On the PET Workshop Panel "Mix Cascades Versus Peer-to-Peer: Is One Concept Superior?"

Rainer Böhme[1], George Danezis[2], Claudia Díaz[3],
Stefan Köpsell[1], and Andreas Pfitzmann[1]

[1] Technische Universität Dresden, Germany
{rainer.boehme, sk13, pfitza}@inf.tu-dresden.de
[2] University of Cambridge, United Kingdom
george.danezis@cl.cam.ac.uk
[3] Katholieke Universiteit Leuven, Belgium
claudia.diaz@esat.kuleuven.ac.be

Editors' note. Following the panel discussion on Mix Cascades versus P2P at PET 2004, we invited the original panel proposers to write a summary of the discussion for the proceedings. This is their contribution.

Abstract. After almost two decades of research on anonymous network communication the development has forked into two main directions, namely Mix cascades and peer-to-peer (P2P) networks. As these design options have implications on the achievable anonymity and performance, this paper aims to elaborate the advantages and disadvantages of either concept. After clarifying the scope of the discussion, we present arguments for Mix cascades and P2P designs on multiple areas of interest: the level of anonymity, the incentives to cooperate, aspects of availability, and performance issues. Pointed thesis and antithesis are given for both sides, before a final synthesis tries to articulate the status quo of the discussion.

1 Introduction

David Chaum's initial work [6] on Mixes led to a vast number of proposals on how to provide anonymous communication on the Internet. Some of these approaches have already been put into practice while others still rest as blueprints. They all have in common, that multiple Mixes are used to establish a certain amount of anonymity. The most salient difference between those approaches is the way, in which the Mixes are connected and organised. Two idealised concepts set the range on a continuum of possible designs. On the one end, we have Mix cascades: dedicated servers joining traffic from a large set of users and uniformly redirecting it on a predefined route. The other end is defined by peer-to-peer (P2P) systems: widely distributed and equal client applications unpredictably routing their traffic over all possible routes. The design of a Mix system has implications on the achievable anonymity and performance.

D. Martin and A. Serjantov (Eds.): PET 2004, LNCS 3424, pp. 243–255, 2005.

This article tries to cover a wide range of aspects, which are all related with this essential design decision. It is not so much focused on detailed analysis of certain specific implementations (e. g., [12, 13, 29]), but rather on the underlying explicit or implicit threat models. As the area of relevant aspects is broad and evidence still sparse, this paper is unlikely to deliver solid proofs. It should rather be regarded as an attempt to collect softer arguments—call it assumptions or beliefs—for both sides of the discussion. Arguments, which we consider as highly important, but which do not fit into the usually better grounded research papers because they are so hard to quantify [14, 26, 28]. Apart from documenting these points, we try to structure the discussion and eventually make it more salient to the community.

We assume that the reader is already familiar with the basic concepts of Mixes, so that our paper is structured straight off. In the next section, we propose a scheme to arrange the different approaches along two dimensions: *flexibility of routing* and *task sharing* (resources as well as trust and liability). In Section 3, we pick up the arguments for Mix cascades and evaluate the impact of the respective designs on four aspects: anonymity, incentives to cooperate, availability, and performance. We underline our claims with a number of pointed thesis. In Section 4 we contrast these points with arguments for peer-to-peer systems and assert a set of antitheses. Finally, a concluding synthesis is given in Section 5.

2 Classification of Approaches

To clarify the subject of the discussion, we propose to break down the properties of the different approaches on two dimensions. The first difference between Mix cascades and P2P networks is the freedom of choice of traffic routing. Typical Mix cascades offer no choice to their users while free choice of link partners—and hence full *flexibility of routing*—is a key feature of P2P concepts. The advantages and drawbacks of precisely this design issue have been addressed in the literature, for example in [5] and [8]. However, none of the pure concepts seems to dominate the other one in all aspects.

The second difference between Mix cascades and P2P networks concerns the organisation of the system. Mix cascades are typically provided by a small set of entities. Their Mixes are located at a small number of places, usually run on dedicated servers, and are administered by professionals. In contrast to this institutionalised approach, pure P2P networks avoid any exposed instances and organise themselves in a rather anarchical manner. All nodes act as equal peers and there is no allocation of duties. Hence, we name the second dimension *task sharing.* The division includes technical resources (e. g., load balancing) as well as intangible aspects such as trust and responsibility.

According to these two dimensions, we can arrange the different approaches for anonymity in networks in a two-by-two matrix as shown in Table 1 (p. 245).

The pure concept of Mix cascades is characterised by asymmetric task sharing and fixed routes. On the opposite, P2P networks consist of equal peers performing the same tasks and routing their traffic over a multiple of user-selected routes.

Table 1. Classification of different concepts for anonymous networks

	Flexibility of routing	
Task sharing	System defined	User's choice
Asymmetric	Mix cascade	Mix network
Symmetric	DC-net, Broadcast	P2P network

Table 2. Extended classification of approaches for network anonymity

	Flexibility of routing			
	System defined		User's choice	
Task sharing	Fixed	Variable	Restricted	Free
Asymmetric	A_1	A_2	A_3	A_4
Symmetric	S_1	S_2	S_3	S_4

Mix networks are between these two extremes. They allow users to choose their respective routes, but still rely on dedicated Mix servers, which handle different tasks than the multiple of clients. Further topologies for anonymous network communication, such as DC-nets [7] and broadcast [20], exceed the scope of this discussion.

The proposed model helps to structure the topic of discussion, because certain advantages or disadvantages can be precisely linked with one of the dimensions. However, the routing dimension may need a further refinement, because argumentation on the pros and cons of the pure concepts tends to drift somewhere in the middle. For example, the literature responds to the critics of fully connected networks with restricted routes in sparse networks [8]. Also the recent *synchronous batching* approach tries to join the predictable timing feature from Mix cascades with decentralised topologies [17]. Thus it might be useful to subdivide the routing dimension into four sections, as shown in Table 2.

In the remainder of this paper we will discuss the impact of design decisions on each of the dimensions on the total quality of an anonymity service. The next section will show, why some scholars believe that the solutions A_1 and A_2 provide the highest anonymity, coupled with the best performance in case of A_1. In Section 4 we will elaborate why other researchers consider the solutions S_3 and S_4, or at least A_3 and A_4 as more desirable.

3 Arguments for Mix Cascades

The quality of anonymity services can be broadly divided into aspects of security and usability. However, as usability affects the size of the anonymity set, it also matters for the security of a system [2]. Hence, the ideal system can be described as follows: It provides anonymous access to, or sending of any information (*availability*), by hiding all information about the recipient's and/or sender's identity (*anonymity*) within a maximum large set of users (*incentives to cooperate*), with minimum degradation in usable bandwidth and response time (*performance*). To evaluate how Mix cascades and P2P networks perform in realising these goals, we analyse the impact of (1) *flexibility of routing* and (2) *task sharing* on the above-mentioned aspects.

3.1 Anonymity

The maximum anonymity that can be provided by Mix cascades means, that

- all other senders or recipients of the messages of a particular time interval, or
- all Mixes

have to cooperate to trace a message against the intention of its sender or recipient. A proof for this fact in a possibilistic as well as a probabilistic setting is given in [25][1].

The effects of flexible routing on anonymity are described in [5]. Assuming a globally listening and participating adversary, the authors conclude: "If only one Mix of a route is trustworthy, then the achievable anonymity is distinctly lower in a Mix network compared to a synchronously working Mix cascade" (p. 37).

Thesis 1. *P2P networks assume adversaries outside a closed group of people.*

So, it is evident that the requirements for an anonymity service heavily depend on the threat model considered. However, even if the threat model "all other senders or recipients . . . , or all Mixes" is deemed too strong, there are good arguments for modifying the parameters rather than replacing the design. First, the anonymity level of a cascade can be downgraded by reducing the number of Mixes or the number of messages required per batch. Both measures have favourable side effects: They lead to an increase in performance and quality of service. Second, the upholding of a cascade design keeps the advantages of a clear structure of the system: In contrast to distributed approaches, cascades are easy to analyse and hence easy to prove.[2] This means that the system is more robust

[1] The idea of the proof is also outlined in this document: `http://petworkshop.org/2004/talks/pfitza.pdf`

[2] The degree of complexity of P2P systems apparently inspires researchers to write fancy papers. However, as a consequence of this complexity, some really important aspects are regularly either neglected (e. g., exit policies) or simplified with unrealistic assumptions (e. g., low number or small fraction, resp., of colluding nodes).

to remaining threats from information outside of the considered model. Third, when the threat model changes because stronger anonymity may be required in future, the switching costs are kept to moderate levels only if a cascade infrastructure is already set up: Changing parameters is far cheaper than switching to a new topology.

However, on the task sharing dimension, the low number of known Mix servers makes Mix cascades more vulnerable against adversaries that try to gain control over these servers [1]. Cascade proponents argue that symmetric task sharing in P2P networks is even more dangerous, because the peer nodes are run by end-users on out-of-the-box operating systems. This combination is less likely to withstand decent attacks compared to dedicated Mix servers administrated by security experts as in the asymmetric case. Equal peers in a symmetric architecture are also more likely to be down, hence forcing their users to change to another route. Frequent route switching increases the probability of using at least one time only collusive nodes.

Thesis 2. *P2P proponents err in assuming that the sheer number of nodes implies that only a minority colludes.*

This thesis has implications in terms of nodes, and in terms of links. The danger of a powerful attacker participating with a large set of nodes is quite well understood. Some measures have been proposed, such as reputation systems [15, 18], which make this attack more difficult at least. But a node does not necessarily need to be malicious because of its owner’s bad intentions. It is also possible, that an attacker selectively throws out precisely those nodes, which impede his observation. Thus, the often-cited strength of distributed systems against *denial of service* (DoS) does at the same time attract active attackers, just because routes are dynamically switched and partial failures keep unnoticed. Here are obvious relations to aspects of availability, which are discussed in the next section.

3.2 Availability

Availability of anonymity services includes three steps: first, the possibility to reach an access-point, second, the correct operation of the Mixes and their communication, and third, the accessibility of requested information. The first step concerns possible blocking efforts of authoritarian states or organisations. Depending on the details of the filter method, a powerful blocker can always restrict access to anonymity services. However, it is obvious that publicly known or even central access points are more vulnerable than distributed networks.

Concerning the first step, symmetric systems dominate asymmetric ones if, and only if, their protocols do not unveil too much information about the network’s topology (which else could be exploited to block packet forwarding—another rarely addressed aspect in the literature). Also the second step seems to be more robust with a symmetric structure because denial of service attacks would have to hit a large set of peers instead of some central servers. But Mix cascades can also be equipped with redundant backup servers. In addition, the professional administration makes Mix servers less vulnerable than user-run peers. The last step is probably the most difficult to discuss. If the peers used white-lists to manage their exit-policies (see below) the probability to get arbitrary information from the Internet would be quite low. However, institutionalised last Mixes of cascades are also likely to suppress access to certain content, depending on the respective jurisdiction.

Thesis 3. *Concerning availability, P2P seems to dominate the pure (no redundancy) cascade approach. Given redundant cascades, no concept is superior.*

3.3 Incentives to Cooperate

It is evident that a large user base is a prerequisite for strong anonymity. As a common implication, researchers discuss usability and performance aspects to evaluate the incentives to participate. These aspects depend on both flexibility of routing and task sharing.

Apart from that, also on the task sharing dimension, the responsibility of exit-nodes is a very important point, which is only marginally addressed in the literature [1]. For a risk averse user, being accountable for arbitrary crimes that are linkable with one's IP-address or computer is the major drawback of P2P structures. If the first case of, say, "music industry sues participant of P2P anonymity service" went public, the user-base is in danger to vanish. The juridical risk of participation is a major disincentive for users with honourable intentions.

Even if we assume that each user can restrict the access to a limited amount of obviously innocuous websites by administrating exit policies (usually black- or white-lists), the cost of managing these policies will exceed the resources for the majority of participants. As black-lists will never completely evade the risk, and demand a huge effort to keep them up to date, white-lists might be used. This will probably exclude most of the requested information from the network and thus render the system useless.

Thesis 4. *P2P systems are unlikely to receive support by an ample community.*

So, if the masses will be using Mixes at all, strong arguments suggest it will be Mix cascades. Talking about masses means considering the end users, individuals often described as spoiled and reluctant. Here, apart from what has been said before, performance will be an equally critical success factor.

3.4 Performance

P2P proponents often state that centralised routes set an upper limit to the service's performance and thus Mix cascades would perform worse. While the first statement is true, the second one needs further consideration. In fact, the batch size (or more general: the flushing strategy) sets the upper limit for the level of anonymity a service can provide. The frequency of packet arrivals determines the response latency of each Mix. Hence, up to a certain limit, packets pass Mixes the faster the more packets arrive. As Mix cascades usually are connected with higher bandwidth than distributed peers, the upper limit for a cascade is far beyond the limited bandwidth between P2P nodes. Because of this atypical relationship between volume and delay, Mix cascades dominate P2P systems in both, performance and batch size.

Thesis 5. *High load on cascades leads to reduced response latencies for a given batch size. P2P can never reach such capacity effects and therefore P2P always performs worse.*

Dummy traffic has been described as effective measure to prevent long-term intersection attacks [4]. The designers of many P2P systems suggest using dummy traffic—and hence using bandwidth—to reduce the risk of traffic analysis by an observing adversary. However, dummy traffic between two adjacent Mixes does not prevent attacks from insiders, i.e., Mixes, because they always can separate dummy packets from real data. To make dummy traffic indistinguishable from real data, it also has to be routed over multiple peers. This leads to further inefficiencies because dummy packets—now per definition indistinguishable—must be treated with the same quality of service as payload packets and thus cause additional load on already critical bottlenecks in the network topology.

Thesis 6. *Given an insider adversary, dummy traffic in flexible routing systems either is useless or jams connections. In both cases, performance suffers for little reward.*

Summing up all arguments on a more general level, we can put them into two points: First, the security of the cascade design can be proven with little assumptions. So we should not replace this design by a more obscure one, unless we have very good reasons. Second, many people tend to give up privacy if it is inconvenient. So if anonymity systems shall appeal a broader public then quality of service and low costs of maintenance are crucial. Mix cascades provide both very well.

4 Arguments for Mix Network Designs

Mix systems need to be trusted to hide the correspondence between input and output messages, something that cannot be proved or observed in any other way. There is a need to distribute Mix functionality in order to distribute this trust, necessary to provide anonymity, and in order to balance the load across the system. The Mix cascades provide some distribution of trust, but since all traffic is routed through all nodes in a Mix cascade no load balancing at all.

Antithesis 1. *Greater capacity, through load balancing, is a security property.*

General Mix networks allow for both distribution of trust and load balancing. Each new node that is added to the network provides extra capacity, and provided that there is sufficient traffic to prevent traffic analysis, increases the anonymity of all traffic. At the same time the latency of the anonymous communications remains relatively low, since path lengths do not need to grow nearly as fast as the size of the network [8]. This has to be contrasted with the Mix cascade approach, where new cascades need to be constructed to accommodate more traffic. These cascades do not mix traffic amongst them, and as a result provide less anonymity to their users. Therefore our thesis holds that a system that is able to mix together more traffic, is in the long run not simply more scalable. In the case of anonymity properties, that intrinsically rely on other people being present, it is also more secure.

Antithesis 2. *Robustness and availability are security properties.*

Mix cascades have intrinsic single points of failure. The failure of any node in the cascade will bring the operation of the whole cascade to a halt. Bypassing the failed node will require manual intervention, and key redistribution. This makes Mix cascades very fragile, in comparison with fully connected Mix networks, where failures in the network do not interrupt service: new routes that do not use the unavailable nodes are constructed, and used to route traffic.

The fragility of cascades makes them more susceptible to denial of service attacks. It is not necessary to subject the whole network to such an attack, since flooding a single node (such as the entry node to the cascade, that needs to be publicly visible) would be sufficient. The same applies for legal or compulsion attacks: it is sufficient to stop the operation of one node to disrupt all communications. Since by default there can be only fewer nodes participating in a cascade, due to the traffic load, such legal or compulsion attacks are easier to mount from a technical point of view.

Finally Mix cascades are vulnerable to even a small minority of insiders that would attempt to disrupt service by dropping packets, or flooding subsequent nodes. A rich literature exists on how to make cascade designs publicly verifiable, yet most of them rely on extremely expensive cryptographic primitives, and extremely complex protocols [24]. None of them has so far been implemented. On the other hand, two more practical suggestion to provide robustness, batch signing [6, 3] and random partial checking [22], can be equally well applied to Mix networks and Mix cascades.

Unreliable anonymous communication channels are likely to frustrate users and drive them away from using the system all together. This will reduce anonymity sets, and therefore lower the overall security of the channel. At the same time, denial of service itself can be used to assist other attacks, such as the $n-1$ attack [29].

Antithesis 3. *Trust means choice!*

The key to Mix mediated anonymous communications is that the user trusts that the Mixes will not reveal the relation between input and output messages. This choice cannot, and must not, be 'outsourced' to any other third party. Furthermore it is desirable to be able to easily set up a specific Mix node, for the use of particular communities that would trust it. Mix networks can easily accommodate such a trust model, and deployment model. On the other hand, the cost of running a cascade and its rigid structure makes it impossible for small communities to run trusted nodes, or to join and blend in the anonymity of larger groups.

The assumption that all but one Mix nodes are going to be corrupt, as the proponents of the cascade paradigm often do, is based on the false premise that there is a fixed set of nodes that everybody trusts and uses. On the other hand Mix networks allow for different users trusting different subsets of nodes. In extreme cases this would split the anonymity sets: two disjoint trusted groups will emerge, with different user bases. In most cases users will choose to trust overlapping sets of Mix nodes, in such a way that the anonymity sets are still confounded, and entangled. This provides maximal anonymity, and the ability of users or operators to make their own trust judgements.

Restricted routes networks, where the network graph is not complete, allows Mix server operators to make trust judgements, and only interconnect with a small set of others. This again increases the resilience of the network against Sybil attacks [19], or other ways a large number of corrupt nodes could infiltrate the network.

Antithesis 4. *Mix networks increase the* attack surface*.*

Mix networks allow traffic to come in and out of many nodes in the network. Therefore a Global Passive Adversary (GPA) or a Global Active Adversary (GAA) needs to make an effort proportionate to the number of nodes in the network to retain its capabilities. Furthermore using the peer-to-peer paradigm [21, 27] to do mixing increases even further the cost of the attacker, by multiplying the number and making nodes transient. Therefore it is likely that an attacker will never be able to attain the status of GPA or GAA.

This has to be contrasted with Mix cascade structures that offer very well defined entry and exit points. These can be observed at a fixed cost, and intersection attacks can be mounted against the participants [23, 9]. Combined with the intrinsically smaller anonymity sets, such an attack would be devastating. In other words by trying to protect against an assumed very powerful adversary, Mix cascades make the existence of such an adversary easily possible.

The single point of entry and exit also makes traffic analysis of anonymised streams easier. In the absence of a lot of cover traffic, which none of the fielded systems over the Internet have been able to provide, it is easier for an adversary to gain all the information necessary to perform traffic analysis [11]. Mix network based system, such as Onion Routing [16], face the same problems, but make it more difficult for an adversary to gain all the information necessary by using more nodes and links.

Antithesis 5. *Anonymity is hard, general purpose anonymous channels are even harder!*

Anonymising traffic between users requires the system to make all traffic 'look the same'. In the same way as Quality of Service algorithms operate, perfect anonymity systems require an intimate knowledge of the traffic characteristics they will carry. Anonymous remailers do so, by assuming that mail messages will be of a certain size, and can tolerate very high latencies. Peer-to-peer systems, that attempt to facilitate file sharing or covert communications try to use the application specific knowledge they have to construct more robust anonymous channel for their specific purpose. Mix networks are the natural structure of such channels since the established topologies, the trust judgements, and the pre-existing connections can be used to carry the anonymous channel and secure it.

On the other hand Mix cascades require a lot of cooperation to set up, that is specific to Mix cascade channel, and map with difficulty to any other pre-existing structure that nodes might have established amongst them. It is difficult to imagine how complete collaborative applications could be built to setup cascades.

Antithesis 6. *Mix networks offer the flexibility to handle unforeseen problems and opportunities.*

Mix cascades can be seen technically as a Mix network with an extremely restricted topology, namely a cascade. Systems that support Mix networks can therefore during their operation be turned into cascades [10], if it is proven necessary. On the other hand a cascade based system does not carry the information necessary (the routing information) to be easily converted into any other topology.

Mix networks can also be used to provide hybrid solutions relating to the topology. A solution such as a ‘core cascade’ with peer-to-peer nodes as the entrance points and the exit points, could for example be implemented. Mix network systems can also be modified more easily to environments, where cascades are not possible, such as anonymising ad-hoc wireless traffic, where messages have to travel across a set of wireless points restricted by the physical layout of the network.

5 Conclusions

In this paper we have discussed the issues that should be taken into account when choosing an anonymous communication system. We have classified existing systems according to the *flexibility of routing* and the *task sharing* dimensions.

The choice between symmetric and asymmetric systems and the appropriate flexibility of routing are dependent on the threat model considered; the requirements of the services that are implemented on top of the anonymous infrastructure, in terms of performance, anonymity and availability; and the incentives for the participants in the system.

In order to provide a good anonymity service, we need to attract a large number of users. Therefore the quality of service and the liability issues should be taken into account. In this respect, asymmetric systems seem to be more appropriate than symmetric systems because the users are not liable for other’s actions, they require less resources and the available bandwidth is higher (better quality of service).

Regarding the resistance towards attacks, Mix networks require that the attacker is able to cover more surface of attack, given that the number of entry and exit points is larger. Moreover, Mix cascades are more vulnerable towards Mix failures, insider adversaries or denial of service attacks than Mix networks. Mix cascades require more trust from the user than Mix networks, given that the user cannot choose which nodes he wants to trust, nor he can add his own Mix to the cascade. Symmetric systems are more vulnerable to attacks than asymmetric systems because the security level of the nodes is lower. Contrary to the claims of many P2P designs, we state that the fact of having many nodes in the network does not imply that a strong attacker is not able to control a significant number of these nodes.

Symmetric systems typically offer a much larger number of entry and exit points than asymmetric systems. This is a feature that enhances the availability of the system, specially towards strong adversaries who want to prevent the users from accessing the anonymity service (these symmetric systems must conceal the topology of the network in order to prevent blocking the access to the service). Regarding the flexibility of routing dimension, Mix networks have better availability properties than cascades, because the number of entry and exit points is larger, and it is also more difficult for an adversary to provoke a denial of service attack that shuts down the anonymity service.

As final conclusion, we should say that more research and empirical data are needed in order to find concrete answers, as well as to develop policies or methodologies that can simplify the decision on the type of system we should implement according to the requirements of our application. We hope that this paper will help identifying the important issues that need to be taken into account by the designers of systems for anonymous network communication.

Acknowledgements

This paper summarises a panel discussion chaired by Claudia Díaz at the Privacy Enhancing Technologies Workshop 2004 in Toronto, Canada. It would not have been possible to collect this wide range of arguments without the input from the panelists, namely George Danezis, Christian Grothoff, Andreas Pfitzmann, and Paul Syverson, as well as many engaged contributions from the audience.

References

1. Acquisti, A., Dingledine, R., and Syverson, P.: On the Economics of Anonymity. In: Wright, R. N. (ed.): Financial Cryptography (FC 2003), LNCS 2742, Springer-Verlag, Berlin Heidelberg (2003) 84–102
2. Back, A., Möller, U., Stiglic, A.: Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems. In: Moskowitz, I. S. (ed.): Information Hiding (IH 2001), LNCS 2137, Springer-Verlag, Berlin Heidelberg (2001) 245–257
3. Berthold, O., Federrath, H., Köpsell, S.: Web MIXes: A System for Anonymous and Unobservable Internet Access. In: Federrath, H. (ed.): Anonymity 2000, LNCS 2009, Springer-Verlag, Berlin Heidelberg (2001) 115–129

4. Berthold, O., Langos, H.: Dummy Traffic against Long Term Intersection Attacks. In: Dingledine, R., and Syverson, P. (eds.): Privacy Enhancing Technologies (PET 2002), LNCS 2482, Springer-Verlag, Berlin Heidelberg (2003) 110–128
5. Berthold, O., Pfitzmann, A., Standtke, R.: The Disadvantages of Free MIX Routes and How to Overcome Them. In: Federrath, H. (ed.): Anonymity 2000, LNCS 2009, Springer-Verlag, Berlin Heidelberg (2001) 30–45
6. Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM **24** (1981) 84–88
7. Chaum, D.: Security without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM **28** (1985) 1030–1044
8. Danezis, G.: Mix-Networks with Restricted Routes. In: Dingledine, R. (ed.): Privacy Enhancing Technologies (PET 2003), LNCS 2760, Springer-Verlag, Berlin Heidelberg (2003) 1–17
9. Danezis, G.: Statistical Disclosure Attacks: Traffic Confirmation in Open Environments. Proceedings of Security and Privacy in the Age of Uncertainty (SEC2003), Athens (2003, May) 421–426
10. Danezis, G., Dingledine, R., Mathewson, N.: Mixminion: Design of a Type III Anonymous Remailer Protocol. Proceedings of the IEEE Symposium on Security and Privacy (2003, May)
11. Danezis, G.: The Anonymity of Continuous Time Mixes. Paper presented at the Privacy Enhancing Technologies Workshop, Toronto, Canada (2004, May)
12. Díaz, C., Preneel, B.: Reasoning about the Anonymity Provided by Pool Mixes that Generate Dummy Traffic. Paper presented at the 6th International Workshop on Information Hiding, Toronto, Canada (2004, May)
13. Díaz, C., Sassaman, L., Dewitte, E.: Comparison between Two Practical Mix Designs. Paper to be presented at the 9th European Symposium on Research in Computer Security (ESORICS 2004, Sep 13–15), Sophia Antipolis, France
14. Díaz, C., Seys, S., Claessens, J., Preneel, B.: Towards Measuring Anonymity. In: Dingledine, R., and Syverson, P. (eds.): Privacy Enhancing Technologies (PET 2002), LNCS 2482, Springer-Verlag, Berlin Heidelberg (2003) 54–68
15. Dingledine, R., Freedman, M. J., Hopwood, D., Molnar, D.: A Reputation System to Increase MIX-net Reliability. In: Moskowitz, I. S. (ed.): Information Hiding. Fourth International Workshop, LNCS 2137, Springer-Verlag, Berlin Heidelberg (2001) 126–141
16. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The Second-Generation Onion Router. Proceedings of the 13th USENIX Security Symposium (2004, August)
17. Dingledine, R., Shmatikov, V., Syverson, P.: Synchronous Batching: From Cascades to Free Routes. Paper presented at the Privacy Enhancing Technologies Workshop, Toronto, Canada (2004, May)
18. Dingledine, R., Syverson, P.: Reliable MIX Cascade Networks through Reputation. In: Blaze, M. (ed.): Financial Cryptography (FC 2002), LNCS 2357, Springer-Verlag, Berlin Heidelberg (2002)
19. Douceur, J.: The Sybil Attack, Proceedings of the 1st International Peer To Peer Systems Workshop (IPTPS 2002, March)
20. Farber, D. J., Larson, K. C.: Network Security Via Dynamic Process Renaming. Fourth Data Communications Symposium, Quebec City, Canada (1975, October) 8-13 – 8-18
21. Freedman, M. J., Morris, R., Tarzan: A Peer-to-Peer Anonymizing Network Layer. Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002), Washington, DC (2002, November)

22. Jakobsson, M., Juels, A., Rivest, R. L.: Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking. Proceedings of the 11th USENIX Security Symposium (2002, August)
23. Kesdogan, D., Agrawal, D., Penz, S.: Limits of Anonymity in Open Environments. In: Petitcolas, F. A. P. (ed.): Information Hiding. Fifth International Workshop, LNCS 2578, Springer-Verlag, Berlin Heidelberg (2003)
24. Neff, C. A.: A Verifiable Secret Shuffle and its Application to E-Voting. Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS 2001), ACM Press (2001, November) 116–125
25. Pfitzmann, A.: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. Universität Karlsruhe, Fakultät für Informatik, Dissertation, Feb. 1989, IFB 234, Springer-Verlag, Heidelberg (1990)
26. Pfitzmann, A., Köhntopp, M.: Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology. In: Federrath, H. (ed.): Anonymity 2000, LNCS 2009, Springer-Verlag, Berlin Heidelberg (2001) 1–9
27. Rennhard, M., Plattner, B.: Practical Anonymity for the Masses with MorphMix. Proceedings of Financial Cryptography (FC ’04), LNCS 3110, Springer-Verlag, Berlin Heidelberg (2004)
28. Serjantov, A., Danezis, G.: Towards an Information Theoretic Metric for Anonymity. In: Dingledine, R., and Syverson, P. (eds.): Privacy Enhancing Technologies (PET 2002), LNCS 2482, Springer-Verlag, Berlin Heidelberg (2003) 41–53
29. Serjantov, A., Dingledine, R., Syverson, P.: From a Trickle to a Flood: Active Attacks on Several Mix Types. In: Petitcolas, F. A. P. (ed.): Information Hiding. Fifth International Workshop, LNCS 2578, Springer-Verlag, Berlin Heidelberg (2003) 36–52