Dynamic Model for Anonymity Measurement Based on Information Entropy*

Jun Ye[1]†, Yong Ding[2], Xing-zhong Xiong[3], and Shu-lin Wu[1]
[1]School of Science
Sichuan University of Science & Engineering, Zigong, Sichuan, China
yejun@suse.edu.cn, wushulin_sh@163.com
[2]School of Mathematics and Computational Science
Guilin University of Electronic Technology, Guilin, Guangxi, China
stonedingy@126.com
[3]Key Laboratory of Artificial Intelligence
Sichuan University of Science & Engineering, Zigong, Sichuan, China
xzxiong@suse.edu.cn

Abstract

With the rapid development of network, anonymous communication system has been widely investigated, indicating that anonymity measurement becomes more and more important. A mathematical model for the measurement of anonymity is therefore needed. In this paper, we analyze some necessary characteristics for anonymity measurement model, and then propose a dynamic model based on information entropy, which is corresponding to the variational ability of the attackers. For the proposed model, impact factor is considered according to the effect of every node to the system. That makes our model be able to measure the system anonymity dynamically with the variation of send/receive probability of each node, the number of the nodes with the maximum send/receive probability, and the ability of attackers. Furthermore, some analyses as well as the feasibility of our model are illustrated with examples. Finally, comparisons with other models are made to show advantages of our model.

Keywords: Anonymity Measurement, Information Entropy, Impact Factor, Model

1 Introduction

As more and more applications of Internet are deployed and utilized, network security vulnerabilities are gradually coming to light. Related security techniques and security protocols are put forward, while most of them are for communication content.

Often, in the end nodes for message packet transmission, some crucial information not directly related to the content are not encrypted during the data transmission, including sending/receiving address and port information, user identity, network structure and so on. The attacker can indirectly learn communication network position, identity, and the structure of the local network by packet interception and packet traffic analyses.

In the swiftly developing cyber world today, Internet has become a common tool for communication, and people can obtain information more conveniently than ever. However, there is an increasing concern about the protection of anonymity and privacy in electronic services, and the problem of privacy invasion

Journal of Internet Services and Information Security (JISIS), volume: 4, number: 2, pp. 27-37

*The preliminary version of this work appeared in the 5-th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2013) available at `http://voyager.ce.fit.ac.jp/conf/incos/2013/`.

†Corresponding author: Tel: +86-18392190113

becomes more and more serious. Anonymity is of great importance for email and web browsing, and it is a very essential part in electronic payment [8, 18, 6], electronic voting [12, 1] as well as electronic auction [9]. To date, there are many technical solutions used to hide the identities of users in various applications and services. A model to measure the anonymity of a system is highly required.

1.1 Related Work

Research is being carried out since the past 20 years to incorporate anonymity in online transactions. There have been several attempts to quantify the degree of anonymity of a user provided by an anonymous connection system.

Reiter and Rubin [11] define the degree of anonymity as $1-p$ for the first time, where p is the probability assigned to a particular user by the attacker. In this way the anonymity of the object in the same system can be measured, but it does not work in the case of different systems. Berthold et al. [2] define the degree of anonymity as $log_2 N$, where N is the number of users in the system. The anonymity cannot be measured when the probability of every object is different. Models for anonymity measurement are proposed in order to measure the degree of anonymity in [10, 3, 4, 14, 15, 16, 7, 13]. Anonymity [17] is an important indicator to measure the security of a system. Many researchers do plenty of works on it, and have proposed some models for anonymity measurement based on information entropy, such as models in [3, 4, 14]. Besides, the ratio of the entropy under attack with the maximum entropy of system is used to measure the anonymity. In these models, every node in the system is treated as the same, while on the contrary these models do not accord well with the real-life ones since their send/receive probabilities are not totally the same. It is indicated in [5] that these models cannot accurately describe the anonymity of the system at the attackers position. Another kind of models based on conditional entropy are proposed in [10] and [7], but the anonymity of the systems with different number of members can not be compared. Then an optimal scheme is proposed in [15] and a joint-entropy-based anonymity metrics model with multi-property is given in [16] to improve it. The anonymity of a multi-attribute system can be measured with the anonymity factors in these models, but they cannot describe the anonymity of the system accurately, with the subjective anonymity factors as given by experts.

1.2 Our Contributions

Through the study of anonymous system and anonymity measurement model, some necessary characteristics for anonymity measurement model are analyzed. A dynamic objective model for anonymity measurement based on information entropy is proposed in this paper. This model can measure the system anonymity according to the different attack capabilities of different adversaries.

The organization of this paper is as follows. Models in [3, 4, 14] and [5] are analyzed in Section 2. In Section 3 some indispensable features for anonymity measurement model are generalized at the attacker's position, and a dynamic model based on information entropy is put forth. The anonymity measurement is more accurate in this model with the objective anonymous factors of different nodes, which are assigned in terms of the degree of anonymity and the ability of attackers. In Section 4 some properties mentioned in section 2 are analyzed in our model. The feasibility of our model is illustrated by some examples in Section 5. At last, some comparisons among the models in [3, 4, 14, 16] and [5] are made to show advantages of our model in Section 6.

2 Analysis of the Models in [3, 4, 14] and [5]

Firstly, we consider the systems with 10 nodes in the models presented in [3] and [4]. The send/receive probability of each node is as in Table 1 for system S_1 and system S_2. From the probabilities, it can

Table 1: Send/Receive Probability Distribution of System S_1 and S_2

System	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7	Node 8	Node 9	Node 10
S_1	0.2	0.2	0.2	0.2	0.05	0.05	0.05	0.05	0	0
S_2	0.2	0.2	0.2	0.1	0.1	0.1	0.1	0	0	0

Table 2: Send/Receive Probability Distribution of System S_3 and S_4

System	Node 1	Node 2	Node 3	Node 4	Node 5	Node 6	Node 7	Node 8	Node 9	Node 10
S_3	0.15	0.15	0.15	0.15	0.15	0.125	0.125	0	0	0
S_4	0.15	0.15	0.15	0.15	$\frac{0.4}{3}$	$\frac{0.4}{3}$	$\frac{0.4}{3}$	0	0	0

be predicted that the anonymity of the two systems is not equal. However, we get the same anonymity $d_1 = d_2 = 0.819382$ from the models in [3] and [4].

Another example with the send/receive probability of each node in system S_3 and S_4 is given as in Table 2. It can be directly concluded that the anonymity of system S_3 is better than that of system S_4. Unfortunately, using the models in [3] and [4], we get $d_3 = 843704 < d_4 = 0.84437$. That is to say, the anonymity of system S_3 is better than that of the system S_4. It is not accordance with real-life instance.

Secondly, we consider the model in [14], with the systems S_5 and S_6 including 100 nodes. The send/receive probability of each node in system S_5 and S_6 are $\{0.2, \frac{0.8}{99}, \frac{0.8}{99}, \dots, \frac{0.8}{99}\}$ and $\{0.2, 0.2, \frac{0.6}{98}, \frac{0.6}{98}, \dots, \frac{0.6}{98}\}$ respectively. It can be inferred that the anonymity of systems S_5 and S_6 are the same values $d_5 = d_6 = 0.2$ computing form the model in [14]. But the anonymity of the two systems is not equal obviously.

The reason for these collisions is the impact of each node on the anonymity of the system being treated as equal in the models in [3, 4, 14]. In fact, at attacker's position, the influence is different for nodes with different send/receive probabilities. Model in [5] is an improved model of the model proposed in [14], but the difference for the send/receive probability of each node is not considered either. However, attacker can easily identify different nodes with different probabilities. So each node should be given a corresponding impact factor.

3 Model for Anonymity Measurement

3.1 Preliminaries

According to the analysis in section 2, there are some shortcomings when only information entropy is used to measure the anonymity of the system. In our view, a model for anonymity measurement should at least satisfy the following basic properties:

1. If the send/receive probability of one node is more, lower is the anonymity of the system. If the probability of a node to be identified is more, then the attacker can easily locate the actual node which transmits/ receives messages

2. If more nodes have the same send/ receive probability, it is very difficult for the attacker to find out the real node.

3. The anonymity of the system should be varied according to the ability of the attackers.

There are some definitions which will be used in our model.

Definition 3.1 ε-Indistinguishable Boundary

The probability p in an interval around of a probability p^* is indistinguishable, that is, there exists $\varepsilon > 0$, such that every probability p which satisfies $|p - p^*| < \varepsilon$ is treated as p^*. Here ε is called ε-indistinguishable boundary.

Definition 3.2 Indistinguishable Probability and Indistinguishable Probability Set

p is called an indistinguishable probability with respect to p^* under ε-indistinguishable boundary, if the probability p in the set $\Phi(p) = \{p||p - p^*| < \varepsilon\}$ is treated as p^*. Here the set $\Phi(p)$ is called indistinguishable probability set.

3.2 Our Model

There exist some nodes with an indistinguishable probability p. These corresponding nodes of indistinguishable probability are called indistinguishable nodes and forms an indistinguishable probability set $\Phi(p)$. We use $\varphi(p)$ to denote the number of nodes in the set $\Phi(p)$, and let

$$\overline{p} = \frac{1}{\varphi(p)} \sum_{i=1}^{\varphi(p)} p_i$$

be the value of indistinguishable probability $(p_i \in \Phi(p), i = 1, 2, \ldots, \varphi(p))$.

Usually attacker may regard the nodes of high send/receive probability as the suspects of real send/receive nodes. Suppose there are N nodes in the system, after monitoring the system, attacker gets the send/receive probability of each node $p_1, p_2, \ldots, p_N$. Here we suppose $p_1 > p_2 > \cdots > p_N$. Typically, an attacker usually thinks the real node in the $\varphi(\overline{p}_1)$ corresponding nodes of $\Phi(\overline{p}_1)$ with respect to the indistinguishable probability. And the more nodes in $\Phi(\overline{p}_1)$, the better anonymity of the system, for the more difficulties of attacker to find out the real node from these nodes. We use $\frac{\varphi(\overline{p}_1)}{N}$ to denote the factor of these indistinguishable probabilities about the system anonymity.

We get the following model with information entropy,

$$\begin{aligned} d &= \frac{\varphi(\overline{p}_1)}{N} \frac{-\sum_{i=1}^{m} \varphi(\overline{p}_i)\overline{p}_i \log_2 \overline{p}_i}{\log_2 N} \\ &= -\frac{\varphi(\overline{p}_1)}{N} \frac{\sum_{i=1}^{m} \varphi(\overline{p}_i)\overline{p}_i \log_2 \overline{p}_i}{\log_2 N} \end{aligned}$$

Here $\sum_{i=1}^{m} \varphi(\overline{p}_i)\overline{p}_i = 1$ (m denotes the number of groups about the indistinguishable probability of N nodes), and these indistinguishable probability sets are disjoint.

4 Analysis and Application of Our Model

4.1 Analysis of properties

From the model we get $0 \leq d \leq 1$, the greater of d the better anonymity of the system. And the anonymity of the system gets to maximum $d_{max} = 1$, if and only if the send/receive probability $p_i = \frac{1}{N}$. And the anonymity of the system gets to minimum $d = 0$, when the send/receive probability of some node gets to 1 ($p = 1$).

Property 4.1. The anonymity of system d decreases by the increasing of the indistinguishable probability $\overline{p}_1$, for the fixed N and $\varphi(\overline{p}_1)$.

Proof.

$$d = -\frac{\varphi(\overline{p}_1)}{N}\frac{\sum_{i=1}^{m}\varphi(\overline{p}_i)\overline{p}_i\log_2\overline{p}_i}{\log_2 N}$$

$$= -\frac{\varphi(\overline{p}_1)}{N}\frac{\varphi(\overline{p}_1)\log_2\overline{p}_1 + \cdots + \varphi(\overline{p}_m)\log_2\overline{p}_m}{\log_2 N}$$

Here

$$\overline{p}_m = \frac{[1-\varphi(\overline{p}_1)\overline{p}_1 - \cdots - \varphi(\overline{p}_{m-1})\overline{p}_{m-1}]}{\varphi(\overline{p}_m)}$$

$$\triangleq \frac{1-a-\varphi(\overline{p}_1)\overline{p}_1}{\varphi(\overline{p}_m)}$$

$$\varphi(\overline{p}_m) = 1-\varphi(\overline{p}_1) - \cdots - \varphi(\overline{p}_{m-1}) \triangleq n-b-\varphi(\overline{p}_1)$$

So

$$\frac{\partial d}{\partial \overline{p}_1} = \frac{\varphi^2(\overline{p}_1)(\ln\overline{p}_1) - \ln\frac{1-a-\varphi(\overline{p}_1)\overline{p}_1}{n-b-\varphi(\overline{p}_1)}}{N\ln N}$$

For $\overline{p}_1$ is the maximum indistinguishable probability, so

$$\overline{p}_1 > \frac{1-a-\varphi(\overline{p}_1)\overline{p}_1}{n-b-\varphi(\overline{p}_1)},$$

that is

$$\ln\overline{p}_1 > \ln\frac{1-a-\varphi(\overline{p}_1)\overline{p}_1}{n-b-\varphi(\overline{p}_1)}.$$

So

$$\frac{\partial d}{\partial \overline{p}_1} < 0.$$

Hence d decreases due to increase in $\overline{p}_1$.

Note. For the fixed $\varphi(\overline{p}_1)$, the greater of $\overline{p}_1$, the smaller of other probabilities and the greater identified probability of the attacker, and then the less anonymity of the system.

Property 4.2. The anonymity of system d increases by the increasing of $\varphi(\overline{p}_1)$, for the fixed N and each sum of the indistinguishable probabilities $\varphi(\overline{p}_i)\overline{p}_i(i = 1,2,\ldots,m)$.

Proof. Let $q_i = \varphi(\overline{p}_i)\overline{p}_i, i = 1,2,\ldots,m$, therefore q_i is fixed. So

$$d = -\frac{\varphi(\overline{p}_1)}{N}\frac{q_1\ln\frac{q_1}{\varphi(\overline{p}_1)} + \cdots + \frac{q_m}{\varphi(\overline{p}_m)}}{\ln N}$$

$$= -\frac{\varphi(\overline{p}_1)}{N}\frac{q_1\ln\frac{q_1}{\varphi(\overline{p}_1)} + \cdots + \frac{(1-a)}{\varphi(\overline{p}_m)}}{\ln N}$$

Here

$$q_m = 1-q_1-\cdots-q_{m-1} \triangleq 1-u$$

$$\varphi(\overline{p}_m) = 1-\varphi(\overline{p}_1) - \cdots - \varphi(\overline{p}_{m-1}) \triangleq n-b-\varphi(\overline{p}_1)$$

Hence

$$\frac{\partial d}{\partial \varphi(\overline{p}_1)} = \frac{-\varphi(\overline{p}_1)}{N \ln N}[q_1 \ln \frac{q_1}{\varphi(\overline{p}_1)} + \cdots + q_m \ln \frac{q_m}{\varphi(\overline{p}_m)} + (\frac{q_m}{\varphi(\overline{p}_m)} - \frac{q_1}{\varphi(\overline{p}_1)})]$$

For

$$\frac{q_m}{\varphi(\overline{p}_m)} = \overline{p}_m, \frac{q_1}{\varphi(\overline{p}_1)} = \overline{p}_1, \overline{p}_1 > \overline{p}_m,$$

so

$$\frac{q_m}{\varphi(\overline{p}_m)} < \frac{q_1}{\varphi(\overline{p}_1)},$$

then

$$\frac{\partial d}{\partial \varphi(\overline{p}_1)} > 0.$$

So d increases due to increase $\varphi(\overline{p}_1)$.

Note. More the nodes with maximum indistinguishable probability, better is the anonymity of the system, and it becomes more difficult for the attacker to find out the real node from these nodes.

4.2 Applicability of Our Model

Now we consider two groups of nodes. The first group, there are $\varphi(\overline{p}_1)$ nodes in it, and the send/receive probability of each node is p_1, the sum probability is $\varphi(\overline{p}_1)p_1 = p$. The second group, there are $N - \varphi(\overline{p}_1)$ nodes in it, and the send/receive probability of each node is p_2, the sum probability is $1 - p$. Here we suppose $p_1 > p_2$.

In this case, when $p_1 = \frac{p}{\varphi(\overline{p}_1)}$ and $p_2 = \frac{1-p}{N-\varphi(\overline{p}_1)}$ is considered as indistinguishable probabilities by the attacker, that means the probability of each node is in the interval $[\frac{1}{N} - \varepsilon, \frac{1}{N} + \varepsilon]$, and the measurement of anonymity about this system is 1. But when an attacker can distinguish p_1 from p_2, the anonymity of the system is declining rapidly. For $p_1 > p_2$ an attacker realizes the real node is in the $\varphi(\overline{p}_1)$ nodes of the largest probability p_1. And the attack range is reduced from N nodes to $\varphi(\overline{p}_1)$ nodes. In our model, when the attacker can distinguish p_1 and p_2, the anonymity of system is declining from 1 to $\frac{\varphi(\overline{p}_1)}{N}$ rapidly. So the anonymity measurement in our model corresponds to the changes of real anonymity system.

4.3 Examples

In this section two examples are given to show the feasibility of our model.

I. Indistinguishable boundary $\varepsilon = 0$.

Case 1. There are 2 nodes in the system. An attacker gets the send/receive probability of node 1 as p_1, and $p_2 = 1 - p_1$ for node 2. So the anonymity measurement is

$$d = \frac{\varphi(\overline{p}_1)}{N} \frac{-\sum_{i=1}^{2} \varphi(\overline{p}_i)\overline{p}_i \log_2 \overline{p}_i}{\log_2 N}$$

When $p_1 = \frac{1}{2}$ then $d = 1$, this is the highest anonymity of the system.

When $p_1 > \frac{1}{2}, \varphi(p_1) = \varphi(p_2)$, then $d = -\frac{1}{2}[p_1 \log_2 p_1 + (1 - p_1)\log_2(1 - p_1)]$. In this case, the changes of anonymity are illustrated in Figure 1. The anonymity of system d decreases with the increment of p_1.

From Figure 1, we know if we make p_1 close to 0.5, the anonymity of system is improved. As every probability is distinguished for the attacker, the highest anonymity of the system is 0.5, when $p_1 > \frac{1}{2}$.

Case 2. There are 10 nodes in the system. An attacker gets the send/receive probability of 3 nodes as $p_i = \frac{p}{3}, i = 1,2,3$, and $p_j = \frac{1-p}{7}, 4 \leq j \leq 10$ for other nodes.

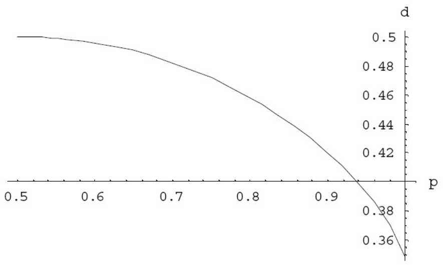

Figure 1: Anonymity degree variation of tow nodes

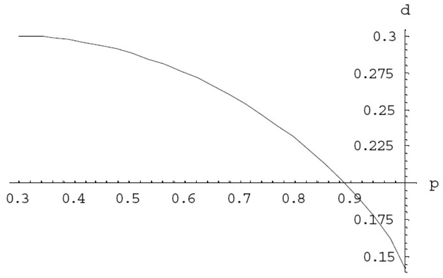

Figure 2: Anonymity degree variation when $p > 0.3$

When $\frac{p}{3} = \frac{1-p}{7}$, that is $p = 0.3$, then the send/receive probability of each node is the same. In this case, $d = 1$.

When $\frac{p}{3} \neq \frac{1-p}{7}$,

1. $\frac{p}{3} > \frac{1-p}{7}$.

   That is $p > 0.3$, then $\varphi(\overline{p}_1) = 3, \varphi(\overline{p}_2) = 7$, the anonymity of system is

$$d = -\frac{3}{10}\frac{p\log_2(\frac{p}{3} + (1-p)\log_2\frac{1-p}{7})}{\log_2 10}$$

   In this case, the changes of anonymity are illustrated in Figure 2.

2. $\frac{p}{3} < \frac{1-p}{7}$.

   That is $1-p > 0.7$, then $\varphi(\overline{p}_1) = 7, \varphi(\overline{p}_2) = 3$, the anonymity of system is

$$d = -\frac{7}{10}\frac{p\log_2(\frac{p}{3} + (1-p)\log_2\frac{1-p}{7})}{\log_2 10}$$

   In this case, the changes of anonymity are illustrated in Figure 3.

From Figure 2 and Figure 3, we get better anonymity when $1-p > 0.7$ than the condition of $p > 0.3$. For there are 3 according nodes of the greatest send/receive probability when $p > 0.3$, it is a great probability event for an attacker to identify the real node. But there are 7 nodes with the greatest send/receive probability when $1-p > 0.7$, and it is a low probability event for an attacker to identify the real node. So the maximum value of anonymity is close to 0.7.

II. Indistinguishable boundary $\varepsilon = 0.05$.

The probabilities of 10 nodes in two different systems are illustrated in Table 3.

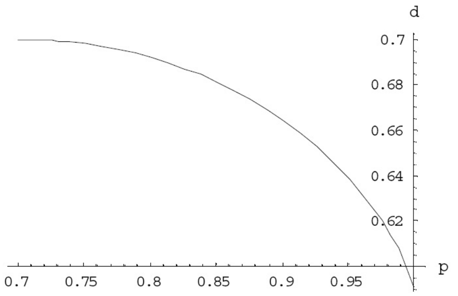

Figure 3: Anonymity degree variation when $1-p>0.7$

Table 3: Send/Receive Probability Distribution of System S_7 and S_8

System	Node 1	Node 2	Node 3	Node 4	Node 5
S_7	0.18	0.18	0.18	0.16	0.16
S_8	0.12	0.12	0.12	0.11	0.11
System	Node 6	Node 7	Node 8	Node 9	Node 10
S_7	0.07	0.07	0	0	0
S_8	0.11	0.1	0.1	0.1	0.01

For system 7 and Table 3 we know $p_1 = 0.18$,

$$\Phi(p_1) = \{p||p-0.18| < 0.05\} = \{0.18, 0.16\}.$$

$\overline{p}_1 = 0.172$, $\varphi(\overline{p}_1) = 5$, $\overline{p}_2 = 0.07$, $\varphi(\overline{p}_2) = 2$, $\overline{p}_2 = 0$, $\varphi(\overline{p}_2) = 3$.

So the anonymity of system 7 is

$$d_7 = -\frac{5}{10}\frac{0.86\log_2 0.172 + 0.14\log_2 0.07}{\log_2 10} = 0.41.$$

And for system 8, $p'_1 = 0.12$,

$$\Phi(p'_1) = \{p||p-0.12| < 0.05\} = \{0.12, 0.11, 0.1\}.$$

$\overline{p}'_1 = 0.11$, $\varphi(\overline{p}'_1) = 9$, $\overline{p}'_2 = 0.01$, $\varphi(\overline{p}'_2) = 1$.

So the anonymity of system 8 is

$$d_8 = -\frac{9}{10}\frac{0.99\log_2 0.11 + 0.01\log_2 0.01}{\log_2 10} = 0.87.$$

In this case, the anonymity of system 8 is better than that of system 7.

5 Comparisons of Models

5.1 Comparisons with models in [3, 4, 14] and [5]

The impact of the different send/recieive probabilities of the nodes on the anonymity of system is not considered in the models proposed in [3, 4, 14] and [5]. So the anonymity of some systems is not accurately measured by these models.

We consider the systems S_1 to S_6 mentioned in section 2; obviously we know that the anonymity of S_1 and S_2 is $d_1 \neq d_2$, and the anonymity of S_3 and S_4 is $d_3 > d_4$. But we get $d_1 = d_2 = 0.819382$ for system S_1 and S_2 from the models in [3, 4], and $d_3 = 0.843704$, $d_4 = 0.84437$ for system S_3 and S_4. And measured by our model, $d_1 = 0.327753$, $d_2 = 0.245815$, $d_3 = 0.421852$, $d_4 = 0.337748$.

From systems S_5 and S_6, obviously we can get the anonymity of the tow system is not equal, but we get $d_5 = d_6 = 0.2$ from the model in [14]. And measured by our model, $d_5 = 0.0091$, $d_6 = 0.0162$. From this we know, there is no similar error to the results of our models. And our model is much better than which presented in [3, 4, 14].

The model proposed in [5] is the improvement of the model proposed in [14], and the impact of the probability of each node is not considered yet. So our model is more complete.

5.2 Comparisons with Models in [16]

The anonymity factors in the model proposed in [16] are given by experts. There are two problems to this. On one hand the model cannot get the result of anonymity measurement if there is no expert to give the anonymity factors, and on the other hand, there are some subjective judgments for anonymity factors given by experts. There is some influence of human factors to the results of model.

The effects of each node on the anonymity of system is considered at the attacker's position in our model, and the anonymity factors is defined by the send/receive probability of each node. Thus there is no subjective effect in our model.

6 Conclusion

Nowadays large amounts of data are transmitted via networks. Many schemes on anonymity were presented in order to protect the identifiable information of senders and receivers. Anonymity can shield the privacy of users, and prevent the attackers from obtaining information about users. To evaluate the security of a system, the measurement and comparison of anonymity system are very critical. Motivated by this, our paper presents a dynamic model for anonymity measurement based on information entropy. The anonymity of system can be measured dynamically in light of the variations of the send/receive probability of each node and the ability of attacker. And the anonymity factors are objectively given according to the influence of each node on the system anonymity. The computation is simple and convenient in our model, and the model can be widely used for anonymity measurement and anonymity comparison among different systems.

Acknowledgement

The work described in this paper is supported by the Science Founding of Artificial Intelligence Key Laboratory of Sichuan Province (2014RYJ06); The scientific research fund project of Sichuan University of Science & Engineering (2013KY02); NSFC (No.11301362); The 2012 Open Fund of State Key Laboratory of Integrated Service Networks; 2012 Open Foundation of Key Laboratory of Guangxi wireless broadband communications and signal processing; National Natural Science Foundation of China (No. 60963024); National High Technology Research and Development Program (2012AA011705); Project of Innovative Research Team in University of Sichuan (NO.13TD0017); Science Founding of Artificial Intelligence of key laboratory of Sichuan Province (No. 2012RYJ05); The high-quality goods resource sharing courses ”mathematical modeling” of Sichuan province (2012-57); Science Founding of Science School of Sichuan university of science & engineering(10LXYB05); ”mathematical modeling teaching group” of Sichuan University of Science & Engineering (2009-142-01).

References

[1] A. Al-Shammari, A. Villafiorita, and K. Weldemariam. Towards an open standard vote verification framework in electronic voting systems. In *Proc. of the 7th International Conference on Availability, Reliability and Security (ARES'12), Prague, TBD, Czech Republic*, pages 437–444. Springer-Verlag, August 2012.

[2] O. Berthold, A. Pfiztmann, and R. Standtke. The disavantages of free mix routes and how to overcome them. In *Proc. of International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability, Berkeley, California, USA, LNCS*, volume 2009, pages 30–45. Springer-Verlag, July 2001.

[3] C. Diaz, J. Claessens, and S. Seys. Entropy based method for measuring anonymity. In *Proc. of the 23rd Symposium on Information Theory, Louvain la Neuve, Belgium*, pages 1–8. IEEE, October 2002.

[4] C. Diaz, J. Claessens, S. Seys, and B. Preneel. Towards measuring anonymity. In *Proc. of the 2nd International Workshop on Privacy Enhancing Technologies (PET'02), San Francisco, California, USA, LNCS*, volume 2482, pages 54–68. Springer-Verlag, April 2002.

[5] G. Duan, W. Wang, and J. Wang. A new anonymity measure based on partial entropy. In *Proc. of the 2008 IEEE International Conference on Communications (ICC'08), Beijing, China*, pages 1484–1488. IEEE, May 2008.

[6] A. Dwivedi, A. Dwivedi, S. Kumar, S. Pandey, and P. Dabra. A Cryptographic Algorithm Analysis for Security Threats of Semantic E-Commerce Web (SECW) for Electronic Payment Transaction System. In *Proc. of the 2nd International Conference on Advances in Computing and Information Technology (ACITY'12), Chennai, India, LNCS*, volume 178, pages 367–379. Springer-Verlag, 2012.

[7] Y. Guan, X. Fu, R. Bettati, and W. Zhao. An optimal strategy for anonymous communication protocols. In *Proc. of the 22nd IEEE International Conference on Distributed Computing Systems (ICDCS'02), Vienna, Austria*, pages 257–266. IEEE, July 2002.

[8] C. Kim, T. Wang, N. Shin, and K. Kim. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, 9(1):84–95, February 2010.

[9] M. Li, J. S. Juan, and J. H. Tsai. Practical electronic auction scheme with strong anonymity and bidding privacy. *Information Sciences*, 181(12):2567–2586, June 2011.

[10] S. Micali, M. Rabin, and S. Vadhan. Verifiable random functions. In *Proc. of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS'99), New York, NY, USA*, pages 120–130. IEEE, 1999.

[11] M. K. Reiter and A. D. Rubin. Anonymity for web transactions with crowds. *Communications of the ACM*, 42(2):32–48, February 1999.

[12] L. Rura, B. Issac, and M. Haldar. Analysis of image steganography techniques in secure online voting. In *Proc. of the 2011 International Conference on Computer Science and Network Technology (ICCSNT'11), Harbin, China, LNCS*, volume 178, pages 120–124. Springer-Verlag, December 2011.

[13] C. Shields and B. Levine. A protocol for anonymous communication over the internet. In *Proc. of the 7th ACM conference on Computer and Communications Security (CCS'00), Athens, Greece*, pages 33–42. ACM, November 2000.

[14] G. Toth, Z. Hornak, and F. Vajda. Measuring anonymity revisited. In *Proc. of the 9th Nordic Workshop on Secure IT Systems (Nordsec'04), Helsinki University of Technology, Finland*, pages 85–90, November 2004.

[15] Z. Wu and J. Ma. A joint-entropy-based anonymity metrics model with multi-property. In *Proc. of Chinacrypt 2004, Beijing, China*, pages 390–397. Science Press, 2004.

[16] Z. Wu and J. Ma. A joint-entropy-based anonymity metrics model with multi-property. *Journal of Computer Research and Development*, 43:1240–1245, 2006.

[17] K. Xie, L. Deng, and R. Li. Measuring anonymity in P2P anonymous communication system. 28(12):3190–3190, 2008.

[18] Y. Yen, T. Wu, N. Lo, and K. Tsai-KSII. A fair-exchange e-payment protocol for digital products with customer unlinkability. *KSII Transactions on Internet and Information Systems (TIIS)*, 6(11):2956–2979, 2011.

Author Biography

Jun Ye received the MS degree in Cryptography at the Guilin University of Electronic Technology in 2011. He is a lecturer at Sichuan University of Science and Technology. He is a doctoral candidate at the Xidian University. His research interests include cryptography and information security.

Yong Ding received the Ph.D. degree in telecommunication engineering at the Xidian University. He is currently a professor in the Guilin University of Electronic Technology, and his research interests include cryptography and information security.

Xing-zhong Xiong received the B.E. degree in electronic engineering from the Sichuan University of Science & Engineering (SUSE), Sichuan, China, in 1996, the M.E. degree in signal and information processing from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2006, and the Ph.D. degree in communication and information system from UESTC, in 2009. He is currently a professor in the SUSE. His research interests include signal and information processing and multiple access techniques in communication systems.

Shu-lin Wu received the Ph.D. degree in computational mathematics at the Huazhong University of Science and Technology in 2010. He is an associate professor at Sichuan University of Science and Technology. His research interests include cryptography and information security.