International Journal of Database Theory and Application
Vol.9, No.7 (2016), pp.215-232
http://dx.doi.org/10.14257/ijdta.2016.9.7.19

BIG – MIX: A Mapping-Based Approach towards Measuring Anonymity

Tianbo Lu[1], Cheng Wang[1], Xiaofeng Du[2] and Yang Li[1]

[1]*School of Software Engineering, Beijing University of Posts and Telecommunications, 100876, Beijing, China*
[2]*School of Computer Science, Beijing University of Posts and Telecommunications, 100876, Beijing, China*
lutb@bupt.edu.cn, ChWang_bupt@163.com

Abstract

As the Internet is becoming a virtual platform for people's sharing information and communicating daily, more and more people are connected together and the contact area between their personal privacy and the outside world turn to be unprecedented large. Therefore, the users of the Internet are faced with an enormous privacy threat. Anonymous P2P technology is a good way to solve the above problems. The ultimate goal of all anonymous P2P systems is to obtain the anonymity. Anonymity assessment on different anonymous P2P systems can be used to compare the amount of anonymity offered by different systems or to adjust the parameter setting of the same system according to different need, which is of great guiding significance to improve anonymous communication systems. In this paper, from the angle of relationship anonymity between the sender and the receiver, we presents the BIG-MIX anonymity method, taking the paths cross of different messages into consideration, to make anonymity assessment on anonymous P2P networks with the use of mapping. And with this method, this paper makes a quantitative analysis on the relationship anonymity of anonymous P2P networks under the mechanism of Threshold Mixes, Timed Mixes or Pool Mixes.

Keywords*: Anonymous P2P networks, Mapping, BIG-MIX, Anonymity assessment*

1. Introduction

It is ever since David Chaum [1] propose the concept of mix and the idea that allows messages to be sent or received anonymously, more and more anonymous communication systems appear, many papers have been dedicated to the design and evaluation of anonymous communication systems.

According to Pfitzmann and Waidner [2], anonymous communication systems includes three types of anonymities: sender anonymity, recipient anonymity, and unlinkability of sender and receiver. Sender anonymity means that the identity of the information sender is hidden, and recipient anonymity means that the identity of the information receiver is hidden. Unlinkability of sender and recipient refers to the property that the sender and recipient of a communication cannot be identified even if the sender and receiver are known to be of communicating with someone. From previous anonymity assessment researches we know that compared with sender anonymity and receiver anonymity, unlinkability of sender and recipient is rarely concerned.

In terms of unlinkability of sender and recipient, Matthew Edman [3] first propose a new system-wide metric, based on the permanent of a matrix, which measures the amount of additional information needed to reveal the whole communication pattern between senders and recipients in the system, there exists a one-to-one relation between inputs to and outputs from the anonymity system .We stress that our approach is not intended to replace the existing entropy-based metrics. But when the attacker has the ability to track

ISSN: 2005-4270 IJDTA

message, this method is no longer applicable. At this time, parameter setting within the system effect the anonymity must be considered. What's more, they apply the method to threshold mixes, timed mixes and pool mixes and make a comparison of the anonymity performance of these three mechanisms. However, they assume the attacker only observe one Mix's initial input message, and all input messages along the same path (Mixes) output system, it means each round just have one Mix, this assumption couldn't reaction the actual situation between path cross in a real system.

In this paper, based-on the method of Matthew Edman, we will propose BIG-MIX method. This method allows a round between multiple Mixs and Mix can participate in any cross pass messages, the initial input message can be multiple paths output system. Because this method put the multiple Mixs round as confused more input and output messages, so named it as BIG-MIX. The method taking the paths cross of different messages into consideration, to make anonymity assessment on anonymous P2P networks with the use of mapping. And all messages are no longer limited to a single path through anonymous communication systems, taking into account the system path between different messages the cross-cutting issues.

2. Related Work

The mainly studied of anonymous communications technology is how to make the identity of the sender or the identity of the recipient or the corresponding relationship between sender and recipient to get hidden in the process of communication. Its research originated the notion of mix proposed by David Chaum [1] in 1981.

Many people have been being focusing on the quantitative metrics research with the use of much knowledge of different fields.

In the aspect of set theory, in 1988, Chaum introduced the concept of an anonymity set in his DC-networks [4], The anonymity set is used to hide the real sender or recipient. In this opinion, as the size of anonymity set increases, so does the degree of anonymity. With the concept of anonymity set, Kesdogan, Egner and Buschkes [5] evaluated their design of Stop-and-Go MIXes. Reiter and Rubin [6] define the anonymity as the probability $1 - \mathrm{p}$, where p is the probability of the user being the original sender. In 2001, Berthold [7] defines the degree of anonymity as $\mathrm{A} = \log_2 N$, where N is the number of all possible senders of a message in an anonymous system. In 2002, Claudia Diaz *et al* [8-9] define the degree of anonymity d as:

$$d = \frac{S}{S_{max}} \qquad (2-1)$$

Where S is as above and S_{MAX} is the maximum entropy of the system. And Serjantov *et al*. [10] define a concept of effective anonymity set.

In the aspect of Information Theory, In the middle of 19th century, Claude E. Shannon[11] [12] created a new science called information theory. Serjantov[10] also defines the entropy of an anonymous system as:

$$\mathrm{S} = -\sum_{u-1}^{n} p_u \log_2(p_u) \qquad (2-2)$$

Where n is the number of users of the system and p_u is the probability that a user u acts as a role $r \in \{sender, recipient\}$ for a particular message.

In the aspect of Combinatorial Mathematics,in 2007, Matthew Edman *et al* [3] reference to Claudia Diaz's *et al* [8] [9] normalization method define the anonymity of the system, And he first propose a combinatorial approach to measure anonymity as follows:

$$\mathrm{d} = \begin{cases} 0 & n = 1 \\ \dfrac{\log(perA)}{\log(n!)} & n > 1 \end{cases} \qquad (2-3)$$

In 2008, Benedikt Gierlichs *et al* [13] think Matthew's approach fails to capture the anonymity loss caused by subjects sending or receiving more than one message. Based on this method they propose an idea which can be applied to cases where subjects send and receive an arbitrary number of messages. In addition, Jean-Charles Gregoire[14] and Rajiv Bagai [15] are also to improve Matthew Edman's method , considering the anonymity in the condition of the communication subject to send or receive multiple messages and system in the infeasibility of attacks.

3. BIG-MIX Anonymity Method

3.1. The BIG - MIX System Model

An anonymous P2P communication system is a peer-to-peer distributed application in which the nodes or participants are anonymous or pseudonymous. The participants of anonymous system is usually achieved by special routing overlay networks that hide the physical location of each node from other participants. Member of this system can be anonymous service users, also can be anonymous service providers.

Figure3-1 is used to describe the BIG-MIX system model of anonymous P2P networks, the body of this model is the peer to peer network consisting of Mix nodes. While the initial sender and the ultimate recipient can be a member of anonymous P2P network, also can be a node outside of anonymous P2P network, the only assumption on sender and recipient is that they can only send or receive one message.

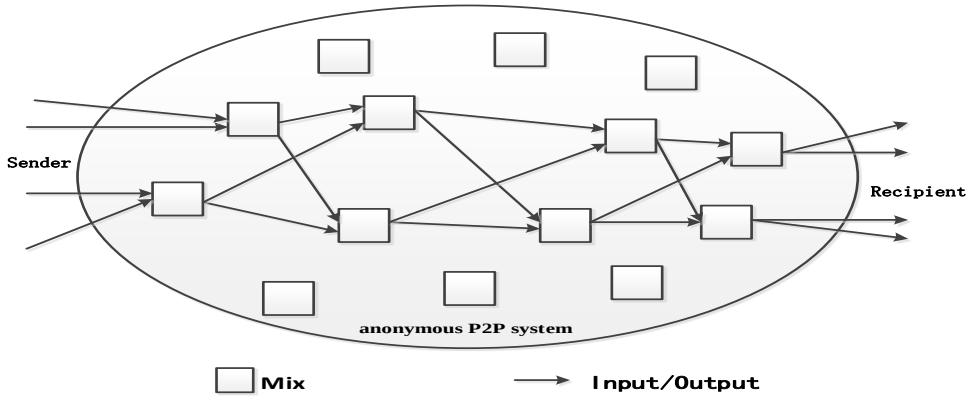

Figure 3-1. The BIG-MIX System Model

Threshold Mixes, Timed Mixes, Pool Mixes are three kinds of output mechanism of Mix. In this paper, we will assess the anonymity when change parameters of these three mechanisms, the assessment of none obfuscation capabilities such as encryption, decryption and resource discovery are not involved. We suppose that under the same conditions these abilities are the same.

3.2. The BIG-MIX Attack Model

Figure 3-2 is a BIG-MIX attack model, the assumptions of attacker's are as follows: An attacker can observe some messages entering and exiting the anonymous P2P network, here called "incoming" and "outgoing" refers to an attacker can find some entity of the initial message sender or the ultimate recipient, can determine which message is sent by the initial sender to enter the networks, which message is to leave network to reach the final recipient.

We also assume that every message the attacker is able to see entering the anonymous P2P network will be among the message he is able to see leaving the system, and vice versa. It means that there exists a one-to-one mapping between inputs and outputs from

the anonymity system. Meanwhile, all input messages through the same number of Mix, the confused times of each message is the same, regard all nodes in each Mix round as a BIG-MIX, attacker can put BIG-MIX as units of the global message tracking.

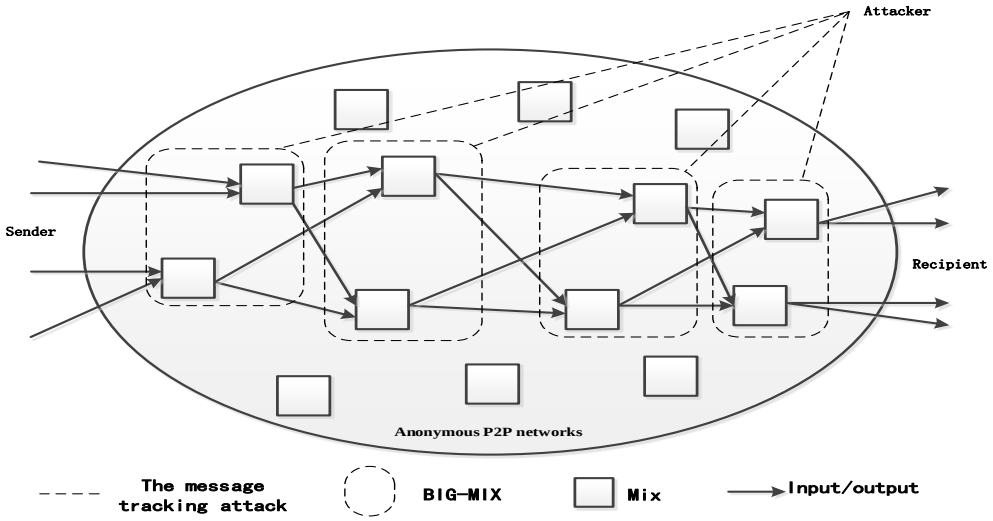

Figure 3-2. The BIG-MIX Attack Model

3.3. The BIG-MIX Evaluation Process

In this paper, we consider the anonymity of sender and recipient. Since the sender only sends one message, and the recipient only receives one message too, there exists a one-to-one mapping between inputs and outputs from the anonymity system. Due to the sender and the input message, the recipient and the output message are one-to-one mapping, after a successful message tracking attack by an attacker, some input-output pairings can be found, that is find the correct sender- recipient pairs, decreasing the level of anonymity of the system. Figure 3-3 is the BIG-MIX flow chart for assessing anonymity between sender and recipient.

The following we will describes this process. Let the inputs of anonymous P2P network be denoted by the set $S_1 = \{s_i\}, i = 1, \ldots n$ and the outputs by $R_1 = \{r_j\}, j = 1, \ldots n$. Assuming that the final output message needs to go through r times round. Figure 3-4 presents an example with four senders and four recipients in anonymous P2P network, each message sent by sender Transmitted to the recipient after 3 Mix nodes, that is $\mathrm{r} = 3$.

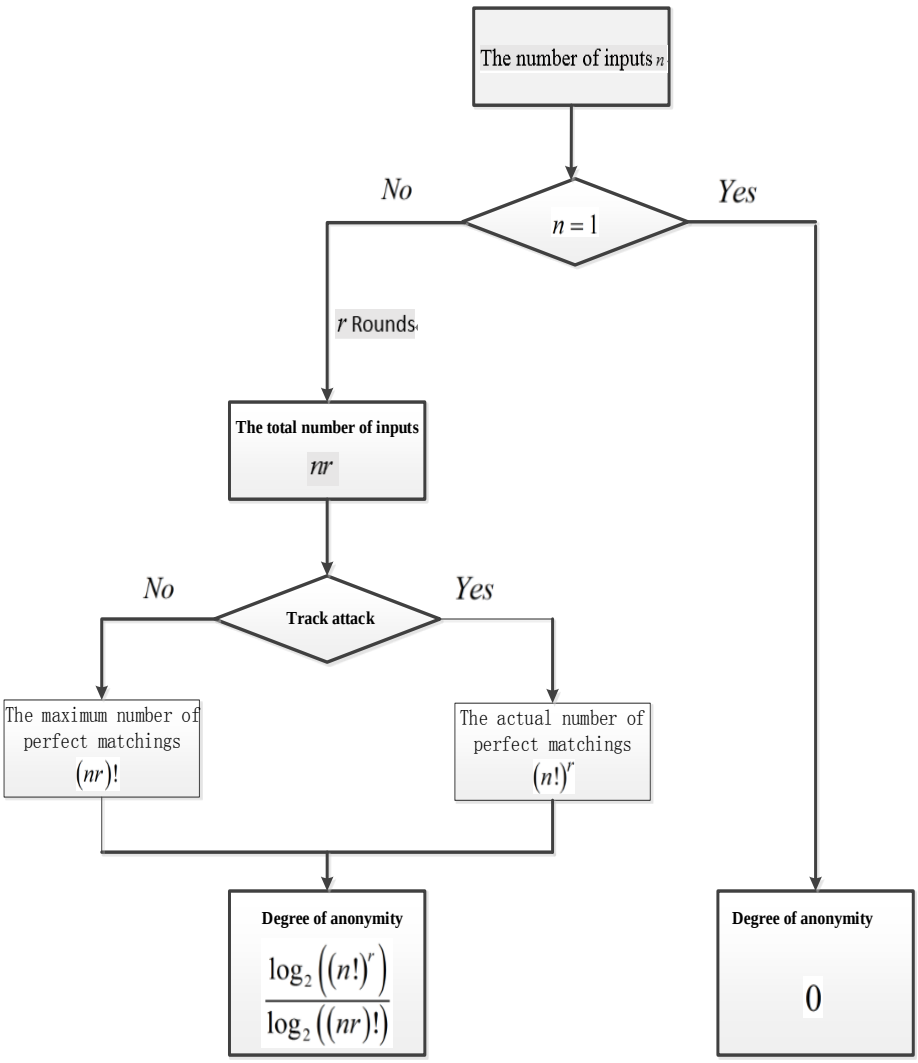

Figure 3-3. BIG-MIX Evaluation Process

By attacking model assumed to be seen an attacker can observe the input message and output messages for each BIG-MIX round, so the message path after r times confusing can be seen as the number of BIG – MIX is r , after each round, system increases n input messages and n output messages. Figure 3-5 is corresponding with Figure 3-4 and shows an attacker may look the possible message paths between the BIG-MIX.

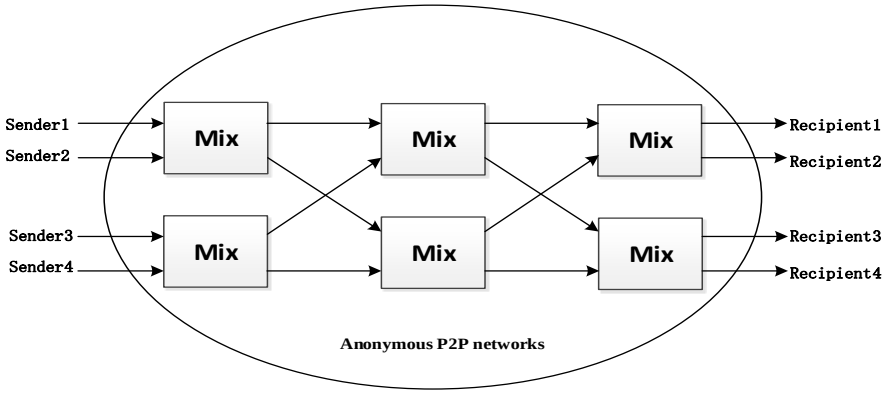

Figure 3-4. The Actual Path in Anonymous P2P Networks

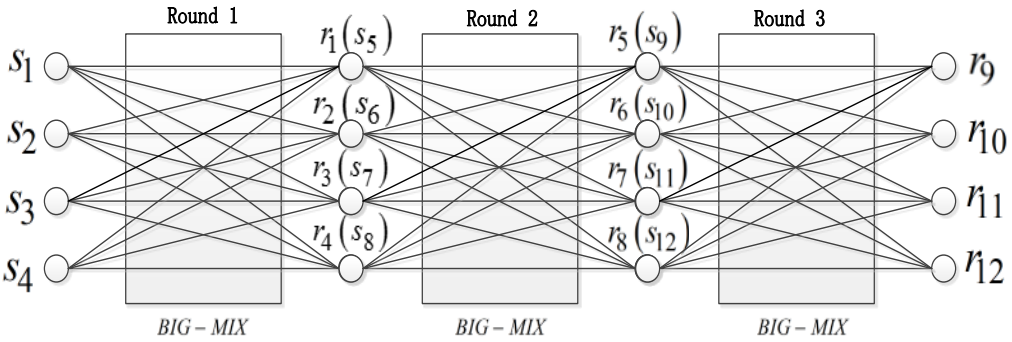

Figure 3-5. An Attacker May Look the Possible Message Paths Between the BIG-MIX

In order to give possible mapping between input message and output message, we reference method of Matthew Edmand [3], given a set of possible associations between inputs and outputs, we construct a bipartite graph $G = (S, R, E)$ to represent the system, Where S、R respectively the input set $S_1 = \{s_i\}, i = 1, \ldots n$ and the outputs set $R_1 = \{r_j\}, j = 1, \ldots n$ and E is the set of edges representing all possible (s_i, r_j) mappings. A bipartite graph $G = (S, R, E)$ can be represented by its adjacency matrix A; a (0-1)-matrix of size $(nr) \times (nr)$, for each $s_i \in S, i = 1, \ldots nr$ and $r_j \in R, j = 1, \ldots nr$, if the edge (s_i, r_j) exists in G, the entry $A(i, j)$ is set to 1, otherwise it is set to 0. It is known that counting the number of perfect matching in G is equivalent to the permanent of A, which is given by:

$$\text{per A} = \sum_{j_1 j_2 \cdots j_n} a_1 j_1 a_2 j_2 \cdots a_n j_n \qquad (3-1)$$

A term in the summation is 1 if and only if all entries $a_1 j_1 a_2 j_2 \cdots a_n j_n$ are 1, which means that G has a perfect matching. From all possible relationship between input messages and output messages in the system and its corresponding adjacency matrix by attacker tracking the inputs and outputs in each BIG-MIX. One BIG - MIX input can only correspond to the same BIG - MIX output, so the permanent of this adjacency matrices is $(4!)^3$. In the same way, n is the number of initial input messages, r is the number of round times, the corresponding permanent of adjacency matrices is $\text{per A} = (n!)^r$.

When the anonymity provided by anonymous P2P networks is maximal, every vertex in S set are connected with all the vertices in R, and vice versa. At this moment, G is a complete bipartite graph with $(nr) \times (nr)$, so the number of perfect matchings is $(nr)!$, it's the maximum number of perfect matchings of this complete bipartite graph. Due to there exist at least one perfect matching between S set and R set to indicating the true communication pattern, this complete bipartite graph achieve at least one perfect matching. Therefore, the number of perfect matchings is bounded by $1 \le \text{per A} \le (nr)!$.

Refer to Matthew Edman's [3] definition on system's anonymity level (formula 2-3) and Claudia Diaz [8-9] (formula 2-1) regularization method, In this paper, we define the degree of anonymity, d, as:

$$d(A) = \begin{cases} 0, n = 1 \\ \dfrac{\log_2(perA)}{\log_2((nr)!)} = \dfrac{\log_2((n!)^r)}{\log_2((nr)!)}, n > 1 \end{cases} \qquad (3\text{-}2)$$

Where $(nr)!$ is the permanent of the all-1 matrix, where we call $\log_2((nr)!)$ is the Maximum information when an attacker get the correct mapping relationship between inputs and Outputs an $(per\ A)$ is some information which exclude some mappings, and $\log_2(per\ A)$is the number of correct mappings between input and output. When $n = 1$, it means only one input and one output in the system, the anonymity of the system is 0. For the system in Figure 3-4, the level of anonymity can be computed as $\log_2((4!)^3)/\log_2((4\times 3)!) = 0.4770$.

4. Application of BIG-MIX Evaluation Method

4.1. Application to Threshold Mixes

When a threshold mixes collects input messages reach the threshold N, for each received message the Mix applies a cryptographic transformation, and then sent all N messages in a random order to their next destination. We refer this process as a mix round. Anonymous P2P networks under the mechanism of Threshold Mixes, a BIG-MIX is composed of several Threshold Mixes.

For any threshold mixes with a threshold N, suppose there are s mixes in each round, over r rounds the original incoming messages is$n = s \times N$, the number of perfect matching between input message and output message is $((s\times N)!)^r$,so we can compute the overall degree of anonymity of the mix as follows:

$$d(A) = \frac{\log_2(per(A))}{\log_2((nr)!)} = \frac{\log_2(((s\times N)!)^r)}{\log_2((s\times N\times r)!)} \qquad (4-1)$$

Next we will assess degree of anonymity when change these parameters: Figure (4-1) shows when $r=1, r=3, r=5, r=10$, In the case of an attacker has the ability to track message, with the change of each mix's threshold N and the number of mix s in each BIG-MIX round, the degree of anonymity trends. After observation we conclude as follows: (1) Figure (4-1-a) shows when $r=1$, the attacker didn't get any order information between input and output in BIG-MIX confusion, for $\forall N$ and $\forall s$, the degree of anonymity d obtain maximum 1.Under the ideal circumstances that there only existence message tracking attack in Anonymous P2P network, $r=1$can meet the needs of the biggest anonymity, but for most anonymous P2P networks it will face a variety of attacks, therefore we need to consider the impact of various factors s, N, r on anonymity comprehensively. (2) Figure (4-1-b), (4-1-c), (4-1-d) shows: for $r>1$, degree of anonymity d increases with s and N increasing, and the increasing trend gradually slowing. If s and N continue to increase, then the degree of anonymity will reduce to 0. It means that we can't in order to increase the degree of anonymity, unlimited increase threshold N and the number of Mix s. (3) By comparing r and maximum degree of anonymous d in Figure (4-1-b), (4-1-c), (4-1-d), we find that with the increase of r, d decrease gradually, r and N increase interval also decrease accordingly. This enlightens us the greater of r, the smaller adjusting range of r and N when setting parameters of anonymous system. Note that adjustment in the valid range, to avoid wasting system resources. (4) In the aspect of symmetry, by observing these four pictures can be found these images on the plane of symmetry, this plane is determined by the

line $N = s$ and line $N = 1$ （$s = 1$）, it means that when r unchanged, the impact on anonymity of N And s is peer.

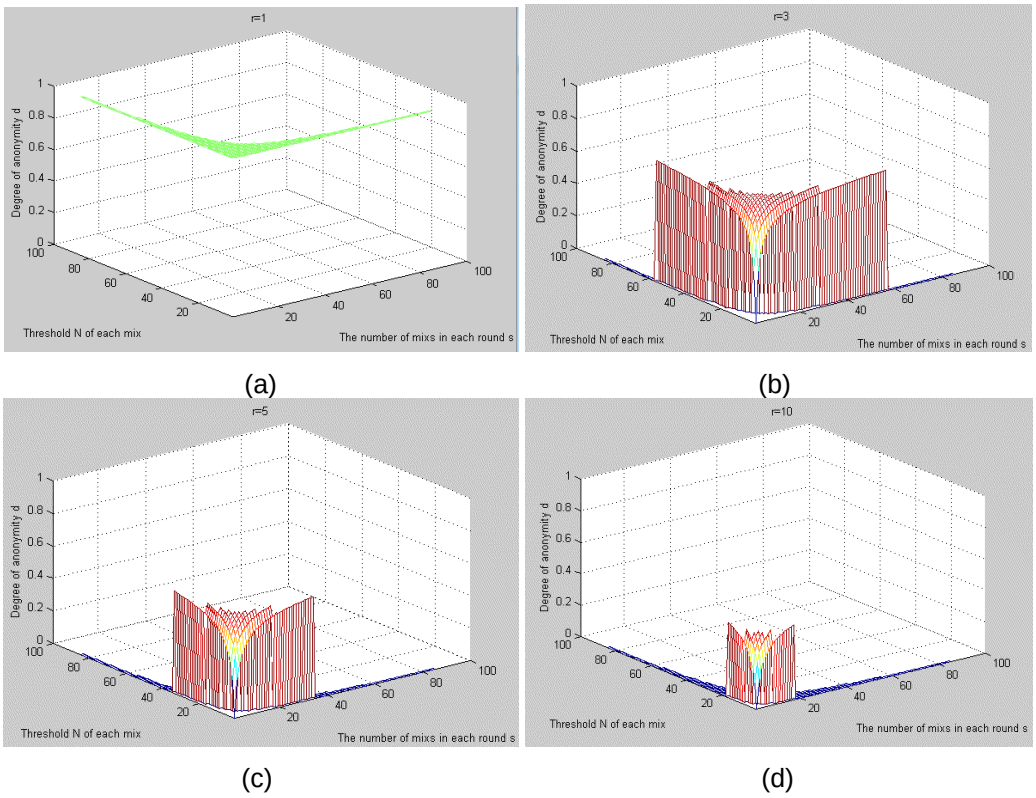

Figure 4-1. When r is a Fixed Value, Threshold N and the Number of Mix S Effect the Degree of Anonymity d

Figure (4-2) visually display that when s and N are fixed value, round times r effect the degree of anonymity, we can conclude as follows: (1) When $r = 1$, the degree of anonymity d obtain maximum 1, with the increase of r, the degree of anonymity d gradually reduced.(2) when s is a fixed value, the smaller the threshold N, the slower speed of d decreased to 0 with the increase of r. To ensure the system under the condition of anonymity, the corresponding round's changeable range became larger. (3) When s is a fixed value, to ensure the system under the condition of anonymity, the degree of anonymity d increases as the threshold N increases. (4) From the above conclusion we know that s and N is symmetrical, so switch s and N in conclusion (2) (3) is also established

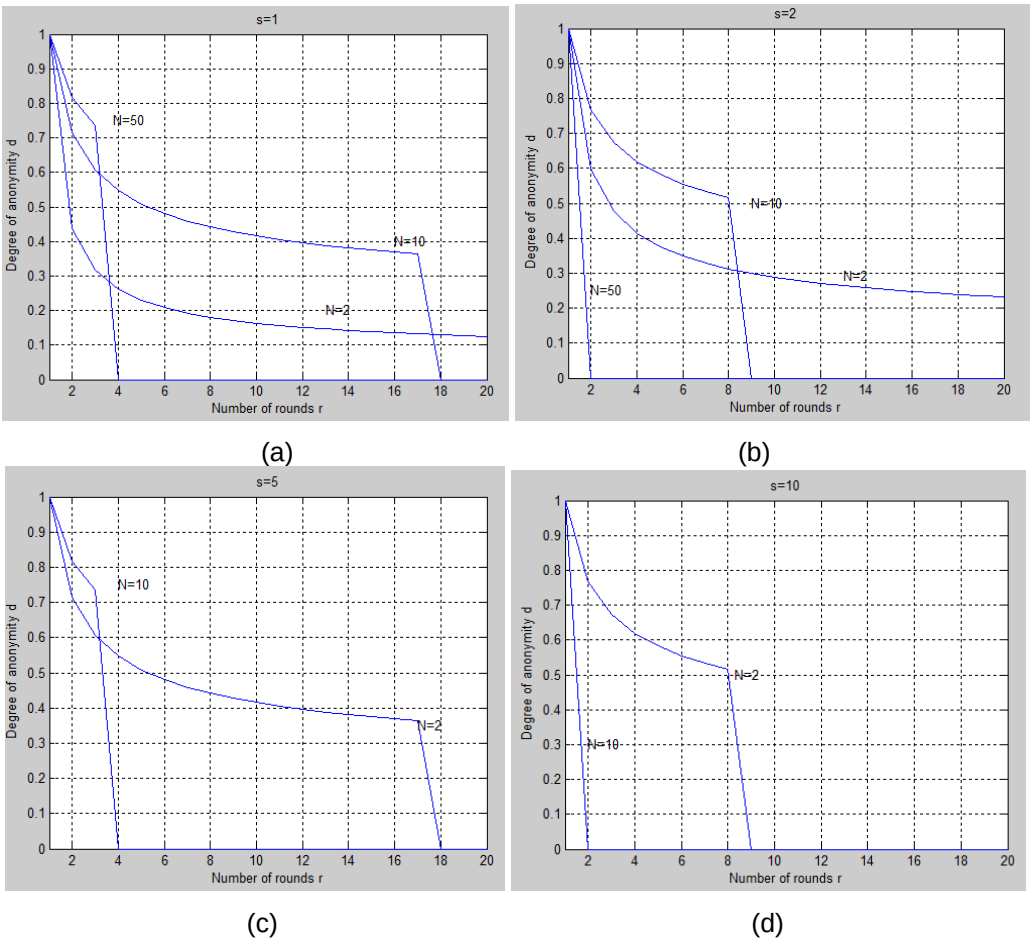

Figure 4-2. When the Number of Mix s and Threshold N in each BIG-MIX Round are Fixed Value, Round Times r Effect the Degree of Anonymity d

Figure (4-3) visually display that when r and N are fixed value, the number of mix s effect the degree of anonymity, we can conclude as follows: (1) When $r=1$, N is an arbitrary number, the degree of anonymity d obtain maximum 1, the changes of s had no effect on d . (2) When $r>1$, for the fixed value N , The system maximum degree of anonymity(less than 1) existence and uniqueness, d increases with s increasing, and the increasing trend gradually slowing, when d obtain maximum 1,If s continue to increase, then d will reduce to 0.(3) To ensure the system under the condition of anonymity, for the same r ,the larger the threshold N , the smaller the changeable range of s in each mix round.

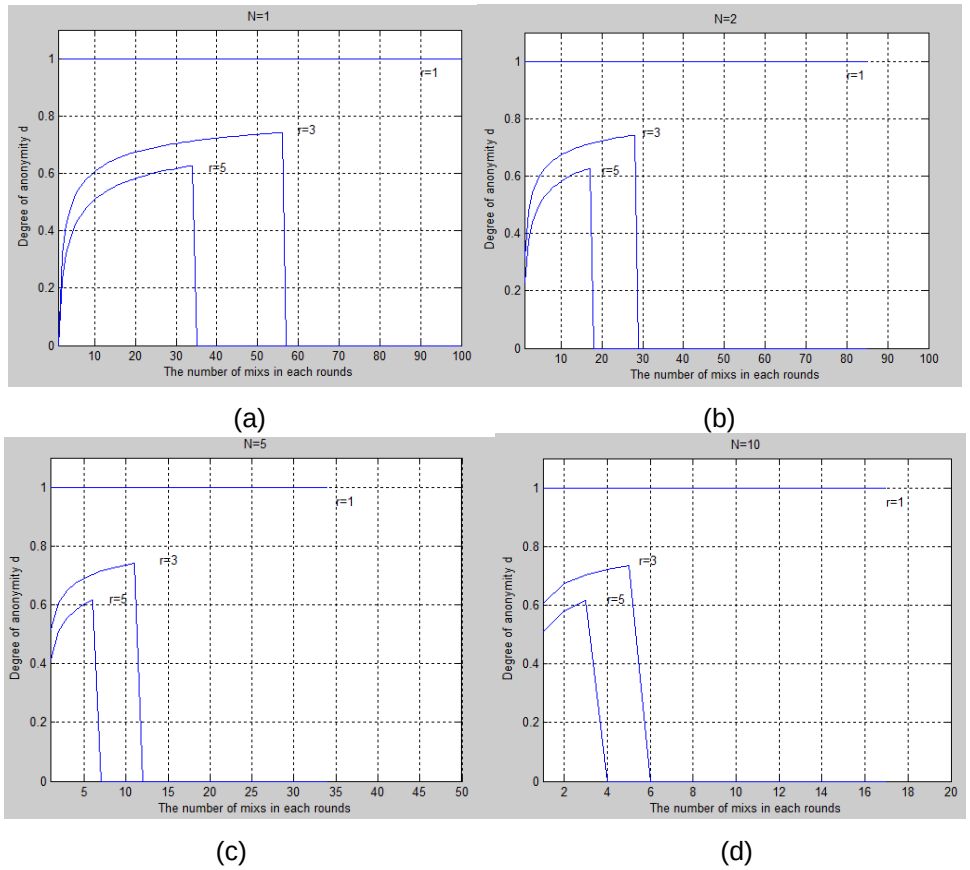

Figure 4-3. When Round Times r and Threshold N are Fixed Value, the Number of Mix s in Each BIG-MIX Round Effect the Degree of Anonymity d

Figure (4-4) visually display that when r and s are fixed value, threshold N effect the degree of anonymity, we can conclude as follows :(1) when $r=1$, s is an arbitrary number, the degree of anonymity d obtain maximum 1, the changes of N had no effect on d .(2) When $r>1$, for the fixed value s, The system maximum degree of anonymity(less than 1) existence and uniqueness, d increases with N increasing, and the increasing trend gradually slowing, when d obtain maximum 1 ,If N continue to increase, then d will reduce to 0. (3) To ensure the system under the condition of anonymity, for the same r, the larger the number of mix s, the smaller the changeable range of N in each mix round.

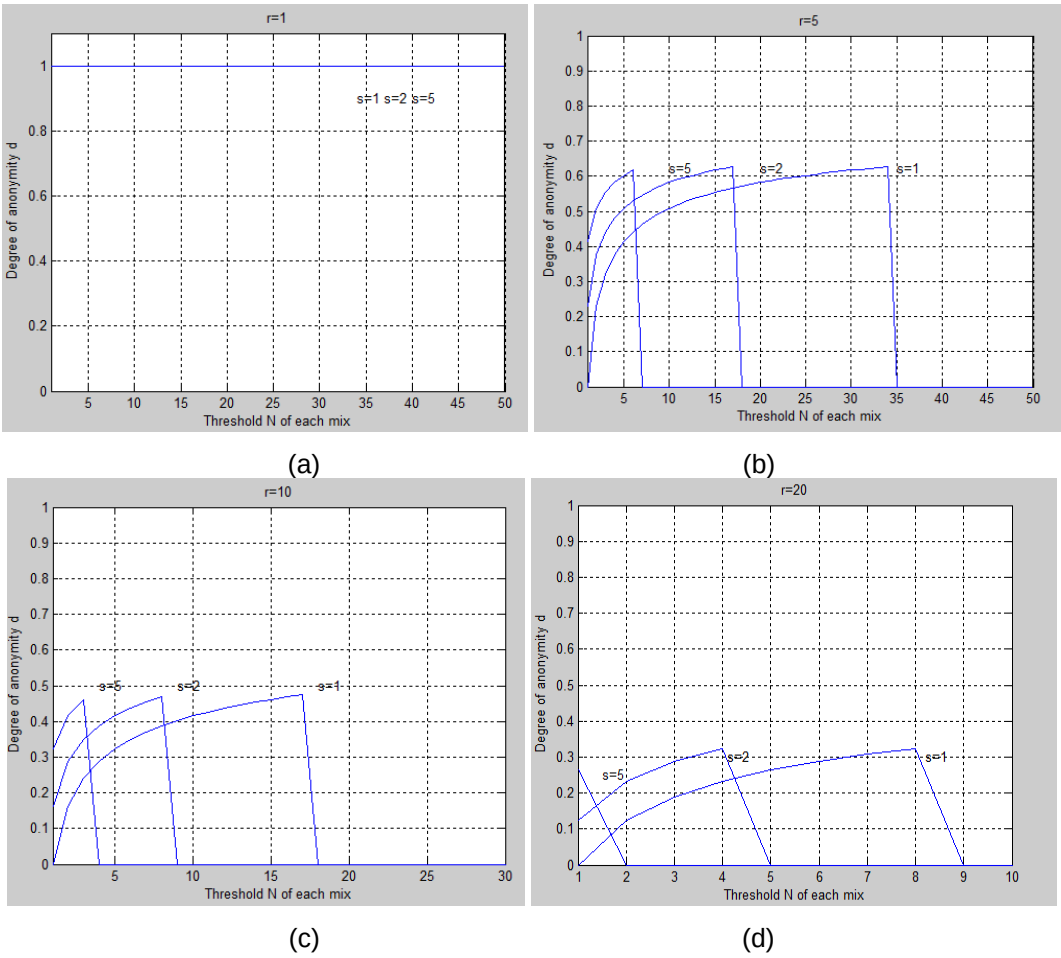

Figure 4-4. When Round Times r and the Number of Mix s in Each BIG-MIX Round are Fixed Value, Threshold N Effect the Degree of Anonymity d

4.2. Application to Timed Mixes

When a Timed Mixes collects messages for t seconds, for each received message the mix applies a cryptographic transformation, and then sent all message to their next destination in a random order. We refer this process as a Timed Mixes round. Anonymous P2P networks under the mechanism of Timed Mixes, a BIG-MIX is composed of several Timed Mixes.

For any Timed Mixes with the time period for the t, suppose there are s Timed Mixes in each BIG-MIX round, the arrival rate of messages into the mix be c messages per second. The average number of messages arriving to and exiting from the mix during a single round of length t is then $c \times t$, so the average number of messages arriving to and exiting from the BIG-MIX during a single round of length t is then $s \times c \times t$, after r rounds the original incoming messages is $n = s \times c \times t$, the number of perfect matching between input message and output message is $((s \times c \times t)!)^r$, so we can express the degree of anonymity for a Timed Mixes as follows:

$$d(A) = \frac{\log_2(per(A))}{\log_2((nr)!)} = \frac{\log_2(((s \times c \times t)!)^r)}{\log_2((s \times c \times t \times r)!)} \qquad (4-2)$$

Figure (4-5) shows when the arrival rate of messages is $c = 1, c = 3$, Timed Mixes round $r = 1, r = 3, r = 5, r = 10$, in the case of an attacker has the ability to track message, with the change of each round length t and the number of mix s in each BIG-MIX round, the degree of anonymity d trends. After observation we conclude as follows:

(1) Figure (4-5-a) and Figure (4-5-e) shows for any messages arrival rate c, when $r = 1$, the attacker didn't get any order information between input and output in BIG-MIX confusion, for $\forall t$ and $\forall s$, the degree of anonymity d obtain maximum 1.Under the ideal circumstances that there only existence message tracking attack in Anonymous P2P network , $r = 1$ can meet the needs of the biggest anonymity, but for most anonymous P2P networks it will face a variety of attacks, therefore we need to consider the impact of various factors s, c, t, r on anonymity comprehensively.

(2) For $r > 1$, when messages arrival rate c is a fixed value, degree of anonymity d increases with s and t increasing, and the increasing trend gradually slowing. If s and t continue to increase, then the degree of anonymity will reduce to 0. It means that we can't in order to increase the degree of anonymity, unlimited increase round length t and the number of mix s.

(3) By comparing r and maximum degree of anonymous d in Figure (4-5-b)~ Figure (4-5-h), when messages arrival rate c is a fixed value, we find that with the increase of r, the system maximum degree of anonymity d decrease gradually, t and s increase interval also decrease accordingly. This enlightens us the greater of r, the smaller adjusting range of t and s when setting parameters of anonymous system. Note that adjustment in the valid range, to avoid wasting system resources.

(4)In the aspect of symmetry, by observing these pictures can be found these images on the plane of symmetry, this plane is determined by the line $s = t$ and line $t = 1 (s = 1)$, it means for the fixed messages arrival rate c and r unchanged, s and t impact on anonymity are equal.

Figure (4-6) shows when the arrival rate of messages is $c = 1, c = 3$, the number of mix s in each BIG-MIX round is $s = 1, s = 2, s = 5, s = 10$,in the case of an attacker has the ability to track message, with the change of round length t and round times r, the degree of anonymity d trends. After observation we conclude as follows: (1) when $r = 1$, the degree of anonymity d obtain maximum 1, with the increase of round times r, the degree of anonymity gradually reduced.(2) To ensure the system under the condition of anonymity, for the same messages arrival rate c, the larger the number of mix s, the smaller the changeable range of round length t in each mix round.(3) From the above conclusion we know that s and t is symmetrical, so switch s and t is also established.

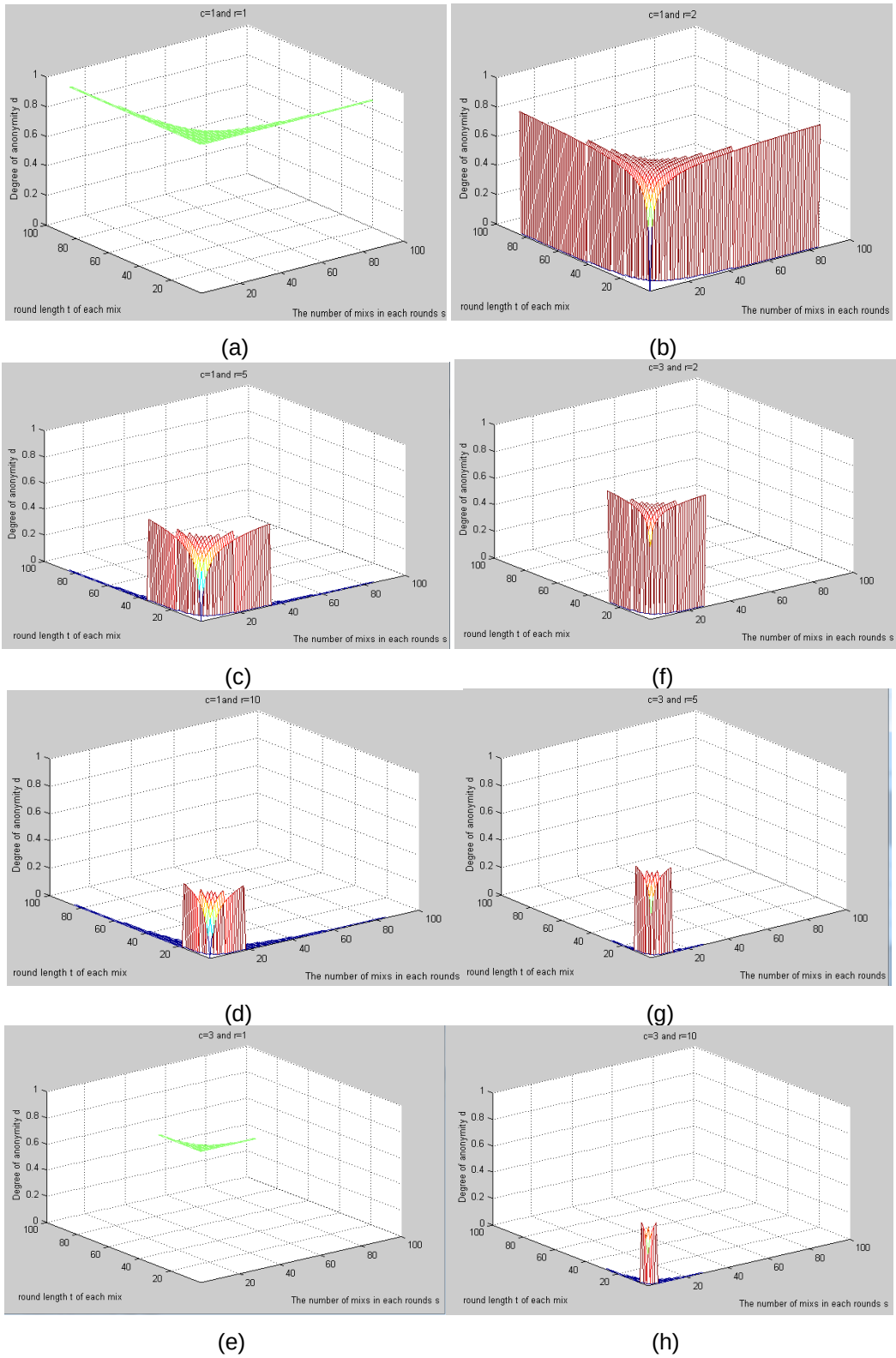

Figure 4-5. When Round Times r and Messages Arrival Rate c are Fixed Value, Round Length t and the Number of Mix s in Each BIG-MIX Round Effect the Degree of Anonymity d

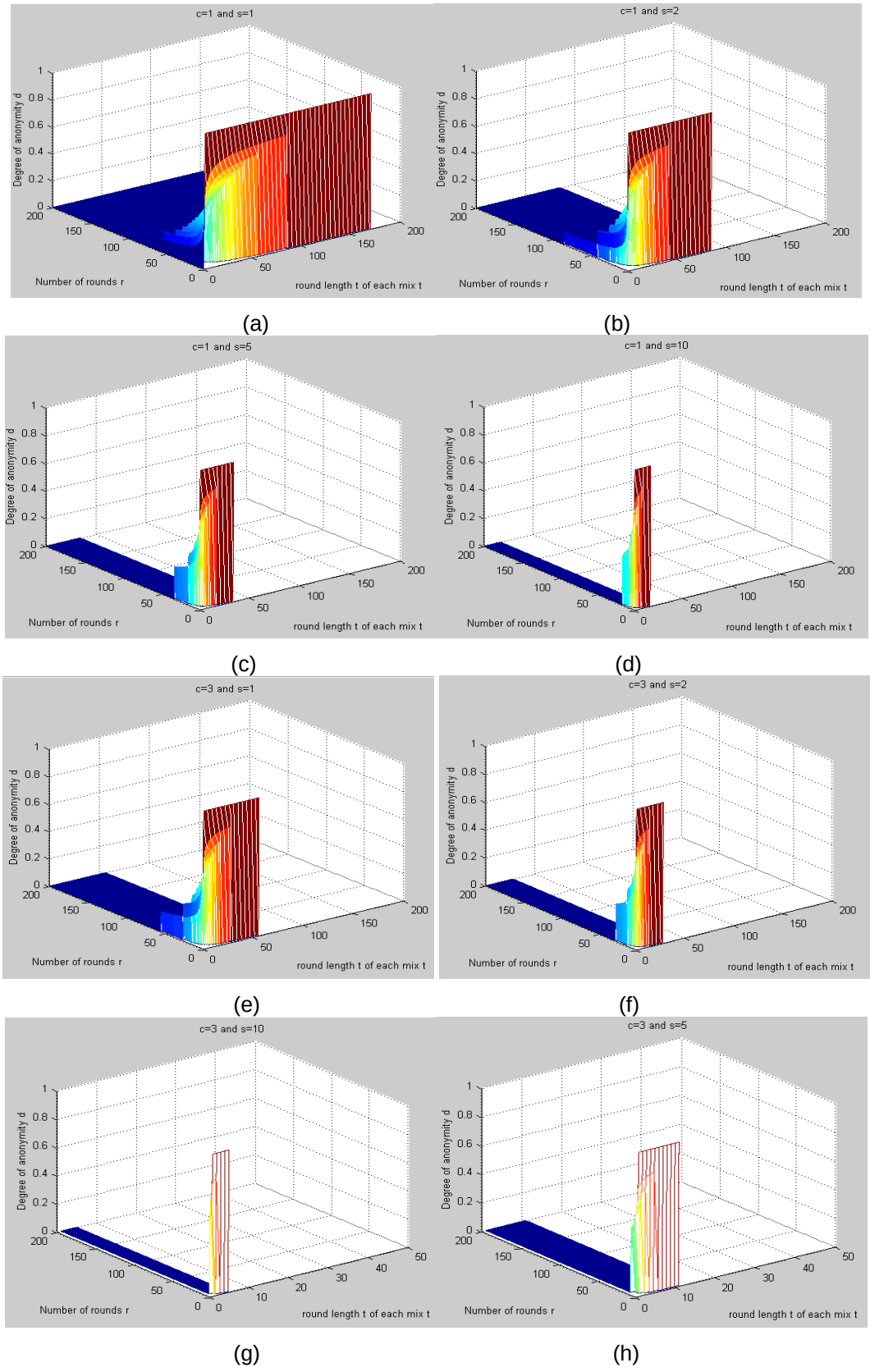

Figure 4-6. When Messages Arrival Rate c and the Number of Mix s in Each BIG-MIX Round are Fixed Value, Round Length t and Round Times r Effect the Degree of Anonymity d

4.3. Application to Pool Mixes

When receiving the first message, it will produce n false messages which are created by the mix itself .When a pool mix collects N input messages, the mix will selected N output messages randomly from a pool of $N+n$ messages. Then the Mix applies a cryptographic transformation, and then sent all N messages in a random order to their next destination. There will be n messages retained in the mix for the next round. Indeed, an output message may correspond to any previous message which has ever entered the Pool Mix before .One message will remain in the mix indefinitely is a non-zero probability. Each pool mixes are able to blend messages across multiple rounds of the mix($r\to\infty$),unlike simple threshold or timed mixes only can blend together messages within the same round (r=1).

From the perspective of individual message, Serlantov & Danezis [10] pointed that the probability of a message remaining in the mix for r rounds decreases as r increases. They proved that the probability a message outputting the pool mix at round r corresponds to a message that previously entered the mix at round x is:

$$p(r,x) = \frac{N}{N+n} = \left(\frac{n}{N+n}\right)^{r-x} \qquad (4-3)$$

The range of x is $0 < x \le r$, each individual existing the mix at round r then has a probability of $p(r,x)/N$ corresponding to each input at some previous round x. From the perspective of the whole system, attackers observed that there is a non-zero probability for a portion of the input messages will existence in the mix forever. So the attacker needs to observe greater than or equal to an infinite amount of time to g*et al*l the output messages corresponding to all the input messages. But in terms of the actual situation, an attacker could only implement a limited times of message tracking attack, they can't wait indefinitely. Therefore, in this mechanism, attacker obtain the input message doesn't necessarily have a corresponding output messages, and vice versa. The attacker can't determine the set of input and output messages. So it is impossible to establish mappings between inputs and outputs. It means they can't implement effective attack, the degree of anonymity can be considered to achieve maximum 1.

5. Conclusion

In this paper, we propose BIG-MIX anonymity evaluation method based on the mapping. And with this method, we make a quantitative analysis on the relationship anonymity of anonymous P2P networks under the mechanism of Threshold Mixes, Timed Mixes or Pool Mixes. Especially make the quantitative analysis on the relationship anonymity of anonymous P2P networks under the mechanism of Threshold Mixes, Timed Mixes.

This article exist the following problems and research space: the BIG-MIX method assumes that a sender only sends one message and a recipient only received one message too, so the sender and the input message is one-to-one mapping, and recipient and the output message is the same. This means that the correct mapping relationship between inputs and outputs is corresponding to the sender's and recipient's actual communication relationship. However, in most cases, a sender may have more than one corresponding recipient, a recipient may have more than one corresponding sender too, so there may exist one-to-one, one-to-many, many-to-one and many-to-many relationships between sender and recipient, therefore, the further research is to extend this method to communication subject can send/receive any message.

Acknowledgements

This work is supported by the following programs: the National Natural Science Foundation of China under Grant No.61170273; 2010 Information Security Program of China National Development and Reform Commission with the title "Testing Usability and Security of Network Service Software".

References

[1] D. Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms", Communications of the ACM, vol. 24, no. 2, **(1981)**, pp. 84-88.
[2] P. M. Waidner, "Networks without user observability - design options", Computers and Security, vol. 6, no. 2, **(1987)**, pp. 158-166.
[3] M. Edman, F. Sivrikaya and B. Yener, "A Combinatorial Approach to Measuring Anonymity", Proceedings of Intelligence and Security Informatics, IEEE, **(2007)**.
[4] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability", Journal of Cryptology, vol. 1, **(1988)**, pp.65-75.
[5] D. Kesdogan, J. Egner and R. Büschkes, "Stop-and-Go-MIXes Providing Probabilistic Anonymity in an Open System", LN CS, vol. 1525, **(1998)**, pp. 83-98.
[6] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transactions", ACM Transactions on Information and System Security, **(1998)**, pp. 66-92.
[7] O. Berthold, H. Federrath and S. Kopsell, "Web MIXes: A System for Anonymous and Unobservable Internet Access", In Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, Springer-Verlag, **(2001)**, pp. 115-129.
[8] C. Diaz, S. Seys and J. Claessens, "Towards measuring anonymity", Privacy Enhancing Technologies (PET2002), Springer-Verlag, **(2002)**, pp. 54-68.
[9] C. Diaz, "Anonymity and Privacy in Electronic Services", Doctoral Dissertation, Leuven: Electrical Engineering department of Katholieke Universiteit, **(2005)**, pp. 23-40.
[10] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity", Privacy Enhancing Technologies workshop (PET'02). San Francisco, **(2002)**, pp. 41-53.
[11] C. E. Shannon, "The Mathematical Theory of Communication", Bell System Technical Journal, vol. 27, no. 3, **(1948)**, pp. 379-390.
[12] C. E. Shannon, "Communication in the Presence of Noise", PROC IRE, vol. 37, no. 1, **(1949)**, pp. 10-21.
[13] B. Gierlichs, C. Troncoso, C. Diaz and B. Preneel, "Revisiting a Combinatorial Approach Toward Measuring Anonymity", **(2008)**.
[14] J. C. Grégoire and A. M. Hamel, "A Combinatorial Enumeration Approach for Measuring Anonymity", eprint arXiv: 0902.1663, **(2009)**.
[15] R. Bagai, H. Lu and R. Li, "An Accurate System-Wide Anonymity Metric for Probabilistic Attacks", Privacy Enhancing Technologies LNCS, vol. 6794, **(2011)**, pp. 117-133.

Authors

Tian-Bo Lu, was born in Guizhou Province, China, 1977. He is an Associate professor in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information security and computer network.

Cheng Wang, was born in Inner Mongolia, China, 1991. She is a graduate student in School of Software Engineering, Beijing University of Post s and Telecommunications, China. Her technical interests in clude information and network security, anonymous communication.

Xiao-feng Du, was born in Shaanxi Province, China, 1973.He is a Lecturer in School of Computer, Beijing University of Posts and Telecommunications, China. His technical interests include information security and computer network.

Yang Li, was born in Hunan Province, China, 1978. He is a PhD and his technical interests include information security, distributed computing and P2P network.