A New Information Leakage Measure for Anonymity Protocols

Sami Zhioua

King Fahd University of Petroleum and Minerals
Saudi Arabia
zhioua@kfupm.edu.sa

Abstract. The main goal of anonymity protocols is to protect the identities of communicating entities in a network communication. An anonymity protocol can be characterized by a noisy channel in the information-theoretic sense. The anonymity of the protocol is then tightly related to how much information is being leaked by the channel. In this paper we investigate a new idea of measuring the information leaked based on how much the rows of the channel probabilities matrix are different from each other. We considered each row of the matrix as a point in the n-dimensional space and we used statistical dispersion measures to estimate how much the points are scattered in the space. Empirical results showed that the two proposed measures KLSD and KLMD are sensitive to the modifications of the attacker capabilities and most importantly they are stable when the a priori distribution on the secret events changes. We show that a variant of KLSD coincides with the classical notion of mutual information which gives the latter an interesting geometric interpretation. The same idea of statistical dispersion is used in a new decision function when the protocol is re-executed several times.

1 Introduction

The ubiquitous popularity of the Internet as a means of communication and information dissemination is creating regularly during the last few decades several security concerns. Most of the security efforts have been devoted to the privacy of communications. Although encrypting communication can help protect the privacy of data, the identities of the communicating entities remain generally known. For example, in the Internet Protocol (IP), each IP packet carries the IP addresses of the sender as well as the receiver. Even if this information is made invisible, an attacker can still reveal the identities of the communicating entities by using traffic analysis (e.g. tracking encrypted packets, analyzing the time delays between packets, comparing the payload size, etc.).

A variety of methods have been proposed to provide anonymous connections over the Internet. These include protocols such as Mix based systems [1] Crowds [2], Onion-routing [3], DC-Net [4], Hordes [5], etc. Most of these protocols use the idea of blending into a crowd, that is, hiding a user's action within the actions of many others. On the positive side, this idea suggests that the mere availability of other users offers the actual initiator some degree of deniability. On the negative side, a user may be incorrectly suspected of initiating a message.

In the last decade and with the increasing need to analyze anonymity systems in more formal and mathematical-based approaches, a significant number of works have been

S. Jajodia and J. Zhou (Eds.): SecureComm 2010, LNICST 50, pp. 398–414, 2010.

dedicated to exploring the notion of anonymity from an information-theoretic point of view. In this regard, we see a natural progression from anonymity set [4], to entropy-based measures [6,7] then to mutual information [8] and finally to capacity [9,10]. A detailed account of related work is given in the next section.

In this research, we adopt the same information theory based approach where a protocol is considered as a noisy channel. A noisy channel is a concept from information theory [11] which represents the link between a set of anonymous events A and a set of observable events O. Events in A represent the information to hide from a potential attacker while events in O are the ones that the attacker actually observes. A good anonymity protocol should make it hard to the attacker to guess the anonymous event given the observable event. The extreme case is when the distributions A and O are completely independent. This is called *noninterference* and achieving it, unfortunately, is often not possible because in most of the cases the protocol needs to reveal information about A. For example, in an election protocol, the individual votes should be secret but ultimately, the result of the votes must be made public which reveals information about individual votes. Hence the degree of anonymity of a protocol is tightly related to the amount of information leaked about the anonymous event when an observation is observed.

In information theory, the information leaked by a noisy channel is given by the notion of mutual information which measures the amount of information that one random variable (O) contains about another random variable (A). Recently, Smith [12] showed through an interesting example that when an adversary tries to guess the value of the anonymous event in a single try, an information-leak measure based on Renyi min-entropy [13] is more suitable than mutual information. However, both mutual information and Smith's measure depend on the knowledge of the a priori distribution (the probabilities that a user did some action) while in general this distribution is not known. Capacity on the other hand is an abstraction of mutual information obtained by maximizing over the possible a priori distributions. Unfortunately, it has been argued that the capacity is too strong [14] and there is no analytical formula to compute it for arbitrary channels.

The contributions of this paper are threefold:

- Starting from the fact that a noisy channel can be represented as a matrix of the conditional probabilities $p(o|a)$ for $o \in O$ and $a \in A$, we present a new family of measures based on how much the rows of the matrix are different from each others and we adopt a geometric approach to assess how much the corresponding points in the n-dimensional space are scattered. Empirical analysis show very promising properties of this measure compared to mutual information and Smith's measure. In particular we strongly think that these measures hold the promise of much less dependence on the a priori distribution.
- We illustrate an interesting relationship between the new measure and the classical concept of mutual information. To the best of our knowledge, this is the first time that such geometric interpretation is given to mutual information.
- The same idea of statistical dispersion is used in a new decision function when the protocol is re-executed several times. The decision function turns out to be more reliable than the one based on maximum likelihood (ML).

2 Related Work

Chaum [4] introduced the notion of anonymity set which is the set of users who are likely to be the sender or receiver of a particular message. Naturally, the anonymity of the users increases if the size of the anonymity set increases. Serjantov and Danezis [6] defined the effective set size based on the concept of entropy after they showed that the simple anonymity set is inadequate when not all the users are equally likely to have sent a particular message. For instance, an attacker analyzing emails will assign a lower probability to a German sender of an email in arabic which arrived in Dubai. Diaz et al. [7] proposed independently a similar measure and took the next step in attempting to normalize the entropy and thus define a degree of anonymity as a number between 0 and 1. These two simple entropy measures were the first to explore the anonymity notion from an information theoretic point of view and as such they have since been the subject of various discussions and comparisons. Newman et al. [15] argued that those measures focused on how well protected the actions of a particular user are and do not examine how much protection a system provide to its users collectively. Toth et al. pointed out that by using simple entropy the focus is to quantify how many bits of information an adversary needs in order to perfectly match a message to a respective use [16]. They refer to this approach as global and propose another approach that uses the maximal probability of the distribution that they refer to as local measure and they show through several interesting examples that from the user's point of view, the local approach is more appropriate. The main difference with respect to our approach is that in those works, the measure reflects the lack of information (uncertainty) that an attacker has about the distribution of users whereas in this paper, we focus on measures that reflect the capability of protocol to disguise this information given the attacker's knowledge about the observables. In other words, we focus on the difference between the a priori and a posteriori distributions and not on analyzing the a posteriori distribution only.

In information theory, the notion of mutual information quantifies the information leaked by a noisy channel and can be seen as the difference between the a priori distribution (Shannon) entropy and the a posteriori distribution (Shannon) entropy. In [8], Zhu and Bettati proposed to use mutual information as a measure of anonymity and applied it to several mix based anonymity systems. Recently, Smith [12] showed that if the attacker tries to guess the value of the anonymous event in a single try, mutual information is not a suitable measure. The example he used is very close to the examples of Toth et al. [16]. He proposed then a new information leak measure which is the difference between the Reny Min-entropies [13] of the a priori and a posteriori distributions. The main problem with these two measures, mutual information and Smith's measure, is that they require the knowledge of the a priori distribution which is generally not possible in practice. Channel capacity which is an important notion in information theory have been used as an anonymity measure [9,14]. Capacity is the maximum mutual information over all possible a priori distributions and hence it is an abstraction of mutual information which is independent from the a priori distribution. However, it has been argued that capacity in some cases is too strong and most importantly, for arbitrary channels, there is no analytical formula to compute its value. The best one can do is to approximate it using for example Blahut-Arimoto algorithm [11].

In this paper we still consider an anonymity protocol as a noisy channel which can be represented as a conditional probabilities matrix. The main contribution is to propose a new anonymity measure based on the vector configuration of the matrix. This is to the best of our knowledge the first attempt to establish a connection between the information leaked and the vector configuration of the matrix. Edman et al. [17] proposed an anonymity metric based on the permanent of a matrix. The matrix in their case represents possible input-output correlations in a network of mixes. The permanent of that matrix will give the number of perfect input-output matchings in the system. The main difference with our work lies in the interpretation of the matrix. In their matrix, the inputs are the messages entering a mix node or a mix network and the outputs are the messages leaving the mix. In our matrix, the inputs are information to keep secret and the output are the observations the attacker observes. Newman et al. [15] used a matrix they called traffic matrix to assess how good a Traffic Analysis Prevention (TAP) system is. Intuitively, the matrix will represent all observations made by an attacker in a period of time and if the number of possible matrices is large enough this indicates a good amount of protection. Clearly, this is very different from our interpretation of the matrix.

Finally we mention that Chatzikokolakis et al. [18] proposed to consider the probability of error as a measure of leakage. In our view, this work falls in the same class as [12] and [16].

3 Anonymity Protocols as Noisy Channels

Information theory turns out to be very useful in analyzing anonymity protocols [19,9]. Indeed, an anonymity protocol can be represented as a memoryless noisy channel where the input is the information to be kept secret and the output is the observed events. The attacker's challenge is then to guess the secret information based on the observed event. The set of observables depends on the capabilities of the attacker. So each attack scenario can be represented by a different channel.

A channel is a tuple $(A, O, p(\cdot|\cdot))$ where A is a random variable representing the inputs with n values $\{a_1, \ldots, a_n\}$, O is a random variable representing the outputs (observables) with m values $\{o_1, \ldots, o_m\}$, and $p(o|a)$ is a conditional probability of observing $o \in O$ given that $a \in A$ is the input.

The channel is noisy because an input might lead to different outputs with different probabilities. The probability values $p(o|a)$ for every input/output pair constitutes the channel matrix. Typically, the inputs are arranged by rows and the outputs by columns.

Generally, the channel matrix and its conditional probabilities $p(o|a)$ can be easily computed manually. It can also be computed analytically or by means of a model-checking tool like PRISM [20]. The first step is to define the sets A of secret inputs and O of observables. The inputs are generally the identities of the senders (assuming the goal is sender anonymity) and the outputs are the attacker's observables. Chatzikokolakis [21] gives a detailed description of how channel matrices are computed.

The probability distribution $p(\cdot)$ over A is called the a priori distribution and is generally not known in advance. When an output o is observed, the probability that the input is a certain a is given by the a posteriori probability of a given o ($p(a|o)$).

As example, let us determine the channel matrix for Crowds protocol under the collaborators attack[1] [2].

Consider a Crowds protocol with n users among them c are compromised (c collaborators) and with p_f as probability of forwarding. The set of inputs is the set of the identities of the users $\{u_1, u_2, \ldots, u_n\}$. Recall that in collaborators attack, a set of corrupted users collaborate to figure out the identity of the initiator. An observable action in the protocol happens when a (honest) user i forwards the message to a collaborator. This action is denoted d_i and means that user i is detected. Hence, the set of observable actions is the set $\{d_1, d_2, \ldots, d_n\}$. It is easy to note that there is a form of symmetry in the corresponding channel matrix. Indeed, once a user is detected, the probability that it is actually the initiator is the same regardless of which user is the actual initiator. According to the proof of Theorem 5.2 in [2], this probability is

$$\alpha = c\,\frac{1-(\frac{n-c-1}{n})\,p_f}{n-(n-c)\,p_f}.$$

The probability of detecting a user other than the initiator is the same for all other users and is $\beta = \alpha - \frac{c}{n}$. Hence the conditional probabilities of the matrix are[2]:

$$p(o_j|a_i) = \begin{cases} \dfrac{\alpha}{s} & \text{if } i = j \\ \dfrac{\beta}{s} & \text{otherwise} \end{cases}$$

where $s = \alpha + (n-1)\beta$.

Crowds protocol with $n = 10$ users, $c = 3$ collaborators, and $p_f = 0.8$ has the following channel matrix:

	d_1	d_2	…	d_{10}
a_1	0.4462	0.0615	…	0.0615
a_2	0.0615	0.4462	…	0.0615
⋮	⋮	⋮	⋱	⋮
a_{10}	0.0615	0.0615	…	0.4462

3.1 Channel Matrix Analysis

Anonymity protocols can be seen as noisy channels where the noise is a manifestation of the efforts of the protocol to hide the link between the inputs and the outputs[3].

[1] Sometimes called predecessor attack.

[2] The matrix probabilities are computed by conditioning on the event that some user was detected. The situation when no user is detected corresponds to absolute privacy and anonymity is not an issue in that case.

[3] In the rest of the paper, the terms secret information and input will be used interchangeably and so are observation and output

The more noise there is in the channel, the more anonymous the protocol is. One promising approach to analyze these protocols is the quantitative theory of information flow which focuses on "how much" information is being leaked. Indeed, initially, there is an initial uncertainty about the secret information. After the protocol executes and the adversary observes the output, the uncertainty might decrease. The idea of the quantitative approach of information theory is to quantify the amount of initial uncertainty (a priori), the remaining uncertainty after observing the observation (a posteriori) and then deduce the amount of information leaked.

In Shannon information theory, the information leaked by a noisy channel is given by the notion of mutual information. Mutual Information of A and O, noted $I(A;O)$, represents the correlation of information between A and O and is defined as:

$$I(A;O) = H(A) - H(A|O) \tag{1}$$

where $H(A)$ is the Shannon entropy of A and $H(A|O)$ is the conditional entropy of A given O. Channel capacity is the maximum mutual information over all a priori distributions.

$$C = \max_{p} I(A;O) \tag{2}$$

Most of previous works [4,6,7] use a different interpretation of the anonymity degree which is based only on the capabilities of the attacker after the protocol executes, that is, the uncertainty (entropy) of the a posteriori distribution on the inputs. The approach we use in this paper which is based on how much information is being leaked by the protocol is more adequate and more reliable than the simple a posteriori entropy approach. Indeed, it is easy to think of two channels with significantly different a priori distributions but with the same a posteriori uncertainty. For example, consider the following two channels (recall that the inputs are arranged by rows and the outputs by columns):

$$C_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0.5 & 0.5 & 0 \\ 0.5 & 0 & 0.5 \end{pmatrix} \qquad C_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

In channel C_1 the number of inputs is 3 so if we assume a uniform a priori distribution $[\frac{1}{3}, \frac{1}{3}, \frac{1}{3}]$, the entropy $H(A)$ will be equal to 1.58. In channel C_2, the number of inputs is 5 so the uniform distribution is $[\frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}]$ and the corresponding entropy is $H(A) = 2.32$. Hence, initially there is more uncertainty in channel C_1 than in C_2. The a posteriori distributions in C_1 and C_2, however, have very similar uncertainty values. Indeed, $H(A|O)$ in C_1 is equal to 0.79 and in C_2 it is 0.8. That is, after observing an observation, an attacker in C_1 will have the same uncertainty as an attacker in C_2. So measures that rely only on the a posteriori distribution will declare both protocols with similar anonymity degrees. This is not accurate because C_1 is clearly better than C_2 since it leaks less information and preserves better the uncertainty on the input distribution. Mutual information as well as the measures we propose in this paper reflects this difference. For instance, Mutual Information for C_1 is 0.79 while it it 1.52 in C_2.

As an alternative to Shannon entropy, one can use the concept of probability of error of an adversary [18]. In an anonymity protocol, the attacker tries to guess the secret information based on the information she observes. Her goal is to use a decision function so that to minimize the probability of error (probability of guessing wrong). The decision function $f : O \rightarrow A$ gives for every output o, the guessed input a. The probability of error associated to f is the averaged sum over all outputs of making a wrong guess:

$$P_e = \sum_{o \in O} p(o)(1 - p(f(o)|o)) \tag{3}$$

The two most known decision functions are MAP (Maximum A Posteriori Probability) and ML (Maximum Likelihood).

If an observation o has been observed, the MAP decision function chooses the input that maximizes the a posteriori probability $p(a|o)$:

$$f(o) = a \quad \Rightarrow \forall b \in A,\ p(a|o) \geq p(b|o).$$

The probability of error with the MAP criterion is then:

$$1 - \sum_{o \in O} \max_{a \in A}(p(o|a)\ p(a)). \tag{4}$$

The ML decision function chooses the input that maximizes the likelihood $p(o|a)$:

$$f(o) = a \quad \Rightarrow \forall b \in A,\ p(o|a) \geq p(o|b).$$

The corresponding probability of error is thus:

$$1 - \sum_{o \in O} \max_{a \in A}(p(o|a))\ p(a). \tag{5}$$

It is well known that the best decision function is based on the MAP rule and the corresponding probability of error is called Bayes risk. It is known also that ML is only an approximation of MAP when the a priori distribution is not available. This explains why in some cases the ML deviates considerably from MAP [22].

The probability of error is not a measure of information leakage. Instead, it can be used to measure the attacker's initial capability (based on the a priori distribution) and also the attacker capability after observing the output (based on the a posteriori probability). A notion of "difference" between these probabilities of error can give rise to an information leakage measure. Smith [12] introduced an information leakage measure along this idea but in his formulation, he used Rényi entropy [13]:

$$InformationLeak = H_\infty(A) - H_\infty(A|O) \tag{6}$$

where

- $H_\infty(A) = \log \dfrac{1}{\max\limits_{a \in A} p(a)}$
- $H_\infty(A|O) = \log \dfrac{1}{\sum\limits_{o \in O} \max\limits_{a \in A} p(o|a)p(a)}$

Equation (6) can be formulated as follows :

$$InformationLeak = \log \frac{\sum_{o \in O} \max_{a \in A} p(o|a)p(a)}{\max_{a \in A} p(a)} \tag{7}$$

In this paper we refer to this measure as min-entropy information leak. Smith showed through an interesting example that when an adversary tries to guess the value of the input in a single try, min-entropy information leak is more suitable than mutual information. The example features two systems with the same mutual information, the same a priori uncertainty, but with very different MAP probabilities of error.

4 Scattering of the Channel Matrix Rows

The new family of measures we present in this paper are based on how much the rows of the matrix are different from each others. Since the inputs are arranged by rows, every row of the matrix is a probability distribution on the observations for a given input : $(p(o_1|a), p(o_2|a), \ldots, p(o_m|a))$. Intuitively, the more these rows are similar to each other, the more the protocol is anonymous because the observation of the output in that case does not help much the attacker to guess the right input. On the other hand, the more the rows are different from each other, the less anonymous the protocol is because the knowledge of the output carries significant information about the input. To measure how much the rows are different from each others, we consider every row as a point in the $m-$dimensional space. If the rows are different, then the associated points will be very scattered in the space and if they are similar they will be close to each others. We consider two measures of statistical dispersion: mean difference and standard deviation and we propose variants of theses measures we call Kullback-Leibler mean difference (KLMD) and Kullback-Leilbler standard deviation (KLSD).

Definition 1. *Let M be a channel matrix where $|A| = n$ and $|O| = m$.*

$$KLMD(\, M, p\,) = \frac{1}{n(n-1)} \sum_{a \neq b \in A} p(a)\; p(b)\; D_{KL}(\overrightarrow{R_a} \,||\, \overrightarrow{R_b}) \tag{8}$$

$$KLSD(\, M, p\,) = \sqrt{\sum_{a \in A} p(a)\; D_{KL}(\overrightarrow{R_a} \,||\, \overrightarrow{Mean_p})^2} \tag{9}$$

where

- *D_{KL} is the Kullback-Leibler distance (know also as relative entropy)*
- *$\overrightarrow{R_a}$ denotes the matrix row associated to input a*
- *$\overrightarrow{Mean_p}$ is the mean distribution with respect to the prior distribution p. $Mean_p(o) = \sum_a p(a)\; p(o|a)$.*

In addition to mean difference and standard deviation, we tried other statistical dispersion measures such as variance but the most promising empirical results were obtained with the selected two measures. On the other hand, the choice of relative entropy

is motivated by the fact that in information theory, the divergence between two probability distributions is given by the relative entropy. We tried also to use Euclidean norm but again the empirical results were clearly better with relative entropy. That said, our plans for future work include the investigation of other statistical dispersion measures and probability distribution metrics and different combinations of them.

The measures (8) and (9) have a geometric flavor and they are based on relative entropy. Interestingly, we could establish a link between a variant of KLSD and the classical mutual information notion. This gives an interesting geometrical interpretation to mutual information. To the best of our knowledge, this fact has not been mentioned in the literature so far.

Theorem 1.

$$I(A;O) = \sum_a p(a)\, D_{KL}(\overrightarrow{R_a} \,||\, \overrightarrow{Mean_p})$$

Proof.

$$\begin{aligned}
\sum_a p(a)\, D_{KL}(\overrightarrow{R_a} \,||\, \overrightarrow{Mean_p}) &= \sum_a p(a) \sum_o p(o|a)\ \log\left(\frac{p(o|a)}{Mean_p(o)}\right) \\
&= \sum_a p(a) \sum_o p(o|a)\ \left(\log(p(o|a) - \log(Mean_p(o))\right) \\
&= \left(\sum_a p(a) \sum_o p(o|a) \log(p(o|a))\right) \\
&\qquad - \left(\sum_a p(a) \sum_o p(o|a) \log(Mean_p(o))\right) \\
&= -\sum_a p(a) H(\overrightarrow{R_a}) - \left(\sum_o \sum_a p(a) p(o|a) \log(Mean_p(o))\right) \\
&= -\sum_a p(a) H(\overrightarrow{R_a}) + H(\overrightarrow{Mean_p}) \\
&= H(\overrightarrow{Mean_p}) - \sum_a p(a) H(\overrightarrow{R_a}) \\
&= H(O) - H(O|A) \\
&= I(A;O) \qquad (10)
\end{aligned}$$

4.1 Empirical Analysis

To see how these new measures compare to mutual information and Smith's min-entropy information leak, we performed empirical study on Crowds [2], Onion-routing [3], and ring-based DC-Net [4] anonymity protocols under the collaborators attack [2,23]. Two types of experiments are performed. The first experiment aims at showing how the different measures behave as the capabilities of the attacker increase. The second experiment focuses rather on the impact of changing the a priori distribution on the different measures.

For Crowds, the experiment consists in considering a crowd of 20 users, a fixed probability of forwarding of 0.8 and then computing the different measures while increasing

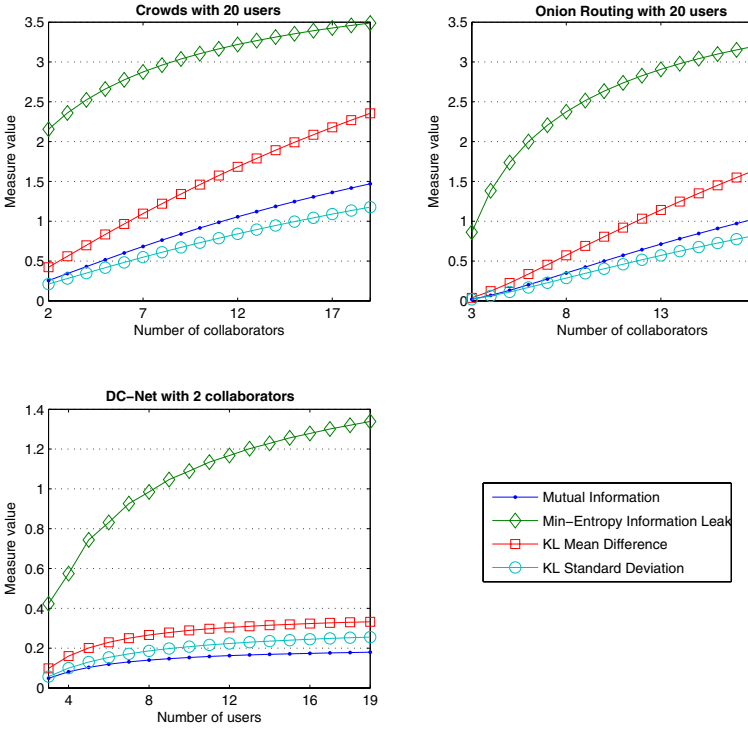


Fig. 1. Comparison of the four different measures on three protocols under collaborators attack while increasing the number of collaborators

the number of collaborators from 2 to 19. The upper left plot of Figure 1 shows how the four measures behave. The upper right plot of the same figure shows the result of the same experiment but on Onion-routing (20 users and the number of collaborators increasing from 3 to 19). For the ring-based DC-Net an attack with more than 2 collaborators is difficult to analyze. To avoid dealing with this complexity, a slightly different experiment is carried out which consists in fixing the number of collaborators to 2 and decreasing the number of users from 19 to 3. This is equivalent to increasing the attacker capabilities. The results are depicted in the lower left plot of Figure 1.

A good information leak measure should be sensitive to the increase of the attacker capabilities. If the number of collaborators increases, for instance, this should be reflected by the measure. Overall, min-entropy information leak is the more sensitive to the attacker capabilities increases. For Crowds and Onion-routing, KLMD is interestingly sensitive to the attacker capabilities modification. For all protocols mutual information and KLSD behave very similarly. This can be explained by the Thoerem 1.

In experiment 2, we fix the attacker capabilities and play on the a priori distribution. For each protocol, the different measures are computed for different a priori distributions starting from a distribution peaked in one input and then flattering until reaching

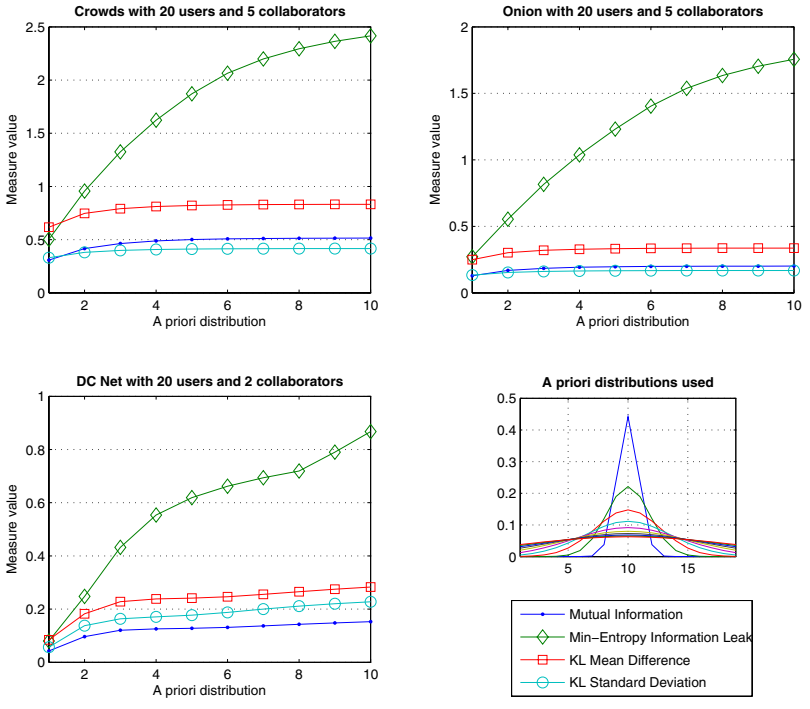


Fig. 2. Comparison of the four different measures on three protocols under collaborators attack using different a priori distributions

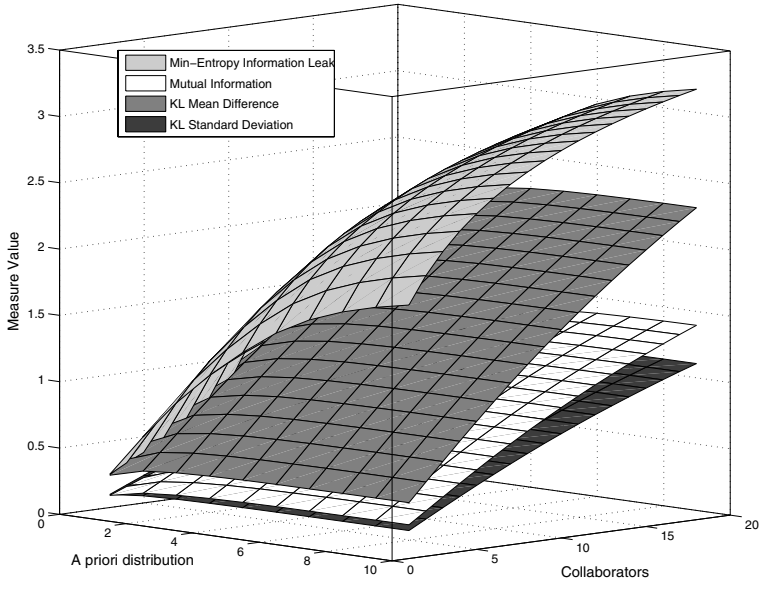
the uniform distribution. The lower left plot of Figure 2 illustrates the distributions graphically. It is easy to see from the rest of plots of Figure 2 that the min-entropy information leak is very sensitive to the a priori distribution unlike the other measures. This does not constitute a desirable property for an anonymity measure. Indeed, generally, the a priori distribution is not assumed to be known and hence a good anonymity measure should be as independent as possible from that distribution. Such good measure should be determined uniquely by the matrix. Dependence on the a priori distribution has always been an argument against the MAP rule because this makes it look as an artificial rule. The fact that min-entropy information leak measure is inspired by the MAP probability of error explains the sensitivity of this measure with respect to the a priori distribution as depicted in Figure 2. The rest of the measures: mutual information, KLMD, and KLSD are more stable when the a priori distribution changes.

To further see how each measure behaves for each protocol under the collaborators attack, we combined the results of experiment 1 and experiment 2 in a single 3-d chart. Figure 3 illustrates the measures for Crowds: the x axis represents the a priori distribution, the y axis the number of collaborators and the z axis the different measures values. Note that on the x axis, only the min-entropy information leak values increase considerably while on the y axis, the slope is neat for all measures, in particular the KLMD measure.

5 Re-executing the Protocol Multiple Times

Most of anonymity attacks are passive attacks in the sense that they don't draw attention to themselves and consequently may continue for a long period of time. In particular, a collaborators attack that last for a long period of time may detect several messages from the same session (initiated by the same user). If the path used in that session does not change, then the collaborators will not gain additional information even if the attack lasts forever because it is always the same user which is detected. However, protocols such as Crowds, Onion-routing, and Hordes change their paths periodically because some users join the protocol, some others leave and also to improve the performance of the protocol by balancing the load among all users. By changing the path during the same session, the collaborators will have more information to identify the initiator since several users will be detected and it is easy to see that the true initiator will be more likely to be detected than any other user. The same situation happens if the path is fixed but the set of collaborators (compromised users) change periodically which corresponds to a second variant of the collaborators attack called called Roving adversary [24].

From an information theoretical standpoint, changing the path several times during the same session can be regarded as re-executing the protocol several times with the same input. Since an anonymity protocol is typically represented as a noisy channel, re-executing the protocol will yield to a sequence of possibly different observations. It is assumed that the protocol is memoryless, that is, each time it is re-executed, it works according to the same probability distribution, independently from what happened in previous sessions.



rent measures on Crowds protocol for different numbers of collaborators
different a priori distributions.

Fig. 3. The four measures applied on Crowds in a 3-d graphics

Let $a \in A$ be the input and suppose that the protocol is re-executed k times with the same input a. The attacker has to infer the input a based on the k observations she obtains. Let $\overrightarrow{o}$ denotes the sequence of k observations $o_1, o_2, \ldots o_k$. The total number of possible sequences is :

$$ns = \frac{(m+k-1)!}{k!\,(m-1)!}$$

where $m = |O|$ is the number of observations. The probability of an observation sequence $\overrightarrow{o}$ given an input a is :

$$p(\overrightarrow{o} \mid a) = \Pi_{i=1}^{k} p(o_i|a).$$

Re-executing the protocol k times can be represented by a bigger channel matrix where the n inputs $a_1, a_2, \ldots, a_n$ are arranged by rows and the ns possible sequences $\overrightarrow{o_1}, \overrightarrow{o_2}, \ldots, \overrightarrow{o_{ns}}$ are arranged by columns. The probability at row i and column j represents $p(\overrightarrow{o_j}|a_i)$.

Let f_k be a decision function adopted by the attacker to infer the input from the sequence of k observations. Similarly to the the single execution case, there are mainly two types of decision functions: one based on the MAP rule and one based on ML rule. A MAP rule based decision function returns the input that maximizes the a posteriori prbability :

$$p(a|\overrightarrow{o}) = \frac{p(\overrightarrow{o}|a)\,p(a)}{p(\overrightarrow{o})}.$$

That is,

$$f_k(\overrightarrow{o}) = a \qquad \Rightarrow \qquad p(\overrightarrow{o}|a)p(a) \geq p(\overrightarrow{o}|a')p(a') \;\; \forall a' \in A.$$

According to the ML rule, the decision function returns the input that maximizes the likelihood $p(\overrightarrow{o}|a)$. That is,

$$f_k(\overrightarrow{o}) = a \qquad \Rightarrow \qquad p(\overrightarrow{o}|a) \geq p(\overrightarrow{o}|a') \;\; \forall a' \in A.$$

Hence the probability of error after k executions according to the MAP rule is:

$$1 - \sum_{\overrightarrow{o}} \max_a (p(\overrightarrow{o}|a)p(a)).$$

According to ML rule, it is:

$$1 - \sum_{\overrightarrow{o}} \max_a (p(\overrightarrow{o}|a))p(a).$$

In the same spirit as the new anonymity measures introduced in Section 4, we propose an alternative decision function based on how close $\overrightarrow{o}$ is from the channel matrix's rows. Let $freq(\overrightarrow{o})$ be a vector composed of the frequencies of each o in $\overrightarrow{o}$. $freq(\overrightarrow{o})$ can be seen as a probability distribution on O and consequently a point in the $m-$dimentional space. Hence, we can think of a decision function that chooses the input a whose row is the closest to the point associated to $freq(\overrightarrow{o})$. The proposed decision function is as follows:

$$f_k(\overrightarrow{o}) = a \qquad \Rightarrow \qquad D_{KL}(\overrightarrow{R_a} \,||\, freq(\overrightarrow{o})) \leq D_{KL}(\overrightarrow{R_{a'}} \,||\, freq(\overrightarrow{o})) \;\; \forall a' \in A$$

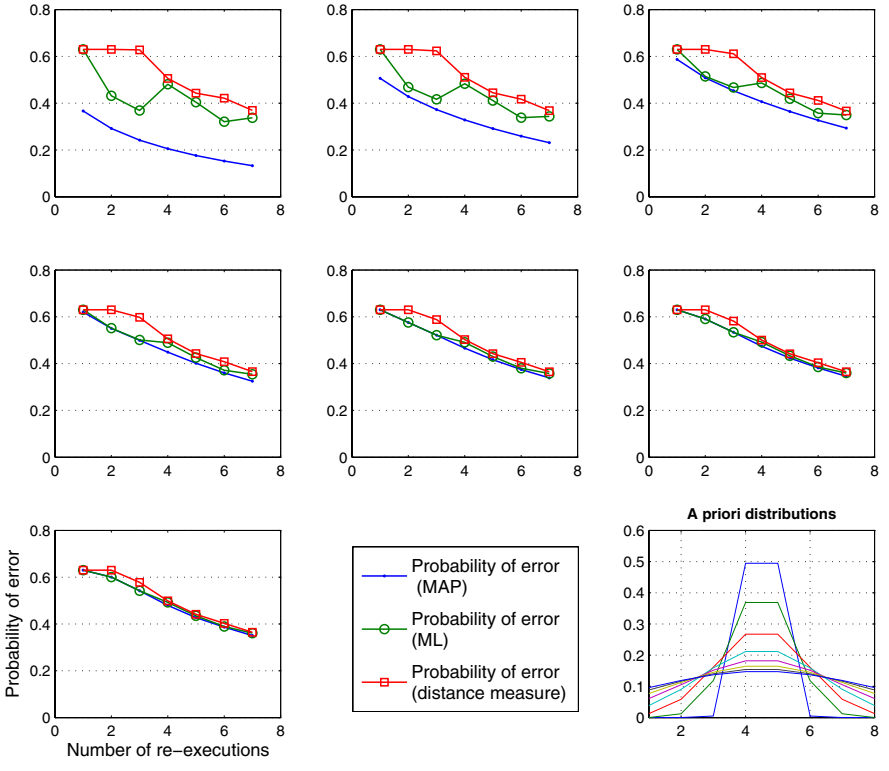


Fig. 4. Comparison of the three probabilities of error using different a priori distributions

where $D_{KL}(\cdot \,||\, \cdot)$ is the KL divergence (relative entropy).

The probability of error based on this decision function is:

$$1 - \sum_{\overrightarrow{o}} p(\overrightarrow{o}|a_{min\,\overrightarrow{o}})\; p(a_{min\,\overrightarrow{o}})$$

where

$$\forall \overrightarrow{o},\;\; a_{min\,\overrightarrow{o}} = \arg\min_{a} D_{KL}(\overrightarrow{R_a}||freq(\overrightarrow{o})).$$

To compare these probabilities of error, we did a set of empirical experiments on Crowds protocol. We considered a Crowds protocol (8 users, 2 collaborators, and $p_f = 0.9$) and a set of a priori distributions ranging from a distribution peaked in 2 inputs to the almost uniform distribution as shown in the lower right plot of Figure 4. The experiment consists in repeating the execution of the protocol 1 time, 2 times, etc. until 8 times and seeing how the 3 probabilities of error compare to each others. Each plot of Figure 4 shows the result of the experiment for a different a priori distribution. The first plot (upper-left), for instance, corresponds to the distribution peaked in two inputs. In all plots, the probabilities of error are decreasing. This is expected because the more the protocol is re-executed, the less uncertain the attacker will be about the input.

The only exception concerns the probability of error with ML as the 3 first plots exhibit a strange situation where an increase in the number of re-executions yields to a larger probability of error which is clearly counter intuitive. This can be explained by the inconsistent values of ML probability of error in some extreme situations as discussed in Section 3.1.

According to Figure 4, MAP rule yields the best decision function. This confirms a result in [9] stating that even when the protocol is re-executed, the MAP rule based decision function remains the best. As of the probability of error we proposed, according to Figure 4, it is not minimal but it is more reliable than ML. Also, from the same figure we can note that as the a priori distribution approaches the uniform distribution, the different probabilities of error become almost the same.

6 Conclusion

In this paper we have investigated a new idea of measuring the information leaked by a protocol by analyzing the vector configuration of the channel probabilities matrix. We considered each row of the matrix as a point in the n-dimensional space and we used statistical dispersion measures to estimate how much the points are scattered in the space. Empirical results showed that the two proposed measures KLSD and KLMD are sensitive to the modifications of the attacker capabilities and most importantly they are stable when the a priori distribution on the secret events changes. In the light of this second property, we strongly think that this new approach holds the promise of much less dependence on the a priori distribution on secret events. On the other side, compared to existing information-theoretic anonymity measures ([6,**?**]) which focus on the lack of information that an attacker has about the identities of users, the proposed approach focuses rather on the capability of the protocol to disguise this information given the attacker's knowledge about the observables. In other words, we focus on the difference between the a priori and a posteriori distributions and not on analyzing the a posteriori distribution only. This makes our approach more general. We mention also that the proposed measures are easy to compute compared for instance to channel capacity.

In this paper, we compared the proposed measures with mutual information by trying them on Crowds, Onion-Routing, and DC-Net protocols. It turns out that the channel matrices for these particular protocols are symmetric and hence the capacity reaches its maximum in the uniform distribution. We plan to carry out comparisons on other protocols and attack scenarios where capacity reaches its maximum in a non-uniform distribution. It is important to mention however that in order to fairly compare the proposed measures as well as Smith's measure with Capacity, one has to find the distribution that maximizes every one of these measures. This is part of our future work.

In both proposed measures, we used relative entropy (or Kullback-Leibler divergence) to compute the "distance" between two probability distributions (rows the matrix). Our plans for future work include the investigation of other statistical dispersion measures such as average (mean) deviation and interquartile range and also other probability distribution metrics such as Hellinger distance and Levy metric [25]. Our goal is to find the best combination of statistical dispersion measure and probability distribution metric that reveals the connection between the vector configuration of the matrix

and the information leaked. We plan also further analyze the proposed family of measures when applied on other anonymity systems, in particular Mix-based ones [26] and Tor [27].

Acknowledgement

This research has been initiated by an informal discussion with Catuscia Palamidessi and a large part of it took place under the supervision of Prakash Panangaden. We sincerely thank them for their help and their support. Research funded in part by FQRNT (McGill University, Canada) and Junior Faculty Grant (KFUPM, Saudi Arabia).

References

1. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24(2), 84–90 (1981)
2. Reiter, M., Rubin, A.: Crowds: Anonymity for web transactions. ACM Transactions on Information and System Security 1(1), 66–92 (1998)
3. Syverson, P., Goldschlag, D., Reed, M.: Anonymous connections and onion routing. In: Proceedings of the 1997 IEEE Symposium on Security and Privacy (SP 1997), Washington, DC, USA. IEEE Computer Society, Los Alamitos (1997)
4. Chaum, D.: The dining cryptographers problem: unconditional sender and recipient untraceability. Journal of Cryptology 1(1), 65–75 (1988)
5. Shields, C., Levine, B.: A protocol for anonymous communication over the internet. In: Proceedings of the 7th ACM Conference on Computer and Communications Security, pp. 33–42. ACM, New York (2000)
6. Serjantov, A., Danezis, G.: Towards an information theoretic metric for anonymity. In: Dingledine, R., Syverson, P.F. (eds.) PET 2002. LNCS, vol. 2482, pp. 41–53. Springer, Heidelberg (2003)
7. Diaz, C., Seys, S., Claessens, J., Preneel, B.: Towards measuring anonymity. In: Dingledine, R., Syverson, P.F. (eds.) PET 2002. LNCS, vol. 2482, pp. 54–68. Springer, Heidelberg (2003)
8. Zhu, Y., Bettati, R.: Anonymity vs. information leakage in anonymity systems. In: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS 2005), Columbus, Ohio, pp. 514–524 (2005)
9. Chatzikokolakis, K., Palamidessi, C., Panangaden, P.: Anonymity protocols as noisy channels. Information and Computation 206(2-4), 378–401 (2008)
10. Moskowitz, I., Newman, R., Crepeau, D., Miller, A.: Covert channels and anonymizing networks. In: WPES 2003: Proceedings of the 2003 ACM workshop on Privacy in the electronic society, pp. 79–88. ACM, New York (2003)
11. Cover, T., Thomas, J.: Elements of Information Theory. Wiley-Interscience, New York (1991)
12. Smith, G.: On the foundations of quantitative information flow. In: de Alfaro, L. (ed.) FOSSACS 2009. LNCS, vol. 5504, pp. 288–302. Springer, Heidelberg (2009)
13. Rény, A.: On measures of entropy and information. In: Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics, and Probability, pp. 547–561 (1960)
14. Moskowitz, I., Newman, R., Syverson, P.: Quasi-anonymous channels. In: IASTED CNIS, pp. 126–131 (2003)
15. Newman, R., Moskowitz, I., Syverson, P., Serjantov, A.: Metrics for traffic analysis prevention. In: Dingledine, R. (ed.) PET 2003. LNCS, vol. 2760, pp. 48–65. Springer, Heidelberg (2003)

16. Tóth, G., Hornák, Z., Vajda, F.: Measuring anonymity revisited. In: Liimatainen, S., Virtanen, T. (eds.) Proceedings of the Ninth Nordic Workshop on Secure IT Systems, Espoo, Finland, pp. 85–90 (November 2004)
17. Edman, M., Sivrikaya, F., Yener, B.: A combinatorial approach to measuring anonymity. In: 2007 IEEE Intelligence and Security Informatics, pp. 356–363 (2007)
18. Chatzikokolakis, K., Palamidessi, C., Panangaden, P.: On the bayes risk in information-hiding protocols. Journal of Computer Security 16(5), 531–571 (2008)
19. Clark, D., Hunt, S., Malacaria, P.: Quantitative analysis of the leakage of confidential data. Electrical Notes in Theoretical Computer Science 59, 238–251 (2001)
20. University of Oxford: Prism, `http://www.prismmodelchecker.org`
21. Chatzikokolakis, K.: Probabilistic and Information-Theoretic Approaches to Anonymity. PhD thesis, Laboratoire d'Informatique (LIX), École Polytechnique, Paris (October 2007)
22. MacKay, D.: Information Theory, Inference and Learning Algorithms. Cambridge University Press, Cambridge (2003)
23. Wright, M., Adler, M., Levine, B., Shields, C.: An analysis of the degradation of anonymous protocols. In: Proceedings of the Network and Distributed Security Symposium (NDSS 2002). IEEE Computer Society, Los Alamitos (2001)
24. Syverson, P., Tsudik, G., Reed, M., Landwehr, C.: Towards an analysis of onion routing security. In: Proceedings of the international workshop on Designing privacy enhancing technologies, pp. 96–114. Springer, New York (2001)
25. Gibbs, A., Su, F.: On choosing and bounding probability metrics. International Statistical Institute 70, 418–435 (2002)
26. Danezis, G., Diaz, C.: A survey of anonymous communication channels. Technical Report MSR-TR-2008-35, Microsoft Research (January 2008)
27. Dingledine, R., Mathewson, N., Syverson, P.: Tor: the second-generation onion router. In: Proceedings of the 13th Usenix Security Symposium (August 2004)