# A longitudinal approach to measuring the impact of mobility on low-latency anonymity networks

Stephen Doswell
Department of Computer Science and Digital Technologies
Northumbria University Newcastle
Newcastle upon Tyne, United Kingdom NE1 8ST
Email: stephen.doswell@northumbria.ac.uk

Nauman Aslam
Department of Computer Science and Digital Technologies
Northumbria University Newcastle
Newcastle upon Tyne, United Kingdom NE1 8ST
Email: nauman.aslam@northumbria.ac.uk

David Kendall
Department of Computer Science and Digital Technologies
Northumbria University Newcastle
Newcastle upon Tyne, United Kingdom NE1 8ST
Email: david.kendall@northumbria.ac.uk

Graham Sexton
Department of Computer Science and Digital Technologies
Northumbria University Newcastle
Newcastle upon Tyne, United Kingdom NE1 8ST
Email: g.sexton@northumbria.ac.uk

***Abstract*—The increasing mobility of Internet users is becoming an emerging issue for low-latency anonymity networks such as Tor. The increase in network churn, generated by a growing mobile client base recycling connections, could impact maintaining the critical balance between anonymity and performance. New combinatorial approaches for measuring both anonymity and performance need to be developed in order to identify critical changes to the network dynamics, and trigger intervention if and when required. We present $q$-factor, a novel longitudinal approach to measuring anonymity and performance within highly dynamic environments. By modelling $q$-factor, we show that the impact of mobility, over time, on anonymity is significant. However, by using $q$-factor, we are able to anticipate and significantly reduce the number of these critical events occurring. In order to make more effective strategic design and/or real-time network decisions in the future, low-latency anonymity networks will be required to adopt an even more proactive approach to network management. The potential impact from increasing mobile usage needs to be considered, as what may initially be perceived as a good solution, may in fact degrade, or in the worst case could destroy the anonymity of users over time.**

***Keywords: Anonymity, Privacy-Enhancing Technology, Security Monitoring and Management.***

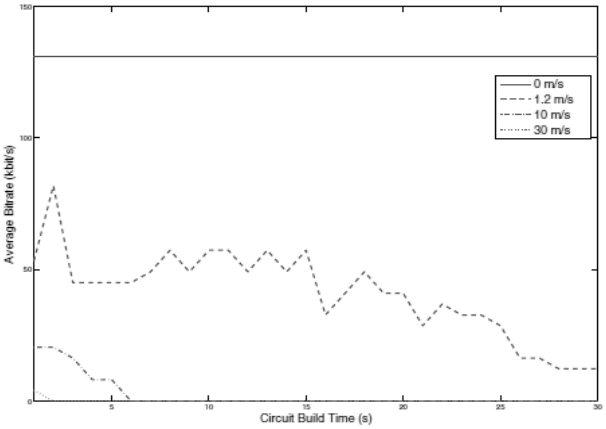


Fig. 1. The effect of mobility on client performance, over the Tor network, at different mobility speeds and circuit build times from Doswell *et al.* (2013) [5]. NB: The results for 30 m/s are not clearly visible, as almost linear to the X-axis, due to only a few downloads being successfully completed during the scenario at a circuit build time of approximately 1 to 2 seconds.

## I. Introduction

Maintaining the optimal balance between anonymity and performance is critical for low-latency anonymity networks, such as Tor [1]. Design considerations including the number of 'hops' within a circuit, is one example of how the need to maintain this balance has influenced design [2]. Research also shows that poor performance, by deterring usage, can impact anonymity by reducing the number of concurrent users and subsequently the overall size of the anonymity set [3].

The development of smartphone technology is increasing Internet usage from wireless-enabled devices. However, anonymity networks are currently designed for wired Internet connections. Mobile users may access the Internet from a range of networks and/or service providers (cellular, Wi-Fi). However, even for the same service such as BT Wi-Fi, which currently provides more than 5 million hot-spots within the United Kingdom, the service allocates a different external IP address after each hand-off [4]. Due to the current design of Tor, the connection to the Tor network breaks whenever a client's external IP address changes, requiring an extended time-to-recovery while building new Tor circuits, as shown in Figure 1 [5].

In 2010, Orbot was released enabling access to the Tor network from mobile Android™ devices. A limited amount of research has so far examined the impact of mobile usage on low-latency anonymity networks, such as Tor [5][6][7][8]. Although an important starting point, the previous studies do not address the impact of mobility on *both* anonymity and performance, over time, from mobile users recycling their connections.

978-1-4799-5344-8/15/$31.00 ©2015 IEEE

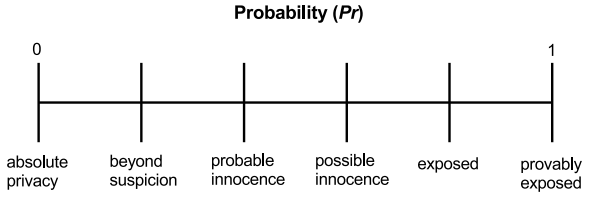


Fig. 2. An anonymity scale, proposed by Reiter and Rubin, in which the degree of anonymity depends on the probability that an agent engaged in some communication event, as determined by an attacker [10].

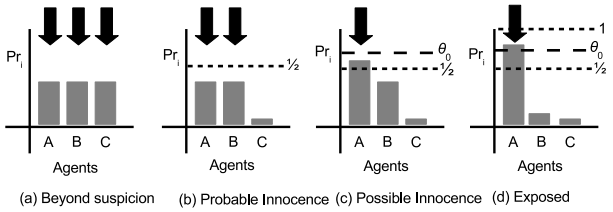


Fig. 3. Pre (a) and post-attack (b, c, d) anonymity dynamics, adapted from Kelly *et al.* (2012) [9].

In this paper, by modelling mobility and network churn, we illustrate the potential impact from mobile usage, over time, on low-latency anonymity networks. We present a new metric ($q$-factor) for measuring both anonymity and performance. Finally, we enable more strategic design and, potentially, support dynamic network management, in the future.

## II. Measuring anonymity and performance

Anonymity networks, such as Tor, were originally designed for persistent Internet connections, and therefore anonymity metrics have evolved accordingly. The increasing mobility of users requires a new approach for measuring anonymity, as Kelly *et al*. state, "wired-based anonymity metrics have limited applicability to mobile, wireless environments" [9].

Accurately measuring anonymity is a long-standing research problem. The simplest, most general, method to measure anonymity is to use an anonymity set (AS). The degree of anonymity provided by an AS is directly proportional to the size of the set, i.e. to the number of agents it contains. For example, if Alice is a member of an AS of size $N$, and Eve observes a message originating from that set, then, in the absence of further information, the probability, $P$, that Alice is the sender of the message is determined by Eve to be $\frac{1}{N}$. Figure 2 shows the anonymity scale, proposed by Reiter and Rubin, in which the degree of anonymity depends on the probability that an agent engaged in some communication event, as determined by an attacker [10]. We observe that, with increasing network churn, as the circuits of mobile users are recycled, the degree of anonymity may vary dynamically due to the susceptibility of agents to statistical disclosure or intersection attacks [11]. This is illustrated for sender anonymity in Figure 3 and also described below [9]:

1) Absolute privacy: the probability, $Pr_x$, that an agent $x \in$ AS sent the message is determined to be 0. This would be the case when the sending of a message was unobserved by the attacker;
2) Beyond suspicion: agent $x$ is no more likely to have sent the message than anyone else. This is also known as total, perfect, or strongly probabilistic anonymity, see Figure 3(a);
3) Probable Innocence: agent $x$ is no more likely to have sent the message than not to have sent the message. In Figure 3(b), agents A and B have $Pr_A = Pr_B = 0.45$, and so are probably innocent, but C is beyond suspicion since $Pr_C = min(Pr_i) = 0.10 < Pr_A$;
4) Possible innocence: there is a non-trivial probability that an agent other than $x$ sent the message. In Figure 3(c), $\theta_0$ is a parameter chosen to specify the threshold of non-trivial probability, and we have $\theta_0 > Pr_A = \max(Pr_i) > 0.5 > Pr_B > Pr_C$. As $Pr_A$ is slightly above 0.5 but is below the threshold, $\theta_0$, there is a non-trivial probability that some other agent sent the message, and therefore agent A is regarded as possibly innocent. Agent B is probably innocent, while agent C is beyond suspicion;
5) Exposed: it is very likely that agent $x$ is the sender of the message or $Pr_x = max(Pr_i) >= \theta_0$. As Figure 3(d) shows, agent A is exposed;
6) Provably exposed: The attacker knows agent $x$ sent the message or $Pr_x = 1$.

It is noted that other approaches for measuring anonymity, such as the use of entropy, are also widely used [12][13]. However, entropy-based approaches are more effective when low-level information, such as 'user-agent' headers, can be observed [14]. As the primary aim of this study is to demonstrate q-factor, a pluggable combinatorial metric, a simple anonymity set will be adopted for the high-level modelling.

Anonymity networks also provide challenges in terms of measuring performance due to their inherent nature, i.e., maintaining the anonymity of users. Network-based metrics are primarily used by Tor as a general indicator of performance rather than any user-specific data [15]. For example, Tor measures the performance that a relay provides for the network and uses this data to assign each relay a weighting based on the bandwidth provided. The observed bandwidth is then used for path selection, during circuit building, in order to distribute load toward relays with available network resources [16]. A number of studies have investigated more dynamic approaches to path selection within the Tor network, such as using round trip times (RTT) to measure real-time congestion on circuits, and drop and/or ignore circuits if congested [17]. However, in the current design of Tor, once a circuit is built it remains fixed, and is therefore unable to react automatically to any anonymity and/or performance issues for the user, however critical.

## III. $q$-factor

As previously stated, maintaining both anonymity and performance is critical for low-latency anonymity networks. The 'promise' of anonymous browsing on the World Wide Web (WWW) attracts millions of users to anonymity networks such as Tor [15]. In general terms, the higher the number of users, the larger the anonymity set (AS) and potentially the anonymity provided, i.e., the old adages of 'safety in numbers' and 'plausible deniability'. However, if performance degrades to a level where users are deterred (or even prevented) from

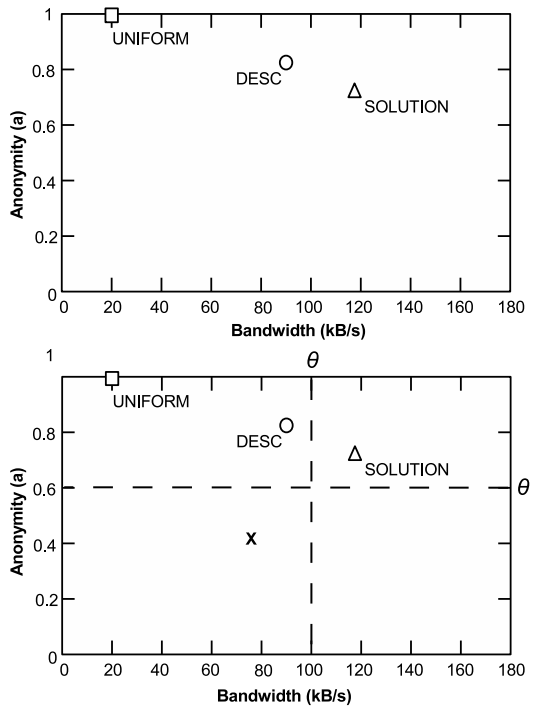


Fig. 4. Mapping anonymity and performance, adapted from Panchenko, Lanze, and Engel (2012), with (arbitrary) thresholds ($\theta$) applied, and an indicative marker (X) to illustrate a 'failed' solution [18].

using the network, then the anonymity set will reduce in size, potentially in a vicious cycle, where eventually the number of concurrent users offers little or no anonymity [12]. This suggests it is more appropriate to adopt a holistic approach, measuring anonymity and performance together, rather than separately, as more commonly used.

Panchenko, Lanze, and Enkel explored the critical balance between anonymity and performance while assessing different circuit path selection algorithms [18]. If thresholds are applied, in this case arbitrarily, to the mapping used by Panchenko, Lanze, and Enkel, it is easier to assess whether the minimum requirements for both anonymity and performance are met, either individually and/or together, as shown in Figure 4. For example, based on their findings, circuit path selection within the current design of Tor (DESC), although performing better overall than randomly allocating routers (UNIFORM), still does not meet the minimum requirements compared to the proposed solution (SOLUTION).

Although an important contribution, adopting this one-off 'snapshot' approach requires care, as any proposed solution could initially appear to provide the best overall balance between anonymity and performance, but when observed over time, may fall below one or both of the required thresholds. Additionally, although adopting a 'mean' value approach, in this case bandwidth (kB/s), is commonly used for performance, using the mean anonymity is considered flawed. The weakness of adopting this approach for measuring anonymity is that any occurrences where the level falls below the required threshold ($\theta_a$), i.e., a critical event, may not be captured. For example, a mean anonymity of $a = 0.67$, above $\theta_a$ = 0.50, may at

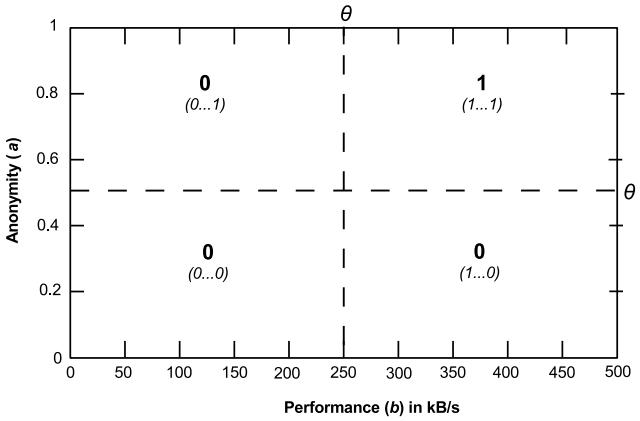


Fig. 5. The calculation of $q$-factor as the conjunction of both anonymity and performance based on specified thresholds.

certain points in time drop below the threshold and the degree of anonymity, provided by the solution, rather than *beyond suspicion* should actually be rated at best *possible innocence*, or *exposed/provably exposed* in the worst case scenario [10].

The risk from using the existing approaches to measuring the effectiveness of low-latency anonymity networks is that strategic design and/or or dynamic network management decisions are being made, which at best deliver poor performance, or in the worst case scenario compromise user anonymity. Therefore, any new approach should fully consider the effect of network churn over time, generated by mobile users recycling their connections, on anonymity and performance combined.

A proposed metric, known onwards as $q$-factor, for measuring both anonymity and performance, over time, is presented. The remainder of this paper defines the $q$-factor metric and illustrates how this novel approach can quickly help make more effective strategic design, or dynamic network management, decisions in the future.

Building upon the work of Panchenko, Lanze, and Enkel, if either anonymity and/or performance falls on or below the threshold at any point during the scenario, this event needs to be captured. To achieve this, a snapshot of both anonymity and performance are calculated periodically at an individual user, path, and network-wide level. This generates boolean values for both anonymity ($v_a$) and performance ($v_b$), based on specified thresholds, $\theta_a$ and $\theta_b$, for anonymity and performance, respectively, where:

$$v_a \equiv a > \theta_a \quad \text{and} \quad v_b \equiv b > \theta_b$$

The $q$-factor is calculated as simply the conjunction of $v_a$ and $v_b$, i.e. $q = v_b \cdot v_b$, as shown in Figure 5. A value of 0 for the $q$-factor indicates that some network management intervention is required, otherwise the network can continue to operate as it is.

## IV. Method

We restrict our attention to simple models of anonymity and performance in order to focus attention on the benefits of the $q$-factor approach. We note, however, that the approach can be easily adapted to work with more sophisticated models. Additionally, even though Tor is currently the most widely

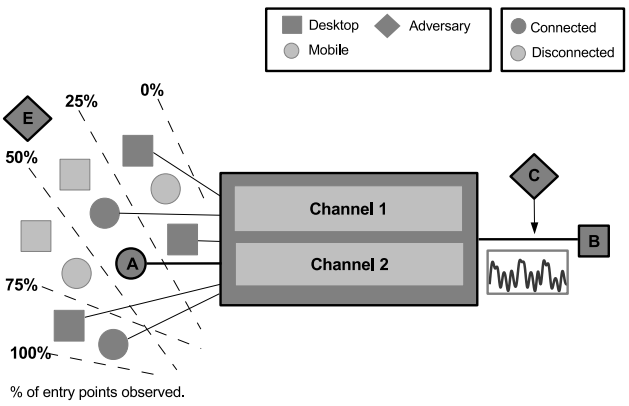


Fig. 6. The two-channel anonymous communication system used to assess the effectiveness of the $q$-factor metric, also illustrating the pervasive dynamics for Alice's (A) communications with Bob (B), observed by Charlie (C) and Eve (E).

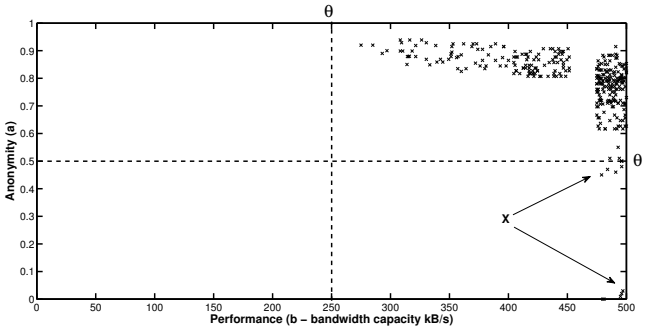


Fig. 7. The effect on anonymity and performance, over time, from the network churn of mobile users recycling connections. Observations, at 60-second intervals, showing the distribution of $q$ with critical events ($q = 0$) in bottom-right quartile (highlighted by X).

used anonymity network, to avoid excluding interest from other current and/or future designs of anonymity networks, a generic simulation, developed in Matlab™ is used for measuring the effectiveness of $q$-factor, as shown in Figure 6. Therefore, only two alternative paths, through the anonymity network, are implemented in order to provide rudimentary load-balancing. The two channels have different fixed bandwidth capacities assigned, of 2000kB/s and 3000kB/s, to help generate varying performance across the network, for the benefit of positive illustration. The small set of users ($N = 20$) is also intentional, in order to ensure anonymity falls below the required threshold during the scenario. The users are configured to randomly connect / disconnect at intervals of approximately 2 to 3 minutes during the scenario, reflecting the daily walk of one of the authors to University. The brisk 35 to 40-minute walk (3.7 km), covers five different Internet service providers (ISP) and a number of wireless access points within those networks, usually generating 15 hand-offs in total. Although the duration of the walk is longer, the analysis runs only for 10 minutes in order to reflect an existing security feature of Tor, whereby all circuits are recycled every 600 seconds, once downloads have been completed. During the scenario, the user is mobile and travelling at a constant velocity (speed and linear direction) as broadly in-line with the walk. More complex mobility models, e.g. Brownian motion, could be used if required but, in this case, would not add to the main thrust of the argument. As also used by Tor in the form of a 'circuit window', each user has a 500kB/s bandwidth cap applied, as application-level client throttling, in order to provide a fair distribution of resources, and maintain steady traffic flow, across the network. Based on the combined network capacity of 5000kB/s, the maximum number of connected users, and circuit window size, a performance threshold of $\theta_b = 250$ kB/s is chosen so that a range of performance levels on either side of the threshold can be observed.

An anonymity threshold of $\theta_a = 0.50$ is adopted, setting an 'acceptable' degree of anonymity at *probable innocence* or above, throughout the duration of the scenario.

Snapshots are taken of both anonymity and performance at one-second intervals, and $q$-factor ($q$) is derived for each user. If intervention is required (i.e., $q = 0$), then the remedy for anonymity is to simply re-direct one user to the failing channel. In the case of poor performance, the exact opposite is required, that is, to redirect one user away to the other channel, in order to recover bandwidth for the original channel. At the next scheduled interval, the anonymity network is then re-evaluated, intervention applied (again) if required, in order try and constantly maintain a $q$-factor of $q = 1$, continuing each interval thereafter until the end of the scenario. To assess the effectiveness of this approach, the following four schemes are compared:

- Scheme 1: No intervention ('stock');
- Scheme 2: Intervention (anonymity only);
- Scheme 3: Intervention (performance only);
- Scheme 4: Intervention (anonymity and performance).

The first scheme, Scheme 1, i.e., providing no intervention, acts as a baseline reflecting current anonymity network approaches ('stock'), such as found in Tor [1]. The second and third schemes assess whether applying only one type of intervention can improve, but maybe also impact the other element and subsequently the $q$-factor, and finally the results of applying both (Scheme 4), which is also hypothesised as being the optimum approach. The results are presented for each scheme as:

1) the percentage of snapshots where $q = 1$,
2) the network utilisation, and finally,
3) the recovery rate for cases with borderline anonymity.

## V. Results

The impact from mobility and increased network churn is illustrated, highlighted by X, in Figure 7. In this example, just by plotting the $q$-factor every 60 seconds, rather than a one-off observation, on a number of occasions anonymity ($a$) can be seen falling below its threshold, and returning $q$ = 0. It is important to note, in this example, that the $q$-factor, and underpinning $a$ and $b$ values, are still being calculated at one-second intervals, however the results are presented here, at every 60 seconds, for improved visual clarity.

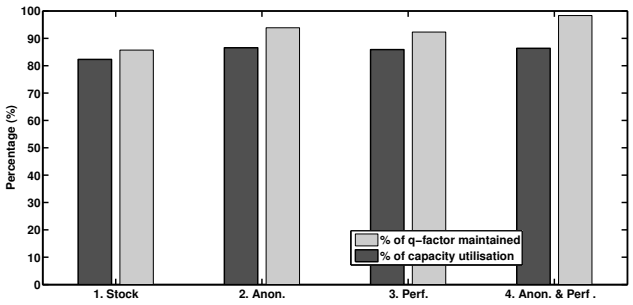


Fig. 8. A summary of the results showing the overall performance, both percentage of positive $q$-factor achieved and network capacity utilisation, after applying each of the schemes.

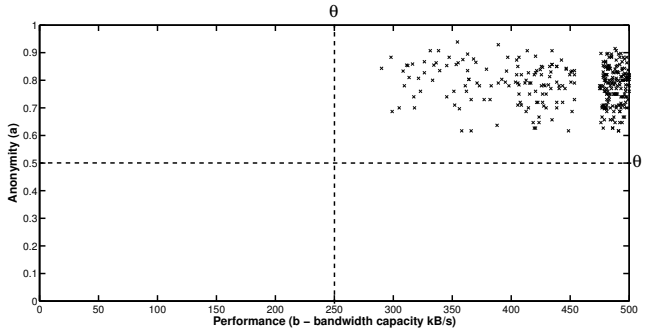


Fig. 9. The results from Scheme 4, with full intervention for both anonymity and performance, showing the distribution of $q$-factor move to the top-right quartile and the elimination of critical events compared to Figure 7.

At a high level, using the stock configuration without any form of intervention (Scheme 1), the overall percentage of $q$-factor being maintained ($q = 1$) is lowest at 85.70%, see Figure 8. By applying schemes 2 and 3, this increases to 93.86% and 92.31%, with an improvement of 9.52% and 7.71% respectively against the baseline figure (i.e. Scheme 1). Finally, Scheme 4, with full intervention for both anonymity and performance, provides the best overall performance at 98.32%, which is a 14.73% increase against baseline, and 4.75% over its nearest competitor. Also shown, in Figure 8, is the network-wide capacity utilisation, where, although the result is less clear-cut, again Scheme 1 provides the lowest performance, with each of the other schemes providing approximately 5% improvement over baseline.

At a more detailed level, the effectiveness of the intervention is clearly shown in Figure 9, where the previous cases (X) in Figure 7, have been eliminated, with distribution now completely secured within the top-right quartile ($q = 1$) or the proverbial 'goldilocks' zone. In this example, the overall percentage of borderline cases where the level of anonymity is either stabilised at the threshold or fully recovered is 83.92%, compared to no intervention where only 1.25% of cases are resolved 'organically' through natural network churn.

In summary, the best overall performing scheme is Scheme 4, providing intervention for both anonymity and performance and stock (Scheme 1), with no intervention, performing worst.

## VI. Discussion

The impact of mobility, over time, while trying to maintain the critical balance between anonymity and performance, is an emerging issue for low-latency anonymity networks such as Tor. Increasing network churn, generated by a growing mobile client base recycling connections, can significantly impact levels of anonymity, as shown within this study. However, intervention is currently, and predominantly, only used to maintain performance. This is *probably* still in part a valid approach, due to the relationship of performance on anonymity; and based on the findings from this study, better than no intervention at all. However, in the future, the validity of the current approaches used in maintaining the effectiveness of low-latency anonymity networks is debatable.

The $q$-factor metric, presented for the first time within this study, is a contribution to a solution to the problems being faced. At this early stage, it is clear that a more proactive approach, especially in maintaining anonymity, is required. It is found that, by even using relatively simple intervention approaches, a significant improvement in anonymity can be achieved. Therefore, the 'real-time' approaches currently being researched to improve performance across the Tor network, should also be evaluated for anonymity, preferably in a combinatorial form. However, the wider impact of any proposed solution will require careful consideration. For example, the overhead of redirecting users, as in the case of Tor, may take a few seconds in order to build a new circuit on a different path. Also, as observed during the modelling, intervention may generate 'strange' behaviour on the network, such as the 'oscillation' of users between channels, at each interval, especially when there is a very low number of users connected, which again may significantly impact performance if the redirection overhead is too high.

The critical importance in maintaining effective management of low-latency anonymity networks remains constant. However, the currently used approaches for measuring this effectiveness need to be adapted in order to respond to changing environments, such as the increased mobility of users, and to become more effective in supporting design and/or real-time network decisions in the future.

## VII. Conclusions

Based on our findings, we conclude that network churn, arising from an increasing mobile client base, can generate a critical impact on levels of anonymity and/or performance when observed over time. New and/or enhanced combinatorial approaches for measuring both anonymity and performance, as presented here in the form of $q$-factor, are required not only to evaluate the effectiveness of an anonymity network more accurately, but also to report any critical events. By adopting a more proactive approach to counteracting the impact from mobile usage, by using real-time intervention in order to mitigate any critically low anonymity and/or performance levels, low-latency anonymity networks such as Tor will continue to provide an essential service in the foreseeable future.

## References

[1] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[2] K. Bauer, J. Juen, N. Borisov, D. Grunwald, D. Sicker, and D. McCoy, "On the optimal path length for Tor," *HotPets in conjunction with Tenth International Symposium on Privacy Enhancing Technologies (PETS 2010), Berlin, Germany*, 2010.

[3] N. Borisov, G. Danezis, P. Mittal, and P. Tabriz, "Denial of service or denial of security? How attacks on reliability can compromise anonymity," in *Proceedings of CCS 2007*, October 2007.

[4] BT Wi-fi, "Find a hotspot," Website, 2015. [Online]. Available: http://www.btwifi.co.uk/find/

[5] S. Doswell, N. Aslam, D. Kendall, and G. Sexton, "The novel use of Bridge Relays to provide persistent Tor connections for mobile devices," in *2013 IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications: Mobile and Wireless Networks (PIMRC'13)*, London, September 2013.

[6] S. Doswell, N. Aslam, D. Kendall, and G. G. Sexton, "Please slow down! The impact on Tor performance from mobility," in *Proceedings of the Third ACM workshop on Security and Privacy in Smartphones and Mobile devices (CCS'13 - SPSM)*, Berlin, November 2013, pp. 87–92.

[7] C. Andersson and A. Panchenko, "Practical anonymous communication on the mobile internet using Tor," *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, pp. 39–48, 2007.

[8] R. Wiangsripanawan, W. Susilo, and R. Safavi-Naini, "Design principles for low latency anonymous network systems secure against timing attacks," in *Proceedings of the fifth Australasian symposium on ACSW frontiers (ACSW '07)*. Darlinghurst, Australia, Australia: Australian Computer Society, Inc, 2007, pp. 183–191.

[9] D. Kelly, R. Raines, R. Baldwin, M. Grimaila, and B. Mullins, "Exploring extant and emerging issues in anonymous networks: A taxonomy and survey of protocols and metrics," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 2, pp. 579–606, Second 2012.

[10] M. Reiter and A. Rubin, "Crowds: Anonymity for web transactions," *ACM Transactions on Information and System Security*, vol. 1, no. 1, June 1998.

[11] G. Danezis and A. Serjantov, "Statistical disclosure or intersection attacks on anonymity systems," in *Proceedings of 6th Information Hiding Workshop (IH 2004)*, ser. LNCS, May 2004.

[12] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*, R. Dingledine and P. Syverson, Eds. Springer-Verlag, LNCS 2482, April 2002.

[13] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*, R. Dingledine and P. Syverson, Eds. Springer-Verlag, LNCS 2482, April 2002.

[14] P. Eckersley, "How unique is your web browser?" in *Proceedings of the 10th Privacy Enhancing Technologies Symposium*, July 2010, pp. 1–18.

[15] The Tor Project, "Tor metrics," Website, 2015. [Online]. Available: https://metrics.torproject.org

[16] A. Johnson, C. Wacek, R. Jansen, M. Sherr, and P. Syverson, "Users get routed: Traffic correlation on Tor by realistic adversaries," in *Proceedings of the 20th ACM conference on Computer and Communications Security (CCS 2013)*, November 2013.

[17] T. Wang, K. Bauer, C. Forero, and I. Goldberg, "Congestion-aware Path Selection for Tor," in *Proceedings of Financial Cryptography and Data Security (FC'12)*, February 2012.

[18] A. Panchenko, F. Lanze, and T. Engel, "Improving performance and anonymity in the Tor network," in *Proceedings of the 31st IEEE International Performance Computing and Communications Conference (IPCCC 2012)*, December 2012.