Instant Degradation of Anonymity in Low-Latency Anonymisation Systems

Thorsten Ries, Radu State, Thomas Engel

Instant Degradation of Anonymity in Low-Latency Anonymisation Systems

Thorsten Ries, Radu State, Thomas Engel

Interdisciplinary Centre for Security, Reliability and Trust
University of Luxembourg
{thorsten.ries, radu.state, thomas.engel}@uni.lu

Abstract. Low-latency anonymisation systems are very popular, both in academic research and in operational environments. Several attacks against these systems exist aiming to reveal the identity of a particular user, mostly by trying to assign the real IP address of the sender to a known connection. Nevertheless, the hidden identity of a user is not only based on the IP address, also location information can be of relevance. In this paper, we propose an alternative approach to instantly disclose the location of users based on *Round Trip Time* measurements. Even if the identity of a user can not be revealed, the correlated location information may already provide sufficient information to degrade the level of anonymity significantly. Our attack is based on virtual network coordinate systems, mapping physical nodes to a n-dimensional space to reveal a geographical proximity. Taking advantage of this feature, we define a model that leverages network coordinates based on only a single connection of a user to a malicious website for instance. Evaluation on the Planet-Lab research network proves that by the use of our proposed model a local attacker has good chance to disclose the location of a user and to utilise this information to create an low-latency anonymity system independent anonymity measure.

1 Introduction

In today's world of extensive online communication, the need of staying anonymous is day-to-day business for many people [3]. The reasons may vary, but the proper operation and performance are essential criteria for users. Particularly if it comes to low-latency anonymisation systems, which allow the use of interactive applications as web browsing for instance. Surprisingly, only a few of the many scientific approaches in this area are practically usable. One common architectural pattern is the operation of intermediate nodes to mediate between the sender and receiver. Basically, two groups are currently deployed: Onion Routing and simple proxy based solutions. The latter is attractive in its simplicity, but lacks anonymity and security. As most times only one intermediate node is

operated, harvesting sensitive information and linking a connection to a sender is very attractive and easily achieved. Onion Routing [20] instead tries to avoid these issues by sending multi-encrypted messages over a path of intermediate nodes, everyone only obtaining the minimum information necessary to forward the message to the next node. Over the last years, the Onion Routing approach has been further extended and resulted in Tor [13], the current predominant low-latency anonymisation system used by approximately 400,000 users per day [5]. Tor supports dynamic changes of the message path, provides anonymity also for servers by operating location-hidden services and protocol cleaning (i.e., removing unnecessary protocol headers before sending the message). Based on a similar approach, JonDonym [2] operates static cascades of either two or three nodes in contrary. Nevertheless, all these approaches can not offer perfect anonymity because of the need of making concession for the benefit of acceptable performance. In this context, recent studies have shown the trade-off between performance and the expected degree of anonymity (e.g., [21]).

Proper functioning of an anonymity system does not rely on a single measure, it consists of a combination of several aspects. Even a basic latency or *Round Trip Time* (RTT) information can reveal sufficient information to disclose the location of a user. Hopper et al. [15] recently presented a general vulnerability of Tor and multi-proxy-based anonymisation to identify the location of users with the help of a network oracle like a *virtual network coordinate system* (VCS). Their main limitations are the applicability of the attack to Tor and multi-proxy systems only and the very high number of required RTT measurements. Therefore, we propose an alternate approach, which is not limited to these constraints by treating the anonymisation system as black box and incorporating VCSs to a wider extend. Particularly the use of VCS's allow a large-scale attack without the need of large-scale measurements. Our aim is to compare the precision of typical low-latency anonymisation systems in terms of success rates for different location sizes (i.e., Country, Autonomous System (AS) and routable Internet network), using as few as possible (malicious) RTT-measurements to predict a users location and to utilise this information to create a system independent anonymity measure.

The rest of the paper is structured as follows: First, section 2 presents the related work and existing attacks on anonymisation systems. Then, the attack model is being described. Practical measurements and evaluation show the applicability of the attack and its implications on the

degree of anonymity in section 4. Finally, we summarise and conclude the work and give an outlook to future work in section 5.

2 Related Work

Naturally, the purpose of low-latency anonymisation networks raises the interest of people to lever out its security features and even more important its anonymity. In fact many attacks against these networks exist; some are of more theoretical value, others can be practically capitalised. While operating a malicious node in an anonymisation system is certainly the easiest and cheapest way to infiltrate communications and to gather sensitive information, many other attacks exist. For instance, timing attacks have been shown to be a powerful type of attacks against anonymisation networks [7, 16, 18, 23]. The basic idea is that attackers observe and correlate message timing patterns between the sender and receiver in order to link the two parties.

VCS-based attacks

Virtual coordinate systems are widely used to predict the distance between nodes in the Internet. They are based on latency or RTT measurements and position network nodes in an d-dimensional coordinate system in order that the distance $d(a, b) \approx latency$ (or RTT respectively) between nodes a and b in the physical network. The aim of such systems is to increase topology awareness and as such to optimise network traffic behaviour by predicting latency with scalable measurements: $O(N)$ complexity instead of $O(N^2)$. Global Network Positioning (GNP) [19], Vivaldi [11] or Phoenix [9] are well known systems in this area.

Approaches to exploit RTT information already exist for some while. As the first, Back et al. [6] analysed traffic in low-latency anonymisation systems, describing a general vulnerability against latency-based attacks and discussing the trade-off's between the degree of anonymity and performance. Based on this work, Hopper et al. [15] use latency measurements to determine the location of a victim node by calculating the remaining entropy of the system [12]. With every connection to a malicious web site certain bits of information are collected and with the help of an assisting malicious node, the RTT between the victim and the entry node of the anonymisation system is being calculated. In order to determine the exact RTT, they perform max. 1,000 RTT measurements per server visit, so in total, up to 50,000 measurements are required to operate the attack

successfully when concluding that the attacker needs 41 server visits of the potential victim in a multi-proxy environment and 50 visits when the victim is using Tor. As a result, a static location of the victim is required during the attack. We would like to stress that the attack relies on the existence of different entry nodes to determine the victims' location and thus is limited to the two discussed anonymisation systems.

3 Attack methodology

Considering the anonymisation system as a black box allows to attack and quantify location anonymity of all practically systems used. Contrary to Hopper et al., there is no need of iterative client access on the malicious server, neither the need of pre-required attacks like the necessary identification the first node in the anonymisation system via e.g. Tor path discovering [8, 17]. The objective is to identify the location of a user instantly, thus also covering victims with frequent changes of their network location and by this to quantify the systems' anonymity.

The attack model necessitates only a single connection from the victim u_i to a malicious node N_m. Optimally, N_m requires a certain number of collaborative landmarks $\{k_1, ..., k_p\} \in K$ in different locations $\{l_1, .., l_n\} \in L$ and $k_h \in l_j$ (see Fig. 1). Depending on the expected granularity, a location can be a country, AS or a routable Internet network location. This in turn means that a certain uncertainty about the accurate location of the node still remains, depending on the location size (i.e. number of possible victim nodes within), but for a correct identification of the location, the degree of anonymity is potentially degraded nevertheless.

The landmarks in known locations serve as reference points and are required as neighbours in the VCS calculation to achieve precise node placements. Based on the RTT data captured between u_i and the landmarks, the attacker computes such a VCS (here: Phoenix) taking the available landmarks, the victim and himself into account. The main idea of Phoenix is that through factorisation, the linear dependence among rows in most Internet distance matrices is characterised best. Therefore Phoenix creates two $n \times d$-matrices X and Y with X storing the linear coefficients and Y the basic vectors for all n nodes in d dimensions to calculate the overall distance matrix $D = X \cdot Y$. We refer to [9] for more details on the computation.

D is used to prove our assumption that nodes with corresponding row values in D, are also neighbours in the physical network. The predicted distance (D^p) between two nodes a and b is then:

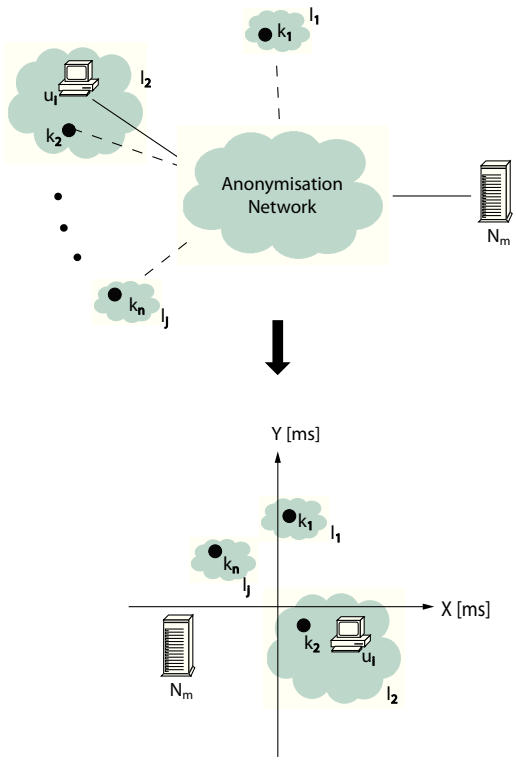

Fig. 1. Schematic description of the location model. Locations in the physical network are mapped in a virtual coordinate system, aiming to reflect real-world distances.

$$D^p(a,b) = \sum_{i=1}^{d} X(a,i) \cdot Y(b,i) \tag{1}$$

Based on D, the location of the different nodes needs to be determined. Hence, the attack is successful if the physical location l_j of a victim u_i can be disclosed. As classifier, e.g. k-nearest neighbour [10] or instance-based learning [4] can be considered. This group of supervised learning methods analyses the given data (D', a $n-1 \times m$ matrix, corresponding to D, but the row of u_i being removed) and predicts the class (l_j) for an input(u_i) based on classification patterns. In our case using the Phoenix coordinate system, $l_j(u_i)$ is predicted based on the similarity of the matrix rows for two corresponding nodes. Using instance-based learning and n nodes,

$l_j(u_i)$, the closest neighbour of u_i can be calculated using the Euclidian distance as follows [4]:

$$k = f\left(D, \min_n \left(\sqrt{\sum_{q=1}^{d}(D_{i_q} - D'_{n_q})^2}\right)\right) \tag{2}$$

where D_i is the row vector of u_i and q the column (node) index of D, f being a function to map the closest distance to the corresponding node in K. If $l_j(u_i) = l_j(k)$, the attack is successful.

The main advantage of this approach is that virtual coordinate systems generally do not require a full set of measurements. Consequently, the usage of virtual coordinate systems allows us large-scale attacks of all anonymisation systems without the need of large-scale measurements.

4 Experimental Evaluation

In order to evaluate our model, we rely on the PlanetLab research network [14] with known locations and the ability to perform distance measurements from every node. The test-bed consisted of 90 nodes located in 25 Countries and the nodes were further distributed in 53 AS's and 58 routable Internet locations. We first carried out reference measurements using direct links (without the use of any anonymisation system) to allow a general validation of our approach. Then the same measurements have been repeated against the selected anonymisation networks:

- a single proxy server located in Steinsel/Luxembourg,
- JonDonym using a premium cascade with nodes in the Czech Republic, Luxembourg and the Netherlands[1],
- Tor with standard configuration.

All measurements have been performed during 5 days in April 2011.

Round-Trip time measurements

Using typical TCP mechanisms to measure RTTs through anonymisation services may cause incorrect results as e.g. the entry node of Tor acknowledges packets immediately so that the RTT is actually measured between the client and the entry node [15]. For our measurements, we

[1] JonDonym is the commercial version of JAP [1]. JonDonyms' free cascades of only two intermediate nodes have a much higher anonymity set, but due to their popularity, they are very often overcrowded and reject additional connections.

therefore used a self-developed client-server application measuring the RTT between the nodes on application level by sending and requesting one Byte messages (plus the corresponding TCP and IP headers). The results may vary from 'real' RTT measurements by processing delay and slightly increased package size. We accept this systematic error that also incorporates into the VCS, but which is not expected to have a significant impact in classification the nodes.

Table 1. Mean and Standard deviation of RTT measurements

Anon Sys	**Mean RTT**	**Standard Deviation**
No Proxy	192ms	169ms
Single proxy	278ms	192ms
JonDonym	509ms	299ms
Tor	737ms	464ms

Table 1 shows the mean RTT's as well as the high standard deviation of our measurements. Even without anonymisation service, the standard deviation is very high and depicts the additional problem of overloaded nodes and related traffic congestion in PlanetLab. This aspect introduces a certain impreciseness and impact on the attack, which we do not expect to such a degree in a 'real world' environment.

Evaluation

In a first evaluation all available nodes have been considered as collaborative landmarks. As already mentioned, we chose Phoenix because of its high prediction accuracy compared to other VCSs. Furthermore Phoenix converges quickly to a steady state, which is of particular importance for the intended small number of measurements and its robustness against measurement anomalies. Another advantage is the resistance against the triangle inequality violation (TIV) [9], which is persistent on the Internet [22] and particularly in overlay-routing, as the routing nodes can easily cause additional delays.

For the classification, we used the instance-based classifier [4] to identify the location of the nodes on the different levels based on a distance measure that compares the rows of the matrix D. Previous experiments have shown this algorithm for being most efficient. Based on $n = 90$ nodes

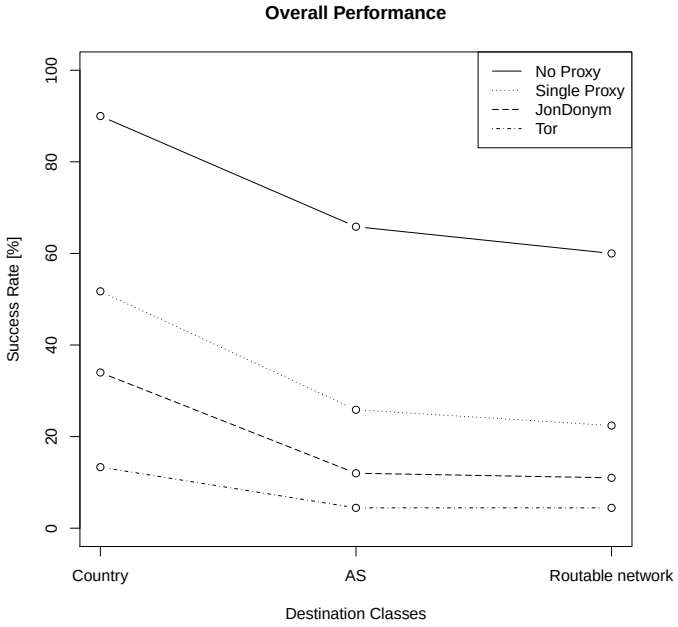

Fig. 2. Success rates for all anonymisation systems

and $m = 100$ Phoenix runs, the success rate has been calculated for every node (NSR):

$$NSR = \frac{\sum_{i=1}^{m} hit(u_i)}{m} \tag{3}$$

$$hit(u_i) = \begin{cases} 0 & \text{if classification fails} \\ 1 & \text{if } u_i \text{ is correctly classified} \end{cases}$$

The success rates for every node are then summarised to describe the system success rate (SR) (equation 4):

$$SR = \sum_{j=1}^{n} \frac{NSR_j}{n} \tag{4}$$

Figure 2 shows the classification rates achieved for all systems including the computed reference values without anonymisation. While achieving a disclosure rate of 0.9 on country-level the values decrease on AS and Internet routable network level and depict the difficulty of exact node-positioning and classification with current coordinate-based systems and

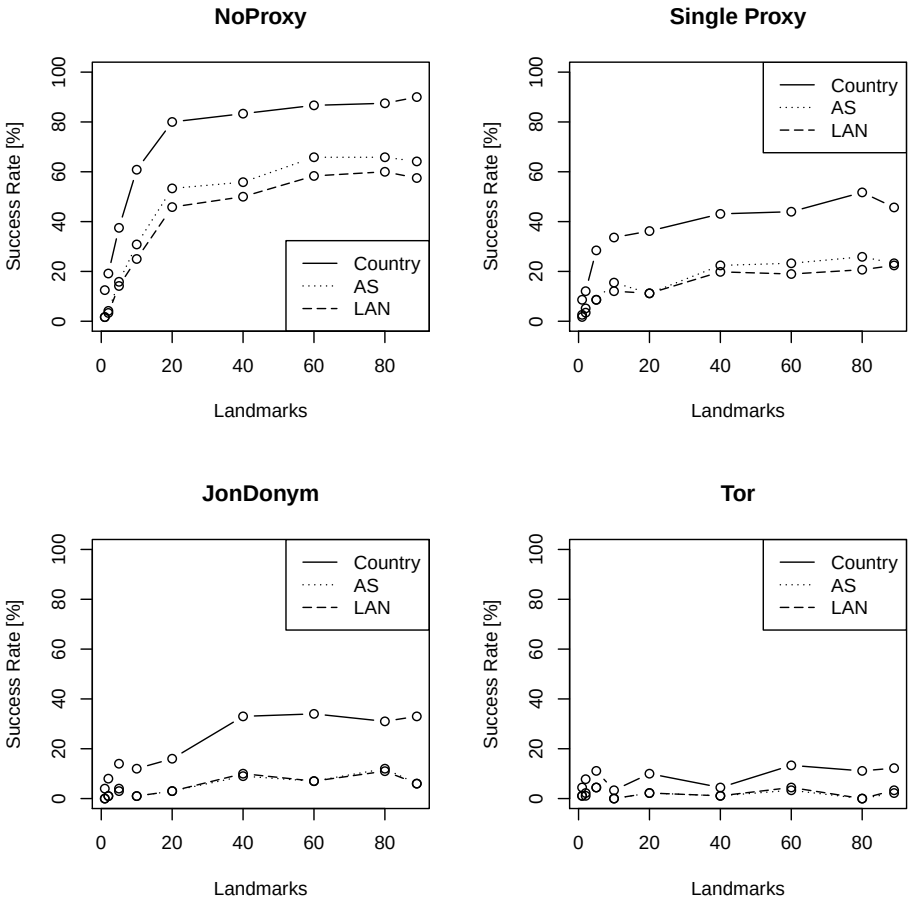

Fig. 3. Performance comparison using different number of landmarks

leaves room for improvement. The problem is mainly based on very similar node characteristics in D and the high variation of measurements, which cause difficult location assignments.

The proxy generally showed the worst protection against our attack, for which we achieve a disclosure rate of 0.51 on country-level. Though the values decrease to 0.25 on AS- and 0.22 on subnet-level, the vulnerability against this kind of attacks is apparent. Overall, Tor shows the best resistance against the attack, having disclosure rates of 0.13 on country-level and only 0.04 on AS- and 0.03 on Internet routable network level, which basically does not allow much inference on the location. Slightly

higher rates of 0.34, 0.12 and 0.11 have been achieved for the comparable anonymisation approach of JonDonym. The differences are mainly the static circuit/cascade and the higher available bandwidth. The study shows that the overall resistance of the systems against such a RTT-based attack seems to depend on the variance of the measurements. The higher the variation, the better the protection. However, the values allow the description of anonymity system in regard to the disclosure of a users location and thus as a measure of anonymity.

We also evaluated the systems performance for different numbers of landmarks, with the results shown in Figure 3. Again, we ran calculations for every node acting a victim and the values in the graphs depict the percentage of cases in which a node has been identified successfully. The results are comparable to the previous evaluation but show that an attacker only needs approximately 20 cooperative landmark nodes in order to execute the disclosure attack effectively and thus keeps the needed number of landmarks reasonable in regard the time needed to perform the measurements.

5 Conclusion and Future work

This work presents an initial system independent approach to disclose the location of users with the help of virtual coordinate systems aiming to define an anonymity measure, with a low complexity. We show that an attacker may be in a position to instantly locate a user who connects to a malicious web server on several levels of precision. Therefore we set up a test bed in Planet-Lab and combined the principle of virtual network coordinates with instance-based class if to a practical attack.

Our evaluation shows that an attacker has a good chance to disclose a victims' location on country level. The success rates in more fine-grained locations are lower, but still show a potential for further improvement, so future work will therefore be directed towards improved node-mapping and classification approaches as well as approaches to explore the attack in a 'real world' environment in order to minimise errors due to PlanetLab overload. However, even if the victim node is not located in one of the observed classes, the classification reveals a geographic proximity and can provide useful information especially for location-based services. Thus, though a detailed identification of a user may be not possible directly, the anonymity set size can be reduced, hence the degree of anonymity.

In low-latency anonymisation networks, mitigation against our attack and latency or RTT-based attacks in general is rather difficult without

decreasing performance. If, for instance higher variance are incorporated, interactive applications may get unusable. As a side effect, users may get disappointed about the low performance, not further use the system(s) and thereby decreasing the size of the anonymity set and consequently the degree of anonymity.

Acknowledgements This experimental research was conducted using the Planet-Lab research network and we thank Emmanuel Nataf from INRIA Nancy - Grand Est for quickly and simply providing us access to the network.

References

1. JAP Anonymity and Privacy. [Online]. Available: http://anon.tu-dresden.de.
2. JonDonym. [Online]. Available: http://anonymous-proxy-servers.net/.
3. Proxy Server Usage. [Online]. Available: http://www.statowl.com/network_behind_proxy_server.php?1=1&timeframe=last_12&interval=month&chart_id=6&fltr_br=&fltr_os=&fltr_se=&fltr_cn=&chart_id=4.
4. David W. Aha, Dennis Kibler, and Marc K. Albert. Instance-based learning algorithms. *Mach. Learn.*, 6:37–66, January 1991.
5. Jacob Appelbaum and Roger Dingledine. How governments have tried to block tor. 28th Chaos Communication Congress (28C3). [Online]. Available: http://events.ccc.de/congress/2011/Fahrplan/events/4800.en.html, December 2011.
6. Adam Back, Ulf Möller, and Anton Stiglic. Traffic analysis attacks and trade-offs in anonymity providing systems. In *Proceedings of the 4th International Workshop on Information Hiding*, IHW '01, pages 245–257, London, UK, UK, 2001. Springer-Verlag.
7. Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. Low-resource routing attacks against Tor. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2007)*, Washington, DC, USA, October 2007.
8. Sambuddho Chakravarty, Angelos Stavrou, and Angelos D. Keromytis. Traffic analysis against low-latency anonymity networks using available bandwidth estimation. In *Proceedings of the 15th European conference on Research in computer security*, ESORICS'10, pages 249–267, Berlin, Heidelberg, 2010. Springer-Verlag.
9. Yang Chen, Xiao Wang, Cong Shi, Eng Keong Lua, Xiaoming Fu, Beixing Deng, and Xing Li. Phoenix: A weight-based network coordinate system using matrix factorization. *IEEE Transactions on Network and Service Management*, 8(4):334–347, December 2011.
10. Thomas M. Cover and Peter E. Hart. Nearest neighbor pattern classification. *IEEE Transactions on Information Theory*, 13:21– 27, 1967.
11. Frank Dabek, Russ Cox, Frans Kaashoek, and Robert Morris. Vivaldi: A decentralized network coordinate system. In *SIGCOMM*, pages 15–26, 2004.

12. Claudia Diaz, Stefaan Seys, Joris Claessens, and Bart Preneel. Towards measuring anonymity. In Roger Dingledine and Paul Syverson, editors, *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*. Springer-Verlag, LNCS 2482, April 2002.
13. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: the second-generation onion router. In *Proceedings of the 13th conference on USENIX Security Symposium - Volume 13*, pages 21–21, Berkeley, CA, USA, 2004. USENIX Association.
14. PlanetLab Europe. PlanetLab Europe Website. [Online]. Available: http://www.planet-lab.eu.
15. Nicholas Hopper, Eugene Y. Vasserman, and Eric Chan-TIN. How much anonymity does network latency leak? *ACM Trans. Inf. Syst. Secur.*, 13:13:1–13:28, March 2010.
16. Brian N. Levine, Michael K. Reiter, Chenxi Wang, and Matthew K. Wright. Timing attacks in low-latency mix-based systems. In Ari Juels, editor, *Proceedings of Financial Cryptography (FC '04)*, pages 251–265. Springer-Verlag, LNCS 3110, February 2004.
17. Steven J. Murdoch and George Danezis. Low-cost traffic analysis of tor. In *In Proceedings of the 2005 IEEE Symposium on Security and Privacy. IEEE CS*, pages 183–195, 2005.
18. Steven J. Murdoch and Piotr Zieliński. Sampled traffic analysis by internet-exchange-level adversaries. In Nikita Borisov and Philippe Golle, editors, *Proceedings of the Seventh Workshop on Privacy Enhancing Technologies (PET 2007)*, Ottawa, Canada, June 2007. Springer.
19. T. S. Eugene Ng and Hui Zhang. Towards global network positioning. In *Proceedings of the First ACM SIGCOMM Workshop on Internet Measurement*, pages 25–29, 2001.
20. Michael G. Reed, Paul F. Syverson, and David M. Goldschlag. Anonymous connections and onion routing. *Selected Areas in Communications, IEEE Journal on*, 16(4):482 –494, may 1998.
21. Thorsten Ries, Andriy Panchenko, Radu State, and Thomas Engel. Comparison of low-latency anonymous communication systems - practical usage and performance. In *Proceedings of the Australasian International Security Conference (AISC 2011)*, 2011.
22. Han Zheng, Eng Keong Lua, Marcelo Pias, and Timothy G. Griffin. Internet routing policies and round-trip-times. In *In PAM*, 2005.
23. Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati, and Wei Zhao. On flow correlation attacks and countermeasures in mix networks. In *Proceedings of Privacy Enhancing Technologies workshop (PET 2004)*, volume 3424 of *LNCS*, pages 207–225, May 2004.