MEASURING ANONYMITY WHILE SENDING AND RECEIVING MULTIPLE MESSAGES

A Thesis by

Abdus Samad

Bachelor of Computer Science & Information Technology,
NED University of Engineering & Technology, Pakistan, 2007

Submitted to the Department of Electrical Engineering and Computer Science
and the faculty of the Graduate School of
Wichita State University
in partial fulfillment of
the requirements for the degree of
Master of Science

May 2012

MEASURING ANONYMITY WHILE SENDING AND RECEIVING MULTIPLE MESSAGES

The following faculty members have examined the final copy of this thesis for form and content, and recommend that it be accepted in partial fulfillment of the requirement for the degree of Master of Science with a major in Computer Networking.

_____

Rajiv Bagai, Committee Chair

_____

Murtuza Jadliwala, Committee Member

_____

Esra Büyüktahtakın, Committee Member

DEDICATION

To my family, for their prayers and wishes, which gave me strength and support

ACKNOWLEDGEMENTS

This thesis would not have been possible without the guidance and help of several individuals who have helped me throughout the course of my studies. First and foremost, I would like to thank my advisor, Dr. Rajiv Bagai, for his excellent guidance and continuous support, help, and advice, not only with the completion of this thesis but also throughout my Master's degree program. I would also like to thank Dr. Bin Tang for his constant input and support during my research. I express gratitude to all my colleagues and friends, especially Ahsan Khan, for their help and support all the way to the completion of this thesis. Last, but not least, I thank my parents and my younger brothers for their constant support, encouragement, prayers, and good wishes.

ABSTRACT

Anonymity systems are designed in a way that hides the level of communication between senders and receivers of a message, and the goal of an attacker is to find that communication pattern. It is usually very difficult to completely de-anonymize a system if it presents a black box, in which case only a global adversary can observe all messages going in and out of the system and, based on some attack, can infer the feasibility of messages being sent and received by users. This thesis presents a method to calculate the amount of anonymity present in a system after a global adversary has conducted an attack. The base model considered in this thesis considers a black box system, which allows multiple senders to send multiple input messages and multiple receivers to receive multiple output messages. A couple of approaches taken by previous researches have been analyzed and compared to the method given in this thesis, which shows that one of the methods does not consider an attack, while the other method does not cover the full spectrum of the attack plane.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Anonymity and privacy have been a major concern since the inception of electronic communication; it is human nature to remain anonymous. While it is not always possible to be completely anonymous, relative anonymity can be attained. When talking about anonymity in relation to computers and electronic communication, many solutions have been proposed, based on concepts derived from real life. For example, it is difficult to spot a movement and predict it while passing through a large crowd, which is one of the basic concepts when it comes to anonymity in real life as well as in electronic communication.

In electronic communication, the goal of anonymous systems is to hide correspondence between the sender and receiver. These systems are usually black boxes, which are situated between the sender and the receiver and attempt to hide any identifiable communication. The degree of a system's anonymity can be partly measured using some mathematical function or metrics. The goal of an attacker i.e. a malicious user is to identify the sender and receiver communication pattern so that the real source or destination of a message can be identified. Many researchers have tried to solve the problem by developing a close approximate metric to measure anonymity. Serjantov and Danezis [1] and Diaz et al. [2] proposed an information theoretic metric based on Shannon entropy to measure the uncertainty of an attacker in order to identify the sender or receiver with respect to a single user or message. Taking a step further, Edman et al. [3] proposed a system wide metric considering all incoming messages and outgoing messages. Considering an infeasibility attack over the system, they represented the system in terms of a bipartite graph. In an infeasibility attack, an adversary basically marks some edges as infeasible based on observation and analysis of input and output messages. The number of

feasible perfect matchings between input and output messages after a successful infeasibility attack results in deciding the amount of anonymity the system possesses. Two types of infeasibility attacks are discussed in detail in Chapter 2. In order to validate the metric Edman et al. [3] applied their metric to high-latency mixes such us threshold mix, timed mix and pool mix.

Gierlichs et al. [4] presented the idea that instead of calculating a metric with respect to messages, the goal of an adversary is to identify the sender or receiver of the messages. If an attacker is successful in identifying any one set of perfect matching in an equivalence class between sender and receiver, then the system is deemed vulnerable, and hence the anonymity decreases. In order to present the above concept, Gierlichs et al. [4] used an equivalence relation (~) between the set of feasible perfect matchings resulting in a more accurate metric.

1.1 Contributions of Thesis

This thesis addresses two problems and proposes solutions to both of them. The first contribution involves analysis of the Gierlichs et al. [4] method of computing the size of an equivalence class ~ and showing that in reality it does not cover all possible messages previously defined by Edman et al. [3]. In fact, the size shrinks as the number of messages increases, resulting in a large portion of attack possibilities being missed. The second contribution is a technique that addresses the shortcomings of their work and provides a general method that can be used for all possible attacks.

The method proposed in this thesis uses the set used by Edman et al. [3] and induces equivalence classes. An association matrix is used to represent all incoming and outgoing messages sent and received by senders and receivers where the row sum is the number of messages sent by the senders and the column sum is the number of messages received by the receivers. With the above model in place, when an attack pattern of feasible perfect matchings is

introduced and is superimposed on the complete set, the feasible perfect matchings can be identified. Furthermore, this thesis presents a method to recursively compute the number of feasible perfect matchings in a class used to compute the amount of anonymity in a given system.

1.2 Organization of Thesis

The remainder of this thesis is organized as follows: Chapter 2 provides a literature review, which is divided into two major parts. The first part contains an overview of the underlining model presented by Edman et al. [3] and the metric proposed by them, as well as some examples of the attack models presented by various researchers and their effects on the system. The second part deals with scenarios when senders and receivers having multiple messages are introduced. Furthermore, the groundwork for the metric proposed in this thesis, such as the number of equivalence classes, size of equivalence class, and representation of equivalence class in terms of non-negative integer matrices, is discussed in this section.

Chapter 3 contains the new metric along with a method to compute the weight of an equivalence class. Chapter 4 focuses on the comparison of the two approaches taken by Gierlichs et al. [4] and Grégoire and Hamel [5], showing that the approach taken by Gierlichs et al. [4] is limited to only a small family of attacks, while the approach of Grégoire and Hamel [5] does not consider any attacks. The final chapter provides conclusions and future directions of the work presented in this thesis.

CHAPTER 2

LITERATURE REVIEW

2.1 Anonymity Metric

As mentioned in Chapter 1, Serjantov and Danezis [1] and Diaz et al. [2] provided a technique to measure anonymity of a system with respect to a single user or message. Edman et al. [3] provided a systemwide metric based on the permanent of a matrix, i.e., it considers the overall communication pattern in a system. The above information theoretic metrics are widely adopted today to determine the degree of anonymity provided by an anonymity system.

Anonymity is achieved if a user cannot be uniquely identified based on its characteristics, within a set of users. The set of possible users depends upon the knowledge of an attacker which means that anonymity is relative with respect to the attacker. The more information attacker has the less the anonymity of the system will be.

Before the above methods were presented, some attempts were made to determine the amount of anonymity provided by an anonymity system. For example Reiter and Rubin [6] presented the degree of anonymity of a given system as $1 - p$, where p represents the probability an attacker gives to a sender. The issue with this model is that the users are considered separately, and it does not capture the true anonymity properties. For example, consider a system where there are two users x_1 and x_2, and the attacker assigns probability of 9/10 to the first user x_1 and 1/10 to the next user x_2. Now, according to the model, the degree of anonymity for x_1 is (d = 0.1), while the degree of anonymity for x_2 will be (d = 0.9). Then, consider another system with 100 users, and suppose the first user x_1 is given a probability of 1/10 by the attacker and all other users are given a probability of less than 0.01. In the above scenario, user x_2 in the first case and

user x_1 in the second case will both have a degree of anonymity as ($d = 0.9$), while intuitively, x_1 in the second case is more likely to be the sender then x_2 in the first case.

Another metric, proposed by Berthold et al. [7], relies on the number of users in a given system. They defined the degree of anonymity as $A = \log_2(N)$, where N represents the total number of users in the system. This model, which is similar to the previous model, has many deficiencies. For example, it only considers the number of users and ignores the properties of the system; also, it does not consider the probability distribution of senders, i.e., whether or not an attacker is able to eliminate certain senders by marking them infeasible or giving them low probability of being a possible sender.

In 2002, Serjantov and Danezis [1] and Diaz et al. [2] presented information theoretic metrics based on Shannon's entropy, which later became the basis of research in this field. Following is the underlying model used by Edman et al. [3] to derive the metric.

2.1.1 Underlying Anonymity Model

In order to understand the anonymity model presented by Edman et al. [3], consider X as the total number of input messages and Y as the total number of output messages entering and exiting an anonymity providing system. The number of messages entering the system is equal to the number of output messages; hence, $|X| = |Y|$. The total number of messages accepted by the system at a time, i.e., the threshold of the system, is denoted by $|t|$. An anonymous system running at optimal performance, therefore, will have $|X| = |Y| = t$.

The system that provides the necessary anonymity services uses a number of techniques to conceal the identity of the sender once the messages are received by the system. Randomizing the sequence of packets received, inducing random delays to counter timing analysis, and encrypting or encoding messages to a counter bit pattern analysis are some examples.

Consider two extreme cases in order to understand the system's anonymity. Having a system with threshold $t = 4$ with input messages $x_i = 4$ for all output messages in Y, each message in X is a possible candidate after an attack, resulting in a complete bipartite graph, as shown in Figure 1(a). Since the attacker is not able to infer any perfect matching between any input and output messages, the system produces maximum anonymity. On the other hand, if an attacker is able to identify perfect matchings between the messages in X and Y by eliminating infeasible edges from the complete bi-partite graph, such that all messages in $y \in Y$ show there is only one feasible input message that could have arrived from X, as shown in Figure 1(b), then the system will have no anonymity.

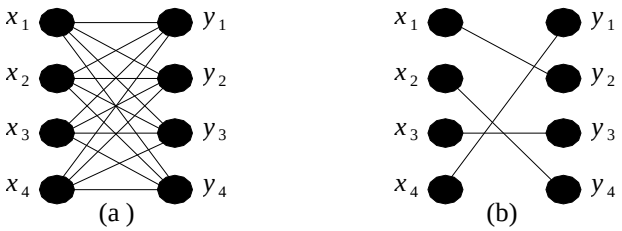


Figure 1: (a) Example of complete anonymity (b) example of no anonymity.

Generally the system would possess a case somewhere between the two extreme scenarios, where the attacker might be able to eliminate some infeasible edges after inducing an attack, thus making a bipartite graph with only feasible edges. In both cases above and hereafter in this thesis, a global adversary is considered, such that an attacker knows the number of incoming and outgoing messages in a system and is able to analyze all input and output traffic. The total number of possible perfect matchings in a system is $t!$.

2.1.2 Some Attack Examples

The concept of black box attacks depends on the simple fact that no matter how well the system has been designed, when two users communicate persistently, a global adversary will

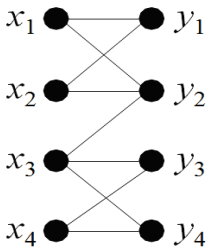
determine the sending and receiving parties by correlating the communication pattern. When it comes to attacks on anonymity systems, a number of attacks have been proposed over the years for a black box system, almost as many as the number of systems available to mitigate those. Berthold et al. [7] proposed some active and passive attacks on a mixed network. One such attack presents the case where a black box system first stores all messages and then randomizes and sends them in random order. Here they try to determine the sender of a stream of messages by intersecting the senders' anonymity set of consecutive messages, i.e., blocking certain messages to reveal the communication pattern. A similar technique was used by Kesdogan et al. [8], which basically tries to determine the number of observations required to break an anonymity system and is related to the method presented by Berthold et al. [7].

Two attacks mentioned by Serjantov and Danezis [1] and Edman et al. [3] are discussed in further detail in this section. In the first, which is a timing analysis attack provided by Edman et al. [3], an adversary notes the time at which the message enters and exits the system, and cross-references it by the minimum and maximum latency time defined by the system.

For example, consider a system with a minimum and maximum latency of 1 and 4 time units, i.e., any message that enters the system must go out between that given time window. As shown in Figure 2(a), if a total of four messages enter a system with their corresponding entry and exit times, y_1 and y_2 are the only possibilities for x_1 because the other options lie outside the defined latency window. If this analysis is continued, then an attacker will have a reduced bipartite graph, as shown in Figure 2(b), with edges connected only to the possible perfect matchings in the system. Finally, the graph is converted into a biadjacency 0-1 matrix having input messages represented by each row and output messages represented by each column, which can be seen in Figure 2(c).

Entry times	Exit times
$x_1 = 1$	$y_1 = 4$
$x_2 = 2$	$y_2 = 5$
$x_3 = 4$	$y_3 = 7$
$x_4 = 5$	$y_4 = 8$

(a)



(b)

	y_1	y_2	y_3	y_4
x_1	1	1	0	0
x_2	1	1	0	0
x_3	0	1	1	1
x_4	0	0	1	1

(c)

Figure 2: (a) Entry and exit time of messages as observed by attacker, (b) graph for attack, (c) corresponding biadjacency matrix.

One factor used to identify a message passing on the wire is its size. If each message sent has a different packet size and an adversary is able to listen to all incoming and outgoing messages and the origin of the message can easily be identified, then this defeats the purpose of anonymity. To counter this type of eavesdropping, anonymity systems use padding to ensure that all messages are the same size. Such a technique has its pros and cons. Too much padding increases the size of the message and therefore utilizes too much bandwidth, and too little padding, or stripping, makes the message short and requires more processing on the receiving end. The amount of padding used is another research topic and out of the scope of this thesis.

Anonymity systems usually send information about all nodes that need to be traversed within the message, making it a fixed length for some required padding limit. Consider a system with three nodes, as shown in Figure 3(a), with a route length of two, i.e., each message passes through only two nodes before reaching its destination. Serjantov and Danezis [1] suggested an attack that uses the knowledge of maximum route length with the help of a global adversary to rule out certain edges as infeasible. Consider the mix-node system represented in Figure 3(a) where input messages are represented by $X = \{x_1, x_2, x_3\}$ and output messages are represented by $Y = \{y_1, y_2, y_3\}$. It can be seen that message y_3 can only come from either x_1 or x_2, since the route length allowed by the system is two. Figure 3(b) shows the resulting graph with $\langle x_3, y_3 \rangle$ being removed as infeasible. A biadjacency matrix representation is shown in Figure 3(c).

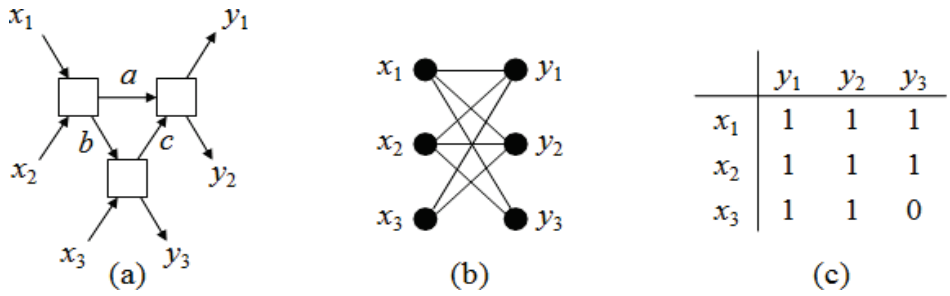


Figure 3: (a) Route length attack, (b) graph showing only feasible edges with the help of attack, (c) biadjacency matrix of graph.

2.1.3 Anonymity Metric

A system's anonymity level can be measured by the number of feasible perfect matchings remaining in a system after an attack. It has been known that counting the remaining perfect matchings in a bipartite graph will result in a number that is equivalent to the permanent of its biadjacency matrix as shown by Asratian et al. [9]. The permanent of any $k \times k$ matrix M can be defined as

$$\text{per}(M) = \sum_{\emptyset \in \Phi_k} M_{1\emptyset(1)} M_{2\emptyset(2)} \dots M_{k\emptyset(k)}$$

where Φ_k is the set of all bijections $\emptyset : \{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, k\}$, which is the permutation of k positive integers.

For any bipartite graph G, at least one perfect matching relates to the actual matching between messages sent and messages received, in which case the equivalent matrix will have one in each of its rows and columns that signifies no anonymity on the part of the system, with the minimum value of the permanent of A being 1. The maximum number of perfect matchings on the other hand will be $t!$, which is when the attacker is not able to eliminate any edge from the graph, thus making the maximum permanent A being $t!$. Therefore, the total number of perfect matchings in a $t \times t$ matrix A the bound will be $1 \leq \text{per}(A) \leq t!$.

Definition 1: For a given $t \times t$ matrix A, Edman et al. [3] defined the system's degree of anonymity as

$$d(A) = \begin{cases} 0 & if\ t = 1 \\ \dfrac{\log(\mathrm{per}(A))}{\log(t!)} & otherwise \end{cases}$$

The value of $d(A)$ will be 0, if and only if A has only one perfect matching, thus signifying that there is no anonymity in the system, and the value of $d(A)$ will be 1 if no perfect matching has been eliminated as infeasible, thus providing full anonymity.

An example of the above metric can be taken from examples in the previous section. For Figure 2(c), the number of perfect matchings is equal to four out of a total of 4!. Therefore, $\log(4)/\log(4!) \approx 0.436$. Figure 3(c) also has four perfect matchings, but the total possible are 3!; therefore, $\log(4)/\log(3!) \approx 0.774$.

2.2 Sending and Receiving Multiple Messages

The metric presented by Edman et al. [3] focused on the incoming and outgoing messages in the system, i.e., the amount of resistance provided by the system to hide perfect matchings to be identified by the attacker. While the metric provides a good idea about the anonymity of the system studied, if a more real-world scenario is analyzed, the goal of an attacker is to identify a sender-receiver pair rather than an input-output message pair. This idea was presented by Gierlichs et al. [4].

To further understand the difference, consider the graph presented in Figure 2. Since a global adversary is considered, we know that the attacker will have all information outside of the system. In order to identify senders and receivers, consider that the first two messages $\langle x_1, x_2 \rangle$ are sent by *Alice* and the other two messages $\langle x_3, x_4 \rangle$ are sent by *Mary*; subsequently, on the receiving end, y_1 is received by *Bob*, while $\langle y_2, y_3, y_4 \rangle$ are received by *John*. After the attack, the

graph shows that the possible perfect matchings are $\langle x_1, y_1 \rangle$ and $\langle x_2, y_2 \rangle$, which indicates 50% certainty on the part of the attackers that the message could have originated from either x_1 or x_2. In the present case, the attacker knows that both messages $\langle x_1, x_2 \rangle$ were sent by the user *Alice*; therefore, the attacker is 100% sure that the message received by *Bob* was sent by *Alice*, which reduces the overall anonymity of the system significantly.

2.2.1 Sender-Receiver Association

In order to further understand the sender-receiver association with respect to input and output messages, consider the following: If m is the number of senders and n is the number of receivers for any $i \in \{1, 2, 3, \ldots, m\}$ and $j \in \{1, 2, 3, \ldots, n\}$, and if X_i is the set of messages sent by i and Y_j is the set of messages received by j, then it can be said that

$$\sum_{i=1}^{m} |X_i| = \sum_{j=1}^{n} |Y_j| = t$$

Clearly, $\{X_i \times Y_j : 1 \leq m, 1 \leq j \leq n\}$ is a partition of $X \times Y$.

For any subset $E \subseteq X \times Y$ of edges in $K_{t,t}$ the sender-receiver association matrix of E is denoted by $Z(E)$ as the non-negative integers given by

$$Z(E)_{ij} = \left| E \cap \left(X_i \times Y_j \right) \right|$$

Therefore, it can be said that any entry $Z(E)_{ij}$ is the number of edges in E from sender i to receiver j. The sum of all entries in $Z(E)$ is $|E|$.

The total number of perfect matchings in $X \times Y$ is found to be $t!$ out of $2^{(t^2)}$ total subsets. For any given perfect matching E having an association matrix $Z(E)$, an additional property can be observed, i.e., the row and column sums are the same as the sender-receiver multiplicities, i.e.,

$$\sum_{k=1}^{n} Z(E)_{ik} = |X_i|, \qquad 1 \leq i \leq m, \text{ and}$$

$$\sum_{k=1}^{m} Z(E)_{kj} = |Y_j|, \qquad 1 \leq j \leq n$$

In order to define an equivalence relation $\bowtie$ of the set of all perfect matchings between X and Y, consider $\mathfrak{P}$ as the set of all $t!$ perfect matchings since an equivalence relation $\bowtie$ on $\mathfrak{P}$ can be defined as follows:

Definition 2: Let $E_1, E_2 \in \mathfrak{P}$; then E_1 and E_2 are equivalent, denoted by $E_1 \bowtie E_2$, if they have the same association matrix, i.e., $Z(E_1) = Z(E_2)$.

In essence, if the total number of messages sent from the sender to each receiver is the same, then the perfect matchings are considered equivalent. Previously, perfect matchings were considered only between input and output messages, which is irrelevant in this case. Therefore, as defined above, the two subsets of $\mathfrak{P}$ having the same association matrix are considered equivalent.

Now consider two distinct perfect matchings E_1 and E_2 in a system with respect to their input and output messages, as shown in Figure 4. The total number of senders in both is $m = 2$, while the total number of receivers is $n = 3$, and the total number of messages in the system is $t = 5$. The senders $\langle X_1, X_2 \rangle$ send $\langle 2, 3 \rangle$ messages, while the receivers $\langle Y_1, Y_2, Y_3 \rangle$ each receive $\langle 1, 2, 2 \rangle$ messages. The layout as well as row and column sums are shown in the association matrix in Figure 4. While the distribution of input and output messages is different in E_1 and E_2, their association matrices are the same. Each equivalence relation in $\mathfrak{P}$ belongs to an equivalence class. The problem regarding total number of equivalence classes in $\mathfrak{P}$ is discussed next. Also, the total number of perfect matchings in an equivalence class is analyzed to understand the new proposed metric.

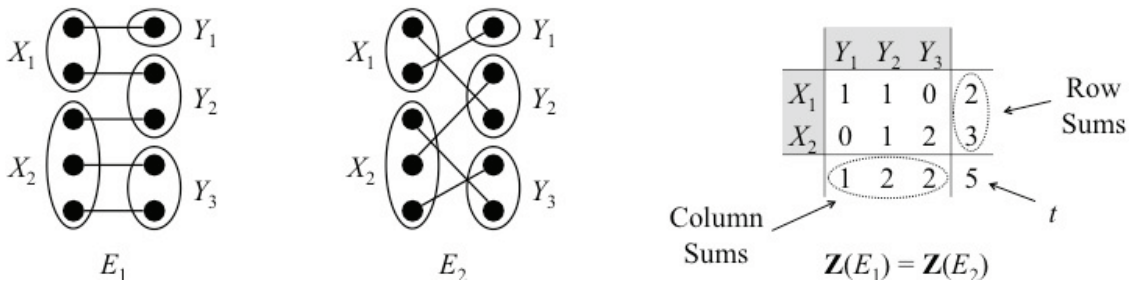


Figure 4: Two equivalent perfect matchings E_1 and E_2 represented by same association matrix.

2.2.2 Number of Equivalence Classes

The number of equivalence classes in a system can be defined as the number of unique association matrices over the set $\mathfrak{P}$. If the sender multiplicities are $S = \langle X_1|, |X_2|, \ldots, |X_m| \rangle$ and the receiver multiplicities are $R = \langle |Y_1|, |Y_2|, \ldots, |Y_n| \rangle$, then all unique $m \times n$ association matrices with S being the row-sum and R being the column-sum vectors represent the total number of possible equivalence classes.

To understand further the complexities of finding an exact number, the work done by researchers must be referenced. The complexity class #P was first introduced by Valiant [10] and is associated with the difficulty of computing the permanent of 0-1 matrices. This class #P consists of the counting version of the decision problem in NP. An example of the problem in NP is as follows: Determine if, in a given list of integers, there exists any subset such that their members add up to a required value. Extending the problem in #P would be to determine the total number of subsets; based on this, any problem in #P is as hard as NP. The exact computation of the permanent of any 0-1 metrics is #P-complete, as introduced by Valiant [10]. Jerrum et al. [11] presented fully polynomial randomized approximation scheme (FPRAS) to approximate the permanent of non-negative matrices. Furthermore, Dyer et al. [12] showed that counting the number of non-negative matrices with some given row and column sum in a

contingency table is #P-complete; while the problem can be tackled with the help of algorithms, they cannot be expected to be polynomial-time algorithms.

Greslin [13] also provided a method, which works recursively to count and generate these kinds of matrices, while Gail and Mantel [14] presented a technique based on recurrence. Grégoire and Hamel [5] presented a method to count the number of classes for a given anonymity system, which was discussed in the technique presented by Macdonald [15].

Surveys regarding the difficulty of a problem and its resolution are presented in Diaconis and Gangolli [16] and Barvinok [17]. Since the exact count is considered to be a very difficult problem Kijima and Matsui [18], Barvinok and Luria [19] and Barvinok and Hartigan [20] presented some techniques to find an approximate answer to such a problem.

2.2.3 Cardinality of Equivalence Class

In this section, a method for counting the number of perfect matchings in a class is discussed. For any given association matrix Z representing a unique equivalence class over the set $\mathfrak{P}$, there could be four possible cases by which the cardinality can be determined. Before describing the cases, consider sender multiplicities as $S = \langle |X_1|, |X_2|, \ldots, |X_m| \rangle$ and receiver multiplicities as $R = \langle |Y_1|, |Y_2|, \ldots, |Y_n| \rangle$.

Case 1: Each sender sends only one message, and each receiver receives only one message; in other words, sender and receiver multiplicities are one. In this case, Z will only be a 0-1 matrix having exactly 1 in all its rows and columns. The total number of perfect matchings will be $t!$, and the number of classes will be the same; therefore, each class in this case will have only one perfect matching.

Case 2: In this case, consider multiplicities on the sender side only, i.e., at least one sender sends multiple messages, while all receivers receive only one message, each $m < t = n$.

Looking at the association matrix Z, the property distinguishing this case is that all the column-sums are 1, i.e., having 1 in each of its column while there might be some rows having multiple inputs showing some sender receiving multiple messages. Now for any given association matrix Z, consider arbitrarily the i^{th} row with $k = |X_i|$ number of 1's in columns $\{j_1, j_2, j_3, \ldots, j_k\}$, with the total number of 1's representing the total messages sent by some sender. The k messages sent by this sender can be sent to the same receivers using any of $k!$ ways, while the association matrix will remain the same. The number of perfect matchings with such association matrix will be

$$\prod_{i=1}^{m} |X_i|!.$$

All equivalence classes in this case will be the same size based on sender multiplicities S and irrespective of Z.

Case 3: This case is similar to the second case in that instead of sender multiplicities there are receiver multiplicities, i.e. all senders will send only one message, represented by only one 1 in each row, while there will be some receivers receiving multiple messages showing multiple 1's in some columns, i.e., $m = t < n$. The number of perfect matchings in this case will be

$$\prod_{j=1}^{n} |Y_j|!.$$

Case 4: This case generalizes cases 1 and 2, when some sender transmits multiple messages, while some receiver gets multiple messages, i.e., $m < t > n$. In this case, for any given Z, start from the top left corner, represented by Z_{11} , i.e., the number of messages sent from the first sender to the first receiver, and move toward the bottom right. Now, the number of

messages sent by $|X_1|$, i.e., the total number of messages sent by the first sender or Z_{11} messages, can be chosen in the following ways:

$$\binom{|X_1|}{Z_{11}} \text{ that is } \binom{\sum_{k=1}^{n} Z_{1k}}{Z_{11}}$$

Also, out of the total number of messages received by the first receiver $|Y_1|$, the selected Z_{11} messages can be chosen in the following ways:

$$\binom{|Y_1|}{Z_{11}} \text{ that is } \binom{\sum_{k=1}^{m} Z_{k1}}{Z_{11}}$$

After identifying the exact Z_{11} sent and received messages between the first sender and first receiver, there will be a total of $Z_{11}!$ perfect matchings; therefore, the total number of ways Z_{11} messages can be sent from the first sender to the first receiver will be

$$\binom{\sum_{k=1}^{n} Z_{1k}}{Z_{11}}\binom{\sum_{k=1}^{m} Z_{k1}}{Z_{11}} Z_{11}!$$

Similarly moving to the second column yields Z_{12}. By applying the above-mentioned method, since Z_{11} has already been chosen, there will be a choice of $|X_1|$ - Z_{11} messages only, i.e., $\sum_{k=2}^{n} Z_{1k}$, making the possible number of ways in this case to be

$$\binom{\sum_{k=2}^{n} Z_{1k}}{Z_{12}}$$

Accordingly, the number of ways Z_{12} messages that can be sent from the first sender to the second receiver will be

$$\binom{\sum_{k=2}^{n} Z_{1k}}{Z_{12}}\binom{\sum_{k=2}^{m} Z_{k2}}{Z_{12}} Z_{12}!$$

By continuing with this pattern, it is possible to calculate the cardinality of any given association matrix *Z*. The same technique shown above can be used to derive a general expression, in this case, the number of ways Z_{ij} messages can be sent by any sender *i* to receiver *j* and depicted by a complete association matrix, as shown in Figure 5. Generalizing the equation

of the number of ways all messages belonging to an association matrix Z being sent or received in the system or formally the cardinality of an equivalence class Z over the set $\mathfrak{P}$ can be computed by

$$\prod_{i=1}^{m}\prod_{j=1}^{n}\binom{\sum_{k=j}^{n} Z_{ik}}{Z_{ij}}\binom{\sum_{k=i}^{m} Z_{kj}}{Z_{ij}} Z_{ij}!$$

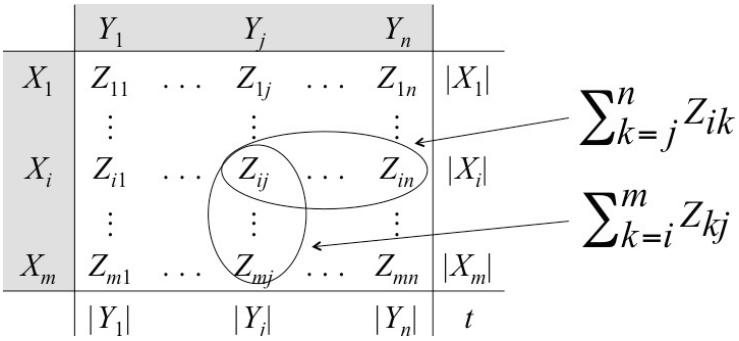


Figure 5: Generalized association matrix Z.

As an example, the association matrix in Figure 4 will result in a cardinality of 24, i.e., the total number of perfect matchings is 24, of which 2 are shown in Figure 4.

CHAPTER 3

A NEW METRIC

The basic goal of a metric for an anonymity system is to provide an accurate measure of the amount of anonymity present in a system. If an attack is induced in a system, the metric should be able to measure the amount of difficulty to de-anonymize a sender-receiver communication such that a sender and receiver can be distinctly identified based on the messages exchanged. The metric presented in this chapter will consider a two-step attack.

As discussed in Chapter 2, under the attack example, an adversary would use certain methods to render some of the perfect matchings in a system as infeasible based on the messages being sent and received, thus resulting in a $t \times t$ biadjacency matrix A of the entire system. The second attack would involve a global adversary that would monitor each input and output message of the anonymity system. This results in an accurate understanding of the sender and receiver multiplicities S, R by an attacker.

It should be noted at this point that these attacks are independent of each other and have an adverse effect on the system's anonymity, even if considered alone, whereas the new metric discussed here measures their combined effect.

The combined effect of these attacks was first demonstrated and presented by Gierlichs et al. [4] because they provided a metric to compute such a problem, but Chapter 4 will discuss further that their metric only works for a small class of biadjacency matrices. Additionally, the effect of multiplicity vectors on the anonymity system without considering biadjacency matrices was presented by Grégoire and Hamal [5].

To sum up the understanding of previous discussion and its effect on computing an accurate systemwide metric as well as the effects of the attacks discussed, consider the perfect matchings shown in Figure 6.

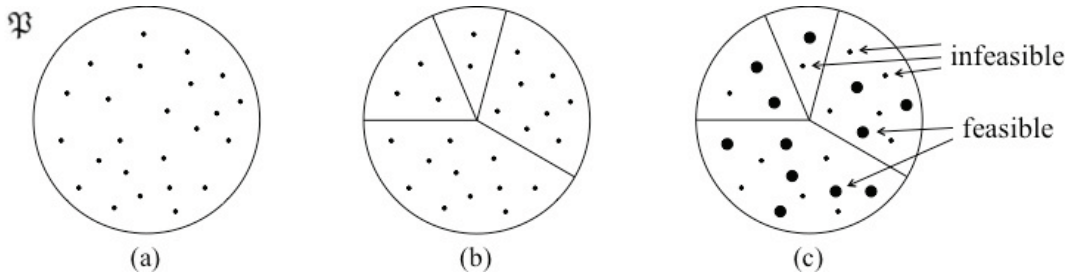


Figure 6: (a) Set of all $t!$ perfect matchings, (b) equivalence classes induced by multiplicity vectors S and R, (c) feasible and infeasible perfect matchings after introduction of biadjacency matrix.

Figure 6(a) shows $\mathfrak{P}$ as the set of all $t!$ perfect matchings in an anonymity system. Figure 6(b) shows the effect of inducing equivalence relations $\bowtie$ over the set $\mathfrak{P}$ by introducing senders and receivers along with their multiplicity vectors S and R. As discussed in Chapter 2, each class is represented by its unique association matrix having S and R as its row and column sum vectors. The total number of perfect matchings in each such association matrix Z can be determined using the expression given in Chapter 2. At this point, if no infeasibility attack is introduced in the system, the class size will lead to probability distribution over all possible association matrices, which can be used to measure anonymity by applying a method such as Shannon entropy. Figure 6(c) shows the state of the system after an infeasibility attack, showing feasible and infeasible perfect matchings. The attack conducted here produces a biadjacency matrix A, which essentially shows that if any message from a sender to a receiver is not possible, then some of the perfect matchings will be rendered as infeasible. In essence, what this attack has done is provided a new measurement, i.e., the number of feasible matchings in a class instead of the raw size of the class.

Equivalence classes are induced in order to group perfect matchings belonging to same

sender receiver communication. Each equivalence class represents a distinct sender receiver communication pattern. Each possible distinct association matrix with fixed row and column sum based on multiplicity vectors represent an equivalence class. By grouping perfect matchings based on sender receiver multiplicities the uncertainty for an attacker is reduced significantly and hence resulting in lower anonymity. The number of perfect matchings in an equivalence class reduces when a biadjacency attack is performed by an attacker. The number of feasible perfect matchings left in an equivalence class which is the weight of that equivalence class now shows the uncertainty of an attacker that the actual perfect matching lies in that class. The sum over all equivalence classes leads to the uncertainty remaining in the system.

The number of equivalence classes in a system is essentially the number of non-negative $m \times n$ integer association matrices having S and R as their row and column sums, which are induced by multiplicity vectors S and R over the set $\mathfrak{P}$. Let $\mathbb{Z}_{S,R}(\mathfrak{P})$ represent the set of all association matrices of perfect matchings in $\mathfrak{P}$. The attack performed on the set $\mathfrak{P}$ resulted in a $t \times t$ biadjacency matrix A. For any association matrix $Z \in \mathbb{Z}_{S,R}(\mathfrak{P})$, the weight assigned following the results of the biadjacency matrix A represented by $\mathcal{W}_A(Z)$ is the number of feasible perfect matchings in the equivalence class associated by Z, the sum of which, over all such association matrices, will add up to become the per(A), which is the total number of perfect matchings marked feasible by the attacker. Therefore, it can be said that

$$\sum_{Z \in \mathbb{Z}_{S,R}(\mathfrak{P})} \mathcal{W}_A(Z) = \mathrm{per}(A)$$

The method for calculating the weight is further explained in the next section of this chapter, while here, we consider the normalized weight as the amount of feasible perfect matchings present in each class represented by Z; therefore, $\omega_A(Z) = \mathcal{W}_A(Z)/\mathrm{per}(A)$. The value of $\omega_A(Z)$ will add up to 1 over all Z and is basically a probability distribution; therefore,

for any given association matrix Z, $\omega_A(Z)$ represents the confidence of an attacker being able to find the required perfect matching to de-anonymize the system.

At this point, the well-known Shannon entropy of a probability distribution is used, because it is considered a well-accepted method for calculating the degree of anonymity, as shown by Serjantov and Danezis [1] and Diaz et al. [2].

Definition 3: Let a $t \times t$ biadjacency matrix A and multiplicity vector S and R be the result of an attack. The system's degree of anonymity after the attack can be defined as

$$\delta_{S,R}(A) = \begin{cases} 0 & \text{if } t = 1 \\ \dfrac{-\sum\{\omega_A(Z)\,.\log\big(\omega_A(Z)\big) : Z \in \mathbb{Z}_{S,R}(\mathfrak{P})\}}{\log(t!)} & \text{otherwise} \end{cases}$$

The above expression is employed upon all probability distributions $Z \in \mathbb{Z}_{S,R}(\mathfrak{P})$ given by $\omega_A(Z)$ to calculate the attacker's uncertainty, where Z represents the actual sender-receiver communication. The above expression presents the same output as that of Edman et al. [3], which is defined in *Definition 1*, with the sender-receiver multiplicities being 1, and as the multiplicities grow, the anonymity value decreases. The given Proposition 1 below can be proven by the definitions.

Proposition 1: For all S, R, and A, $\delta_{S,R}(A) \leq d(A)$, with equality iff all multiplicity values in S and R are 1.

Proof: Let L be number of equivalence classes which means that exactly L values in a probability distribution of weights will be $1/L$. As $Z \in \mathbb{Z}_{S,R}(\mathfrak{P})$, the corresponding values of Z are exactly the ones that have nonzero weights which are further normalized. By definition of log and algebraic substitution we can say that

$$-\sum_{i=1}^{L}\left(\frac{1}{L}\right).\log\left(\frac{1}{L}\right) = \log(L)$$

similarly by monotonicity function of log we can say $\log(L) \leq \log(\text{per}(A))$. Now we need to show that

$$-\sum_{Z \in \mathbb{Z}_{S,R}(\mathfrak{P})} \omega_A(Z) \,.\log\big(\omega_A(Z)\big) < -\sum_{i=1}^{L} \left(\frac{1}{L}\right).\log\left(\frac{1}{L}\right)$$

Although this property of Shannon entropy is well-known in information theory following is a short proof. It is easily seen that, for all $\beta > 0$, we have $2\beta \leq 2\beta$, with equality iff $\beta = 1$. Taking log to the base 2 gives $1 + \log(\beta) \leq \beta$. By substituting $\beta = (1/L)/\,\omega_A(Z)$, and simplifying, we get that for all $Z \in \mathbb{Z}_{S,R}(\mathfrak{P})$, $\omega_A(Z) - \omega_A(Z) \,.\log(\omega_A(Z)) \leq (1/L) - \omega_A(Z) \,.\log(1/L)$, with equality iff $\omega_A(Z) = 1/L$. The resulting simplified form will be,

$$-\sum_{Z \in \mathbb{Z}_{S,R}(\mathfrak{P})} \omega_A(Z) \,.\log\big(\omega_A(Z)\big) \leq -\sum_{i=1}^{L} \left(\frac{1}{L}\right).\log\left(\frac{1}{L}\right) = \log(L) \leq \log\big(\text{per}(A)\big)$$

which is the numerator of the metric given in *Definition 1* while the denominator remains the same. ■

3.1 Weight of Equivalence Class

In this section, in order to complete the expression for the new metric defined in the previous section, an expression will be developed for the weight of an equivalence class $\mathcal{W}_A(Z)$, given a $t \times t$ biadjacency matrix A and an $m \times n$ association matrix Z.

During discussion in the previous section and in Chapter 3, an association matrix Z was introduced, the row-sum of which represents the system's sender multiplicity $S = \langle |X_1|, |X_2|, |X_3|, \ldots, |X_m| \rangle$, and the column sum represents the receiver multiplicity represented by vector $R = \langle |Y_1|, |Y_2|, |Y_3|, \ldots, |Y_n| \rangle$. Similarly, in terms of a biadjacency matrix A, the rows representing the senders will have $|X_1|$ as their first sender with any given multiplicities in the number of rows, while the next sender will be represented by $|X_2|$, and so on. On the columns' side, $|Y_1|$ will

represent the messages received by the first receiver and will have any multiplicity represented by the number of columns; the next receiver will be represented by $|Y_2|$, and so on. Permutation of rows and/or columns at this point will not affect the results of computing the weight.

Considering the two matrices defined, the first row and column in the association matrices will represent the first partition in the $t \times t$ biadjacency matrices A, denoted by $\mathrm{Reg}_{(A;i\to j)}$, for $1 \le i \le m$ and $1 \le j \le n$, such that the matrix A is divided into mn different regions. Each region $\mathrm{Reg}_{(A;\, i\to j)}$ represents a submatrix of A having $|X_i|$ contiguous rows and $|Y_j|$ contiguous columns, as shown in Figure 7(a). As with the biadjacency matrix A, the selected region will provide the feasibility of perfect matchings based on attack related to the chosen subset $X_i \times Y_j$.

For the purpose of calculating the weight using permanent, square submatrices belonging to the regions in A are needed. Consider s as the row and column index set of the biadjacency matrix represented from the set $\{1, 2, 3, \ldots, t\}$, with I and J representing the row and columns, respectively. To represent any given $s \times s$ submatrix of A, i.e., essentially an *s-extract*, we will use the term $A[\![I; J]\!]$, showing an extract of A represented at row numbers I and column numbers J, as shown in Figure 7(b). Therefore, in essence, the indices in I and J represent the corresponding location of input and output messages in any order represented by the s-extract $A[\![I; J]\!]$. The total number of feasible ways to achieve this correspondence will be $\mathrm{per}(A[\![I; J]\!])$, where $0 \le \mathrm{per}(A[\![I; J]\!]) \le s!$.

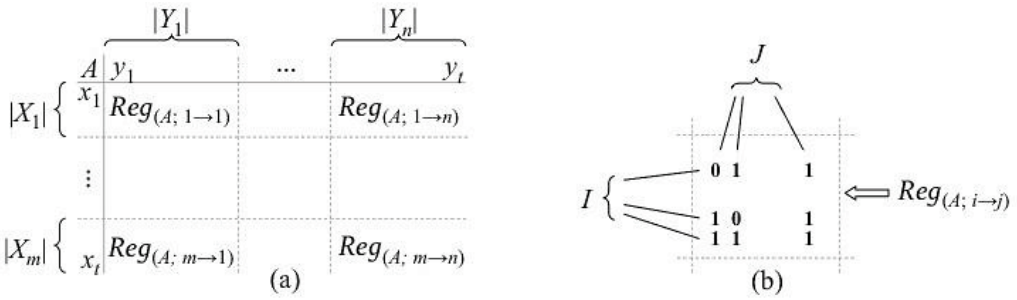


Figure 7: (a) Representation of *A* regions, (b) example of three extracts completely contained within a region.

For the purpose of computing the weight in this thesis, the chosen *s-extracts* are considered if they are contained within the region, depicted as $\text{Reg}_{(A;\ i\to j)}$, which is possible if the following conditions are met:

- $I \subseteq \{c + \sum_{k=1}^{i-1}|X_k| : 1 \le c \le |X_i|\}$
- $J \subseteq \{c + \sum_{k=1}^{j-1}|Y_k| : 1 \le c \le |Y_j|\}$

This essentially means that *I* and *J* should correspond to the region representing the sender and receiver correspondences. While *s-extract* can overlap in multiple regions, only the above-mentioned conditions will be considered, which is based on Z_{ij}-extract of a given association matrix *Z* representing the corresponding region, an example of which is shown in Figure 7(b), where the value of $Z_{ij} = 3$. The total number of extracts is the number of ways in which Z_{ij} rows and columns are chosen from a specified region $\text{Reg}_{(A;\ i\to j)}$, or

$$\binom{|X_i|}{Z_{ij}}\binom{|Y_j|}{Z_{ij}}$$

The set of all such Z_{ij}-extracts can be denoted as $\mathcal{E}_{(A;\ i\to j)}$, which are contained within the region $\text{Reg}_{(A;\ i\to j)}$. The following proposition can be derived based on the above discussion:

Proposition 2: With respect to *A*, the total number of feasible ways of sending Z_{ij} messages from sender *i* to receiver *j* is

$$\sum_{A[\![I;\ J]\!] \in \mathcal{E}_{(A; i \to j)}} \text{per}(A[\![I;\ J]\!])$$

Proof: As discussed above, the set of all Z_{ij}-extracts contained in a region is denoted by $\mathcal{E}_{(A;\, i \to j)}$, while each field in a region $\text{Reg}_{(A;\, i \to j)}$, i.e., the messages sent from sender i to receiver j with a value of 1, represents a possible sender-receiver communication. The possible feasible communication between a sender and receiver is denoted by $\text{per}(A[\![I;\ J]\!])$, which is one of the feasible communications between sender *i* and receiver *j*. The sum of all such possible communication patterns contained in $\text{Reg}_{(A;\, i \to j)}$ will result in the total number of feasible perfect matching's between a sender and a receiver. ■

The above expression represents any given single sender-receiver correspondence. In order to compute the weight $\mathcal{W}_A(Z)$ of a given equivalence class represented by an association matrix *Z*, a product of all such sums can be employed to get the final result.

At the time of selecting a Z_{ij} extract, it should be considered that any selection $A[\![I;\ J]\!] \in \mathcal{E}_{(A;\, i \to j)}$ would render all input messages represented in *I* unavailable to receivers other than *j*, and the received messages represented by *J* unavailable to senders other that *i*. Therefore, as a precautionary measure, all rows and columns of matrix *A* as represented by *I* and *J* can be marked as zero for all of the following computations.

To represent the new matrix, based on the above condition, i.e., zeroing the row and columns of computed extracts for any given extract $A[\![I;\ J]\!]$, the new representation can be supposed as $\hat{A}[\![I;\ J]\!]$, which would be identical to *A* in all other values. It can be said that

$$\hat{\text{A}}[\![I;J]\!]_{pq} \begin{cases} 0 & if\ p \in I\ or\ q\ \in J, \\ A_{pq} & otherwise. \end{cases}$$

The resulting new matrix with at least one row from *I* and/or column from *J* zeroed will result in per $\hat{A}[\![I;\ J]\!]$ of zero, which in turn will result in avoiding duplicate counting and in only

considering a single perfect matching scenario. Therefore, one input message will result in only one output message. Similarly, the element present at row *i* and column *j* of the association matrix *Z* will be zeroed, which will result in a new matrix represented by $\hat{\mathrm{Z}}[\![I; J]\!]$; therefore, as with the case of biadjacency matrix for the association matrix, it can be said that

$$\hat{\mathrm{Z}}[\![\mathrm{I};\mathrm{J}]\!]_{pq}\begin{cases} 0 & if\ p = i\ or\ q = j, \\ Z_{pq} & otherwise. \end{cases}$$

Finally, the expression for the number of feasible perfect matchings in an equivalence class associated with an association matrix *Z* can be derived by taking the product of all feasible sender-receiver-based input-output combinations partitioned by $A[\![I; J]\!]$ and using them recursively until all Z_{ij} are 0.

$$\mathcal{W}_A(Z) = \begin{cases} \sum_{A[\![I;\ J]\!] \in \mathcal{E}_{(A;i\to j)}} \left[\ \mathrm{Per}\ (A[\![I;\ J]\!]).\mathcal{W}_{\hat{\mathrm{A}}[\![I;\ J]\!]}\left(\hat{\mathrm{Z}}[\![I;J]\!]\right)\right] & if\ Z_{ij} \neq 0, for\ some\ i\ and\ j \\ 1 & otherwise. \end{cases}$$

In the above expression, the depth of recursion is the number of nonzero entries in *Z*. Also, since the association matrix is partitioned into regions, any Z_{ij}-extract can be computed and finally summed up with all other extracts to obtain the final value of $\mathcal{W}_A(Z)$.

CHAPTER 4

COMPARISON WITH EXISTING APPROACHES

Looking at similar work to that which was done in this thesis, a couple of significant research papers have been quoted throughout this paper. This chapter closely compares and highlights the difference in approaches taken by those researchers and some issues associated with their approaches. As discussed, Edman et al. [3] were the first to provide a metric based on the number of messages in a system, while Gierlichs et al. [4] enhanced the metric to accommodate senders and receivers instead of messages, because that would be the ultimate goal of an attacker. In this chapter, it will be shown that the metric of Gierlichs et al. [4] is only applicable to a small class of biadjacency matrices. The other noticeable work was done by Grégoire and Hamel [5] who proposed a method to quantify the number of equivalence classes. Their method used the *COUNT* function to obtain the number of equivalence classes, but they did not considered any biadjacency metric. The method proposed by Grégoire and Hamel [5] also appeared in Macdonald [15] and was summarized by Diaconis and Gangolli [16].

4.1 Metric of Gierlichs et al. [4]

As discussed in the previous chapter, the equivalence relation is based on sender and receiver multiplicity vectors only, which are $\langle S, R \rangle$ and are produced over the set $\mathfrak{P}$ of all possible perfect matchings, i.e., $t!$ It is because of this property that the size of any equivalence class also depends on the same. After an attacker concludes its biadjacency matrix and predicts the feasible and infeasible perfect matchings, the weight assigned to any class is calculated in order to determine the degree of anonymity. Gierlichs e al [4] used a single-layered approach, defining an equivalence relation ~ over the set $\mathfrak{I}$ of all per(A) feasible perfect matchings induced by sender multiplicity, receiver multiplicity, and a given biadjacency matrix. Looking at a higher

level, the definition and function of both as well the resulting metric seems to be the same, but the primary difference is that theirs is based on the size of classes of (~), which are in essence weights of the corresponding classes of ⋈. The method provided by Gierlichs et al. [4] to calculate the size of an equivalence class is only limited to a small class of leveled biadjacency matrices, which significantly limits the scope of the metric, especially when the sender and receiver multiplicities increase.

At this point, it is important to define the term "leveled," which is the reason for limitation and shrinking of the scope first presented by Edman et al. [3]. For any given $t \times t$ biadjacency matrix A with any sender i and receiver j, the $\mathrm{Reg}_{(A;\, i \to j)}$ is leveled if all the elements present in them are either both 0's or both 1's and all mn regions in the biadjacency matrix A are leveled. The total number of such leveled matrices will be 2^{mn} and will shrink once the multiplicities begin to grow.

The method proposed by Gierlichs et al. [4] to compute the size of any given class thus depends on the leveled property and does not consider the case where the biadjacency matrix differs at the message level. Two special cases were discussed by Gierlichs et al. [4], i.e., first, having only sender multiplicity while receiver multiplicity is set to 1, and second, having only receiver multiplicity while sender multiplicity remains 1. A general case was also discussed, where both sender and receiver multiplicities are considered and is calculated by an algorithm. They made the following assertion for the first case:

Assertion 1: If $|Y_j| = 1$ for all j, $1 \leq j \leq n$, then all equivalence classes of ~ are of equal size, given by $\prod_{i=1}^{m} |X_i|!$.

In order to understand the missing cases from the set as a result of the above assertion, consider the examples presented in Figure 8. As shown in Figure 8(a), the number of senders m =

1, number of messages $t = 2$, and sender multiplicity $S = \langle 2 \rangle$ while per(A) = 1. As can be seen, the total number of equivalence classes is 1, since there is only one feasible perfect matching and the size of this class is also one.

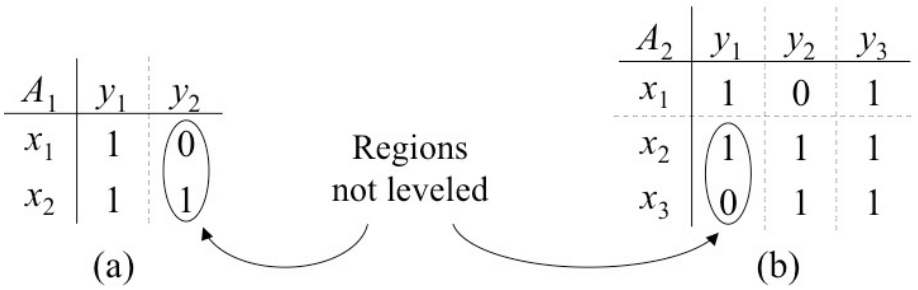


Figure 8: Counter examples of *Asssertion 1* by Gierlichs et al. [4].

Using the assertion by Gierlichs et al. [4], in this case, the size of the class would be $\prod_{i=1}^{1}|2|! = 2$, which is incorrect. Similarly, if we look at the second example, represented in Figure 8(b), in this case, where the total number of senders $m = 2$, number of messages in the system $t = 3$, sender multiplicities $S = \langle 1, 2 \rangle$, and the permanent is per(A_2) = 3, these three perfect matchings are divided into two different equivalence classes of unequal sizes. Using the assertion by Gierlichs et al. [4], again $\prod_{i=1}^{2} 1! \,.\, 2! = 2$, which is different from the actual case, showing that assertion 1 is only viable if A is all leveled; if one of the elements in a given region is different, then assertion 1 will not work. This is given in the *Proposition 3*.

Proposition 3: If $|Y_j| = 1$, for all j, $1 \leq j \leq n$, then all equivalence classes of ~ are of equal size, given by $\prod_{i=1}^{m}|X_i|!$, iff A is leveled.

Proof: When all receiver multiplicities are equal to 1, i.e., $|Y_j| = 1$, the width of all regions will be restricted to one column. Considering the case where A is not leveled, the region indicating the sender s and receiver r represented as $\mathrm{Reg}_{(A;\, s \to r)}$ contains at least one 1 and one 0. The feasible perfect matching in this case will be the one corresponding to the 1 value in the

biadjacency table. If *C* is considered to be the equivalence class of the specified perfect matching, then |*C*| is at most $(\prod_{i=1}^{s-1} |X_i|!). k! . (\prod_{i=s+1}^{m} |X_i|!)$, which is smaller than $\prod_{i=1}^{m} |X_i|!$. ■

The second case, where the sender multiplicities are restricted to one and some receiver multiplicities are more than one, can be proven by symmetric reasoning that $\prod_{i=1}^{n} |X_j|!$ only holds true if *A* is leveled. The third case, which considers both sender and receiver multiplicities, is computed using an algorithm, which, looking closely at Line 9 of the work of Gierlichs et al. [4], works only if the condition of *A* being leveled is fulfilled and Line 5 corresponds to the same scenario when there is only one sender or receiver. From the above discussion, it has been shown that the metric presented by Gierlichs et al. [4] works only when *A* is leveled, while the weight calculation metric proposed in Chapter 3 works in all cases.

The complete discussion above and the comparison of the method proposed in this thesis with the method proposed by Gierlichs et al. [4] shows the major difference in the scope of the metric that is being presented. In order to understand more precisely, Figure 9 represents the different sets of biadjacency metrics. In this figure, Ψ is the set of all $t \times t$ biadjacency matrices, and $|\Psi| = 2^{(t^2)}$, where their permanents are non-negative integer values up to *t*!. The notation $\Psi_{>0}$ represents all matrices in Ψ whose permanents are greater than 0, i.e., all non-negative integer matrices whose permanents are at least one. This means that there is at least one feasible perfect matching that represents the system's actual communication, which was initially represented by Edman et al. [3]. This is also the base case that should be covered for any metric that extends the metric of the work of Edman et al. [3]. The notation Ψ_0 shows the estimated number of matrices of the biadjacency, which has a permanent equal to 0, which helps in estimating the number of matrices that have permanents greater than 0. The notation Ψ_{00} represents a subset of Ψ_0 that contains all matrices, which have at least one row or column, the sum of which adds up to 0, i.e.,

all elements in that row or column are marked zero. It should be noted at this point that when *t* is large, almost all matrices in Ψ_0 also exist in the Ψ_{00} set, as presented by Erdos and Renyi [21]. Therefore, it can be said that $\Psi_0 \approx \Psi_{00}$, which, as stated above, helps in providing an estimate of the number of matrices with permanents greater than 0. Finally, Ψ_L represents a set of all matrices that are leveled, as discussed previously in this section. The total number of such matrices is 2^{mn}, where *m* and *n* are the number of senders and receivers, respectively, while the set depends on the multiplicity vectors *S* and *R*. If the sender and receiver all have multiplicities equal to 1, then $\Psi_L = \Psi$, while on the other side, if the multiplicities increase, *m*, *n*, and Ψ_L will shrink, as shown in Figure 9.

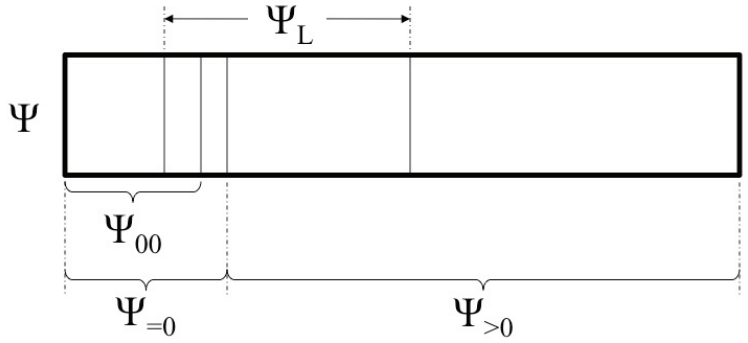


Figure 9: Scope of new method compared with that of Gierlichs et al. [4].

Since the metric presented by Gierlichs et al. [4] only works for Ψ_L, it is not able to cover the complete scope set forth by Edman et al. [3]; therefore, the extension of the metric does not completely satisfy the scope. The metric presented in this thesis, however, does this, as described in Chapter 4.

4.2 Metric of Grégoire and Hamel [5]

The metric proposed by Grégoire and Hamel [5], in essence, only provides a system maximum anonymity, because they have not considered any biadjacency matrix. The final metric presented by Grégoire and Hamel [5] is log(*COUNT*)/log(*t*!), where the term *COUNT* represents

the calculated number of equivalence classes $\bowtie$, as described in previous chapters. The assumption made in calculating the metric is that the biadjacency matrix A contains all 1's, which is not usually the case. The method described in Grégoire and Hamel's paper for calculating the *COUNT* function based on counting the number of non-negative integer matrices resulting from a unique row and column sum was first proposed by Macdonald [15]. Furthermore, the summarization of the function and its use is given by Diaconis and Gangolli [16].

From discussion presented in previous chapters, it can be seen that the value provided by *COUNT* cannot be used as a basis for deriving any proposed metric, but after the introduction of a biadjacency metric and eliminating the infeasible perfect matchings, a metric can be found that will actually quantify the amount of anonymity remaining in the system.

4.3 Example of Metric Calculation

In order to understand the metric calculation and the difference in anonymity, an anonymity system will be analyzed, the results will be demonstrated, and the differences relative to sender-receiver multiplicity as discussed in this thesis and without sender-receiver multiplicity as shown by Edman at el [3] will be shown.

Consider a system having four input messages and subsequently four output messages. Let $\{x_1, x_2, x_3, x_4\}$ be the four input messages, and let $\{y_1, y_2, y_3, y_4\}$ be the four output messages. As discussed in Chapters 2 and 3, a two-pronged attack is considered. In the first case, a global adversary is able to look at all incoming and outgoing messages and establish the number of messages sent by each sender and the number of messages received by each receiver, which in this case results in identifying two senders and three receivers with identification of x_1 and x_2 being sent by sender 1, called X_1, and the remaining x_3 and x_4 sent by sender 2, identified as X_2.

Similarly on the receiving side, y_1 is received by receiver Y_1, while y_2 and y_3 are received by Y_2, and finally y_4 is received by receiver Y_3 ; therefore, $X_1 = \{x_1, x_2\}$, $X_2 = \{x_3, x_4\}$, $Y_1 = \{y_1\}$, $Y_2 = \{y_2, y_3\}$, and $Y_3 = \{y_4\}$. The observation results in $m = 2$ with $S = \langle 2, 2\rangle$ and $n = 3$ with $R = \langle 1, 2, 1\rangle$. Looking at the first observation, an attacker will have marked $mn = 6$ natural regions with their corresponding multiplicities and will be able to divide the total number of perfect matchings, i.e., 4! = 24, into equivalence classes, thus resulting in four distinct association matrices with S as their row-sums and R as their column-sums, as shown in Figure 10.

Z

	Y_1	Y_2	Y_3	
X_1	0	2	0	2
X_2	1	0	1	2
	1	2	1	4

	Y_1	Y_2	Y_3	
X_1	1	0	1	2
X_2	0	2	0	2
	1	2	1	4

	Y_1	Y_2	Y_3	
X_1	1	1	0	2
X_2	0	1	1	2
	1	2	1	4

	Y_1	Y_2	Y_3	
X_1	0	1	1	2
X_2	1	1	0	2
	1	2	1	4

Figure 10: Association matrices representing equivalence classes.

At this point, the second part of the attack, as mentioned in Chapter 2, is considered. This will result in a biadjacency matrix A that renders some of the input/output message pairs as infeasible, as shown in Figure 11(a). Combining the two attacks, the biadjacency matrix A is divided into six regions. If the association matrix Z, as shown with a circle in Figure 10, is superimposed on the biadjacency matrix A, the resulting matrix will be as shown in Figure 11(b). The association matrix Z has three nonzero entries: $Z_{12} = 2$, $Z_{21} = 1$, and $Z_{23} = 1$. To determine the weight of this equivalence class $\mathcal{W}_A(Z)$, the method described in Chapter 3 will be used. Any perfect matching in Z is made up of extracts from the defined three regions of A resulting in a 2 ×

2 extract from $\text{Reg}_{(A;\,1\to 2)}$ and a 1 × 1 extract from regions $\text{Reg}_{(A;\,2\to 1)}$ and $\text{Reg}_{(A;\,2\to 3)}$, an example collection of which is shown in Figure 11 (b). The product of the permanents will be

$$(1 \times 1 + 0 \times 1) \times 1 \times 1 = 1$$

Using the method defined in Chapter 3 for the weight of an equivalence class, all perfect matchings can be enumerated and summed up, which in this case will be 1; therefore, the resulting $\mathcal{W}_A(Z)$ will be equal to 1. A similar method can be used to calculate the weight for the other three equivalence classes represented by association matrices Figure 10, resulting in 5, 1, and 2, making the sum of all association matrices to be per(*A*) = 9. To calculate the normalized weight of all these equivalence classes, the total of each will be divided. The normalized weights of all these association matrices ω_A will be {1/9, 5/9, 1/7, 2/9}. Now, using the metric presented in Chapter 3, *Definition 3*, the normalized weights are placed along with their logs and divided by the total number of messages, thus resulting in $\delta_{S,R}(A) \approx 0.499$.

A	y_1	y_2	*y3*	*y4*
x1	1	1	0	1
x2	1	1	1	0
x3	1	0	1	1
x4	0	1	1	1

(a)

A	*y1*	*y2*	*y3*	*y4*
x1	0	**1**	**0**	0
x2	0	**1**	**1**	0
x3	**1**	0	0	1
x4	0	0	0	**1**

(b)

Figure 11: (a) Biadjacency matrix *A* , (b) collection on *A* with respect to *Z*.

Now, the anonymity with respect to the work of Edman et al. [3] is calculated, which is when each user sends only one message and each receiver gets only one message. Considering the same biadjacency matrix presented in Figure 11, the total number of perfect matchings in the system can be enumerated, which in this case is equal to 9. Now, using the metric described in *Definition 1*, d(*A*) = log(9)/log(4!), which yields d(*A*) ≈ 0.6913. As can be seen, the results from

the metric of Edman et al. [3] are significantly higher than the one presented in this thesis, or 0.499.

CHAPTER 5

CONCLUSION AND FUTURE WORK

After an attack, the association between input and output messages might be hidden to an extent, whereupon Edman et al. [3] developed a systemwide anonymity metric. This metric was modified by Gierlichs et al. [4] to incorporate situations in which system users transmit and/or receive multiple messages. Because an attacker's goal is to expose the communication pattern among users in addition to that between messages, modification of the metric by Edman et al. [3] thus becomes a necessity.

In this thesis, a new metric was developed to measure the anonymity of associations between sender and receiver messages following an attack on a system. Here, an equivalence relation is induced when multiple messages are sent and/or received. The equivalence relation takes place on the set of all perfect matchings between input and output messages of the system. In the contribution of this thesis to the method, the number of perfect matchings was computed among those that were considered feasible after an attack in any equivalence class. The number of perfect matchings can be used to develop a probability distribution of the set of all possible communication patterns between senders and receivers. This probability distribution can be solved using the Shannon entropy method of Diaz et al. [2] to determine a systemwide anonymity level.

A metric to calculate the number of perfect matchings was previously proposed in the work of Gierlichs et al. [4], but in this thesis, it was shown that their metric is applicable only to a small group of attacks. It was shown here that with the increase in number of messages sent and/or received by users, the number of perfect matchings decreased using this metric. It was further shown that another metric, determined by Grégoire and Hamel [5], counts only

equivalence classes and does not take the attack into consideration and thus is not an anonymity metric in the first place.

Bagai et al. [22] developed a generalization of the metric proposed by Edman et al. [3], which assigns probabilities to perfect matchings between input and output messages of the system following an attack, rather than declaring them infeasible. Future work could be done on the generalization of the metric proposed in this paper for such attacks. In another work, Bagai and Tang [23] showed that the anonymity of the system can be increased by implementing data-caching in the system model of Edman et al. [3]. Another direction for future work could be an extension of the metric in this paper by incorporating the data-caching ability.

REFERENCES

LIST OF REFERENCES

[1] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proceedings of the 2nd Privacy Enhancing Technologies Workshop*, 2002, pp. 41–53.

[2] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Proceedings of the 2nd Privacy Enhancing Technologies Workshop*, 2002, pp. 54–68.

[3] M. Edman, F. Sivrikaya, and B. Yener, "A combinatorial approach to measuring anonymity," in *Proceedings of the IEEE International Conference on Intelligence and Security Informatics*, 2007, pp. 356–363.

[4] B. Gierlichs, C. Troncoso, C. Diaz, B. Preneel, and I. Verbauwhede, "Revisiting a combinatorial approach toward measuring anonymity," in *Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society*, Alexandria, VA, 2008, pp. 111–116.

[5] J.-C. Grégoire and A. M. Hamel, "A combinatorial enumeration approach for measuring anonymity," 2009, http://arxiv.org/abs/0902.1663 [cited, April 2012].

[6] Michael Reiter and Aviel Rubin, "Crowds: Anonymity for web transactions," *ACM Transactions on Information and System Security (TISSEC)*, pp. 66-92, 1998.

[7] Oliver Berthold, Andreas Pfitzmann, and Ronny Standtke, "The disadvantages of free MIX routes and how to overcome them," in *Designing Privacy Enhancing Technologies Proceedings of International Workshop on Design Issues in Anonymity and Observability*, July 2011, pp. 10-29

[8] Dogan Kesdogan, Dakshi Agrawal, and Stefan Penz, "Limits of anonymity in open enviroments," in *Information Hiding*, Fabien A. P. Petitcolas, Ed. Vol. 2578 of *Lecture Notes in Computer Science*, pp. 53-69, Springer, 2002.

[9] A. Asratian, T. Denley, and R. Haggkvist, *Bipartite Graphs and Their Applications*. Cambridge University Press, 1998.

[10] L. Valiant, "The complexity of computing the permanent," *Theoretical Computer Science*, vol. 8, no. 2, pp. 189–201, 1979.

[11] M. Jerrum, A. Sinclair, and E. Vigoda, "A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries," *Journal of the ACM*, vol. 51, no. 4, pp. 671–697, 2004.

[12] M. Dyer, R. Kannan, and J. Mount, "Sampling contingency tables," *Random Structures & Algorithms*, vol. 10, no. 4, pp.487–506, 1997.

[13] F. Greselin, "Counting and enumerating frequency tables with given margins," *Statistica & Applicazioni*, vol. 1, no. 2, pp. 87–104, 2003.

[14] M. Gail and N. Mantel, "Counting the number of r x c contingency tables with fixed margins," *Journal of the American Statistical Association*, vol. 72, pp. 859–862, 1977.

[15] J. Macdonald, *Symmetric Functions and Hall Polynomial*. *Clarendon Press*, 1979.

[16] P. Diaconis and A. Gangolli, "Rectangular arrays with fixed margins," in *Discrete Probability and Algorithms*, the IMA Volumes in Mathematics and its Applications (vol. 72), D. Aldous, P. Diaconis, J. Spencer, and J. Steele, Eds. Springer-Verlag, 1995, pp. 15–41.

[17] A. Barvinok, "Matrices with prescribed row and column sums," in *Linear Algebra and Its Applications*, 2011, to appear.

[18] S. Kijima and T. Matsui, "Approximate counting scheme for m_n contingency tables," *IEICE Transactions on Information and Systems*, vol. E87-D, pp. 308–314, 2004.

[19] A. Barvinok, Z. Luria, A. Samorodnitsky, and A. Yong, "An approximation algorithm for counting contingency tables," *Random Structures & Algorithms*, vol. 37, pp. 25–66, 2010.

[20] A. Barvinok and J. Hartigan, "An asymptotic formula for the number of non-negative integer matrices with prescribed row and column sums," *Transactions of the American Mathematical Society*, 2011, to appear.

[21] P. Erdos and A. Renyi, "On random matrices," *A Magyar Tudom´anyos Akad´emia Matematikai Kutat´o Int´ezet´enek K¨ozlem´enyei*, vol. 8, pp. 455–461, 1964.

[22] R. Bagai, H. Lu, R. Li, and B. Tang, "An accurate system-wide anonymity metric for probabilistic attacks," in *Proceedings of the 11th International Privacy Enhancing Technologies Symposium (PETS)*, Waterloo, Canada, 2011, pp. 117–133.

[23] R. Bagai and B. Tang, "Data caching for enhancing anonymity," in *Proceedings of the 25th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, Singapore, 2011, pp. 135–142.