Information Entropy Models and Privacy Metrics for Privacy Protection

Hui Xia¹ and Weiji Yang²
(Corresponding author: Weiji Yang)

School of Software, Shenyang Normal University¹
School of Life Science, Zhejiang Chinese Medical University²
548 Binwen Rd, Binjiang, Hangzhou, Zhejiang, China
Email: yangweiji@163.com
(Received Sept. 3, 2019; Revised and Accepted June 6, 2020; First Online Nov. 9, 2021)

Abstract
The quantification of privacy plays an important role in privacy protection. It can be used to solve privacy metrics as a quantitative measure of information. To realize the privacy metrics, some models of privacy information entropy are proposed according to Shannon’s Information Theory. Those models include the basic information entropy model of privacy protection, the information entropy model of privacy protection with adversary, the information entropy model of privacy protection with subjective feelings and multi-source information entropy model of privacy protection. In those models, the information owner is assumed to be the sender, privacy attacker is assumed as to be the recipient, and the privacy disclosure course can be regarded as a communication channel. Based on those assumptions, the entropy, mutual information, conditional entropy, and conditional mutual information are introduced to describe measurement of privacy, privacy disclosure, and privacy and disclosure with background knowledge for the privacy protection system. Furthermore, the quantitative evaluation of privacy protection strength and adversary ability is provided to support quantitative risk assessment for privacy disclosure. Finally, the specific information entropy model, measurement and analysis of privacy protection algorithms, and adversary ability are supplied for location privacy protection application. The proposed models and the privacy metrics can be used to analyze and evaluate the privacy protection technology and privacy disclosure risk assessment.

Keywords: Communication Model; Information Entropy Model; Privacy Measurement; Privacy Protection

1 Introduction
The study of privacy protection started earlier, but in recent years, the industry and academia have suddenly attracted much attention because of big data Privacy algorithms are mainly focused on anonymity methods, including K-anonymity, diversity anonymity and t-close anonymity and their derived methods. The privacy metrics originate from the related anonymity algorithm [15]. In the research of anonymity privacy protection algorithm, some scholars pay more attention to the problem of privacy quantification. Especially in the area of location service, location and trajectory anonymity algorithms have a lot of preliminary research on privacy measurement [13, 14]. However, there are many factors involved in privacy disclosure. Designing effective privacy protection algorithms is still a challenging problem. From these analyses, the study of privacy metrics has very important theoretical significance and application value.

Information entropy, as an effective tool for information measurement, has shown its important contribution in the field of communication [2]. Privacy as a certain of information, naturally can be represented as entropy. For this reason, many scholars have some researches on entropy, such as event entropy, anonymous set entropy, conditional entropy and so on [1, 7, 11]. But these researches are more fragmented or focus on for a particular area but not for a unified model, such as location privacy protection. Moreover, its scope of application is also limited. People may have different opinions on the same privacy in our space-time nature. Based on the above analysis, This paper aims to propose the communication framework of Shannon’s Information theory [12]. Several privacy protection information entropy models are proposed, Include basic information entropy model, adversary attack model, subjective and privacy protection model with multiple privacy sources. In these models, the information owner is assumed to be the sender, the privacy purveyor is assumed to be the receiver, and the privacy leak channel is assumed to be a communication channel. Based on these assumptions, Privacy information entropy, average mutual information, conditional entropy and conditional mutual information are introduced to describe privacy measure, privacy disclosure measure,
privacy measure and disclosure measure of privacy information system. Based on this, the paper further puts forward the quantitative evaluation of the strength of privacy protection method and the ability of adversary attack, and tries to provide a theoretical support for quantitative risk assessment of privacy disclosure.

Section 2 of this paper describes the related work. Based on the communication model of information entropy, the information entropy model of privacy with common characteristics is proposed in Section 3. Section 4 presents a privacy metric and evaluation system based on the model proposed in Section 3. Section 5 applies the privacy measurement method and evaluation system proposed in this paper to prove the privacy protection method effectiveness. Section 6 gives conclusion.

2 Related Work

The information entropy theory proposed by Shannon [12] solves the theoretical basis of information quantification and communication. Earlier information entropy measure considering privacy research is Diaz et al and Serjantov et al, they proposed using information entropy to measure the anonymity of anonymous communication systems. Assuming the attacker’s intention is to determine the true identity of the sender (or recipient) of the message, each user in the system is guessed as the true sender or receiver of the message with a certain probability, and the attacker guesses that a user is a real sender or receiver as a random variable X, and uses information entropy 

\[ H(X) = -\sum p(x) \log p(x) \]

to quantify the privacy level of the system.

Subsequently, many scholars have applied information entropy to some specific areas of privacy metrics, such as location services, social networks and data mining and other fields [3-6,8-10,13,14]. For different schemes, the probability expression of the random variable is different from the way to deal with entropy. In the field of location-based services, in 2007, Hoh et al. [3,6] proposed privacy measurement based on information entropy to measure uncertainty of trajectory tracking, where the probability of a random variable is represented by the probability that each location instance contains the current tracked vehicle trajectory. In 2009, Ma et al. [10] proposed the privacy measurement method of information entropy in the V2X car network system. Among them, the probability of a random variable performance associated with each location information to the probability that a particular user. The method also takes into account the situation that the probability of a random variable is updated over time, the attacker’s cumulative information on the impact of system privacy. In the same year, Lin Xin and others [8] for the LBS in the continuous query problem, a continuous query attack algorithm. They point out that the anonymity of the set is no longer suitable as a measure of the anonymity of the algorithm and presents a measure of entropy based on information. Where the probability of a random variable is represented by the probability that each user \( u_i \) is the true originator of the query \( q \), the information entropy is calculated as \( H(q) \), and the privacy level of the system is measured by \( AD(q) = 2H(q) \). In 2011, Shokri et al. divided the metrics of location privacy into accuracy, certainty and correctness: The accuracy measure is the confidence interval of the attacker’s guessing event. The deterministic measure is the uncertainty of the attacker’s guess. The correctness measure is the probability of the attacker’s error. Among them, the accuracy of the measurement is based on the measurement method of information entropy. The probability of random variables for each observed event is the probability of real events.

In 2012, Chen and others [3] for LBS query privacy measurement. The probability of a random variable is represented by the probability that the attacker has no background knowledge or background knowledge, and the user \( u_i \) is the conditional probability of the true sender of the query \( q \), and use mutual information \( I(U|q; <r,t,q>) = H(U|q) - H(U|<r,t,q>) \) to measure the privacy level of the system. In the same year, Wang Caimei et al. [14] for the trajectory in LBS privacy protection method Silent Cascade proposed based on the information entropy of privacy measurement method. The probability of a random variable is expressed as the probability of every possible trajectory of a user. The entropy calculation for a particular user is \( H(u_i) \), and use the standard entropy \( D(u_i) = H(u_i)/H_{max}(u_i) \) to measure the privacy level of the system. In 2014, the literature [4] used the information entropy to measure the LBS system’s privacy level.

In summary, at present, the theoretical system of privacy measurement based on information entropy is fragmented and lacks a unified model foundation. Regarding the issue above, in this paper, we try to regard the privacy protection system as a communication propagation model, and try to discuss the more common privacy measure information entropy model, and solve some basic concepts and basic system of privacy measurement.

3 Privacy Protection Information Entropy Model

The starting point of this paper is to assume that the owner of the information as the sender, privacy seekers (adversaries) is assumed to be the receiver, the privacy of the leakage channel is assumed to be communication channels.

The information set owned by the sender is called the privacy source, represented by the random variable \( X \), \( X \) is a privacy message space made up of privacy messages of all discrete basic disclosure events, which is \( \{x_1, x_2, \ldots, x_n\} \), where \( x_i (i = 1, 2, \ldots, n_i) \) is the privacy message of the basic disclosure event; The information collection that the receiver gets is called the privacy sink, with a random variable \( Y \) said, which is made up of all the
basic privacy messages acquired by the adversary, which is \( \{y_1, y_2, \ldots, y_m\} \), where \( y_j (j = 1, 2, \ldots, m) \) is a private information obtained by the adversary. Correspondingly, a specific privacy protection algorithm can be seen as a privacy message conversion, encoding method. It can interfere with the privacy message, and then realize the protection of privacy information. Among them, the privacy protection algorithm of the overall structure of privacy protection mechanism space is called the source of privacy protection mechanism. Adversary in a certain background knowledge of the private information mining and analysis of means of privacy attacks, all privacy methods known as privacy attack space.

Based on this assumption, in this section, we propose several privacy information entropy models based on Shannon information theory \([12]\), including privacy protection basic information entropy model, privacy protection information entropy model with adversary attack, information entropy model with subjective perception and privacy protection information entropy model with multiple privacy sources.

### 3.1 Privacy Protection Basic Information Entropy Model

Here, we first assume that the adversary has no privacy attack ability, the adversary only observes the privacy information through the channel, and only considers the situation of the discrete single privacy source. The model definition is shown in Figure 1.

![Figure 1: Communication model of privacy protection with single privacy information source](image)

The mathematical model of a single private source \( X \) can be expressed as:

\[
\begin{bmatrix}
  X \\
  P(X)
\end{bmatrix} = \begin{bmatrix}
  x_1 & x_2 & \cdots & x_i & \cdots & x_n \\
  p(x_1) & p(x_2) & \cdots & p(x_i) & \cdots & p(x_n)
\end{bmatrix}
\]

Among them, \( 0 \leq p(x_i) \leq 1, \sum_{i=1}^{n} p(x_i) = 1 \). Similarly, the mathematical model of privacy sink \( Y \) can be expressed as:

\[
\begin{bmatrix}
  Y \\
  P(Y)
\end{bmatrix} = \begin{bmatrix}
  y_1 & y_2 & \cdots & y_j & \cdots & y_m \\
  p(y_1) & p(y_2) & \cdots & p(y_j) & \cdots & p(y_m)
\end{bmatrix}
\]

Among them, \( 0 \leq p(y_j) \leq 1, \sum_{j=1}^{m} p(y_j) = 1 \). For this model, we define the entropy \( H(X) \):

\[
H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i)
\]

\( H(X) \) is used to characterize the average amount of privacy information of privacy sources, and also the degree of privacy uncertainty of privacy sources. The greater the \( H(X) \), the less likely the privacy disclosure is, so it can also be used to measure the degree of privacy protection. In the absence of external conditions, the value is a certain value. When the privacy of the client \( Y \) to obtain some privacy information in the conditions, as to the degree of uncertainty of privacy sources, we can introduce the privacy condition entropy \( H(X|Y) \), which is defined as

\[
H(X|Y) = -\sum_{j=1}^{m} \sum_{i=1}^{n} p(x_iy_j) \log_2 p(x_i|y_j).
\]

The conditional entropy means that the privacy source \( X \) is still uncertain after receiving the \( Y \) information. The degree of uncertainty is caused by the interference (privacy protection) of the privacy leak channel, which is adversaries in the long-term observation of the source of privacy in the process, due to the protection of privacy protection mechanism, the opponent of the source of privacy is still some unknown and easy to prove. This entropy of privacy information satisfies the basic properties of Shannon source entropy \([2]\). That has non-negative, symmetry, expansibility, certainty, additivity, extreme value, convexity and so on, and satisfies the maximal discrete entropy theorem, will not repeat here. The following describes the average privacy mutual information \( I(X;Y) \) to describe the degree of privacy disclosure on the channel, defined as

\[
I(X;Y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} p(x_iy_j) \log_2 \frac{p(x_iy_j)}{p(x_i)}
\]

\( I(X;Y) \) denotes the average amount of information exchanged between the privacy source \( X \) and the privacy sink \( Y \), that is, the amount of privacy information propagated on the channel. It can just depict the overall degree of disclosure of privacy, which can be used as a measure of privacy disclosure.

### 3.2 Information Entropy Model of Privacy Protection with Adversary Attack

The privacy entropy model proposed in the previous section describes objectively the privacy measurement problem in the case of invulnerability or non-attack capability. In the actual system, there is often a privacy attack analysis, the adversary can be in a certain background knowledge of attack analysis, the model definition shown in Figure 2.

![Figure 2](image)

In this model, \( Z \) represents the background knowledge.
The attacker can exploit the background knowledge to strengthen the privacy attack. For the attacker, it can combine the privacy message \( Y \) and the background knowledge \( Z \) to carry on the privacy analysis attack and introduce the attack condition entropy:

\[
H(X|YZ) = -\sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{l} p(x_i y_j z_k) \log_2 p(x_i|y_j z_k).
\]

\( H(X|YZ) \) reflects that the attacker obtains the privacy message \( Y \) and the background knowledge \( Z \), with regard to the uncertainty that \( X \) still exists. It can be used as an attack in the means of privacy under the uncertainty of information can also be used as a measure of privacy protection strength. Similarly, the average mutual information of privacy attacks is further defined:

\[
I(X;Y|Z) = \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{l} p(x_i y_j z_k) \log_2 \frac{p(x_i y_j z_k)}{p(x_i|z_k)p(x_j|z_k)}.\]

\( I(X;Y|Z) \) reflects the average mutual information between \( X \) and \( Y \) under the condition that \( Z \) is obtained, that is, the amount of privacy information obtained by the receiver and the degree of privacy disclosure with background knowledge attack.

### 3.3 Information Entropy Model with Subjective Feeling

In reality, the sensitivity of privacy information is usually subjective, and different people feel different about the value of privacy information. In this section, the weights are introduced into the information entropy model of the first two sections, and the information entropy model with subjective feelings are proposed and measurement.

1) Entropy model of privacy protection with subjective feelings

For the privacy message \( x_i (i = 1, 2, \cdots, n) \) of the communication model described in Figure 1, a non-negative real number is set as the sensitivity weight of the message. The greater the weight is, the greater the sensitivity. The weight space is as follows:

\[
H_w(X) = -\sum_{i=1}^{n} w_i p(x_i) \log_2 p(x_i).
\]

\( H_w(X) \) is to describe the subjective sensitivity of different users to privacy messages by weight \( W_i (i = 1, 2, \cdots, n) \), so as to realize the privacy information measure with subjective feelings. The weighted entropy of private sources obviously has the following properties:

- **Non-negative**: That the source of privacy in the event of a privacy disclosure event, which can always provide some privacy information.

- **Continuity**: When the probability of private event occurs, the private information source will form another privacy source. The weight entropy of the two privacy sources before and after the change is continuous. This feature is very effective in characterizing changes in the characteristics of a source of privacy due to temporal changes. Such as in a certain period of time, a person’s life law is fixed, leading to its ability to disclose personal privacy behavior model of the probability distribution is relatively fixed, but with the passage of time, the person’s life will be a continuous pattern of minor changes, and thus be able to reveal their privacy behavior pattern of probability distribution has also been a slight change. However, before and after the behavior change, the weighted entropy of the behavioral population is continuous.

In addition, the weighted entropy of the source information and other properties of information entropy, in the privacy protection system also have the corresponding practical significance.

Likewise, we can define the privacy weighting condition entropy \( H_w(X|Y) \) to describe the condition that privacy seekers obtain some privacy information, about the owner’s privacy information uncertainty of average:

\[
H_w(X|Y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} p(x_i y_j) \log_2 p(x_i|y_j).
\]

Define privacy-weighted average mutual information \( I_w(X|Y) \) to describe the degree of privacy information disclosure with subjective feelings, under the
protection of the privacy protection mechanism. It indicates the amount of private information obtained by privacy seekers by observing the privacy events:

\[ I_w(X; Y) = \sum_{i=1}^{n} w_i \sum_{j=1}^{m} p(x_i y_j) \log_2 \frac{p(x_i y_j)}{p(x_i)} \]

Here, the privacy-weighted condition entropy and the privacy-weighted average mutual information only take into account the subjective feelings and preferences of the privacy source to the privacy message. In the actual system, not only the information owner of their own privacy information has different subjective feelings and preferences, privacy seekers to obtain the privacy information also have different subjective feelings and preferences. It can further explore the private communication model of privacy in the privacy of the subject of privacy messages and give weight to the feelings, and even set up the weight matrix that depicts the privacy source of privacy source and privacy sink.

2) An Entropy Model of Privacy Protection with Subjective Feelings and Attacking

In consideration of the subjective feelings or preferences of the privacy owner of his privacy information, we define the weighting attack condition entropy \( H_w(X|Y,Z) \) to describe the attack effect of privacy sink \( Y \) in background knowledge \( Z \) support, it can also be used as a measure of privacy protection against rival attacks.

\[ H_w(X|Y,Z) = -\sum_{i=1}^{n} w_i \sum_{j=1}^{m} \sum_{k=1}^{l} p(x_i y_j z_k) \log_2 p(x_i|y_j z_k). \]

On this basis, further defined privacy attacks weighted average mutual information \( I_w(X; Y|Z) \); It represents the amount of private information received by the privacy sink under the condition that \( Z \) is obtained, which characterizes the privacy disclosure measure under the condition of background knowledge:

\[ I_w(X; Y|Z) = \sum_{i=1}^{n} w_i \sum_{j=1}^{m} \sum_{k=1}^{l} p(x_i y_j x_k) \log_2 \frac{p(x_i z_k|y_j)}{p(x_i|z_k) p(y_j|z_k)}. \]

### 3.4 Multi-source Privacy Protection Information Entropy Model

Realistic information system owners often have more than one. Thus involving a number of privacy sources of the problem. Therefore, it is necessary to establish a privacy-protected communication model with multiple privacy sources to measure the protection and attack of the privacy information of multiple sources associated with each other. Figure 3 shows the privacy of multiple privacy sources without privacy attacks communication model.

In the communication model shown in Figure 3, privacy source \( X_1 \) and privacy source \( X_2 \) together constitute the source of privacy \( X \). The mathematical model is:

\[
\begin{aligned}
X_1 \\
P(X_1) = \left[ \begin{array}{cccc}
X_{11} & X_{12} & \cdots & X_{1n1} \\
p(x_{11}) & p(x_{12}) & \cdots & p(x_{1n1})
\end{array} \right] \\
0 \leq p(x_{1i}) \leq 1, \sum_{i=1}^{n_1} p(x_{1i}) = 1, i_1 = 1, 2, \ldots, n_1
\end{aligned}
\]

\[
\begin{aligned}
X_2 \\
P(X_2) = \left[ \begin{array}{cccc}
X_{21} & X_{22} & \cdots & X_{2n2} \\
p(x_{21}) & p(x_{22}) & \cdots & p(x_{2n2})
\end{array} \right] \\
0 \leq p(x_{2i}) \leq 1, \sum_{i=2}^{n_2} p(x_{2i}) = 1, i_2 = 1, 2, \ldots, n_2
\end{aligned}
\]

The mathematical model of privacy sink \( Y \) is described by Equation (4). The definition of multi-source joint source of privacy information source entropy \( H(X_1, X_2) \). The source entropy characterizes a number of privacy measures with associated privacy owners:

\[
\begin{aligned}
H(X_1, X_2) &= -\sum_{i_1=1}^{n_1} \sum_{i_2=1}^{n_2} p(x_{1i_1}, x_{2i_2}) \log_2 p(x_{1i_1}, x_{2i_2}) \\
&= H(X_1) + H(X_2|X_1).
\end{aligned}
\]

The multi-source federated privacy condition entropy of private source \( X \) under the condition of known privacy client \( Y \) can be defined as \( H(X|Y) = H(X_1, X_2|Y) - H(Y) \). The definition of the number of associated with the source of privacy in the implementation of privacy protection. The average degree of joint uncertainty of the privacy information is obtained by the privacy information acquirer after observing the privacy event.

Simultaneously, the multi-source joint average mutual information \( I(X_1, X_2; Y) \) can be defined to characterize the degree of privacy disclosure of the associated plurality of privacy sources:

\[
I(X_1, X_2; Y) = \sum_{i_1=1}^{n_1} \sum_{i_2=1}^{n_2} \sum_{j=1}^{m} p(x_{1i_1}, x_{2i_2}, y_j) \log_2 \frac{p(x_{1i_1}, x_{2i_2}|y_j)}{p(x_{1i_1}, x_{2i_2})}
\]

- Privacy protection information entropy model with multiple privacy sources and privacy attack.
Based on the information entropy model with privacy attack, privacy protection was proposed in Section 2.2, introducing a plurality of associated information owners, forming a new associated multi-privacy source, constructing the privacy protection information entropy model of multi-privacy source with adversary attack, as shown in Figure 4.

![Figure 4: Communication model of privacy protection with multi-source of privacy information and attacks](Image)

Figure 4 shows the source model of the communication model as shown in Equation (3) and Equation (4), the mathematical model of privacy sink Y is described in Equation (1). The multi-source joint entropy of this model is:

\[
H(X) = H(X_1, X_2),
\]

multi-source joint privacy attack condition entropy is:

\[
H(X_1, X_2 | Y, Z),
\]

multi-source joint privacy attack condition average mutual information is:

\[
I(X_1, X_2; Y | Z),
\]

among them, multi-source joint privacy attack condition entropy represents the uncertainty of the privacy information of the joint privacy source under background knowledge attack; multi-source federated privacy attack condition average mutual information is the degree of privacy disclosure of the joint privacy source under background knowledge attack, among them,

\[
H(X_1, X_2 | Y, Z) = H(X_1, X_2) - H(Y, Z)
\]

I\((X_1, X_2; Y | Z) = H(X_1, X_2) - H(X_1, X_2 | Y, Z).\)

4 Privacy Metrics and Their Evaluation Mechanisms

Information entropy and average mutual information can be related to the measurement of privacy information, based on this, the establishment of anti-attack ability evaluation method of privacy protection mechanism is realized.

4.1 Privacy Measurement Methods

In the basic information entropy model, the privacy condition entropy \(H(X|Y)\) can be used to measure in the privacy protection mechanism. The privacy source still has a degree of uncertainty so that it can evaluate the strength of the privacy protection algorithm. If the A records for a specific privacy protection, then \(H_p(X|Y)\) is in the implementation of protection with \(I(X,Y)\) after the privacy of the destination (adversary) Y is still on the unknown amount of privacy, from a privacy owner’s perspective, it is desirable that the condition \(I(X,Y)\) indicates that the privacy information X is protected by the privacy protection mechanism. The average amount of privacy information acquired by the sink Y, similarly, \(I_{p_i}(X,Y)\) is the privacy information received by Y after being protected by \(p_i\). It should be as small as possible.

**Property 1.** Privacy condition entropy \(H(X|Y)\) and privacy mutual information \(I(X;Y)\) have the consistency of privacy measure.

**Proof.** From Equation (2) shows:

\[
I(X;Y) = \sum_{i=1}^{n} \sum_{j=1}^{m} p(x,y) \log_2 \frac{p(x|y)}{p(x)}
\]

\[
= \sum_{i=1}^{n} \sum_{j=1}^{m} p(x,y) \log_2 \frac{1}{p(x)} - \sum_{i=1}^{n} \sum_{j=1}^{m} p(x,y) \log_2 \frac{1}{p(x|y)}
\]

\[
= \sum_{i=1}^{n} p(x) \log_2 \frac{1}{p(x)} - \sum_{i=1}^{n} \sum_{j=1}^{m} p(x,y) \log_2 \frac{1}{p(x|y)}
\]

\[
= H(X) - H(X|Y).
\]

So there \(I(X;Y) = H(X) - H(X|Y)\). The larger the privacy condition entropy, the smaller the mutual information of privacy meaning, and they are consistent.

4.2 Privacy Protection Mechanism and Privacy Attack Evaluation and Analysis

4.2.1 Privacy protection of the Basic Information Entropy Model

The purpose of the privacy protection mechanism (algorithm) is to protect the privacy of information owners. The aim is to make \(H(X|Y)\) as small as possible. That is, through some kind of privacy protection mechanism, so that the amount of information \(I(X;Y)\) obtained by the privacy gatherer is as small as possible, preferably 0.

**Definition 1.** If under the protection of some kind of privacy protection, privacy, average mutual information \(I(X;Y)\) (private sink received from the source to the privacy of the privacy information is 0), it is said that the privacy protection mechanism for this source is completely privacy protection.

**Definition 2.** For the same privacy source X, privacy protection mechanisms \(p_i\) and \(p_j\) are used to protect:

- If \(H_{p_i}(X|Y) < H_{p_j}(X|Y)\) or \(I_{p_i}(X;Y) > I_{p_j}(X;Y)\), then the privacy protection mechanism \(p_j\) is better than the \(p_i\) privacy protection. Abbreviated as partial order relation \(p_i < p_j\).
• If \( H_{p_i}(X|Y) = H_{p_j}(X|Y) \) or \( I_{p_i}(X;Y) = I_{p_j}(X;Y) \), then said the privacy protection mechanism \( p_i \) and \( p_j \) privacy protection equivalence. Abbreviated as equivalence relation \( p_i \cong p_j \).

**Theorem 1.** Partial order relation and equivalence relation of privacy protection mechanism are defined as defined in definition 2, then partial ordering relation is transitivity, and equivalence relation has reflexivity, transitivity and symmetry.

Proof. If \( p_i \prec p_j \), \( p_j \prec p_k \), and by definition there are 
\( H_{p_i}(X|Y) < H_{p_j}(X|Y) \) and \( H_{p_j}(X|Y) < H_{p_k}(X|Y) \). According to the nature of information entropy, easy to get 
\( H_{p_i}(X|Y) < H_{p_k}(X|Y) \), namely \( p_i \prec p_k \). Similarly, if \( I_{p_i}(X;Y) > I_{p_j}(X;Y) \) and \( I_{p_j}(X;Y) > I_{p_k}(X;Y) \), according to the nature of 1, easy to prove \( I_{p_i}(X;Y) > I_{p_k}(X;Y) \). Then there is \( p_i \prec p_k \). That is, partial order relations are transitivity. Similarly, it’s easy to verify the equivalence of the three characteristics.

**Definition 3.** (privacy protection validity distance). In the basic entropy model of privacy protection, privacy protection mechanism \( p_i \) and \( p_j \) are used to protect the same privacy source \( X \), if the amount of private information received by privacy sink \( Y \) is \( I_{p_i}(X;Y) \) and \( I_{p_j}(X;Y) \), respectively. The validity distance between these two privacy protection mechanisms is defined as 
\[ d_j = |I_{p_i}(X;Y) - I_{p_j}(X;Y)|. \]

In the privacy protection basic information entropy model, the privacy protection validity distance depicts the effectiveness of two different privacy protection mechanisms to protect the same privacy information. Clearly, \( d_j \) smaller, the smaller the difference between the two effectiveness of privacy protection algorithms; The greater the \( d_j \), the greater the difference in the effectiveness of the two privacy protection algorithms.

**4.3 The Privacy Protection Mechanism and Privacy Attack Evaluation with Adversary Attack**

In the actual system, the goal of the privacy protection mechanism is: In the case of various types of privacy attacks against opponents. The privacy information of the information owner is still made available to the privacy seeker as little as possible. That is, through a privacy protection mechanism to resist the opponent in the certain background knowledge of privacy attacks, making privacy seekers get the amount of private information \( I(X;Y|Z) \) as small as possible, preferably 0.

**Definition 4.** For a privacy protection system with an adversary attack, if \( I(X;Y|Z) = 0 \), that is, in the opponent in the context of knowledge \( Z \) attack, if the privacy protection mechanism can make the owner of the information disclosure of privacy information is 0, then said the privacy system is perfect privacy protection.

**Definition 5.** For a privacy protection system with an adversary attack, if the adversary adopts the privacy attack means \( A_r \) to carry on the attack, the system respectively uses the privacy protection mechanism and to carry on the protection:

- If \( H_{p_i,A_r}(X|Y) < H_{p_j,A_r}(X|Y) \) or \( I_{p_i,A_r}(X;Y) < I_{p_j,A_r}(X;Y) \), then the resistance to \( A_r \) attack, the privacy protection mechanism \( p_j \) is better than the \( p_i \) privacy protection, recorded as partial order relation \( p_i(A_r) < p_j(A_r) \);
- If \( H_{p_i,A_r}(X|Y) = H_{p_j,A_r}(X|Y) \) or \( I_{p_i,A_r}(X;Y) = I_{p_j,A_r}(X;Y) \), then it is said that the privacy protection mechanism \( p_i \) and \( p_j \) privacy protection equivalence, recorded as partial order relation \( p_i(A_r) \cong p_j(A_r) \);
- If \( H_{p_i,A_r}(X|Y) > H_{p_j,A_r}(X|Y) \) or \( I_{p_i,A_r}(X;Y) > I_{p_j,A_r}(X;Y) \), then it is said that under the protection of privacy protection mechanism \( p_i \), privacy attack \( A_r \) more effective than the \( A_r \), recorded as partial order relation \( A_r(p_i) > A_r(p_j) \).

**Theorem 2.** If partial relation and equivalence relation are defined as Definition 5 or Definition 7, partial ordering relation satisfies transitivity, and equivalence relation \( \cong \) satisfies reflexivity, symmetry and transitivity.

Proof. Similar to the proof of Theorem 1, abbreviated.

**Definition 8.** (privacy attack validity distance). In the privacy protection information entropy model with the adversary attack, under the same privacy protection mechanism \( p_i \), adversaries use privacy attacks \( A_r \) and \( A_q \) to
attack, the validity distance between the two privacy attacks is called \( d_l(p_l) = |I_{p_l:A_y}(X;Y) - I_{p_l:A_y'}(X;Y)| \).

In the information entropy model of privacy protection with adversary attack, the validity of privacy attack distance \( d_l(p_l) \) depicts the difference of adversary attack ability, which gives the measure of adversary attack ability.

**Theorem 3.** In the privacy protection communication model with the adversary attack, suppose the rival’s background knowledge is \( Z \). Then \( I(X;Y) \leq I(X;YZ) \).

**Proof.** From the calculation of the average mutual information equation:

\[
I(X;Y) = H(X) - H(X|Y) \\
I(X;YZ) = H(X) - H(X|YZ).
\]

Let (22) be subtracted from (21) to obtain:

\[
I(X;YZ) - I(X;Y) = H(X|Y) - H(X|YZ).
\]

By the nature of information entropy \( H(X|Y) \geq H(X|YZ) \), so \( H(X|Y) \geq 0 \) and \( I(X;YZ) \geq I(X;Y) \).

The theorem states: adversary in a certain background knowledge of privacy attacks and analysis, the adversary to obtain the privacy information is not less than its background information cannot get the privacy information. This also provides a direction for privacy protection, that is, the privacy information intercepted by the adversary and the background information associated with it as small as possible, so as to maximize the protection of privacy information.

### 5 Experiments and Simulations

The privacy protection information entropy model proposed above and its measurement method belong to the general situation, applicable to different scenarios. The following is a simple location privacy protection application for the example of the effectiveness of the model analysis. Assume that a user \( A_u \) moves in an area divided into \( M \) blocks, denote \( R = \{r_1, r_2, \cdots, r_M\} \) is the set of different areas of \( M \) blocks, that is, the location space, the purpose of the attacker is to determine the user’s real location.

#### 5.1 Location Privacy Protection Communication Model

Corresponding to the privacy protection information entropy model with adversary attack, the privacy source is the location distribution \( R \) for which the user may be located, and the value of the random variable \( R \) indicates that the user \( u \) is in a certain location area \( r_i \), using \( \{r_1, r_2, \cdots, r_M\} \) indicates the position of the region in which the user space, assuming that the probability of each region is \( p(r_i) \), has \( 0 \leq p(r_i) \leq 1 \), \( \sum_{i=1}^{M} p(r_i) = 1 \), the probability model of \( R \) can be expressed as:

\[
\begin{bmatrix}
R \\
P(R)
\end{bmatrix} = \begin{bmatrix}
r_1 & r_2 & \cdots & r_i & \cdots & r_M \\
p(r_1) & p(r_2) & \cdots & p(r_i) & \cdots & p(r_M)
\end{bmatrix}
\]

The true location distribution information of the user is privacy information, in order to prevent the attacker from obtaining the real area of the user directly, it is necessary to protect the position distribution \( R \) of the user, through a location privacy protection mechanism (Including location generalization, taking pseudonyms, hiding or adding virtual locations, etc.) after performing the privacy protection process on the position distribution \( R \), becomes an observable position distribution \( R' \) that can be directly observed by an attacker, set up \( R' = \{r'_1, r'_2, \cdots, r'_M\} \), where \( r'_i \) is the area of the user \( u \) that can be observed by the attacker after privacy protection, and the probability model of observable position distribution \( R' \) is:

\[
\begin{bmatrix}
R' \\
P(R')
\end{bmatrix} = \begin{bmatrix}
r'_1 & r'_2 & \cdots & r'_i & \cdots & r'_M \\
p(r'_1) & p(r'_2) & \cdots & p(r'_i) & \cdots & p(r'_M)
\end{bmatrix}
\]

After the attacker obtains the observable position distribution \( R' \), combined with the background knowledge of the user \( u \) to attack the location, we get the inferred position \( \hat{R} \) of the attacker, set up \( \hat{R} = \{\hat{r}_1, \hat{r}_2, \cdots, \hat{r}_M\} \), among them, \( \hat{R} \) that the attacker guessed the user \( U \) is the real region, its probability model is:

\[
\begin{bmatrix}
\hat{R} \\
P(\hat{R})
\end{bmatrix} = \begin{bmatrix}
\hat{r}_1 & \hat{r}_2 & \cdots & \hat{r}_i & \cdots & \hat{r}_M \\
p(\hat{r}_1) & p(\hat{r}_2) & \cdots & p(\hat{r}_i) & \cdots & p(\hat{r}_M)
\end{bmatrix}
\]

0 \leq p(\hat{r}_i) \leq 1, \sum_{i=1}^{M} p(\hat{r}_i) = 1

Figure 5 shows the communication model of the location privacy protection scene, which can be regarded as a concrete example of privacy protection information entropy model with adversary attack.

![Communication model of location privacy](image)

**5.2 Comparison of Different Privacy Protection Mechanisms under the Same**

Background Knowledge In the initial stage, the user \( u \) is in a real region \( r_i \). The probability that the user is in the
region \( r_i \) is 1. The probability of being in other regions is 0. Specifically

\[
\begin{bmatrix}
R \\
p(R)
\end{bmatrix} = \begin{bmatrix}
r_1 & r_2 & \cdots & r_i & \cdots & r_M \\
0 & 0 & \cdots & 1 & \cdots & 0
\end{bmatrix}
\]

In this case, the entropy of the entropy of the source information, that is, the location distribution \( R \), is \( H(R) = -\sum_{i=1}^{M} p(r_i) \log p(r_i) = 0 \).

1) **Weak privacy protection intensity of privacy measures**

If the location generalization is used as the location privacy protection mechanism, if the user \( u \)'s publishing location is generalized from area \( r_i \) to \( \{r_{i-1}, r_i, r_{i+1}, r_{i+2}\} \), the probability model of observable location distribution is as follows:

\[
\begin{bmatrix}
R' \\
p(R')
\end{bmatrix} = \begin{bmatrix}
r_i' & \cdots & r_{i-1}' & r_i' & r_{i+1}' & r_{i+2}' & \cdots & r_M' \\
0 & \cdots & 1 & 0 & 1 & 0 & \cdots & 0
\end{bmatrix}
\]

Then the entropy of observable position distribution is \( H(R') = -\sum_{i=1}^{M'} p(r_i') \log p(r_i') = 2 \), it is equivalent to the entropy containing privacy information entropy model adversary under \( H(X|Y) \). After the attacker obtains the observable position distribution, combined with their own background knowledge for analysis, in a certain background knowledge, the probability distribution model of the inferred location of user \( u \) is analyzed as follows:

\[
\begin{bmatrix}
R \\
p(R)
\end{bmatrix} = \begin{bmatrix}
r_i & \cdots & r_i & r_{i+1} & r_{i+2} & \cdots & r_M \\
0 & \cdots & 1 & 0 & 1 & \cdots & 0
\end{bmatrix}
\]

At this point, we can get \( H(\hat{R}) = -\sum_{i=1}^{M} p(\hat{r}_i) \log p(\hat{r}_i) = 1.75 \), it indicates the degree of uncertainty of the location of the user under the condition of background knowledge, it is equivalent to the entropy privacy information entropy model adversary under \( H(X|Y,Z) \).

2) **Strong privacy protection intensity of privacy measures**

When we take the generalization of the location area becomes larger, that is, strong privacy protection means, we take the release location of user \( u \) from area \( \{r_{i-1}, r_i, r_{i+1}, r_{i+2}\} \) to \( \{r_i, r_{i+1}, \cdots, r_{i+2}\} \). The probabilistic model of observable location distribution is

\[
\begin{bmatrix}
R \\
p(R)
\end{bmatrix} = \begin{bmatrix}
r_i & \cdots & r_i & r_{i+1} & r_{i+2} & \cdots & r_M \\
0 & \cdots & 1 & 0 & 1 & \cdots & 0
\end{bmatrix}
\]

At this point, we can get \( H(\hat{R}) = -\sum_{i=1}^{M} p(\hat{r}_i) \log p(\hat{r}_i) = 2.3125 \), it represents attacker uncertainty measure the user’s location under conditions having background knowledge, equivalent to the entropy privacy information entropy model adversary under \( H(X|Y,Z) \). From 2.3125 > 1.75 can be verified with the adversary attack privacy protection information entropy model \( H_{p,A_r}(X|Y,Z) < H_{p,A_\hat{r}}(X|Y,Z) \) is established.

### 5.3 Comparison

Comparison of the Effects of Different Privacy Attacks under the Same Privacy Protection Mechanism:

1) The privacy measure of weak privacy attack strength. The privacy measure of the intensity of weak privacy protection is the same as in Section 5.2.

2) Strong privacy attack strength of privacy measures. The privacy protection mechanism with the weak privacy protection in Section 5.2 of the privacy measure, the attacker to obtain the observable position distribution, combined with their background knowledge of the analysis, in strong privacy attack strength. The probability model for the more accurate inferred positional distribution for user \( u \) is analyzed as follows:

\[
\begin{bmatrix}
R \\
p(R)
\end{bmatrix} = \begin{bmatrix}
r_i & \cdots & r_i & r_{i+1} & r_{i+2} & \cdots & r_M \\
0 & \cdots & 1 & 0 & 1 & \cdots & 0
\end{bmatrix}
\]

At this point, we can get \( H(\hat{R}) = -\sum_{i=1}^{M} p(\hat{r}_i) \log p(\hat{r}_i) = 1.418 \), it represents attacker uncertainty measure the user’s location under conditions having background knowledge, equivalent to the entropy privacy information entropy model adversary under \( H(X|Y,Z) \). From 1.418 < 1.75 can be verified with the adversary attack privacy protection information entropy model \( H_{p,A_r}(X|Y,Z) < H_{p,A_\hat{r}}(X|Y,Z) \) is established.

### 6 Conclusion

In this paper, several privacy protection information entropy models are proposed based on Shannon information theory. The key point is to regard the privacy protection system as a communication model. The methods of privacy information measurement, privacy protection intensity quantification and attack capability quantification in different occasions are given preliminarily by defining the concepts of source, destination and channel/introducing information entropy, average mutual information quantity, conditional entropy and conditional mutual information. Although this work only gives a relatively basic information entropy model, it solves the privacy protection system to quantify the problem to establish a viable system foundation. I believe the related research can continue to deepen study. At the same time, as the privacy information has attributes of space-time, subjectivity, fuzziness. The next step I will consider the use of generalized information theory, fuzzy information theory, such as the study of privacy information entropy model.

### Acknowledgments

This work is partially supported by Scientific Study Project for Institutes of Higher Learning, Ministry of
Education, Liaoning Province (LQN201720), and Natural Science Foundation of LaionGing Province, China (20170540819). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References


Biography

Hui Xia received his B. S. and M. S. degree from Xi-dian University, China, in 2003, 2006, respectively. He is currently a associate professor with Shenyang Normal University. His research interests include cloud computing, cryptography and information security.

WeiJi Yang received his B. S. degree from Zhejiang Chinese Medical University, China, in 2005, M. S. degrees from Beijing University of Posts and Telecommunications, China, in 2009. He is currently a Research Associate with ZheJiang Chinese Medical University. His research interests include Information Security and Traditional Chinese Medicine Informatics.