On the Fundamentals of Anonymity Metrics

Christer Andersson and Reine Lundin

Karlstad University, Department of Computer Science
Universitetsgatan 2, 651-88 Karlstad, Sweden
{christer.andersson, reine.lundin}@kau.se

Abstract. In recent years, a handful of anonymity metrics have been proposed that are either based on *(i)* the number participants in the given scenario, *(ii)* the probability distribution in an anonymous network regarding which participant is the sender / receiver, or *(iii)* a combination thereof. In this paper, we discuss elementary properties of metrics in general and anonymity metrics in particular, and then evaluate the behavior of a set of state-of-the-art anonymity metrics when applied in a number of scenarios. On the basis of this evaluation and basic measurement theory, we also define criteria for anonymity metrics and show that none of the studied metrics fulfill all criteria. Lastly, based on previous work on entropy-based anonymity metrics, as well as on theories on the effective support size of the entropy function and on Huffman codes, we propose an alternative metric – the scaled anonymity set size – that fulfills these criteria.

1 Introduction

Anonymity can be defined as follows: "anonymity of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set" [12]. This definition underlines both that anonymity can be quantified on a relative scale and that there might be a (situation-dependent) threshold where anonymity begins. Anonymity both involves *(i)* maintaining unlinkability between user / application data and the corresponding user with whom these data is concerned (data level anonymity) and *(ii)* hiding with whom a user is communicating (communication level anonymity). *Sender anonymity* means that a message cannot be linked to the sender of that message, while *recipient anonymity* implies that a message cannot be linked to the receiver(s) of that message [12]. The scope of the paper is limited to sender anonymity, although most ideas are valid also for recipient anonymity.

This paper discusses *anonymity metrics*, metrics that can be applied to measure the degree of anonymity in a certain scenario. State-of-the-art anonymity metrics are normally based on either *(i)* the number participants in the given scenario, *(ii)* the probability distribution in an anonymous network regarding which participant is the sender / receiver, or *(iii)* a combination thereof. In this paper, we first discuss the basics of measurements and anonymity metrics. Then, a basic model for anonymity attacks is proposed and some recent anonymity metrics are presented. Thereafter, we define a set of "typical" scenarios for anonymous communication and quantify the degree of anonymity in these scenarios using the earlier introduced metrics. In the scenarios, the Crowds [14] system, a theoretically well studied and intuitive protocol, is used for providing anonymous communication. On the basis of this evaluation of the scenarios – and taking elementary properties of each anonymity metric into account – we thereafter propose a set of criteria that an anonymity metric should meet and assess whether the studied anonymity metrics fulfill these criteria.

A result from the evaluation of the criteria is that although some metrics fulfill most criteria, there is no anonymity metric that fulfill all criteria. Using existing entropy-based anonymity metrics [4, **?**] as a starting point, we therefore propose and evaluate an alternative anonymity metric that better fulfills the stated criteria. We denote this anonymity metric the *scaled anonymity set size*, and to explain the underlying semantics of this metric, we use concepts such as Huffman codes / Huffman trees [3] and the effective support size of the entropy function [9].

This paper has the following structure. Section 2 introduces Crowds and presents a model for anonymity attacks. It also explains the basics of measurements and introduces a set of state-of-the-art anonymity metrics. Section 3 evaluates the behavior of these anonymity metrics when applied in a number of scenarios using the Crowds system. This section also proposes a set of criteria for anonymity metrics and evaluates the studied anonymity metrics against these criteria. As no metric fulfills all criteria, Section 4 proposes and explains an alternative entropy-based metric designed to meet these criteria – the scaled anonymity set size. Finally, Section 5 concludes the paper.

2 Preliminaries

2.1 Introduction to Crowds

This paper later presents four scenarios building on the *Crowds* system [14] – a mechanism for anonymous web browsing based on traffic forwarding through virtual paths. For this reason, this section contains a brief description of Crowds. The anonymity set in Crowds is denoted a *crowd*, and all users in the crowd run a *jondo* application. Also, a *blender* application administrates user membership and key distribution. Paths in Crowds are created randomly: first, a user extends the path to a random jondo, which, in turn, flips a biased coin (based on the probability of forwarding, p_f) to determine whether the path should be ended (i.e., the request is submitted to the web server), or extended to another jondo which repeats the same procedure.

2.2 A Model for Anonymity Attacks

An *anonymity attack* entails an attacker $\mathcal{A}$ trying to uniquely link an observed message (or set of messages) $\mathcal{M}$ to a user u_i in the anonymity set $\mathcal{U} = \{u_1, u_2, ...,$

$u_n\}$ by gathering knowledge about the system, the user base $\mathcal{U}$, and $\mathcal{M}$. Each of these entities have a set of attribute types / values. The system has attributes such as $a_i = \{$*application*, "Crowds"$\}$ and $a_j = \{p_f, \frac{3}{4}\}$. One essential attribute in the system is the probability distribution $\mathcal{P} = (p_1, p_2, \ldots, p_n)$, where p_i denotes the probability that u_i is the sender of $\mathcal{M}$. $\mathcal{U}$ has attribute sets about its users (or their devices), such as $a_i = \{$*name*, "Bob"$\}$ and $a_j = \{$*IP*, 192.168.10.20$\}$. Lastly, $\mathcal{M}$ shares several attribute types with $\mathcal{U}$, although they are initially empty. Now, an anonymity attack can be described as follows:

1. Initially, $\mathcal{A}$ can be assumed to know at least the public parameters of the system and some information about the users in $\mathcal{U}$.[1] $\mathcal{A}$ initially possess no knowledge about the sender. Hence, $\mathcal{P}$ is initially uniform.
2. Now, $\mathcal{A}$'s objective is to either passively observe or actively trigger events to learn information about $\mathcal{M}$. The triggering can be accomplished using arbitrary active attacks, such as a predecessor [18], intersection [13], or Sybil attack [6]. If $\mathcal{A}$ is successful, the events may enable him to learn one or more attribute values of $\mathcal{M}$'s attribute types, or at least restrict the corresponding value domains.
3. Then, $\mathcal{A}$ analyzes the collected attribute values of $\mathcal{M}$, together with the attributes of the system and the users in $\mathcal{U}$. $\mathcal{A}$'s objective is to calculate a new (less uniform) $\mathcal{P}'$. The way $\mathcal{P}'$ is calculated varies from scenario to scenario; in the included scenarios we base our calculations on the internal structure of Crowds [14].
4. $\mathcal{A}$'s goal is to map a single user in $\mathcal{U}$ to $\mathcal{M}$. Depending on $\mathcal{P}'$, there are three possible next steps: *(i)* if there is a $p_i \in \mathcal{P}'$ that is equal (or very close) to 1, the attacker succeeds; *(ii)* if any of $\mathcal{A}$'s resources are exhausted, he fails; else *(iii)* if $\mathcal{P}'$ cannot bind one u_i to $\mathcal{M}$ with a specifically large likelihood, repeat step two.

When assessing a system's resistance against anonymity attacks, an analyst can simulate these steps. In step three, the analyst can use an anonymity metric to determine the degree of anonymity. In the next section, we discuss the basics of measurement and anonymity metrics and give examples of anonymity metrics.

2.3 Anonymity Metrics

The Basics of Measurements. *Measurement* can be defined as "a mapping from the empirical world to the formal, relational world. Consequently, a *measure* is the number or symbol assigned to an entity by this mapping in order to characterize an attribute" where "the real world is the *domain* of the mapping, and the mathematical world is the *range*" [7]. One important rule is the *representation condition* which asserts that "a measurement mapping M must map entities into numbers and empirical relations into numerical relations in such a way that the empirical relations preserve and are preserved by the numerical relations" [7]. Lastly, a *metric* is a standard of measurement.

[1] Compare for example with the information distributed by the blender in Crowds [14].

Introduction to Anonymity Metrics. An anonymity metric is a mapping from the empirical world (the domain) to the mathematical world (the range), in which numbers or symbols are assigned to entities in a system to describe the degree of anonymity. The *domain* is the knowledge of the attacker $\mathcal{A}$ about the studied entities in the real world – the system and its anonymity set $\mathcal{U} = \{u_1, u_2, ..., u_n\}$. $\mathcal{A}$ may both be a real attacker or a model defined to test the resistance of a system against anonymity attacks. The system can both be a real world instance or a theoretical model. The *mapping* itself can be seen as a function behaving according to set of rules. An important parameter in the mapping is the probability distribution vector $\mathcal{P} = (p_1, p_2, ..., p_n)$ among the users in $\mathcal{U}$ regarding which user is the sender in a communication. Finally, the *range* is the set of possible values from the mapping. Here, there are many options, as different anonymity metrics use different units for presenting the degree of anonymity.

Examples of Anonymity Metrics. Below, we introduce some common metrics.

- *Anonymity set size:* a classic degree is the anonymity set size, $|\mathcal{U}| = n$. The concept of anonymity set was introduced in [2].
- *Crowds-based metric:* in this metric, the degree of anonymity A_i of a user u_i is measured on a continuum between `provably exposed` (0) and `absolute privacy`[2] (1), were $A_i = 1 - p_i = \bar{p}_i$ [14] (p_i is the probability that u_i is the sender). The continuum includes the intermediary points: `possible innocence` (the probability that u_i is *not* the sender is non-negligible, thus $A_i \geq 0 + \delta$, where $\delta > 0$); `probable innocence` (p_i that u_i is the sender is less than 1/2, thus $A_i \geq 1/2$); and `beyond suspicion` (u_i is not more likely than any other $u_j \in \mathcal{U}$ to be the sender, and thus $A_i = \max\{A_1, A_2, ..., A_i, ..., A_n\}$ among $\mathcal{U}$).
- *Source-hiding property:* here, Θ is defined as the greatest probability you can assign to any user u_i of being the sender of a message, thus $\Theta = \max(\mathcal{P})$ [17]. Naturally, $\frac{1}{n} \leq \Theta \leq 1$, where $\Theta = \frac{1}{n}$ denotes maximum anonymity.
- *Entropy-based metrics:* in Serjantov / Danezis's metric [15], "the effective anonymity set size" $\mathcal{S}$ is defined as the Shannon entropy $H(\mathcal{P})$ [16] regarding which user in $\mathcal{U}$ sent a message, with $\mathcal{S} = -\sum_{i=1}^{n} p_i log_2(p_i)$, where $0 \leq \mathcal{S} \leq log_2(n)$. Díaz *et al.* [4] instead calculate the degree of anonymity $d = \frac{H(\mathcal{P})}{log_2(n)}$, where $0 \leq d \leq 1$. Both $\mathcal{S}$ and d output a max degree of anonymity when $\mathcal{P}$ equals the uniform distribution.

2.4 Measuring the Uniformness of Probability Distributions

To study how an anonymity metric behaves when the probability distribution $\mathcal{P}$ change, a function $d(\mathcal{P}, U)$ is needed, where U is the uniform distribution. Such

[2] The latter means that the attacker cannot distinguish between a situation where a potential sender participated in a communication and a situation where he did not [14].

a function $d(\mathcal{P}, U)$ should by some means quantify the distance (or quotient) between $\mathcal{P}$ and U. There are several alternatives for $d(\mathcal{P}, U)$, such as $d(\mathcal{P}, U) = H(U) - H(\mathcal{P})$ or $d(\mathcal{P}, U) = \frac{H(\mathcal{P})}{H(U)}$. Another option that we think could be used as well is to calculate $d(\mathcal{P}, U)$ as the Euclidean distance (ED) in n-space, according to the following:

$$d(\mathcal{P}, U) = \sqrt{\sum_{i=1}^{n}(p_i - \frac{1}{n})^2} \tag{1}$$

Here, $\frac{1}{n}$ is the probability assigned to each of the n users for the uniform distribution. Intuitively, Equation (1) outputs the ordinary distance between the two points $\mathcal{P}$ and U when they are plotted in an n-dimensional space, where $0 \leq d(\mathcal{P}, U) \leq \sqrt{\left(\frac{n(n-1)}{n^2}\right)}$. For $n \to \infty$, $\left(\frac{n(n-1)}{n^2}\right)^{1/2}$ approaches 1. In Figure 1 to the right, ED in 2-space is plotted for one example distribution $\mathcal{P} = (\frac{2}{3}, \frac{1}{3})$.

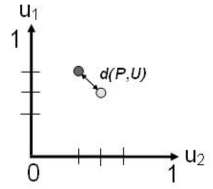


Fig. 1. ED in 2-space between $\mathcal{P} = (\frac{2}{3}, \frac{1}{3})$ and $U = (\frac{1}{2}, \frac{1}{2})$.

3 Evaluation of Anonymity Metrics

This section evaluates the degree of anonymity in a set of example scenarios using *Crowds* [14]. The scenarios involves a user communicating with an external web server through the Crowds network. The following parameters are varied in the scenarios: the number of users n, the number of rogue users c (where $c < n$), and p_f:

- In scenario one, $n = 10$, $c = 1$, and $p_f = 11/20$;
- In scenario two, $n = 1000$, $c = 10$, and $p_f = 11/20$;
- In scenario three, $n = 1000$, $c = 200$, and $p_f = 11/20$;
- In scenario four, $n = 1000$, $c = 200$, and $p_f = 3/4$.

Attacker Model. As Crowds does not provide anonymity against global observers or eavesdroppers directly observing the sender [14], we omit these entities from the attacker model, and instead only include *(i)* the c corrupted users and *(ii)* the web server. In the analysis, we assume that a corrupted user is succeeding the sender in the path.

3.1 Anonymity Evaluations

Below, we evaluate the erlier scenarios against the metrics introduced in Section 2.3. We provide the details of the calculations only for scenario one. For the entropy-based metrics and the source-hiding property, we need the probability distribution $\mathcal{P}$. From the perspective of the c corrupted users, $\mathcal{P} = (0.56, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, 0)$, while from the perspective of the web server $\mathcal{P}$ is uniform. The probability $p_i = 0.56$ is calculated as: $p_i = \frac{n - p_f(n-c-1)}{n} = \frac{10-0.55*8}{10} = 0.56$ [14].

- *Anonymity set size:* against the web server, this metric yields $|\mathcal{U}| = 10$ for $S1$ and $|\mathcal{U}| = 1000$ for $S2 - S4$. The corrupted users only count the honest users $\mathcal{U}' = \mathcal{U} - c$. Thus, in this case $|\mathcal{U}'| = 9$ ($S1$), $|\mathcal{U}'| = 990$ ($S2$), and $|\mathcal{U}'| = 800$ ($S3$, $S4$).
- *Crowds-based metric:* A_i against the web server is `beyond suspicion`, as all users in $\mathcal{U}$ are equally likely of being the sender. If expressing A_i as $1 - p_i$, we get $A_i = \frac{9}{10}$, as p_i that any u_i is the sender is $\frac{1}{10}$. Assuming that one of the c corrupted users succeeds the user u_i in the path, A_i against the corrupted users is `possible innocence`. This is because the following inequality does not hold [14]: $n \geq \frac{p_f}{(p_f - 1/2)} * (c+1)$. Instead, the corrupted users can say with $p_i = 0.56$ that u_i is the sender (i.e., $A_i = 1 - p_i = 0.44$).
- *Entropy-based metrics:* according to Serjantov / Danezis [15], the effective anonymity set size against the corrupted users is calculated as $\mathcal{S} = -\sum_{i=1}^{n}(p_i * log_2 p_i) = 1.83477 \approx 1.83$ bits. According to the metric proposed by Díaz *et al.* [4], the degree of anonymity is instead calculated as $d = \frac{H(\mathcal{P})}{log_2(n)} \approx 0.55$. Regarding the web server, Díaz *et al.*'s metric gives us $d = 1$, as $\mathcal{P}$ is uniform. Using Serjantov / Danezis's metric, we get $\mathcal{S} \approx 3.32$ bits.
- *The source-hiding property:* the greatest p_i the corrupted users can assign to any u_i is $\max(\mathcal{P}) = 0.56$, and thus $\Theta = 0.56$. Against the web server, $\Theta = \max(\mathcal{P}) = \frac{1}{10}$.

In Table 1, we list the degrees of anonymity for the above scenarios. For comparison, we also include $d(\mathcal{P}, U)$ according to the Euclidean distance in n-space.

Table 1: Anonymity evaluation of scenarios (incl. Euclidean distance).

	Scen.	c corrupted users	Web server
Anonymity	`S1`	$\|\mathcal{U}\| = 9$	$\|\mathcal{U}\| = 10$
set size	`S2`	$\|\mathcal{U}\| = 990$	$\|\mathcal{U}\| = 1000$
	`S3 & S4`	$\|\mathcal{U}\| = 800$	$\|\mathcal{U}\| = 1000$
Crowds-	`S1 & S3`	`possible innocence`	`beyond suspicion`
based m.	`S2 & S4`	`probable innocence`	`beyond suspicion`
Entropy-	`S1`	$\mathcal{S} = 1.83$ bits	$\mathcal{S} = 3.32$ bits
based	`S2`	$\mathcal{S} = 6.37$ bits	$\mathcal{S} = 9.97$ bits
metric	`S3`	$\mathcal{S} = 5.23$ bits	$\mathcal{S} = 9.97$ bits
(Serjantov / Danezis)	`S4`	$\mathcal{S} = 6.75$ bits	$\mathcal{S} = 9.97$ bits
Entropy-	`S1`	$d = 0.55$	$d = 1$
based	`S2`	$d = 0.63$	$d = 1$

metric	S3	$d = 0.52$	$d = 1$
(Díaz *et al.*)	S4	$d = 0.68$	$d = 1$
Source-	S1	$\Theta = 0.56$	$\Theta = 1/10$
hiding	S2	$\Theta = 0.46$	$\Theta = 1/1000$
property	S3	$\Theta = 0.56$	$\Theta = 1/1000$
	S4	$\Theta = 0.40$	$\Theta = 1/1000$
Euclidean-	S1	$d(\mathcal{P}, U) = 0.49$ (max: 0.95)	$d(\mathcal{P}, U) = 0$
distance in	S2	$d(\mathcal{P}, U) = 0.46$ (max: 0.995)	$d(\mathcal{P}, U) = 0$
in n-space	S3	$d(\mathcal{P}, U) = 0.56$ (max: 0.995)	$d(\mathcal{P}, U) = 0$
	S4	$d(\mathcal{P}, U) = 0.40$ (max: 0.995)	$d(\mathcal{P}, U) = 0$

Some Observations from the Evaluation Results:

- All metrics except the anonymity set size consider probabilities. This is evident in the results as the difference in the degree of anonymity against the corrupted users and the web server is much less significant for the anonymity set size.
- Although stated in [15], we do not think that Serjantov / Danezis's metrics reflect the "effective anonymity set size" (as the endpoints do not overlap with those of the anonymity set size metric). We also think that the max anonymity (given n) should be made explicit. That is, $\mathcal{S}$ could be expressed as $H(P)$ out of $log_2(n)$ bits.
- Against the corrupted users, most metrics yielded the highest anonymity in $S4$.
- $d(\mathcal{P}, U)$ according to the Euclidean distance in n-space seems to be fairly alike measuring distance based on entropy, although not exactly similar. Further analysis on the deviation between these different measures of $d(\mathcal{P}, U)$ is left as future research.

3.2 Criteria for Anonymity Metrics

As it is essential that an anonymity metric gives an accurate picture about the degree of anonymity, we below state a set of criteria that an anonymity metric should meet.

- A user can be said to be de-anonymized when an attacker can, beyond reasonable doubt, pinpoint a user as the sender of an observed communication (step 3 in Section 2.2). Thus, the analyst must, in one way or another, consider probabilities.

  ⇒ *C1: An anonymity metric should base its analysis on probabilities.*

- The endpoints in an anonymity metric are "no anonymity" and "max anonymity". The meaning of 'max anonymity' can differ between different metrics. In metrics solely based on $\mathcal{P}$, max anonymity occurs when $\mathcal{P}$ is uniform and no anonymity occurs if: $\exists p_i \in \mathcal{P}$; $p_i >> \max\{\mathcal{P} - p_j\}$, where $p_i \neq p_j$. A uniform $\mathcal{P}$ would yield (a special case of) `beyond suspicion` in the Crowds-based metric for any $u_i \in \mathcal{U}$. Yet, max anonymity for u_i in the Crowds-based metric – `absolute privacy` – does not correspond to max entropy, as $p_i = 0$ for u_i, and thus $\mathcal{P}$ is not uniform. Still, an anonymity metric should model these two endpoints in a theoretically sound manner.

  ⇒ *C2: An anonymity metric must have well defined and intuitive endpoints.*
- Intuitively, the more uniform the $\mathcal{P}$, the more uncertain the attacker is. A metric should preserve this relation (recall the representation condition [13]). Thus, a degree of anonymity should increase if the uniformness of $\mathcal{P}$ increases, and vice versa.

  ⇒ *C3: The more uniform the distribution $\mathcal{P}$, the higher the anonymity.*
- Assuming an unchanged uniformity of $\mathcal{P}$: the more the (honest) users in $\mathcal{U}$, the more the potential senders, and thus the higher the attacker's uncertainty. A metric should preserve this relation according to the representation condition. Thus, the degree of anonymity should increase if the number of users increases, and vice versa.

  ⇒ *C4: The more the users in the anonymity set, the higher the anonymity.*
- By studying the degree of anonymity in a scenario, an analyst should be able to judge where in between the two endpoints (no & max anonymity) the current degree is. Thus, all values in the value domain of an anonymity metric should be well defined.

  ⇒ *C5: The elements in the metric's value domain should be well defined.*
- An anonymity metric should use a scale preserving the ordering among elements, such as ordinal, interval, ratio, or absolute scale [13]. Further, it should be fined-grained enough to differ between seemingly similar, but not equivalent, scenarios.

  ⇒ *C6: The value range of the metric should be ordered and not too coarse.*

Next, we evaluate the aforementioned anonymity metrics against these criteria.

3.3 Evaluation of Anonymity Metrics against Criteria

In Table 2, we assess whether the studied metrics fulfill the earlier stated criteria.

Table 2: Evaluation against criteria.

Anonymity set size metric	C1	-	Neither $\lvert\mathcal{U}\rvert = n$ nor $log_2(\lvert\mathcal{U}\rvert)$ consider (dynamic) probabilities.
	C2	-	As this is an absolute measure, the metric always outputs n, which can vary between 1 and ∞. Difficult to state a "good-enough" value for n.
	C3	-	Not fulfilled, as this metric does not consider probabilities.
	C4	+	Fulfilled, as the degree of anonymity is $\lvert\mathcal{U}\rvert = n$.
	C5	+	n simply entails the number of users in the anonymity set ($\lvert\mathcal{U}\rvert$).
	C6	+	Fulfilled, as this metric uses absolute scale.
Crowds-based metric	C1	+	Fulfilled, as output corresponds directly to the probability of being the sender an attacker can assign to the sending user in a system.
	C2	+	The metric varies between `provably exposed` and `absolute privacy`, where each intermediary category is semantically mapped to probabilities.
	C3	-	Not always true as individual probabilities are quantified.
	C4	+	In general fulfilled, assuming that the corresponding $p_i > 0$. Specifically, increasing n helps fulfilling $n \geq \frac{p_f}{(p_f - 1/2)} * (c+1)$ in the scenarios.
	C5	+	Categories are based on the underlying probability of being the sender.
	C6	-	Although ordinal scale is used, the output is fairly coarse.
Entropy-based metric (Serjantov / Danezis)	C1	+	Based on the entropy of the probability distribution.
	C2	-	The endpoints are 0 and $log_2(n)$. The latter is hard to calculate by hand.
	C3	+	Fulfilled, if we assume $d(\mathcal{P}, U) = H(U) - H(\mathcal{P})$.
	C4	+	Fulfilled. Note that the maximum increases with an increasing n.
	C5	-	States that an attacker on average has to find the answer for at least $H(P)$ binary questions to identity the sender which is not perfectly intuitive.
	C6	+	This criterion is fulfilled as ratio scale is used.
Entropy-based metric (Díaz *et al.*)	C1	+	Based on the entropy of the probability distribution.
	C2	+	Clear endpoints: 0 (no anonymity) and 1 (max anonymity).
	C3	+	Fulfilled, if we assume $d(\mathcal{P}, U) = \frac{H(\mathcal{P})}{H(U)}$.
	C4	-	This criterion is not fulfilled, as the resulting d is normalized.
	C5	+	Easy to interpret as d denotes the quotient between $H(\mathcal{P})$ and $H(U)$.
	C6	+	This criterion is fulfilled as ratio scale is used.
Source-hiding property	C1	+	Θ is directly based on the greatest probability in $\mathcal{P}$, as $\Theta = \max(\mathcal{P})$.
	C2	-	The use of an inverted scale is somewhat confusing (best case: $\Theta = 0$).
	C3	-	Although it can be expected to be true in many real scenarios, it may not coincide as the output is merely an individual probability.
	C4	+	Fulfilled, assuming corresponding $p_i > 0$ for added users.

	C5	+	Θ is the max probability (of being the sender) any user in the anonymity set can be assigned of by the attacker. In real scenarios, it will probably often overlap with the probability assigned to the real sender.
	C6	+	This criterion is fulfilled as ratio scale is used.

We can note in Table 2 above that no metric fulfill all criteria.

4 The Scaled Anonymity Set Size Metric

In Section 3.3, we saw that no anonymity metric fulfilled all criteria. For this reason, this section proposes an alternative entropy-based anonymity metric – the scaled anonymity set size metric – that is designed to fulfill these criteria.

Definition 1. *The scaled anonymity set size for a given distribution $\mathcal{P}$ is defined as:*

$$A = 2^{H(\mathcal{P})} \tag{2}$$

Equation (2) increases with an increasing uniformity of $\mathcal{P}$ and varies between 1 (when $\exists p_i \in \mathcal{P}\ ;\ p_i = 1$) and $n = |\mathcal{U}|$ (when $\mathcal{P}$ is uniform). The endpoints are intuitive as $max(A) = n$ equals the the actual size of the anonymity set and $min(A) = 1$ denotes a singleton set (i.e., the sender is identified). In the next sections, the underlying semantics of the scaled anonymity set size are explained. In particular, we show that $H(\mathcal{P})$ denotes a lower bound for the average number of yes-no questions an attacker needs to answer to identity the sender; thus, $2^{H(\mathcal{P})}$ is the the expected number of possible outcomes – or the effective support size of $H(\mathcal{P})$ (see below) – given this lower bound.

4.1 Theoretical Background

This section elaborates on the underlying semantics of the scaled anonymity set size by relating $H(\mathcal{P})$ and $2^{H(\mathcal{P})}$ to concepts such as Huffman codes, Huffman trees, expected number of questions (EQ), and the effective support size of the entropy (ESS).

Source codes and optimality. A *source code* is a mapping that assigns short descriptions (code words) to the most frequent outcomes of a data source (i.e., a random variable) and longer descriptions to less frequent outcomes. Source codes are often used in, e.g., data compression. Formally, the data source outputs symbols from an alphabet, where each symbol is associated with a weight stating the probability that it will be the next produced symbol by the data source. An *optimal* source code yields code words of minimum average length[3]. The following holds for optimal source codes, where L is the average length of the

[3] For more information on source codes and conditions for optimality, see for instance [3].

code words and $H(\mathcal{P})$ is the entropy of the probability distribution $\mathcal{P}$ (i.e., the weights) over the possible outcomes of the data source [16].

$$H(\mathcal{P}) \leq L < H(\mathcal{P}) + 1 \tag{3}$$

Huffman codes. A classical optimal source code is the *Huffman code* [10]. The basic technique for producing Huffman codes is to create a binary tree, called a *Huffman tree*, from which the set of code words can be derived[4]. Each leaf in the tree corresponds to one possible outcome from the data source, and the code word corresponding to the data source is retrieved by traversing the tree from the root note to the given leaf node, while adding '0' to the code if a left branch is selected and '1' if a right branch is selected. See Figure 2 for an illustration, where the grey leaf nodes represent the possible outcomes and the digits to the left of the colons in the branch labels above the leaf nodes denote the respective code words for these possible outcomes.

The game of 20 questions and its relation to Huffman codes. In [3], the game of 20 questions is defined as the act of finding the most efficient series of yes-no questions to determine an object from a class of objects (assuming that we know the probability distribution $\mathcal{P}$ on the objects). It is shown in [3] that an optimal solution to this game is to create a Huffman tree based on $\mathcal{P}$ where the objects constitute the leaf nodes. Then, the strategy is to traverse the Huffman tree from the root node, and at each intermediary node ask the question "Is the sought object below the left branch or right branch?". Using this strategy, the average number of questions needed to identify the object, EQ, will coincide with the expected length L of the Huffman code (where the latter is determined by traversing the Huffman tree). Thus, Equation (3) can be rewritten as:

$$H(\mathcal{P}) \leq EQ < H(\mathcal{P}) + 1 \tag{4}$$

Anonymity attacks and their relation to Huffman codes. The game of 20 questions (see above) corresponds directly to a situation when an anonymity attacker is trying to single out a sender from a group of users by using an optimal divide-and-conquer strategy on the user sets (i.e., binary search). If we assume that the attacker has derived $\mathcal{P}$, he can use the following strategy to identify the sender. First, he creates a Huffman tree, where the users in $\mathcal{U}$ constitute the leaf nodes in the tree (see Figure 2). The attacker then starts at the root node in the tree. Now, he needs to answer a series of yes-no questions of the type "is the sender in the group of users in the subtree below the left branch or below the right branch". By answering a certain number of such yes-no questions, the attacker will eventually end up in one of the leaf nodes in the tree, and now the sender is identified as the user corresponding to the current leaf node. As with the game of 20 questions, the expected number of yes-no questions that the attacker needs to answer, EQ, is bounded by $H(\mathcal{P})$ according to Equation (4).

[4] For more information on Huffman codes and Huffman trees, see for instance [3].

Support size and effective support size. In coding theory, the *support size* of a variable X with a probability distribution $\mathcal{P}$ is denoted $S(\mathcal{P})$. The support size is the size of the value domain of X (only counting outcomes whose corresponding $p_i \in \mathcal{P}$ are greater than zero). For example, if X is the outcome of a toss of a coin, $S(\mathcal{P}) = 2$. The support size is not affected by changes in $\mathcal{P}$ as long as the indvidual probabilities are not set to zero. If, for example, the coin was manipulated so that $\mathcal{P}' = (\frac{1}{10}, \frac{9}{100})$, $S(\mathcal{P}')$ would still yield two. On the other hand, the *effective support size* (ESS) for a variable X with probability distribution $\mathcal{P}$ outputs a value in the range $1 \leq ESS(\mathcal{P}) \leq S(\mathcal{P})$, depending on the degree of uniformity of $\mathcal{P}$, where $ESS(X) = 1$ if $\exists p_i \in \mathcal{P}$; $p_i = 1$ and $ESS(\mathcal{P}) = S(\mathcal{P})$ if $\mathcal{P}$ is uniform [9]. Grendar showed that it is appropriate to define $ESS(\mathcal{P}) = \exp\left(H(\mathcal{P})\right)$ for arbitrary log bases (and thus $ESS(\mathcal{P}) = 2^{H(\mathcal{P})}$ for log base two) [9]. The latter definition corresponds to the definition of the scaled anonymity set size metric. According to Grendar, $ESS(\mathcal{P})$ has a more natural meaning than the entropy $H(\mathcal{P})$, at least in the realms of statistics and probabilities.

On the semantics of the scaled anonymity set size. Above, we stated that the scaled anonymity set size represents the expected number of possible outcomes (alternatively: effective support size) given $H(\mathcal{P})$, which, in turn, is a lower bound for EQ – the expected number of yes-no questions an attacker needs to answer to identify the sender. This section presents a more intuitive explanation of the scaled anonymity set size. First, however, we prove the well known obsevation that the entropy of a variable X_1 with distribution $\mathcal{P}$, where $|X_1| = n$, equals the entropy of a variable X_2 with a uniform distribution, where $|X_2| = 2^{H(\mathcal{P})}$. Below, we state this property more formally in the context of anonymous communication (to improve clarity, the size of the user base is added as a parameter in the entropy expression for the remainder of this subsection).

Theorem 1. *The entropy $H(\mathcal{P}, n)$ of a probability distribution $\mathcal{P}$ over a user base $\mathcal{U}$ with n participants is equivalent to the entropy $H(U, n')$ of the uniform distribution U over a user base $\mathcal{U}'$ with $n' = 2^{H(\mathcal{P},n)}$ participants.*

Proof. [5]

The entropy $H(\mathcal{P}, n)$ in a user base $\mathcal{U}$ with n participants can be expressed as:

$$H(\mathcal{P}, n) = -\sum_{i=1}^{n} p_i log_2(p_i) \tag{5}$$

Now, $H(U, n')$ in a user base $\mathcal{U}'$ with $n' = 2^{H(\mathcal{P})}$ participants can be expressed as:

[5] This proof holds when $2^{H(\mathcal{P},n')}$ is an integer. Using differential entropy, Theorem (1) can be proved in a similar manner also for decimal numbers.

$$H(U,n') = -\sum_{i=1}^{n'} u_i log_2(u_i) = \tag{6}$$

$$-\sum_{i=1}^{2^{H(\mathcal{P},n)}} 2^{-H(\mathcal{P},n)} log_2(2^{-H(\mathcal{P},n)}) = \tag{7}$$

$$H(\mathcal{P},n)2^{-H(\mathcal{P},n)} \sum_{i=1}^{2^{H(\mathcal{P},n)}} 1 = H(\mathcal{P},n) \tag{8}$$

Upon the basis of Theorem 1 and its proof, we can state the following theorem.

Theorem 2. *The degree of anonymity according to the scaled anonymity set size in a user base $\mathcal{U}$ with n participants, $A = 2^{H(\mathcal{P},n)}$, is* equivalent *to the degree of anonymity $A = 2^{H(U),n'}$ in a user base $\mathcal{U}'$ with $n' = 2^{H(\mathcal{P},n)}$ participants, hence $A = 2^{H(\mathcal{P},n)} = 2^{H(U,n')} = n'$.*

Proof. This follows trivially from: $H(\mathcal{P},n) = H(U,n') \Rightarrow 2^{H(\mathcal{P},n)} = 2^{H(U,n')} = n'$.

Informally, this means that a sender that participates in a communication where, for instance, $A = 10$ according to the scaled anonymity set size metric is as anonymous as he would be in a group of 10 users, where all users are equally likely of being the origin sender (regardless of the size of the original user base).

On the relationship between $A = 2^{H(\mathcal{P})}$ and EQ. Finally, to express a relation between $A = 2^{H(\mathcal{P})}$, $ESS(\mathcal{P})$, and EQ, we can rewrite Equation (4) as:

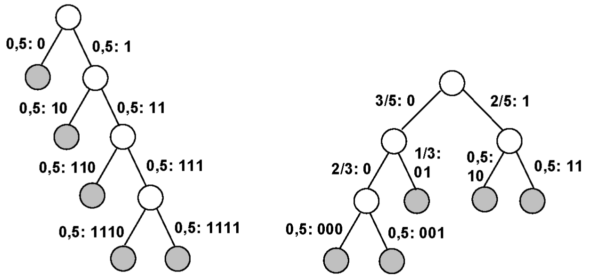
$$2^{H(\mathcal{P})} \leq 2^{EQ} < 2^{H(\mathcal{P})+1} \Rightarrow 2^{H(\mathcal{P})} \leq 2^{EQ} < 2 * 2^{H(\mathcal{P})} \tag{9}$$

From Equation (9) it follows that $1 \leq 2^{EQ} < 2n$, where $n = |\mathcal{U}|$. Thus, the theoretical minimum for the expected size of the solution space $2^{H(\mathcal{P})}$ (or effective support size) does not always match the *actual* expected solution space size 2^{EQ}. Yet, as $2^{H(\mathcal{P})} \leq 2^{EQ}$, the scaled anonymity set size never underestimates the effort an attacker must undertake to identity the sender. Still, in situations when $EQ > H(\mathcal{P})$, you could argue that it (and all other metrics based on entropy) "understates" the degree of anonymity, as in this case the theoretical minimum cannot be reached (as EQ is optimal).

Concluding notes. Above, we showed that entropy (and the scaled anonymity set size) are related to concepts such as optimal source codes and search trees, and, further, that the entropy gives a lower bound for how difficult it is to perform a binary search on the search space (see also [11] for more information). This means that entropy is well suited for quantifying security or anonymity in cases when the attacker conducts a binary search on the search space (i.e., uses a divide-and-conquer strategy), but it may be questionable whether entropy is a good measure in cases when the attacker conducts, e.g., a linear search on the search space (similar to a brute force attack). We suspect that in the context of anonymity attacks, the attacker behaves more intelligently than a simple (probability-based) linear search on the user base. Yet, we leave as future work asserting whether a model for anonymity attacks (such as the one in Section 2.2) corresponds to the anonymity attack based on Huffman codes described above.

4.2 Numerical Examples

Below follows two numerical examples in which we calculate the scaled anonymity set size and EQ. In these examples, we assume an attacker observing a system with five users. The attacker conducts attacks and, based on the information he learns from his attacks, calculates $\mathcal{P}$ regarding who is the sender in a particular communication.



(a) Example one. (b) Example two

Fig. 2. Huffman trees for examples one and two. The numbers to the left of the colons denote the probability for taking the given decision (left / right), while the right digits represent the code for the current position in the tree (0 = left and 1 = right). The leaf nodes represent the users.

Example one. Assuming that the attacker has calculated $\mathcal{P} = (p_{u_1} = \frac{1}{2}, p_{u_2} = \frac{1}{4}, p_{u_3} = \frac{1}{8}, p_{u_4} = \frac{1}{16}, p_{u_5} = \frac{1}{16})$, $H(\mathcal{P}) = 1{,}875$, and $A = 2^{H(\mathcal{P})} = 2^{1{,}875} = 3{,}67$ (max: 5). According to Equation (4), $H(\mathcal{P})$ denotes a lower bound for the expected number of yes-no questions the attacker needs to answer to identify the sender, while the reachable expected number of questions is given by EQ. The latter can be calculated by creating a Huffman tree based on $\mathcal{P}$ (left tree in Figure 2). Then, EQ can be calculated by using basic probability theory as $EQ = \frac{15}{8} = 1{,}875$. Hence, in this example $H(P) = EQ$.

Example Two. In this example, the attacker has obtained the (uniform) distribution $\mathcal{P} = (p_{u_1} = \frac{1}{5}, p_{u_2} = \frac{1}{5}, p_{u_3} = \frac{1}{5}, p_{u_4} = \frac{1}{5}, p_{u_5} = \frac{1}{5})$. Now, he can determine $H(\mathcal{P}) \approx 2,32$, $EQ = \frac{12}{5} = 2,4$ (see the right Huffman tree in Figure 2), and $A = 2^{H(\mathcal{P})} = 2^{2,32} = 5$ (max: 5). Thus, the maximum degree of anonymity is achieved in this example, and, contrary to the former example, the entropy $H(\mathcal{P})$ is here slightly lower than EQ.

4.3 Evaluation against Scenarios and Criteria

In Table 3, we calculate the degree of anonymity according to the scaled anonymity set size metric for the four scenarios defined in Section 3, while in Table 4 the scaled anonymity set size metric is evaluated against the criteria defined in Section 3.3. Table 3 shows that the ordering among the scenarios equals that of the Serjantov / Danezis metric [15]. Yet, we argue that the linear scale in the scaled anonymity set size metric more clearly shows that, e.g., A in scenario one is far lower than in the other scenarios. Further, Table 4 shows that all criteria are fulfilled for the scaled anonymity set size.

Table 3: Degrees of anonymity for the scaled anonymity set size.

	Scen.	c corrupted users	Web server
Scaled anonymity set size	`S1`	$A = 2^{H(\mathcal{P})} = 2^{1.83} = 3.6$ (for $n = 10$)	$A = 2^{log_2(10)} = 10$
	`S2`	$A = 2^{H(\mathcal{P})} = 2^{6.37} = 83$ (for $n = 1000$)	$A = 2^{log_2(1000)} = 1000$
	`S3`	$A = 2^{H(\mathcal{P})} = 2^{5.23} = 38$ (for $n = 1000$)	$A = 2^{log_2(1000)} = 1000$
	`S4`	$A = 2^{H(\mathcal{P})} = 2^{6.75} = 108$ (for $n = 1000$)	$A = 2^{log_2(1000)} = 1000$

Table 4: Evaluation of scaled anonymity set size against criteria.

Scaled anonymity set size	`C1`	+	Fulfilled, as this metric is based on probabilities.
	`C2`	+	Intuitive and well defined endpoints where A varies between 1 and n.
	`C3`	+	This criterion is fulfilled as A is based on the uniformity of $\mathcal{P}$.
	`C4`	+	Fulfilled, as max anonymity increases with n: $\max(2^{H(\mathcal{P})}) = 2^{log_2(n)}$.
	`C5`	+	$A = 2^{H(\mathcal{P})}$ is the size of the corresponding anonymity set in a user base where all users are equally likely of being the sender (see Theorem 2).
	`C6`	+	Fulfilled, as the scaled anonymity set size metric uses ratio scale.

4.4 Related Work on Quantifying Anonymity as $A = 2^{H(\mathcal{P})}$

To the authors' best knowledge, the consequences of quantifying the degree with which a user can be linked to a communication as $A = 2^{H(\mathcal{P})}$ have not previously been formally analyzed. However, in the context of anonymized databases, $2^{H(\mathcal{P})}$ have previously been proposed as measure of the risk of re-identification.

- In [8], Fischer-Hübner proposed to use $2^{H(\mathcal{X}_1,\ldots,\mathcal{X}_n)}$ as a measure of how many combinations of the value ranges of $\mathcal{X}_1,\ldots,\mathcal{X}_n$ that can be used for re-identification. A high value of $2^{H(\mathcal{X}_1,\ldots,\mathcal{X}_n)}$ means that the attacker is more likely to re-identify the user;
- Shortly after the pre-proceedings version of this paper was published, Bezzi proposed in [1] to use $2^{H(\mathcal{R}|s)}$ to quantify the number of different records in an anony-mized database that could correspond to the user, where $H(\mathcal{R}|s)$ denotes the conditional entropy between the anonymized and the original database. In this example, a high value of $2^{H(\mathcal{R}|s)}$ instead indicates a lower risk of re-identification for the user.

5 Summary & Outlook

In this paper, we discussed elementary properties of anonymity metrics. We defined a set of example scenarios for Crowds and quantified the degree of anonymity in these scenarios for some recent metrics. Based on the evaluation and measurement theory, we then defined a set of criteria for anonymity metrics, and assessed whether the studied metrics fulfilled these criteria. Lastly, we proposed to quantify anonymity as $A = 2^{H(\mathcal{P})}$ (denoted the scaled anonymity set size metric) and showed that this metric fulfilled the above criteria. Future work includes further analyzing the underlying semantics of scaled anonymity set size and other entropy-based metrics, formalizing a model for anonymity attacks and relating it to different optimal search strategies, as well as studying the correlation between different ways of quantifying the uniformity of probability distributions and their relation to different metrics.

Acknowledgements

Parts of this work have been funded by the EU FP6 project PRIME (Contract No. 507591) and the IST FIDIS (Future of Identity in the Information Society) Network of Excellence project (Contract No. 507512).

References

1. Michele Bezzi. An Entropy Based Method for Measuring Anonymity. In *Proceedings of the 3^{rd} International Workshop on the Value of Security through Collaboration (SECOVAL 2007) in conjunction with the 3^{rd} International Conference on Security and Privacy in Communication Networks (SecureComm2007)*, Nice, France, 17–20 Sep 2007. IEEE Xplore Digital Library.

2. David Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *J. Cryptography*, 1(1):65–75, 1988.
3. Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley, 1991.
4. Claudia Díaz, Stefaan Seys, Joris Claessens, and Bart Preneel. Towards Measuring Anonymity. In Dingledine and Syverson [5].
5. Roger Dingledine and Paul Syverson, editors. *Proceedings of the* 2nd *Workshop on Privacy Enhancing Technologies (PET 2002)*, volume 2482 of *LNCS*, San Fransisco, CA, USA, Apr 2002. Springer-Verlag.
6. John R. Douceur. The Sybil Attack. In P. Druschel, F. Kaashoek, and A. Rowstron, editors, *Peer-to-Peer Systems: Proceedings of the 1st International Peer-to-Peer Systems Workshop (IPTPS)*, volume 2429, pages 251–260, Cambridge, MA, USA, 7–8 Mar 2002. Springer-Verlag.
7. Norman E. Fenton and Shari Lawrence Pfleeger. *Software Metrics – A Rigorous & Practical Approach*. PWS Publishing Company, 20 Park Plaza, Boston, MA 02116-4324, second edition, 1997.
8. Simone Fischer-Hübner. *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*, volume 1958 of *LNCS*. Springer-Verlag, May 2001.
9. Marian Grendar. Entropy and Effective Support Size. *Entropy*, 8(3):169–174, Aug 2006. Short note.
10. David A. Huffman. A Method for the Construction of Minimum-Redundancy Codes. *Proceedings of the Institute of Radio Engineers*, 40(9):1098 – 1101, Sep 1952.
11. Reine Lundin, This J. Holleboom, and Stefan Lindskog. On the Relationship between Confidentiality Measures: Entropy and Guesswork. In *Proceedings of the 5th International Workshop on Security in Information System (WOSIS 2007), held in conjuction with* 9th *International Conference on Enterprise Information Systems*, pages 135 – 144, Madeira, Portugal, 12–13 Jun 2007.
12. Andreas Pfitzmann and Marit Hansen. Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology v0.29, 31 Jul 2007.
13. Jean-François Raymond. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In H. Federrath, editor, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, volume 2009 of *LNCS*, pages 10–29. Springer-Verlag, July 2000.
14. Michael Reiter and Avi Rubin. Crowds: Anonymity for Web Transactions. In *DIMACS Technical report*, pages 97–115, 1997.
15. Andrei Serjantov and George Danezis. Towards and Information Theoretic Metric for Anonymity. In Dingledine and Syverson [5].
16. Claude E. Shannon. A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27:379–423, Jul 1948.
17. Gergely Tóth and Zóltan Hornák. Measuring Anonymity in a Non-Adaptive, Real-Time System. In David Martin and Andrei Serjantov, editors, *Proceedings of the* 4th *Workshop on Privacy Enhancing Technologies (PET 2004)*, pages 226–241, Toronto, Canada, 26–28 May 2004.
18. Matthew K. Wright, Micah Adler, and Brian Neil Levine. The Predecessor Attack: An Analysis of a Threat to Anonymous Communication Systems. *ACM Transactions on Information and System Security*, 7(4):489–522, Nov 2004.