$, and $\beta$ mentioned in ADI) should be prepared.

#### 4.2.2. Attention drift imitation

To achieve a normal browsing trajectory imitation when it comes to the surveillance of OSN platforms, we designed an attention drift imitation (ADI), which helps to imitate a user's attention variation in one browsing trajectory. Considering the fact that interests and visited contents have an influence on a user's attention in one browsing session caused by interests and visited contents, the ADI is built with the following function:

$$A_{init} = \vec{W}^{\top} \cdot \vec{V}_u \tag{1}$$

$$A_i = \alpha A_{init} + \beta \vec{E_{di}} \quad (\alpha, \beta > 0, \alpha + \beta = 1) \tag{2}$$

where $\vec{W}$ is a random weight vector $[W_1, W_2, ..., W_n]$ ($\sum_{i=1}^{n} W_i = 1(W_i > 0)$), $\vec{V}_u$ is user's interest set in the form of embedded vectors (such as $[V_1, V_2, ..., V_n]$ in Fig. 5(a)), $\alpha, \beta$ are constants, and $\vec{E_{di}}$ is the representation of visited contents $i$.

#### 4.2.3. DecoyRank

We propose DecoyRank based on PageRank algorithm to evaluate the effectiveness of visitable contents in one graph according to connectivity, adjacent similarity, and ADI. The transmission formulas in DecoyRank are given as follows, and the DecoyRank computational results are regarded as Divert Scoring values ($DS$) for these visitable contents:

$$DS(j) = \frac{1-d}{N} + d \sum_{i=0}^{N} e_{i,j} \cdot DS(i) \tag{3}$$

$$e_{i,j} = \frac{\delta \cdot \cos(A_i, A_j) \cdot \cos(A_j, \vec{E_u})}{\sum_{k=0}^{N} \delta \cdot \cos(A_i, A_k) \cdot \cos(A_k, \vec{E_u})} \tag{4}$$

$$A_i = \alpha A_{init} + \beta \vec{E_{di}} \quad (\alpha, \beta > 0, \alpha + \beta = 1) \tag{5}$$

where $d = 0.85$, $e_{i,j}$ is the transmission efficiency from the visitable content $i$ to visitable content $j$($\sum_{j=0}^{N} e_{i,j} = 1$), $N$ is the number of visitable contents in the accessible graph. Besides, $A_i, A_j$ respectively represent user's attentions when visiting visitable content $i$ and visitable content $j$, $\vec{E_u}$ is user's representation, and cos is cosine distance between two vectors. Moreover, when the edge of visitable content $i$ pointing to visitable content $j$ and if that exists, $\delta = 1$, otherwise $\delta = 0$. Firstly, traverse all visitable contents in a common graph and calculate the $DS$ values for all those visitable contents. From there, repeat this step several times until $DS$ value achieves convergence. The convergent $DS$ values are the final outputs. According to the properties of PageRank, the initial $DS$ values of visitable contents are irrelevant to the final convergent $DS$ values, so the initial $DS$ values are commonly set as $1/N$.

### 4.3. Trajectories constructing

There are two browsing trajectory construction algorithms introduced, which are respectively based on local optimum and global optimum. Detailed introductions are shown as follows.

#### 4.3.1. Precondition

Before constructing browsing trajectories, the following must be prepared: an adjacent matrix $G$ (where, $G[i][j] == 1$ means there is a directed edge pointing to visitable content $j$ from visitable content $i$), $DS$ values (where, $DS(N_i)$ means the $DS$ value of visitable content $N_i$ and $DS(T = \{N_1, N_2, ..., N_l\}) = DS(N_1) + DS(N_2) + ... + DS(N_l)$), number of visitable contents $\kappa$, intentional access visitable content $N_d$ and length of desired browsing trajectories $L$.

#### 4.3.2. BGTC: Local optimum

Bidirectional Greedy Trajectories Construction (BGTC) is proposed to generate browsing trajectories rapidly based on the principle of local optimum. We also divide the procedure of browsing trajectories construction into two parts. One is the forward path part, which is pointing to the true intention. The other is the backward path part, which is pointed to by the true intention. Then the local optimum browsing trajectories construction could be represented as two longest single-source paths construction. We take the construction process of a backward path as an example: to construct a longest single-source path, the decoy visit contents are selected one by one with the greedy algorithm (Edmonds, 1971). The selected visit contents must have the highest $DS$ value in all visitable contents, and must also be directly linked with the last selected visitable content. After constructing both the forward path and the backward path, they are connected, and the intention is set as the junction. The computational complexity is about $O(\kappa \times L)$, where $\kappa$ is the number of visitable contents, and $L$ is the length of the desired browsing trajectories. The detailed algorithm flow is shown in Algorithm 1.

**Algorithm 1:** *BGTC*

**Input**: $DS$, $G$, $L$, $\kappa$, $N_d = \eta$
**Output**: AICB trajectory $T$

Randomly select $\xi \in [1, L]$ as the index of $N_d$
// The construction of forward path
$T_f = \{\eta\}$ // Initial $T_f$ only consists of $\eta$
**for** $1 \le l \le \xi$ **do**
  **for** $1 \le i \le \kappa$ **do**
    **if** $G[T_f[0]][i] == 1$ **then**
      $i^* = \arg\max_i \ DS(i)$
    **end**
  **end**
  $T_f = \{i^*, T_f\}$ // Head insert
**end**
Remove Last Content($T_f$)
// The construction of backward path
$T_b = \{\eta\}$ // Initial $T_b$ only consists of $\eta$
**for** $1 \le l \le \xi$ **do**
  **for** $1 \le i \le \kappa$ **do**
    **if** $G[i][T_b[l-1]] == 1$ **then**
      $i^* = \arg\max_i \ DS(i)$
    **end**
  **end**
  $T_b = \{T_b, i^*\}$ // Tail insert
**end**
Remove First Content($T_b$)
$T = \{T_f, \xi, T_b\}$

#### 4.3.3. BDPTC: Global optimum

Bidirectional Dynamic Pro- gramming Trajectories Construction (BDPTC) is proposed to generate browsing trajectories effectively based on the principle of global optimum. Similarly as BGTC,

we represent the global optimum browsing trajectories construction as the construction of forward path and backward path. To solve these two construction processes, a dynamic programming procedure (Forney, 1973) is introduced. We take the construction of the backward path as an example. Observing that the *DS* value of $T_{l\varphi}$ (a $l$-length set of browsing trajectories, the end visitable content, which is defined as $\varphi$) which is the sum of the *DS* value of conjoint fore $(l-1)$-length browsing trajectories and the *DS* value of the $l$-th visitable content: $DS(T_{l\varphi}) = DS(T_{(l-1)\phi}) + DS(\varphi)$ (where, $\phi$ refers to any visitable content which is linked with $\varphi$ directly), we can iterate this formula from $DS(T_{2\varphi^*}) = DS(\phi^*) + DS(\varphi^*)$ in the very beginning to $DS(T_{l\varphi^*}) = DS(T_{(l-1)\phi^*}) + DS(\varphi^*)$ (where, $\varphi^*$ and $\phi^*$ refer to any suitable visitable contents). Moreover, observing that $max\{DS(T_{l\varphi^*})\} = \max\{DS(\{T_{(l-1)\phi^*}, \varphi^*\})\} = \max\{DS(T_{(l-1)\phi^*})\} + DS(\varphi^*)$, we could iterate this formula from $max\{DS(T_{2\varphi^*})\} = \max\{DS(\phi^*)\} + DS(\varphi^*)$ to $max\{DS(T_{l\varphi^*})\}$. Analogously, we could figure out the maximum *DS* value of $l$-length browsing trajectories: $max\{DS(T_l)\} = \max\{max\{DS(T_{l\varphi_1})\}, ..., \max\{DS(T_{l\varphi_\kappa})\}\}$ after several iteration operations. To finish the global optimum browsing trajectories construction, we first set the intentional content as a source, from there in accordance to the aforementional process, we go on to find out the forward path along with the backward path respectively. Finally, these two paths are connected and the intentional content is set as the junction. The whole computational complexity is about $O(\kappa^2 \times L)$, where $\kappa$ is the number of visitable contents and $L$ is the length of desired browsing trajectories. Algorithm flow is shown in Algorithm 2.

**Algorithm 2:** *BDPTC*

**Input**: $DS$, $G$, $L$, $\kappa$, $N_d = \eta$
**Output**: AICB trajectory $T$

Randomly select $\xi \in [1, L]$ as the index of $N_d$
// The construction of forward path
// $T_{\zeta\tau}$ is a $\zeta$-length path and the **first** visitable contents of $T_{\zeta\tau}$ is $\tau$
$T_{1\eta} = \{\eta\}$
**for** $1 \le l \le \xi - 1$ **do**
  **for** $1 \le i \le \kappa$ **do**
    **for** $1 \le j \le \kappa$ **do**
      **if** *($T_{lj}$ exists) and ($G[i][j] == 1$)* **then**
        $j^* = \arg\max_j \ DS(T_{lj})$
      **end**
    **end**
    **if** *$j^*$ exists* **then**
      $T_{(l+1)i} = \{i, T_{lj^*}\}$ // Head insert
    **end**
  **end**
**end**
**for** $1 \le k \le \kappa$ **do**
  $T_f = \arg\max_{T_{\xi k}} DS(T_{\xi k})$
**end**
Remove Last Content($T_f$)
// The construction of backward path
// $T_{\zeta\tau}$ is a $\zeta$-length path and the **end** visitable content of $T_{\zeta\tau}$ is $\tau$
$T_{1\eta} = \{\eta\}$
**for** $1 \le l \le L - \xi$ **do**
  **for** $1 \le i \le \kappa$ **do**
    **for** $1 \le j \le \kappa$ **do**
      **if** *($T_{lj}$ exists) and ($G[j][i] == 1$)* **then**
        $j^* = \arg\max_j \ DS(T_{lj})$
      **end**
    **end**
    **if** *$j^*$ exists* **then**
      $T_{(l+1)i} = \{T_{lj^*}, i\}$ // Tail insert
    **end**
  **end**
**end**
**for** $1 \le k \le \kappa$ **do**
  $T_b = \arg\max_{T_{\xi k}} DS(T_{\xi k})$
**end**
Remove First Content($T_b$)
$T = \{T_f, \xi, T_b\}$

## 5. performance evaluation

Performance evaluation of Aviv is provided in this section.

### 5.1. Simulation setup

#### 5.1.1. Simulation environment

To measure the integrated performance, we implement Aviv on a workstation with 2.20 GHz, 10-core processor, 256GB RAM, and Ubuntu 16.04.

#### 5.1.2. Datasets

The prepared dataset is a follower-followee graph gathered from the Weibo platform, which contains 7.2$k$ users, 751.1$k$ following relationships, and 379.8$k$ microblogs. Furthermore, the original dataset is organized into three digraphs with a different number of visitable contents, and the detailed presentation for these digraphs are shown in Table 1 (Notations in Table: quantity of visitable contents $Q_N$, the number of edges $Q_E$, the number of microblogs $Q_M$).

**Table 1**
Datasets For Performance Evaluation.

| | $Q_N$ | $Q_E$ | $Q_M$ |
|---|---|---|---|
| Digraph 1 | 200 | 2888 | 15770 |
| Digraph 2 | 500 | 12506 | 40793 |
| Digraph 3 | 1000 | 26282 | 81491 |

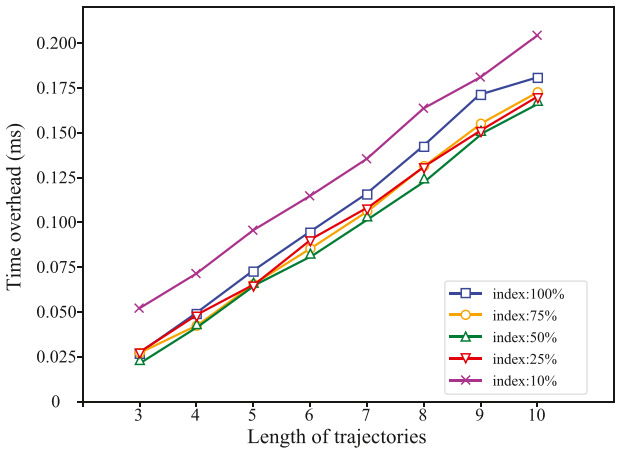
### 5.2. Evaluation

#### 5.2.1. Optimization

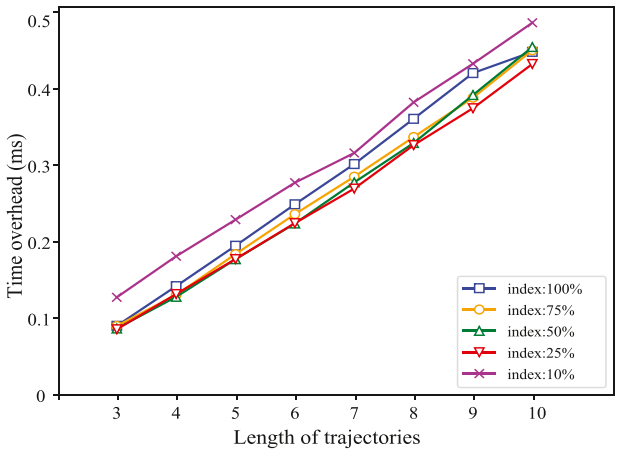
There is a large space for optimization because of the separation design among the adaptive embedding, divert scoring, and browsing trajectories constructing according to diverse usages. For some of the users who use the same scenario, only intentions need to be changed, while embedding results, and *DS* values are unnecessary to be modified. For multi-user, we need to prepare different digraphs for each user, and along with that the intentions, embedding results, and *DS* values are all need to be modified as well. The running time of different intermediate data reusing strategies is shown in Table2. The results show that reusing strategies can reduce running time effectively. The values of notion in Table2 are set as $Q_N = 200, Q_E = 2888, L_P = 7, I_{index} = 3$.

**Table 2**
Optimization By Reusing Intermediate Data.

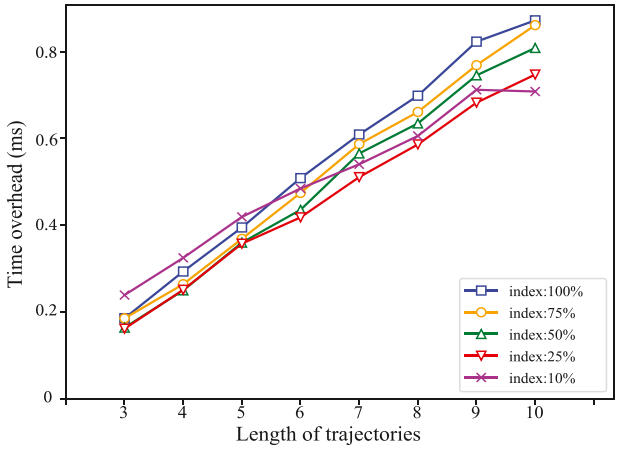
| | Running time | Reusing Strategy |
|---|---|---|
| Original | 137.553s | No data for reusing |
| Optimization 1 | 0.229s | Reusing embedding results |
| Optimization 2 | 0.034ms | Reusing embedding results and *DS* values |




(a) Results with Digraph 1.




(b) Results with Digraph 2.




(c) Results with Digraph 3.

**Fig. 6.** Performance evaluation with BGTC.

*5.2.2. Evaluation plan*

Two core notions are designated for evaluations: index of true intention in one browsing trajectory $I_{index}$ and length of browsing trajectories $L_P$. A detailed plan is shown as follows: $L_P$ variables in [3, 10], $I_{index}$ variables in {10%, 25%, 50%, 75%, 100%} (which means index of intention in browsing path is $\lfloor L_P * I_{index} \rfloor$), and constants variables $Q_N$ and $Q_E$ are related to the applied digraph. During the evaluation experiments, each experiment is repeated 50 times with randomly selected intention and user to reduce contingencies.

*5.2.3. Evaluation results*

In this section we discuss the security of AICB trajectories. The results show that running time is directly proportional to $L_P$ and the scale of an applied digraph. Moreover, the running time turns become smaller when the index of intention becomes closer to the middle of browsing trajectories. With BGTC, Aviv's running time is in signally a low-level, which is almost harmless to user experience. The evaluation results of our experiments are shown in Fig. 6, and Fig. 7.

## 6. Security discussion

Aviv generates AICB trajectories containing the user's true intentions to resist abnormal detection and sudden-intention mining by malicious ESP. Generated AICB trajectories correlate to the users' interests, and the differences between adjacent visitable contents in one AICB trajectory change smoothly. Moreover, k-anonymity is introduced for comparison:

*K-anonymity*: K-anonymity approach randomly selects visitable contents in the graph to generate pseudo browsing sets rather than trajectories for obfuscation regardless of the concomitant information of visitable contents and connectivity in the graph.

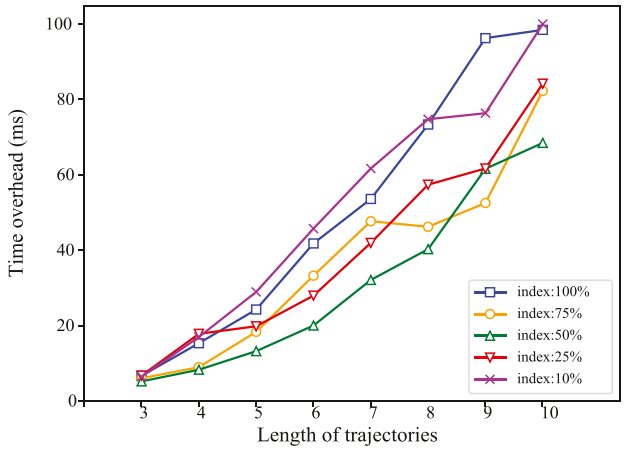
### 6.1. Abnormal detection

*6.1.1. Attack model*

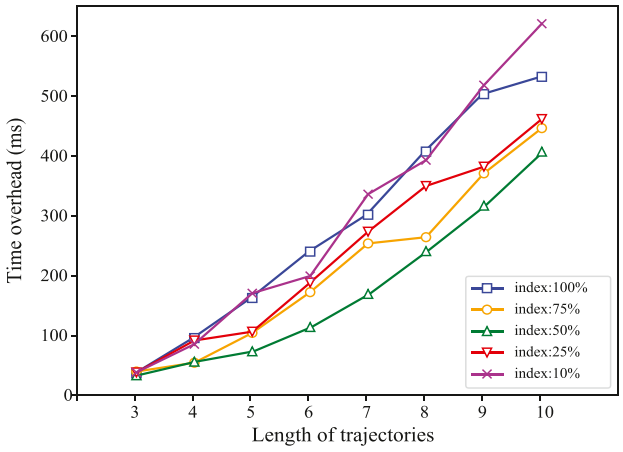
We conduct a classifier based on Recurrent Neural Network (RNN) (Mikolov et al., 2011) to simulate the detection ability of ESP. ESP can distinguish abnormal trajectories (ATs) from online users' normal trajectories (NTs) (Wang et al., 2017). Once we have that in place, we set GRU models as the cells in RNN, and a fully connected layer is added to compress the output of RNN cells into a 2-dimension vector, which represents the classification result. If the AICB trajectories generated by Aviv are not similar enough with NTs, the user's visit queries could be rejected.

*6.1.2. Analysis*

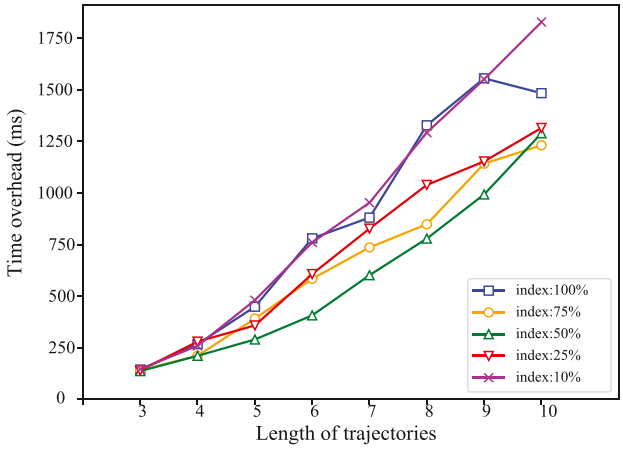
Generated AICB trajectories are in accordance with the user's preference, and similarity values between adjacent visitable contents in one AICB trajectory are at a high-level. Commonly, users




(a) Results with Digraph 1.




(b) Results with Digraph 2.




(c) Results with Digraph 3.

**Fig. 7.** Performance evaluation with BDPTC.

desire to browse content similar to the one they are primarily interested in for research. As a result, to escape the abnormal detection, the selected visitable contents in generated browsing trajectories must be similar to the user's preference. The differences in the aspect of semantics between adjacent visitable contents in one browsing trajectory should change smoothly. Due to the transmission efficiency $e_{i,j}$ (mentioned in DecoyRank), the *DS* value of one visitable content is positively related to the cosine similarity between the representation of the visitable content and user's preference. Thus, the generated AICB trajectories in Aviv theoretically satisfy the requirements mentioned above. To intuitively illustrate this conclusion, we involve in a cosine similarity to evaluate the quantified similarity between representations. An evaluation of the result is shown in Fig. 8 and Fig. 9 (The parameters in evaluation are set as $L_P = 10, I_{index} = 5$). In the Fig. 8, the index of browsing trajectories is $n$ and that means the test result is basically the similarity value between the decoy visit content whose index is $n-1$ and the decoy visit content whose index is $n$. In Fig. 9, the index of browsing trajectories is $n$ and that means the test result shows the average similarity between the first $n$ decoys and user's representation.

#### 6.1.3. Simulation

When it comes to the simulation, the classifier itself is well trained, meaning that its constructed with normal user trajectories (NTs) and abnormal user trajectories (ATs). Furthermore, in order to evaluate the detection results, we select the following indicators: accurate rate, precision rate, and recall rate. With this, the test results are shown in Table 3, and according to those detection results, we can see that the AICB trajectories generated by Aviv have approximate detection resisting capacities with NTs. In other words, the AICB trajectories generated by Aviv resemble enough with NTs under this attack model.

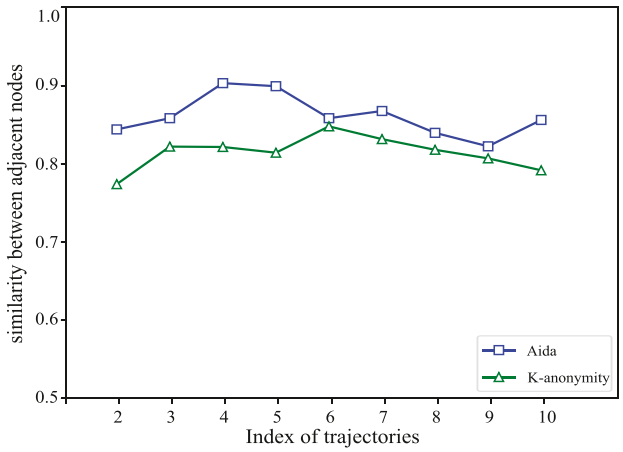
**Table 3**
Test Results In RNN Based Abnormal Detection.

| trajectories | accurate rate | precision rate | recall rate |
|---|---|---|---|
| NT | 326/500 (0.652) | 252/335 (0.752) | 252/343 (0.735) |
| Aviv | 325/500 (0.650) | 250/332 (0.753) | 250/343 (0.729) |

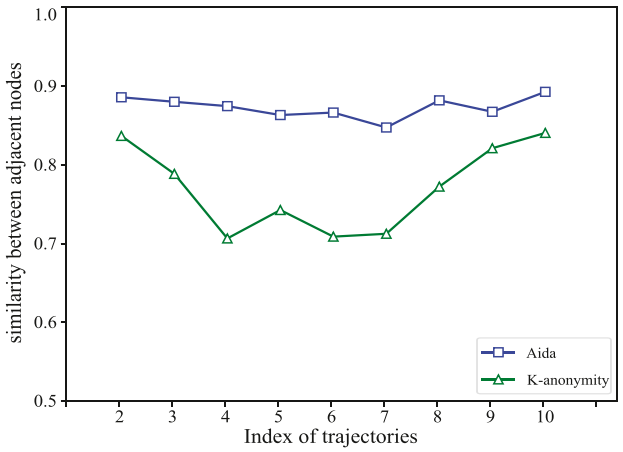
### 6.2. Sudden-intention mining

#### 6.2.1. Attack model

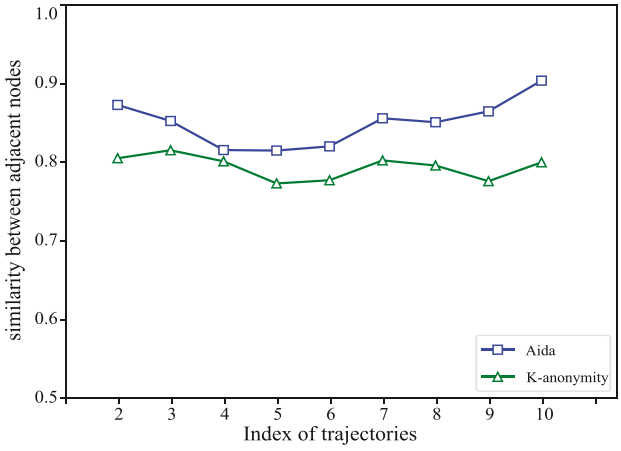
We conduct an intention miner based on the k-clique algorithm (Tsourakakis, 2015) to simulate an ESP's sudden-intention mining ability. ESP have the ability to use their analytical systems in order to distinguish whether or not a single browsing trajectory is a decoy or is in fact a user's true intention. Review the *observation II* in




(a) Results with Digraph 1.




(b) Results with Digraph 2.




(c) Results with Digraph 3.

**Fig. 8.** Similarity between adjacent visitable contents.

**Motivations** to further understand this concept, in our methodology, we disguise intentional content (true intention) as casual visit content. The surrounding visitable contents of a casual visit contents are within one browsing trajectory, and is commonly relevant to itself, but the neighboring visitable contents of an intention are usually not. Intuitively, visitable contents around a casual visit contents vary smoothly, and an intention generally appears abruptly. Based on this truth, ESP could easily distinguish the user's true intention.

*6.2.2. Analysis*

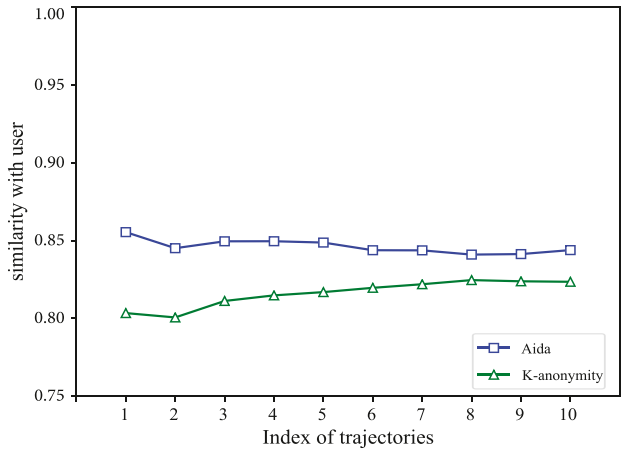
The generated AICB trajectories in Aviv theoretically satisfy the security requirement when defensing sudden-intention mining attacks. The solution to escape the detection of an ESP's intention miner is as follows: The neighboring decoy visit contents must be similar enough with the true intention in the aspect of semantics when it comes to the subjects itself. In other words, the difference between adjacent visitable contents in one browsing trajectory must be low-level. Due to the transmission efficiency in DecoyRank $e_{i,j}$, the *DS* value of one visitable content is positively related to cosine similarity between adjacent visitable contents. As a result, the generated AICB trajectories in Aviv theoretically satisfy the requirement mentioned above. To intuitively illustrate this conclusion, we set the adjacent similarity (similarity between adjacent visitable contents) as an indicator. From that, we obtain an evaluation of the results, as shown in Fig. 8. (The parameters in the evaluation are set as $L_P = 10, I_{index} = 5.$).

**Table 4**
Test Results In K-clique Based Sudden-Intention Mining.

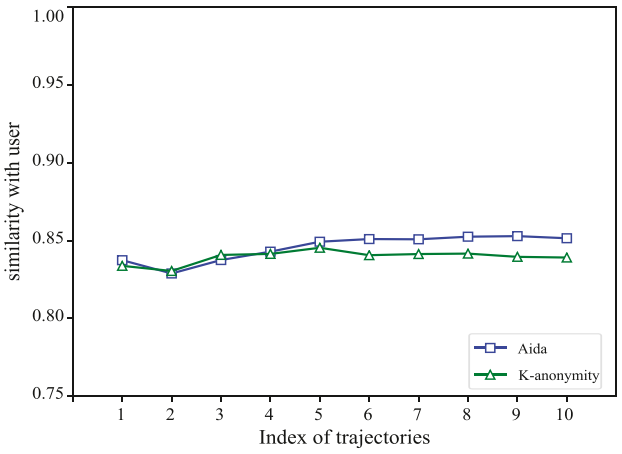
| trajectories | T/All (k=4) | T/All (k=5) | T/All (k=6) |
|---|---|---|---|
| NT | 29/250 (0.12) | 36/250 (0.14) | 31/250 (0.12) |
| K-anonymity | 157/500 (0.31) | 263/500 (0.53) | 117/500 (0.23) |
| Aviv | 22/247 (0.09) | 22/247 (0.09) | 18/247 (0.07) |

*6.2.3. Simulation*

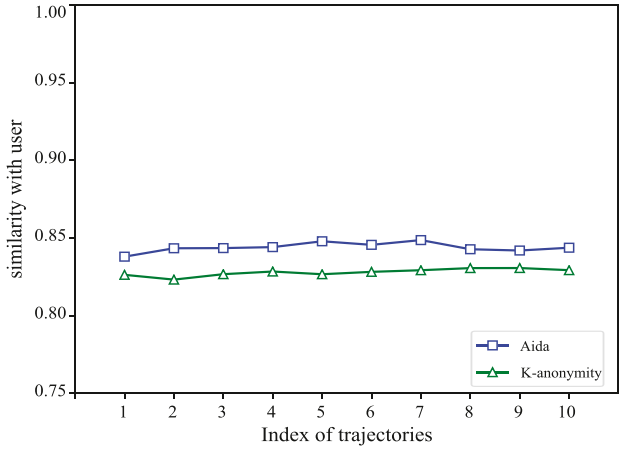
We distinguish the visitable contents which are observably different from surrounding visitable contents in one browsing trajectory based on the k-clique algorithm (Tsourakakis, 2015) and regard them as user's true intentions. The test results are shown in Table 4, where *T* is the number of correct classification results, and *All* is the number of all of the test samples. The mining results show that the intentional visit contents in AICB trajectories generated by Aviv are difficult to be mined out.




(a) Results with Digraph 1.




(b) Results with Digraph 2.




(c) Results with Digraph 3.

**Fig. 9.** Similarity between generated trajectories and user's representation.

**Table 5**
Overview Comparison.

| Approach | Scenario | Perturbation | Privacy model |
|---|---|---|---|
| TMN | search | bogus queries | not mentioned |
| Crowds | search, browse | forwarding queries | entropy |
| MTC | browse | block sensitive pages | not mentioned |
| PPI | search | query replacement | attack confidence |
| MAs | search, browse | obfuscation queries | entropy, profile overlap |
| Aviv | browse | AICB trajectories | adjacent similarity |

### 6.3. Comparison with other approaches

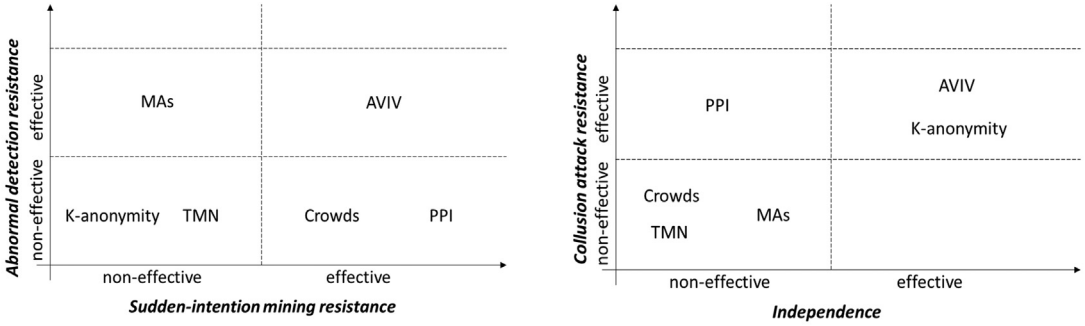
Compared with the traditional solutions, Aviv has obvious advantages in security and availability, and the application scenarios of Aviv are more adaptable.

#### 6.3.1. Overview comparison

Five typical approaches have been selected for comparison: TrackMeNot (TMN) (Toubiana et al., 2011), Crowds (Reiter and Rubin, 1998), MTC (Achara et al., 2016), Privacy-preserving indexing (PPI) (Bawa et al., 2009), and Mediator Accounts Proxy (MAs) (Biega et al., 2017). The perspectives in order to create a comparison are chosen as scenario, perturbation, privacy model and limitations. The detailed contrasts of approaches are shown in Table 5. Conventional researches have its respective limitations: TrackMeNot provides bogus queries, it can not evaluate the privacy, and it is vulnerable to semantic attacks; Crowds users must collaborate, it is vulnerable to collusion attacks; MTC blocks sensitive pages, but it can not provide privacy-protecting mechanisms; Traditional PPI schemes are sensitive to common identity attacks and collusion attacks. Aviv could provide an excellent defense effect when facing abnormal detection, sudden-intention mining, and collusion attacks when enough pretreatment data such as topology of visitable contents and users' interest profiles are provided.

#### 6.3.2. Function comparison

We also introduce five functions to describe these approaches, they are: *intention-concealed, low-discoverability, browsing path design, personalized interest driven, obfuscation traffic*. Individual introductions are given as follows:




(a) Aviv posses excellent abilities of abnormal detection resistance and sudden-intention mining resistance.

(b) Aviv posses excellent abilities of collusion attack resistance and independence.

**Fig. 10.** Security comparison between Aviv and conventional schemes, Aviv gets excellent privacy protection abilities.

**Table 6**
Function Comparison.

| | TMN | Crowds | MTC | PPI | MAs | Aviv |
|---|---|---|---|---|---|---|
| intention-concealed | ○ | ○ | ○ | ○ | ○ | ○ |
| low-detectability | × | ○ | ○ | ○ | ○ | ○ |
| trajectories design | × | × | × | × | × | ○ |
| personalized interest driven | × | × | × | × | × | ○ |
| obfuscation traffic | ○ | ○ | × | ○ | ○ | × |

- *intention-concealed*: whether the approaches could conceal user's intentions.
- *low-detectability*: whether the approaches could guarantee the covertness of the approaches themselves.
- *trajectories design*: whether the approaches provide trajectories which are closer to human browsing behaviors than a set of disordered visit actions or queries.
- *personalized interest driven*: whether the approaches concern users' interests.
- *obfuscation traffic*: whether approaches support obfuscation traffic with internet flows.

The detail functions comparison between these approaches are given in Table 6.

The conventional schemes design concept of probabilistic obfuscation is similar to our solution. However, the difference is that we adopt a more machine language representation method and use text-encoded semantic representation to unify the user's interest characteristics and access content characteristics. The advantage of this representation is that it is closer to the intuitive feeling of real users and is easier to understand from a user-oriented perspective. At the same time, it also adopts the design concept of algorithms serving human beings. Our evaluation index still uses the probability entropy change after the above semantic representation, which is the same as the traditional algorithm design. Compared with the previous research work, our work pays more attention to 1) the independence of privacy protection work, which does not require additional participation of other users but requires publicly collectible information; 2) focuses on the full trajectory generation of access behavior, which The advantage of this design concept is that it can not only obfuscate a certain behavior but also obfuscate an abstract intent, that is, it can achieve intention-cancel. Add the previous definition of intention here. Of course, for simplicity, we usually regard a specific access content as intention. From the perspective of machine quantification, the intention may also be the weighted result of some access content or other more complex representations.

*6.3.3. Security comparison*

Aviv does not require the cooperation of other users nor the cooperation of the service provider platform and can independently complete the privacy protection function while resisting the mining of intentions. Existing related research work usually does not require such strict background conditions and generally adopts the cooperation between users or cooperates with the service platform to improve the privacy protection effect. Because of these background conditions, we formally and qualitatively grade the privacy protection ability of the test scheme by considering whether the test scheme can resist the three proposed attack methods. The comparison proves Aviv is safe and effective. In Fig. 10 we can see Aviv gets excellent privacy protection abilities when compared with conventional schemes. Aviv possesses abilities of abnormal detection resistance, sudden-intention mining resistance, and collusion attack resistance and has enough degree of independence, which means Aviv could achieve privacy protection task without other users' help or cooperation with service providers.

## 7. Related work

With the rise of privacy concerns throughout the internet community, the concept of intention-concealed online browsing has obtained a forefront standing in the minds of researches where they commit themselves to find solutions to such a problem. Thus, relevant studies focus on similar solutions as ours, such as anti-tracking, anti-profiling (Ahmad et al., 2016; Vastel et al., 2018; Xu et al., 2009).

In this section, we discuss some of the typical approaches that are related to our research.

**Tracking and profiling.** Generally, well-designed personalized services are popular. However, these services tend to expose privacy risks, where users log in and leave extensive traces behind, these information can then be taken advantage of by malicious parties (Krishnamurthy et al., 2007; Krishnamurthy and Wills, 2009; 2006). In the area of user tracking and profiling, some researches have been done, especially in the areas of browser tracking (Englehardt and Narayanan, 2016; Lerner et al., 2016; Meng et al., 2016; Yu et al., 2016) and cross-device tracking (Zimmeck et al., 2017). These are primarily empirical studies with an emphasis on identifying the tracking mechanisms, which could help guide the conception of privacy-preserving and intention-concealed approaches.

**Pseudo queries.** TrackMeNot is a lightweight browser extension that helps protect web searchers from surveillance and data-profiling by search engines (Toubiana et al., 2011), it does not practice concealment or encryption (i.e. covering one's tracks), but

instead has another approach which goes by the opposite strategy: noise and obfuscation. Elovici et al. proposed PRAW (Elovici et al., 2002; 2006), and the aim of PRAW is to provide a privacy-preserving service by taking advantage of dummy queries for a group of users sharing a common access point to search engines while surfing or browsing the Internet. GooPIR is another approach providing obfuscation queries when it comes to web searching, and it enables users to conceal their search keywords by sending some false keywords (DomingoFerrer et al., 2009).

**Cooperation.** In Crowds (Reiter and Rubin, 1998), a group of users collaborates to submit their messages to a common Web server. When a specific user sends a message, a user randomly decides to submit it to the server or forward this message to another user, who then repeats this process. Zhu et al. proposed a bundling technique that clusters user profiles into user groups according to semantic relationships between the terms which then leads to satisfying the privacy constraint (Zhu et al., 2010). Biega et al. assigned user requests to Mediator Accounts (MAs) which mimics real users, such that individual user profiles are scrambled across MAs (Biega et al., 2017). PPI (Constable et al., 2015; Fallahi et al., 2017; Tang and Liu, 2015) is usually defined as a set of mapping functions for processing random requests from users. In order to achieve the effect of privacy protection, PPI adopts the form of user cooperative forwarding of requests or encrypted access (Bawa et al., 2009; Shi et al., 2016; Tang et al., 2011). $\epsilon$-PPI is a personalized privacy preserving index, which guarantees quantitative privacy preservation differentiated by personal identities, $\epsilon$-PPI provide effective resistance to common-identity attacks (Tang et al., 2014).

**Blockers.** Another anti-tracker conception is sites-blocker. Just like ad-blockers, blockers could block sensitive sites to protect users' privacy manually or automatically. Some typical approaches like MTC (Achara et al., 2016), PrivacyBadger (Electronic Frontier Foundation, 0000) are popular among online users.

However, among the approaches mentioned above, the continuity of adjacent visitable contents in one browsing trajectory is commonly ignored, which are typical characteristics of user online browsing patterns. Thus, the covertness of approaches themselves is also neglected, leading to a downfall when it comes to the detection systems of the OSN. Moreover, in most existing approaches, users need help from other users, even some cooperation with OSN platforms. Aviv generates AICB trajectories to conceal intentional visit objects and solved these ignored problems. Performance evaluation and security discussion results show Aviv is effective and efficient.

## 8. Conclusion and future work

In this paper, we propose an effective and efficient intention-concealed access framework named Aviv, which acts as a third-party and generates AICB trajectories for users to conceal their true intentions when browsing OSN platforms. Concretely, Aviv consists of three phases: Decoy representing, DecoyRank based Divert scoring, and Trajectories constructing according to the local and global optimum. Unlike the existing approaches, Aviv does not need the assistance of other users or OSN platforms since they may not be compliant in some cases. Aviv pays attention to the quantitative representation of semantic level and user access behavior sequence construction. The experimental results show that this construction idea is more suitable for defending against advanced intention recognition attacks. Security discussion shows Aviv achieves intention-concealed visit ability effectively. Finally, we have applied Aviv to real Weibo datasets, and evaluation results show that Aviv has low communication and calculating costs. Future research will use small data learning technology to explore its cross-platform performance on mobile and edge computing devices.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## CRediT authorship contribution statement

**Helin Li:** Conceptualization, Methodology, Software, Writing – original draft, Data curation, Writing – review & editing. **Hui Zhu:** Conceptualization, Supervision, Writing – review & editing. **Xiaodong Lin:** Supervision, Writing – review & editing. **Rongxing Lu:** Supervision. **Zhipeng Yu:** Project administration. **Wei Lan:** Visualization.

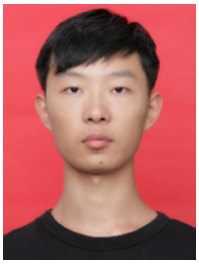
## Acknowledgment

This work was supported by National Natural Science Foundation of China (61972304, 61932015); Natural Science Foundation of Shaanxi Province (2020ZDLGY08-04); Technical Research Program of the Ministry of Public Security (2019JSYJA01).

## References

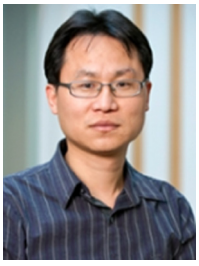
Achara, J.P., Parra-Arnau, J., Castelluccia, C., 2016. Mytrackingchoices: Pacifying the ad-block war by enforcing user privacy preferences. CoRR abs/1604.04495.
Ahmad, W.U., Rahman, M.M., Wang, H., 2016. Topic model based privacy protection in personalized web search. 39th International ACM conference on Research and Development in Information Retrieval - SIGIR.
Atouati, S., Lu, X., Sozio, M., 2020. Negative purchase intent identification in twitter. In: 29th International World Wide Web Conference - WWW.
Barford, P., Canadi, I., Krushevskaja, D., Ma, Q., Muthukrishnan, S., 2014. Adscape: Harvesting and analyzing online display ads. In: 23rd international conference on World Wide Web - WWW, pp. 597–608.
Barkan, O., Koenigstein, N., 2016. ITEM2VEC: neural item embedding for collaborative filtering. 26th IEEE International Workshop on Machine Learning for Signal Processing - MLSP.
Bashir, M.A., Farooq, U., Shahid, M., Zaffar, M.F., Wilson, C., 2019. Quantity vs. quality: Evaluating user interest profiles using ad preference managers. 26th Annual Network and Distributed System Security Symposium - NDSS.
Bawa, M., Bayardo, R.J., Agrawal, R., Vaidya, J., 2009. Privacy-preserving indexing of documents on the network. The VLDB Journal 18 (4), 837–856.
Biega, A.J., Saha Roy, R., Weikum, G., 2017. Privacy through solidarity: A user-utility-preserving framework to counter profiling. In: 40th International ACM Conference on Research and Development in Information Retrieval - SIGIR.
Blei, D.M., Ng, A.Y., Jordan, M.I., 2003. Latent dirichlet allocation. J. Mach. Learn. Res. 3, 993–1022.
Bratman, M., 1987. Intention, Plans, and Practical Reason. Cambridge: Cambridge, MA: Harvard University Press.
Cheng, Y., Park, J., Sandhu, R.S., 2013. Preserving user privacy from third-party applications in online social networks. In: 22nd International World Wide Web Conference - WWW.
Constable, S.D., Tang, Y., Wang, S., Jiang, X., Chapin, S., 2015. Privacy-preserving gwas analysis on federated genomic datasets. In: BMC medical informatics and decision making, Vol. 15. BioMed Central, pp. 1–9.
DomingoFerrer, J., Solanas, A., CastellRoca, J., 2009. h(k)private information retrieval from privacyuncooperative queryable databases. In: Online Information Review, Vol. 33, pp. 720–744.
Edmonds, J., 1971. Matroids and the greedy algorithm. Mathematical programming 1 (1), 127–136.
Electronic Frontier Foundation,. privacybadger. https://privacybadger.org/.
Elovici, Y., Shapira, B., Maschiach, A., 2002. A new privacy model for hiding group interests while accessing the web. 1st ACM Workshop on Privacy in the Electronic Society - WPES.
Elovici, Y., Shapira, B., Meshiach, A., 2006. Cluster-analysis attack against a private web solution (PRAW). Online Inf. Rev. 30 (6), 624–643.
Englehardt, S., Narayanan, A., 2016. Online tracking: A 1-million-site measurement and analysis. In: 23rd ACM Conference on Computer and Communications Security - CCS.
Fallahi, A., Liu, X., Tang, Y., Wang, S., Zhang, R., 2017. Towards secure public directory for privacy-preserving data sharing. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, pp. 2577–2578.
Forney, G.D., 1973. The viterbi algorithm. Proceedings of the IEEE 61 (3), 268–278.
Krishnamurthy, B., Malandrino, D., Wills, C.E., 2007. Measuring privacy loss and the impact of privacy protection in web browsing. In: Proceedings of the 3rd symposium on Usable Privacy and Security, pp. 52–63.
Krishnamurthy, B., Wills, C., 2009. Privacy diffusion on the web: a longitudinal perspective. In: 18th international conference on World Wide Web - WWW, pp. 541–550.

Krishnamurthy, B., Wills, C.E., 2006. Generating a privacy footprint on the internet. In: 6th ACM SIGCOMM conference on Internet measurement - SIGCOMM, pp. 65–70.
Kumar, C., Ryan, R., Shao, M., 2020. Adversary for social good: Protecting familial privacy through joint adversarial attacks. In: 34th AAAI Conference on Artificial Intelligence - AAAI.
Lerner, A., Simpson, A.K., Kohno, T., Roesner, F., 2016. Internet jones and the raiders of the lost trackers: An archaeological study of web tracking from 1996 to 2016. 25th USENIX Security Symposium - USENIX Security.
Liu, B., Sheth, A., Weinsberg, U., Chandrashekar, J., Govindan, R., 2013. Adreveal: improving transparency into online targeted advertising. In: Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks, pp. 1–7.
Meng, W., Lee, B., Xing, X., Lee, W., 2016. Trackmeornot: Enabling flexible control on web tracking. In: 25th International Conference on World Wide Web - WWW.
Meng, X., Wang, S., Shu, K., Li, J., Chen, B., Liu, H., Zhang, Y., 2018. Personalized privacy-preserving social recommendation. In: 32nd AAAI Conference on Artificial Intelligence - AAAI.
Mihalcea, R., Tarau, P., 2004. Textrank: Bringing order into text. In: Proceedings of the 2004 Conference on Empirical Methods in Natural Language Processing - EMNLP.
Mikolov, T., Kombrink, S., Burget, L., Černockỳ, J., Khudanpur, S., 2011. Extensions of recurrent neural network language model. In: 2011 IEEE international conference on acoustics, speech and signal processing - ICASSP, pp. 5528–5531.
Mikolov, T., Sutskever, I., Chen, K., Corrado, G.S., Dean, J., 2013. Distributed representations of words and phrases and their compositionality. In: 27th MIT Press Annual Conference on Neural Information Processing Systems - NeurIPS.
Reiter, M.K., Rubin, A.D., 1998. Crowds: Anonymity for web transactions. ACM Trans. Inf. Syst. Secur. 1 (1), 66–92.
Roelleke, T., Wang, J., 2008. Tf-idf uncovered: A study of theories and probabilities. In: 31st International ACM SIGIR Conference on Research & Development in Information Retrieval - SIGIR.
Shen, T., Jia, J., Li, Y., Ma, Y., Bu, Y., Wang, H., Chen, B., Chua, T., Hall, W., 2020. PEIA: personality and emotion integrated attentive model for music recommendation on social media platforms. In: 34th AAAI Conference on Artificial Intelligence - AAAI.
Shi, H., Jiang, C., Dai, W., Jiang, X., Tang, Y., Ohno-Machado, L., Wang, S., 2016. Secure multi-party computation grid logistic regression (smac-glore). BMC medical informatics and decision making 16 (3), 175–187.
Song, X., Wang, X., Nie, L., He, X., Chen, Z., Liu, W., 2018. A personal privacy preserving framework: I let you know who can see what. In: 41st International ACM SIGIR Conference on Research & Development in Information Retrieval - SIGIR.
Sweeney, L., 2002. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10 (05), 557–570.
Tang, Y., Liu, L., 2015. Privacy-preserving multi-keyword search in information networks. IEEE transactions on knowledge and data engineering 27 (9), 2424–2437.
Tang, Y., Liu, L., Iyengar, A., Lee, K., Zhang, Q., 2014. e-ppi: Locator service in information networks with personalized privacy preservation. In: 2014 IEEE 34th International Conference on Distributed Computing Systems. IEEE, pp. 186–197.
Tang, Y., Wang, T., Liu, L., Meng, S., Palanisamy, B., 2011. Privacy preserving indexing for ehealth information networks. In: Proceedings of the 20th ACM international conference on Information and knowledge management, pp. 905–914.
Tanjim, M.M., Su, C., Benjamin, E., Hu, D., Hong, L., McAuley, J.J., 2020. Attentive sequential models of latent intent for next item recommendation. In: 29th international conference on World Wide Web - WWW, pp. 2528–2534.
Toubiana, V., Subramanian, L., Nissenbaum, H., 2011. Trackmenot: Enhancing the privacy of web search. CoRR abs/1109.4677.
Tsourakakis, C., 2015. The k-clique densest subgraph problem. In: 29th International World Wide Web Conference - WWW.
Vastel, A., Laperdrix, P., Rudametkin, W., Rouvoy, R., 2018. Fp-scanner: The privacy implications of browser fingerprint inconsistencies. 27th USENIX Security Symposium - USENIX Security.
Wang, B., Chen, G., Fu, L., Song, L., Wang, X., Liu, X., 2016. DRIMUX: dynamic rumor influence minimization with user experience in social networks. In: 30th AAAI Conference on Artificial Intelligence - AAAI.
Wang, F., Mickens, J., Zeldovich, N., 2018. Veil: Private browsing semantics without browser-side assistance. 25th Annual Network and Distributed System Security Symposium - NDSS.
Wang, S., Liu, C., Gao, X., Qu, H., Xu, W., 2017. Session-based fraud detection in online e-commerce transactions using recurrent neural networks. In: Machine Learning and Knowledge Discovery in Databases - European Conference - ECML PKDD.
Wang, X., Jin, D., Musial, K., Dang, J., 2020. Topic enhanced sentiment spreading model in social networks considering user interest. In: 34th AAAI Conference on Artificial Intelligence - AAAI.
Wills, C.E., Tatar, C., 2012. Understanding what they do with what they know. In: Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society, pp. 13–18.
Xu, T., Goossen, G., Cevahir, H.K., Khodeir, S., Jin, Y., Li, F., Shan, S., Patel, S., Freeman, D., Pearce, P., 2021. Deep entity classification: Abusive account detection for online social networks. 30th USENIX Security Symposium - USENIX Security.
Xu, Y., Wang, K., Yang, G., Fu, A.W., 2009. Online anonymity for personalized web services. In: 18th ACM Conference on Information and Knowledge Management - CIKM.
Yu, Z., Macbeth, S., Modi, K., Pujol, J.M., 2016. Tracking the trackers. In: 25th International Conference on World Wide Web - WWW.
Zhou, J., Fan, J., 2019. Translink: User identity linkage across heterogeneous social networks via translating embeddings. In: 38th IEEE Conference on Computer Communications - INFOCOM.
Zhu, Y., Xiong, L., Verdery, C., 2010. Anonymizing user profiles for personalized web search. In: 19th International Conference on World Wide Web - WWW.
Zimmeck, S., Li, J.S., Kim, H., Bellovin, S.M., Jebara, T., 2017. A privacy analysis of cross-device tracking. 26th USENIX Security Symposium - USENIX Security.



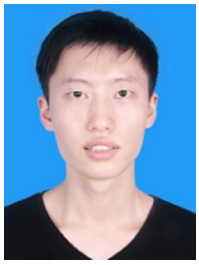
**Helin Li** received his B.E. degree from Xidian University, China, in 2018. He is currently pursuing his Ph.D. degree in the School of Cyber Engineering, Xidian University, China. His research interests include applied cryptography, network security, and privacy.

**Hui Zhu** received the B.Sc. degree from Xidian University, Xian, China, in 2003, the M.Sc. degree from Wuhan University, Wuhan, China, in 2005, and the Ph.D. degree from Xidian University, in 2009. He was a Research Fellow with the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore, in 2013. Since 2016, he has been a Professor with the School of Cyber Engineering, Xidian University. His current research interests include applied cryptography, data security, and privacy.



**Xiaodong Lin** received his first Ph.D. degree in information engineering from the Beijing University of Posts and Telecommunications, China, and his second Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada. He is currently a Professor at the School of Computer Science, University of Guelph, Canada. His research interests include wireless network security, applied cryptography, computer forensics, and software security.

**Rongxing Lu** is Mastercard IoT Research Chair, an associate professor at the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. Before that, he worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore from April 2013 to August 2016. Rongxing Lu worked as a Postdoctoral Fellow at the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious “Governor General’s Gold Medal”, when he received his Ph.D. degree from the Department of Electrical & Computer Engineering, University of Waterloo, Canada, in 2012; and won the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. Also, Dr. Lu received his first Ph.D. degree at Shanghai Jiao Tong University, China, in 2006. Dr. Lu is an IEEE Fellow. His research interests include applied cryptography, privacy-enhancing technologies, and IoT-Big Data security and privacy. He has published extensively in his areas of expertise (with H-index 77 from Google Scholar as of July 2021) and was the recipient of 9 best (student) paper awards from some reputable journals and conferences. Currently, Dr. Lu serves as the Vice-Chair (Conferences) of IEEE ComSoc CIS-TC (Communications and Information Security Technical Committee). Dr. Lu is the Winner of the 2016-17 Excellence in Teaching Award, FCS, UNB.



**Zhipeng Yu** received his B.E. degree from Xidian University, China, in 2019. He is currently pursuing an M.Sc. degree in the School of Cyber Engineering, Xidian University, China. His research interests include applied cryptography, network security, and outlier detection.

**Wei Lan** received his B.E. degree from Xidian University, China, in 2019. He is currently pursuing an M.Sc. degree in the School of Cyber Engineering, Xidian University, China. His research interests include network security and social network privacy.